PRODUCT Reviews Guide 2008

TESTING & ANALYSIS TO HELP YOU MAKE PURCHASING DECISIONS

contents

Information Security **magazine's 2008 Product Review Guide is a compilation of the single and comparative reviews published in 2008, an indispensable guide for information security managers tasked with evaluating and purchasing security hardware and software in 2009.**

INFORMATION SECURITY

VULNERABILITY MANAGEMENT

HotPick INFORMATION SECURITY®

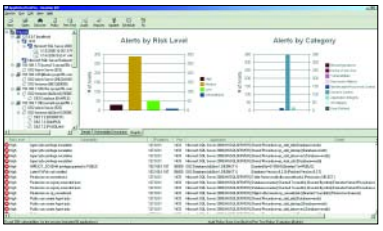
AppDetectivePro

REVIEWED BY MIKE CHAPPLE

Application Security, Inc.

www.appsecinc.com

Price: **$900 per database instance annual subscription fee**



AppDetectivePro fills a critical niche that goes beyond conventional vulnerability scanners, performing "deep dive" inspections of database configuration to identify security issues. It's ideal for internal and external auditors, security professionals, consultants and others who need to perform on-the-fly database vulnerability assessments.

Policy Control B

AppDetectivePro supports Microsoft SQL Server, Oracle, IBM DB2, Sybase and MySQL. The subscription fee includes a comprehensive collection of predefined security checks for each platform.

The checks are updated only monthly, which could mean a significant lag between discovery of a serious flaw and the ability to detect it.

Users may augment the built-in policies with custom checks written in SQL.

Configuration/Management A

Installation and initial configuration is straightforward. The software uses a standard installation wizard and works best when used with a SQL Server database to store results. AppDetectivePro offers three assessment methodologies: database discovery, penetration testing and auditing.

Database discovery allows you to scan a network for the presence of databases that may then be further assessed. Any AppDetectivePro license includes unlimited discovery scanning. You may purchase additional licenses to perform penetration tests and/or audit scans on any discovered database instances. Scan characteristics are highly customizable, allowing you to specify the ports scanned and technique for live host detection.

Penetration testing attempts to gain information about and access to the database without credentials, simulating the access an outsider might be able to gain to your network. It does not actually attempt to exploit any vulnerabilities; it just uses fingerprinting techniques to determine the database version and patch level.

The true value of the product shines through in the database audit functionality. The audit begins by retrieving a large amount of configuration information from the target database (usernames and password hashes, object/privilege listings, details on linked servers, etc.) and stores it locally on the scanning workstation, where AppDetectivePro performs its analysis.

Effectiveness A

AppDetectivePro identified a number of vulnerabilities in our database configuration. These included obvious, glaring errors that we intentionally introduced, such as blank administrator passwords, missing service packs and unapplied patches. It also identified more subtle configuration issues, such as improper permissions on registry extended stored procedures; the use of local SQL Server authentication (a non-recommended practice); the presence of sample databases; and failure to implement best practices for database activity auditing.

The descriptions provide detailed information on the vulnerabilities, their source, potential solutions and references for additional information.

Reporting A-

AppDetectivePro includes nine canned reports that provide useful information for various levels of management and technical staff. These include an application inventory, summary reporting, high-level and detailed vulnerability reports and information on user accounts. You can also generate differential trend reports to evaluate the status of scanned databases over time. Output is available in Crystal Reports, HTML, XML and text.

AppDetectivePro stores results in an Access database on the local system, but you may also configure it to use SQL Server.

Verdict

AppDetectivePro is an excellent solution for auditors, security professionals and consultants to capture snapshots of database security status.

Testing methodology: We tested AppDetectivePro in a VMware environment using Windows Server 2003 and SQL Server 2005.

Review how we grade at searchsecurity.com/grading_criteria.

For an extended online version of this review, see this month's issue on SearchSecurity.com.

APPLICATION SECURITY

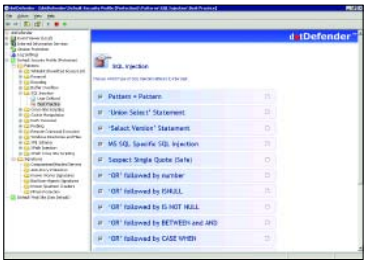
Applicure Technologies dotDefender

REVIEWED BY SANDRA KAY MILLER

Applicure Technologies

www.applicure.com

Price: **Starts at $3,995 per physical server installation**



If you're looking for quick and inexpensive Web application security, dotDefender offers protection against common threats through a software plug-in for IIS, Microsoft ISA and Apache servers.

Installation/Configuration A-

dotDefender installed rapidly and much more easily than hardware-based Web application firewalls (see comparative review, March 2008). Since it's a plug-in, configuration and management for IIS and ISA is handled through the Microsoft Management Console. The Apache version installs as an inline module.

By default, dotDefender deployed in a protective operating mode, leaving us covered against the majority of common attacks we threw at it right out of the box. But, take the time to perform extensive testing on protected websites to ferret out any security settings that interfere with functionality.

Although the documentation to quickly get the product running was excellent, we would have liked to see a more in-depth user guide for advanced features.

Policy A

Tweaking the policies to return our test websites to complete functionality took about an hour per site. Although the default policies and rules were ample to protect against all of our attacks, dotDefender required minor tuning to maintain the usability of the applications on our Web server, such as those that utilized advanced Javascript or built with older Web tools.

Policies center on patterns and signatures. Patterns define what dotDefender looks for in terms of exploits, such as buffer overflows, SQL injection, cross-site scripting, cookie manipulation, etc. Each pattern includes two sub-menus: user defined, where custom rules can be created, and best practices, which includes a check box list of standard defenses/mitigations against known exploits.

Signatures are regularly updated by dotDefender and include a blacklist of compromised/hacked servers, anti-proxy protection, worms, bad user agents, spammer crawlers and MPack protection against infected websites.

Security profiles with unique policy settings can be assigned to different websites hosted on the same server.

Logging and Reporting C

Reporting is dotDefender's weakest aspect. There was very little documentation about the reporting features. Logging provided information that would be useful to an IT administrator, but the reports wouldn't be very valuable to a business unit in regard to its PCI compliance or how its security posture is affecting its business.

Event reports offered basic statistics for individual websites, event categories and client IP addresses.

The logging capabilities are adequate, but lacked the advanced features we have seen in Web app firewall appliances. Log data can be exported to third party monitoring and reporting tools.

Effectiveness B

Using a combination of signatures, session evaluation and pattern recognition, dotDefender examines HTTP requests, either allowing or denying them or in passive mode, logging only according to policy.

dotDefender effectively protected all our websites from a variety of common ills found online, including Internet and browser worms, malicious websites with automated downloads, external vulnerability scans, cross-site scripting, SQL injection and DoS attacks.

Additionally, we were able to customize how suspect HTTP requests were handled. They could be denied, redirected or only logged. There is the option to return either default or customized error pages for denied requests.

Verdict

dotDefender is an inexpensive and no-frills way to protect HTTP sessions on a Web server.›

Testing methodology: We tested dotDefender on Microsoft IIS on Windows Server 2003 hosting a variety of websites.

WEB APPLICATION SECURITY

Cenzic Hailstorm Enterprise ARC 5.7

REVIEWED BY PHORAM MEHTA

Cenzic

www.cenzic.com

Price: **$26,000**

Web application security has moved from a nice-to-have to a must-have requirement, for data protection and compliance. Cenzic's Hailstorm, which we last reviewed in 2005, reflects the growth in the depth and maturity of Web application vulnerability assessment software.

Installation B

Enterprise ARC includes a management server/console; database for checks, assessments and results; ARC Execution Engine (AEE); distributed scanners that run scans with the Web application to run in different parts of the network and the standalone enterprise desktop scanner.

These components can be installed on one or more machines. The only combination that might be a little tricky is the AEE and desktop software on the same box. In this scenario, you have to stop the AEE service before you can run the desktop client.

Use the desktop application for applications needing some manual interaction and constant monitoring during the assessment, and use AEE for assessments that can be completely automated.

The installation wizard is straightforward and walks you through the various options, including setting the network port and passwords for communicating with the database.

Testing methodology: We installed the server, database and desktop client on a Windows 2003 Server and used a Windows XP machine as an execution engine and tested against several Web applications.

Configuration B+

Hailstorm offers three methods to add applications: Users can run an auto-discovery scan on Web application ports, add applications manually, or import a CSV file. You can assign a risk factor, and group applications for better management. Running and scheduling assessments is as simple as it gets.

The desktop application allows custom assessments that are a combination of checks from best practices (OWASP), regulatory standards, and custom attacks created in-house. We selected the OWASP and best practices assessments against a classic ASP/MS SQL and a Joomla (LAMP) Web application, respectively.

Hailstorm offers by far the best attack customization and new attack creation capability in the industry. To offer flexibility, Cenzic has added features such as interactive assessments, where the user navigates through the website manually.

Effectiveness A

The two areas enterprises spend the most time on when using a vulnerability scanner are the home page/central display and the results/reports. Cenzic has remarkable interactive dashboard that shows trends and activities. During the review assessments, we were able to watch the findings and graphs updated as vulnerabilities were discovered. The details on each finding were available instantly, along with the HTTP request/response, complete explanation of how the attack was executed and remediation recommendations.

One feature that sets Hailstorm apart is the Hailstorm Application Risk Metric score, which incorporates the risk factor assigned to each application and the severity of the vulnerabilities discovered. This helps you focus remediation efforts and determine which vulnerabilities present the most risk. It also measures if risk is decreasing and if remediation is effective over time.

Reporting B+

Reporting is by far the most improved module. The reporting engine is a powerful tool to monitor progress, manage compliance and distribute relevant information in a timely manner. The Crystal Reports viewer can export reports in many formats.

Verdict

Enterprise ARC 5.7 is a true enterprise-class solution for managing Web application vulnerabilities.›

APPLICATION SECURITY

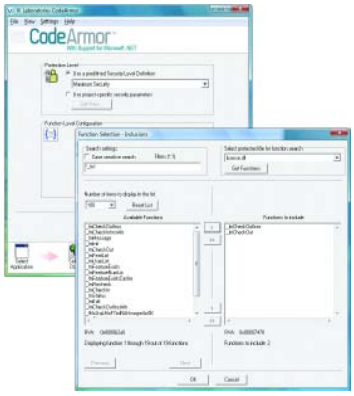
CodeArmor 2.2 for Microsoft .NET

REVIEWED BY STEVEN WEIL

V.i. Labs

www.vilabs.com

Price: **Starts at $18,500 for enterprise applications**



Crackers use sophisticated debuggers, disassemblers, virtual machines and other reverse engineering tools to undo software protection mechanisms. The result? Your company's products can become part of the multibillion-dollar software piracy industry, your intellectual property could be stolen, or code compromised.

CodeArmor 2.2 for Microsoft .NET can protect an organization's applications without requiring their modification. Using deep encryption techniques, it will frustrate even highly skilled crackers. It provides stronger protection than standard obfuscation techniques or hardware dongles.

Configuration and Management B+

Installation was fast and easy. CodeArmor runs on Windows XP/2003/Vista and can protect .NET 2 and 3 applications. The software's useful documentation and intuitive interface made it easy to use.

Simply select a .NET executable file, its associated DLLs and specific functions to protect. CodeArmor then encrypts the selected functions (128 bit RC4 or AES) and embeds a security event monitor in the application. The search interface makes it easy to locate and protect specific application functions.

CodeArmor does not require modification of source code or creation of additional application files.

Testing methodology: We installed CodeArmor on a Windows XP SP2 machine and tested it with a variety of .NET applications.

Policy Control B+

Controls are very granular and flexible; you can select specific application functions and then define how those functions will be protected. For example, during beta testing, you may want to protect many of the application's functions. However, after release, you may only want to protect the code that generates the application's license or that initiates encryption.

By default, CodeArmor handles all application exceptions (e.g., an invalid handle or access violation); such exceptions are often caused by cracking attempts.

CodeArmor can also be configured to prevent an application from running within a virtual machine (a technique commonly used by crackers) or stop other processes from accessing the application.

Reporting C

CodeArmor's reporting is somewhat limited. It can produce a very detailed log file when the application is initially protected. However, we would have liked to see more logging of actions taken in response to attacks on protected applications. CodeArmor also does not have out-of-the-box ability to generate alerts or send notifications of attacks. V.i. Labs says that custom extensions can be created for notifications and event logging.

Effectiveness A

When a protected application is launched, CodeArmor decrypts and then re-encrypts individual functions as soon as they are loaded to minimize the application's exposure to reverse engineering attempts. CodeArmor's security event monitor continually checks the runtime environment to detect any malicious tampering attempts, such as trying to attach a debugger to a protected application. If tampering is detected, the monitor shuts down the application.

We found CodeArmor to be very effective. We were unable to access protected .NET applications with a debugger or disassembler. Protected applications failed to start after we modified their DLL files with a hex editor. It enforced specific security settings, such as preventing an application from running on a virtual machine.

Protected applications ran a bit slower; V.i. Labs says that the performance impact is usually about 3 percent.

Verdict

CodeArmor is an effective and easy-to-use tool for protecting applications but has limited reporting.›

SOFTWARE SECURITY

Klocwork Insight 8.0

REVIEWED BY JAMES C. FOSTER

Klocwork

www.klocwork.com

Price: **Starts at $25,875 (five user licenses, one build server license)**

Klocwork Insight is a source code analysis product that helps automate security vulnerability and quality risk analysis, remediation and measurement. It employs more than 200 different techniques for identifying software flaws for C, C++ and Java.

This kind of tool is increasingly important, as very few people are capable of analyzing and, most importantly, fixing software security flaws.

Installation/Configuration B-

The installation is difficult for a user of any type, requiring several different modules and server components to be installed or loaded prior to use. Plan to spend time on training. The upside to the initial learning curve is scalability and flexibility for large, hybrid or segregated development environments.

Licensing can be centrally managed across multiple teams and updated in seconds via a quick change of the license file. MySQL is utilized as the backend database and can be configured at will, making it easy to schedule backups, modify the default schema, or integrate Insight into other products such as Microsoft SharePoint or BMC Remedy Service Desk. All aspects of the Web interface and server are configurable, as it runs atop Apache Tomcat.

Klocwork supports most development environments and can be installed on a range of *nix and Windows OSes.

Testing methodology: We tested Klocwork on a Windows XP Professional SP2 workstation and on a fully patched Windows 2003 Server against several open source, C/C++ and Java applications utilizing the Eclipse IDE developer plug-in.

Management/Monitoring B

Leveraging the Eclipse and Visual Studio native interfaces for developer integration was key to provide true engineering-level value. From the Eclipse interface, we could easily navigate through the source tree from the Windows Explorer-like folder system, and see the associated identified vulnerabilities and issues.

Double-clicking an issue, such as one we found for NULL pointer dereferencing, opens the associated file directly at the line in question. You can modify and save the code in the IDE as usual, or right-click the issue at the bottom to obtain sample "bad code" and documentation on the potential vulnerability.

Post-installation management is still immature, as DOS batch files are used to start and stop the Klocwork servers on local installations. It is also recommended that you manually stop all of the Klocwork components prior to rebooting your machine.

Since Insight is not yet capable of reviewing JavaScript, PHP and ASP, it is not the tool of choice for Web 2.0 applications. (Support for scripting languages will be available in a future release, Klocwork says.)

Reporting A

We were blown away by Klocwork's reporting capabilities. The Web-based reporting interface, Insight Review, allows users to navigate through findings and recommendations, and drill down into specific components.

You can select one of the current projects your teams set up during configuration—typically, each application, product or tool has a standalone project created in Insight.

Once you select a project, the interface changes into a robust report-creation engine, with the ability to flag and group issues by severity, status and state. These reports are dynamic and contain active links or hyperlinks that allow you to gain further detail on specifics issues. More than 300 issues were identified in one of the tests we ran, and creating the critical issues report took two minutes from start to finish. These issues were divided into logical code directories based upon the build structure.

All data views and graphical reports can be exported to PDF or CSV files, and detailed issue data broken down by file and line can be conveniently exported to XML.

Verdict

Klocwork's enterprise reporting and analysis techniques will help companies with structured programming ties to C/C++ and Java.applications.›

CORE OF THE MATTER

No longer can security managers focus only on perimeter and host security. The application has become the prime target for hackers. We review six leading Web application firewalls that help deliver your critical apps securely.

BY SANDRA KAY MILLER

Consider how much information gets plugged into databases through applications and then regurgitated in queries, reports and content. We live in a world of HTTP and HTTPS, where everything has been ported to Web-based interfaces and consoles. Traditional network firewalls operating lower on the stack have no way of identifying malicious requests traversing TCP ports 80 and 443 to online shopping sites, Web mail or business portals such as online banking and account services.

Add PCI-DSS requirements for application security, and it's easy to see why Web application firewalls, once considered niche technology, are gaining traction in corporate data centers. They prevent attacks that network firewalls, IDS/IPS and antivirus filters cannot by limiting suspect access through combinations of behavioral analysis and policy controls.

In a head-to-head review, *Information Security* examined six application firewall appliances, all of which delivered centralized management, enterprise reporting and comprehensive protection for applications: Barracuda Networks' Web Application Gateway (formerly NetContinuum); Bee Ware's iSentry; Breach Security's WebDefend; Citrix's Application Firewall; F5 Networks' Big-IP 8800 Application Security Manager; and Imperva's SecureSphere Web Application Firewall.

Each product was graded on ease of installation and configuration; administration; depth of security policy control; monitoring, alerting, auditing and reporting; and overall security effectiveness.

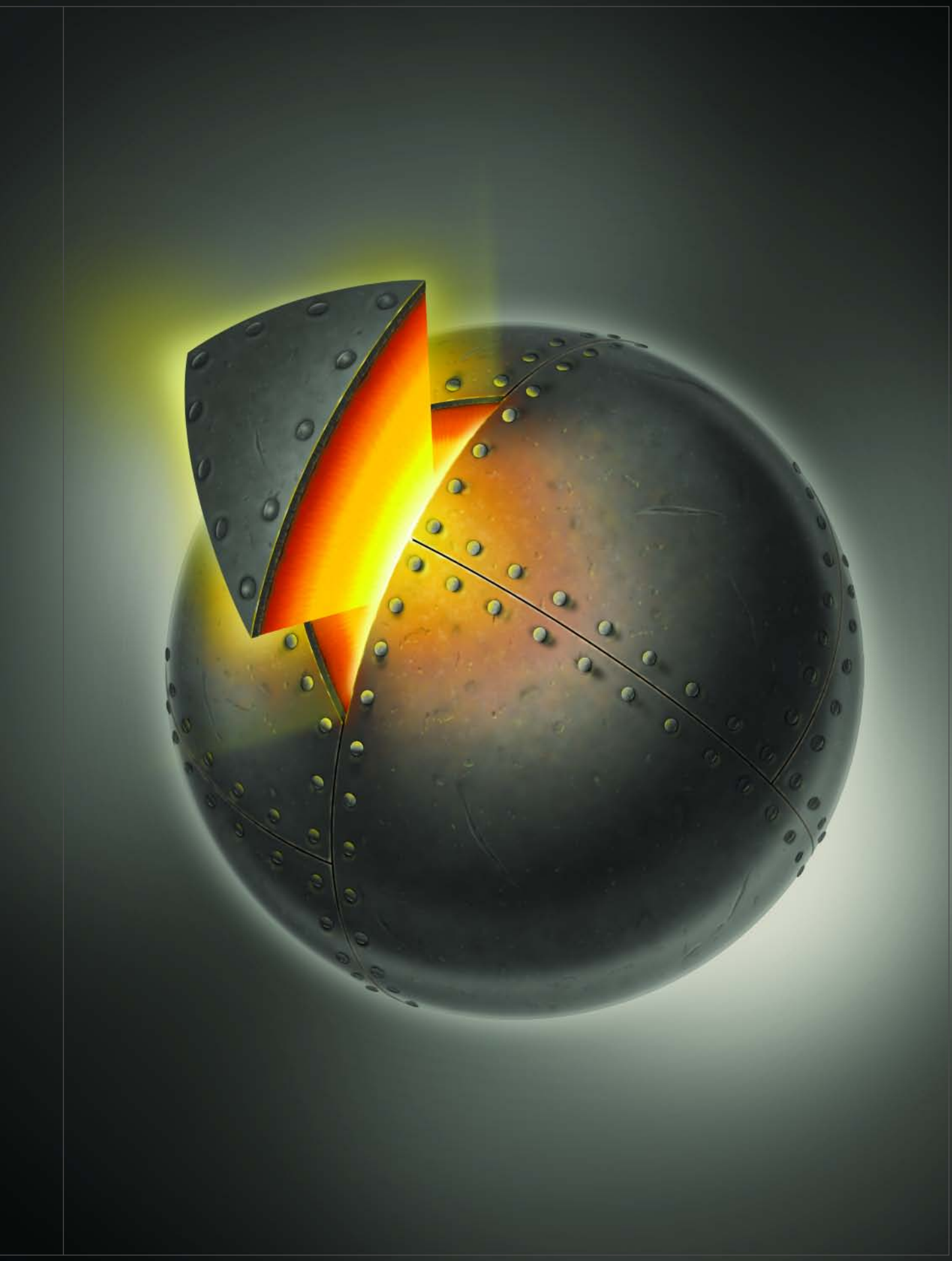


Illustration by JEFF MANGIAT

INSTALLATION AND CONFIGURATION

All the products we tested were 1Uor 2Urack-mounted devices built on hardened appliances. Our first step was to gauge the ease with which each product could be installed and configured. Although each appliance supported a variety of deployment configurations (bridge, router, inline, out-of-line), we set up each as a reverse proxy, except Breach Security's WebDefend, which is designed to operate in a non-linear environment.

Imperva and Breach were easiest to set up and configure. Thanks to their intuitive design and wizards, each took approximately an hour to get running.

Using the Site Manager through Breach's console, we could easily verify that the domains, IP addresses and ports were correct. It even identifies the type of server on which the application is hosted (e.g., IIS). Through the logical tree structure, it's easy to locate and add sites.

Imperva required more manual intervention for the configuration of our servers, Web sites, services and applications. It presented a logical tree structure similar to that of Breach, but lacked the useful at-a-glance verification and instead spread the information among four different tabs. Nonetheless, these were minor points and we found it overall to be on a par with Breach in this category.

Bee Ware's initial installation was similar to our other test subjects, and the configuration wizard stepped us through assigning the basics such as host name, date and time, network interfaces and assigning the destination IP address for our target back-end server. The documentation showed some rough translation issues from the original French, but the configuration wizard led us through a fairly straightforward setup.

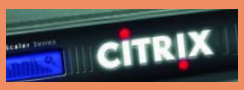
F5's Application Security Manager (ASM) is a part of its BIG-IP port-based multilayer switch built on F5's proprietary TMOS platform, which is designed for traffic management, acceleration and load balancing. After a fairly painless installation onto our network, the configuration required us to spend the better portion of a day understanding how the ASM mod-

About this REVIEW

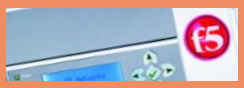
Barracuda Networks Web Application Gateway NC1100

Bee Ware iSentry IS200

Breach Security WebDefend



Citrix Application Firewall



F5 Networks Big-IP 8800 Application Security Manager

Imperva SecureSphere Web Application Firewall

Information Security deployed six application firewall appliances from Barracuda Networks, Bee Ware, Breach Security, Citrix, F5 Networks and Imperva.

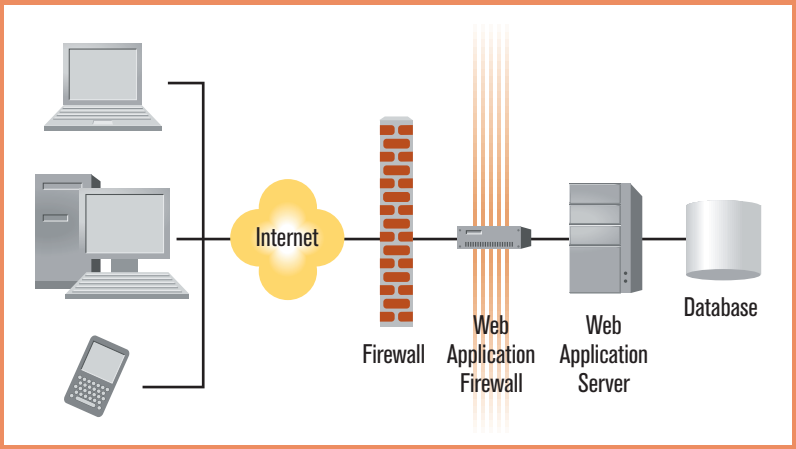
Each product was installed in our test lab between a network firewall and in front of or alongside the application servers *(see "Inside The Lab," below)*, which included an Apache Web server and Microsoft Internet Information Server, each hosting a variety of applications including Web mail, an online forum and a Web site with shopping cart capabilities.

Client machines subjected to attack included systems running Microsoft XP SP2 with Internet Explorer and Linux (Debian 3.1) with Mozilla Firefox. We focused on common attacks against applications including buffer overflows, cookie tampering, SQL injection, session hijacking, cross-site scripting (XSS), cross-site request forgeries (CSRF), forms tampering, remote code execution, malicious code (Internet worms), denial of service, brute force login and forceful browsing.

Additionally, we configured application-side security features, such as Web site cloaking, and attempted to gain network and application configuration via nefarious reconnaissance practices such as identifying operating systems and Web server details through HTTP header data and scanning utilities like Nmap.

Breach's WebDefend was deployed in an out-of-line mode next to our Web servers using a span port.

—SANDRA KAY MILLER



INSIDE THE LAB All application firewall appliances were deployed as reverse proxies (except for Breach Security's, which was attached to a span port) on a network between a traditional stateful inspection firewall and a variety of applications servers, including Microsoft IIS and Apache Web servers, Microsoft SQL, e-commerce applications with credit card transaction capability and an online forum. Browsers included Internet Explorer, Firefox, Netscape and Opera.

ule integrated with the other modules, such as the Local Traffic Manager.

While all of this first appeared extremely complex, F5 features a clean and informative interface coupled with outstanding documentation and technical support. The complexity was offset by the rich load balancing and traffic management features necessary for delivering application security in big pipe environments.

Citrix required a lot of manual entry, but offered a clean Windows-based configuration utility. It wasn't as time consuming as Barracuda's Web Firewall's setup or as complex as F5, which required extensive understanding about network traffic management prior to setting up the security features.

Barracuda is somewhat complex and took a long time to set up. Even though we used Barracuda's Web application wizard, an extensive amount of manual security configuration was required to effectively protect our test applications against our attacks. Since Barracuda boasts of its ability to be set up in a production environment without causing disruption, we initially deployed the box in passive mode, producing logs that identified actions that would have been taken if it was in active response mode—for example, blocking traffic from an IP that was performing a brute force login, forceful browsing or bot activity. This allowed us to effectively tune the appliance prior to switching to active mode—a real plus for security managers without the time or resources to first deploy in a mirrored test environment.

AT THE CORE | Installation and Configuration

THE GOOD NEWS Imperva and Breach are easiest to set up and configure, thanks to their intuitive design and wizards, though Imperva requires a little more manual intervention.

THE BAD NEWS Barracuda is somewhat complex, and setup is time-consuming, requiring a lot of manual configuration.

ADMINISTRATION

Ongoing maintenance and tuning plays a significant role in the continuing effectiveness of these devices, which cover numerous complex technologies and security issues. And, the pervasiveness of Web-based applications presents management challenges that make delegated administration an important factor.

Imperva offers the most granular administrative rights delegation and greatest ease of assigning rights and permissions. An expandable tree allowed us to instantly view administrative groups under which individuals are listed. Rights and permissions can be set globally, per group or per individual through a comprehensive list of available resources and applications. We could quickly set view/edit privileges. Individuals can be assigned to multiple groups as well, giving them different levels of access.

F5's comprehensive set of administrative tools supports its traffic management and load balancing capabilities, and the application security module. It helps tame the overwhelming task of administration by compartmentalizing objects such as virtual servers, URLs and databases for easier, more flexible delegation.

Similarly, Barracuda groups applications and resources into role-based administration silos to facilitate delegation. Navigation throughout the extensive feature set was relatively easy, despite complexity second only to F5. Roles define the user's permissions for command groups (meaning what type of actions) and are accessible for a particular site, so administrative duties can be delegated in a large or distributed environment.

AT THE CORE | Administration

THE GOOD NEWS Imperva offers highly granular features for delegating administration and assigning rights and permissions, with a comprehensive, easy-to-use interface.

THE BAD NEWS Citrix's interface is intuitive and well-designed, but the options are limited, which may not suit some organizations' requirements.

Bee Ware keeps things simple by breaking down administrative tasks into two basic groups—administrators and webmasters. Administrators have access to global configurations and can create, disable or delete services and policies. Webmasters only have configuration rights to the services and policies for which they have been assigned permission. This provides the autonomy needed for different groups to make changes to their HTTP-based content as well as the overall security and oversight to prevent damage to active content pages.

Citrix's administrative capabilities are basic, but well-managed through a simple and intuitive management GUI. We were able to quickly add users for administrative purposes, but our options were limited to either an application administrator or an application guest, whose account could view, but not modify, configuration settings. We felt this was essentially useless.

Breach breaks out administrative tasks into two groups as well—system administrators with access to everything, and site administrators who only have rights to sites assigned to them. Additionally, Breach includes two view-only accounts—a Super Viewer who can see everything and a Viewer with read-only access to sites to which they are assigned.

THE PERVASIVENESS OF WEB-BASED APPLICATIONS PRESENTS MANAGEMENT CHALLENGES THAT MAKE DELEGATED ADMINISTRATION AN IMPORTANT FACTOR.

Assigning sites was effortless, as all active sites are displayed in one window and could be assigned with a mouse click.

CONSIDER THIS

WEB APPLICATION FIREWALLS have additional features, such as those related to traffic management, including SSL acceleration, caches, compression, load balancing and high availability. The growing adoption of high bandwidth technologies requires that solutions are capable of delivering security without latency. Other factors that may influence your purchase decision are regulatory compliance features and out-of-the box policies and signatures to get you started without a lot of customization.

	Appliance Specifications	Load Balancing	Traffic Shaping	High Availability	SSL Acceleration Offloading	Connection Pooling	Cache and Compression	Pre-loaded Policies and Signatures	Regulatory Compliance Features
Barracuda Networks Web Application Gateway	A 2U appliance with a hardened OS, redundant power supply and eight drive bays with a throughput of 500 Mbps.	Yes		Yes	Yes	Yes	Yes	Yes	Yes
Bee Ware iSentry	Built on a Dell PowerEdge 860 with a hardened OS.	Yes		Yes	Yes		Yes	Yes	Yes
Breach Security WebDefend	Hardened 1U appliance with redundant power and four drive bays.			Yes				Yes	Yes
Citrix Application Firewall	A hardened lightweight 1Ufootprint with six 10/100 and two 10/100/1000 Base-T ports.				Yes			Yes	Yes
F5 Networks Big-IP Application Security Manager	A 2U appliance sporting dual core processor with 12 gigabit Ethernet and two 10 GbE ports and redundant power supply.	Yes	Yes	Yes	Yes			Yes	Yes
Imperva SecureSphere Web Application Firewall	A 1U appliance with a hardened OS, three drive bays and six 10/100/1000 Base-T ports.			Yes				Yes	Yes

SECURITY POLICY CONTROL

The real power behind these products lies in their ability to let organizations control access to dynamic applications. Unlike traditional network firewalls that simply permit or deny packets based upon policy, application firewalls must deliver more sophisticated control at the application layer through a variety of contextual rule sets and behavioral analysis.

All of the products included some sort of learning function, either the automatic learning of URLs or learning behavior and traffic patterns. Another significant policy designation was the firewall's ability to operate in a transparent mode, which allowed us to fine-tune actions prior to initializing full security measures, such as blocking and redirecting.

Breach provided the most predefined policy set out of the box, covering known attacks against popular applications such as IIS, Apache and SQL. We are skeptical that its controls have the robustness to be effective against unknown attacks.

The console isn't as complex or icon-driven as the other products, but is laid out in a way that let us drill down through our applications and review and set policies. Best of all, it provided one of the best visual interfaces along with information about security events.

We were particularly engaged by the use of BreachMarks—regular expressions or custom strings used to identify sensitive information, such as credit card numbers.

The first order of business with Citrix was switching from bypass mode to operating mode—basically turning on the firewall. From the same page, we were able to choose whether to include failover protection in our security policy, assign session timeout thresholds and toggle between two diverse degrees of overall security—Enterprise, which included full filtering and blocking, or Express, with basic Web server policies.

Once traffic began passing through the appliance, we had to determine whether to enable failover protection. Initializing this option was difficult, as it required an in-depth understanding as to whether or not pages containing Web forms utilized Javascript or Get calls.

Citrix's Adaptive Learning mode examines traffic to determine what is normal and then builds recommendations that let users apply, edit and apply, skip or ignore. Unfortunately, when a recommendation is ignored, the firewall will no longer view that particular action as a threat when encountered. We would have preferred to see a threshold set for the skip option to allow change to meet new zero-day exploits and adaptive malware.

F5's policy management is quite flexible. Initially, the wizard walked us through each aspect rule definition. F5 also supports an assortment of adaptive learning tools to assist with policy generation. We found the Learning Manager and its counterpart, the Traffic Learning Screen, to be the most helpful in determining policy. Each time we created a potential violation, such as forceful browsing or multiple failed login attempts, the Learning Manager made suggestions as to how to adapt our security policy.

F5 offers the ability to create security policy templates to facilitate large-scale deployments.

Between Barracuda's policy wizard and the dynamic application profiling, we were able to create security policies specific to the traffic generated during our testing. However, it's easy to see how in a high-traffic environment, the constant tweaking would be bothersome and ultimately create a security risk from multiple changes.

AT THE CORE | Security Policy Control

THE GOOD NEWS We especially like BreachMarks tagging. F5 features a good policy toolset, particularly for adaptive learning, and Imperva has an array of out-of-the box policies and attack signatures.

THE BAD NEWS Bee Ware's policy creation is time consuming, poorly organized and difficult to navigate.

Barracuda's passive mode is very good at displaying what results would be if policies were actively enforced. While the other products displayed what was taking place on the network, they didn't offer the extensive understanding of the ramifications of the security policy had it been active.

While Bee Ware's security policies provided adequate protection against our assortment of attacks, setting up polices proved to be difficult. The appliance utilizes blacklists, dynamic whitelists and behavioral analysis, but the logic required to institute rules and patterns is time-consuming and disorganized. Policy creation was spread across a series of tabs. We would have like to been able to create policies from a centralized location using drop-down menus and tables.

Imperva delivered an impressive set of predefined attack signatures. Custom signatures can be easily created through a simple menu system that includes a wide variety of metadata choices (Web, stream, SQL).

The easy-to-navigate interface allowed us to peruse polices through a variety of filters listed in a hierarchical tree on the left side of the policies page.

MONITORING, ALERTING, AUDITING & REPORTING

All the products we examined had features specific to aid compliance auditing and reporting. Security managers want detailed information about malicious activities on their network—the who, what, why, where, when and how details. Auditing and reporting features can make or break a product's chances of ending up at the top of the short list.

Imperva sports a highly configurable real-time interface, in which we were able to monitor all our applications, alerts, events, connections and the overall health of our systems at a glance under the Monitoring tab.

A separate and equally functional tab offers more than 100 types of reports from which to choose—from a list or using Imperva's robust filtering capabilities.

The Admin tab put everything neatly at our fingertips. With a mouse click we could access users, sessions and, most important, the Application Defense Center—a catch-all for updates and information on signatures, policies, protocols, reports, etc.

Breach also offers an assortment of useful reports, many which are obviously focused on PCI compliance reporting. Monitoring our shopping cart application, it took only minutes to compile detailed reports about how credit card information transmitted through specific Web pages.

The Event Viewer offers nine filtering options to drill down on an incredible amount of information, as well as the ability to create customized filters.

Citrix provided adequate monitoring, alerting and logging capabilities. Monitoring is accessed via a dashboard icon on the main interface, as are reports and logs. There are two basic types of logs: The firewall log provides information about security-related events, and the audit log records all activities you select when you configure the box.

Compared to Imperva, the Citrix dashboard is plain and uninformative. We were disappointed by the weak reporting features, which offered only four types of administrative reports—an Executive Summary, a Security Summary, a Configuration Summary and an Inspection Report, which listed the attacks.

In addition to Web Application logs, Barracuda provides syslogs, network firewall logs and Web firewall logs, each with its own page under the Logs tab on the dashboard. Overall, the logging displays were visually confining and dull. Reporting capabilities were as disappointing as those offered by Citrix, limited to alerts, diagnostics and error reports. They lacked the rich level of detail and customization found in Imperva and Breach.

F5 delivers excellent monitoring, alerting, historical and forensic capabilities, but the reporting tools are only mediocre Executive, Events, Security and Attack reports, despite the phenomenal amount of information gleaned through the multiple types of monitors that continuously track HTTP, HTTPS, TCP, FTP and other network protocols.

Bee Ware's monitoring capabilities were limited to real-time application activity and security logs, which are viewed via the administrative interface or exported as syslog log files. Alerting was limited to

AT THE CORE | Monitoring, Alerting, Auditing & Reporting

THE GOOD NEWS Imperva provides a wealth of easy-to-access information, and a virtual cornucopia of reports generated through robust filtering.

THE BAD NEWS Bee Ware is just fair across the board here: no SMS or email alerts, limited monitoring and weak reporting.

SNMP traps and syslog messages. Security administrators require instant notification through a variety of methods, such as SMS and email, the moment a critical event occurs.

Bee Ware only offered two basic types of logs—security and access. Each provides a table of events and each event could be clicked on for additional information. We found the logs to be more helpful than the reports for which they provided the data. Reports were limited and poorly designed in their graphical display.

OVERALL SECURITY EFFECTIVENESS

The Web has opened a multitude of new avenues for hackers to exploit Internet protocols and the applications that utilize them. The core functionality of all the products delivered comprehensive security for HTTP, HTTPS and FTP applications and XML services. In our test rail, all the products delivered a core set of security features, most notably Web site cloaking, protection against common Web vulnerabilities and exploits and data protection.

Our battery of attacks included but was not limited to SQL injections, buffer overflows, cookie tampering, forms tampering, session hijacking, cross-site scripting, remote code execution, malicious code (Internet worms), denial of service, brute force logins and forced browsing. We launched a Java-based Web crawler in an effort to fingerprint the applications and hosted sites behind the product under testing. Additionally, we purposely set up insecure pages that provided access to restricted data (credit card numbers, fake, of course) and attempted to gain access. Each product performed satisfactorily, and all are worthy of enterprise installations.

Given the massive amount of information stored in databases that are touched by Web-facing applications, we found that Imperva's application and database security provided the closest thing to a silver bullet security managers could institute. Using a combination of whitelists, blacklists and adaptive learning ("Dynamic Profiling Technology"), the device examined traffic and behavioral patterns of applications and databases to differentiate between valid traffic patterns and our attacks.

Barracuda uses a combination of Web ACLs, positive and negative security models and Dynamic Application Profiling to identify acceptable traffic. The included signatures for the negative model blocked all the common attacks (SQL, buffer overflow, tampering, etc.), while the positive model locked down all traffic unless defined through the powerful ACLs. We set a variety of ACLs that delivered superior security for our test sites.

Similarly, F5 employs both a positive security model, and a negative model for common attacks, with heuristic analysis of all traffic through the Adaptive Learning and Tuning engine. We credited the strong positive security model for initially blocking some of our legitimate traffic and returned to the transparent mode until we had established a traffic baseline through F5's automated policy builder. Our second attempt at enabling blocking resulted in flawless operation, with all attacks stopped while allowing permitted traffic to proceed.

The granular traffic movement controls allowed us to limit access to applications through customized traffic flow policies.

We started our Citrix testing in bypass mode; while we understood the validity of not filtering in this state, we would have liked to been able to at least log traffic for a comparison once the device was switched to operating mode. Our initial testing was met with a number of false positives requiring us to disable Adaptive Learning and do some manual tuning.

Adaptive Learning made suggestions that we could accept, deny or customize. We found this especially helpful whenever any changes were made to our applications, such as the addition of new sites or pages within sites, especially those containing vulnerable aspects such as forms, logins and dynamic links. All our malicious attacks were blocked in operating mode.

Bee Ware more than held its own under testing against common attacks and exploits such as SQL injection, buffer overflows, XSS and Microsoft and Unix vulnerabilities. Additionally, the behavioral analysis-based security engine offered enough automation of policy creation to make it attractive to smaller IT shops. Bee Ware's learning capabilities quickly identified new sites and pages added within our applications. However, until a new URL has been learned or manually added, it was rejected, leading initially to legitimate sites being blocked.

Breach uses dynamic application profiling combined with inbound and outbound traffic analysis to mitigate threats. Breach also identified imperfections in Web pages, such as miscoded URLs, images and objects that can create vulnerabilities, such as returning error pages displaying identifying information about the Web server or application.

AT THE CORE | Overall Security Effectiveness

THE GOOD NEWS Imperva is the closest thing to a silver bullet for application security, based on its combination of adaptive learning and other techniques.

THE BAD NEWS Citrix delivers good security against attacks, but we would like to see traffic logging for comparison while it is run in passive mode.

We started our testing in learning mode with the option to automatically switch to protect mode once enough traffic has been analyzed. We were pleased to see a change without any false positives once the device initiated an active posture.

There's no doubt that Breach is an excellent solution for PCI compliance. Focusing on security aspects specific to credit card transactions, from masking account numbers to robust SSL protection, we were pleased with the overall performance of the appliance. When we tagged our test

MAKING THE GRADE

	Barracuda Networks Web Application Gateway NC1100 www.barracuda.com	Bee Ware iSentry IS200 www.bee-ware.net	Breach Security WebDefend Version 3.0 www.breach.com	Citrix Application Firewall www.citrix.com	F5 Networks Big-IP 8800 Application Security Manager www.f5.com	Imperva SecureSphere 6.0 Web Application Firewall www.imperva.com
Installation & Configuration 10%	B	B	B+	B-	B	B+
Administration 10%	A-	B+	A-	B-	A-	A
Security Policy Control 20%	B+	C	A-	B+	A-	A-
Monitoring, Alerting, Auditing & Reporting 20%	C	C	A-	C	B-	A
Overall Security Performance 40%	A-	B+	A-	B+	B+	A
VERDICT	**B+** Delivers granular control for applications and Web-based protocols through a combination of technologies. Pros: Flexible role-based administration, powerful ACLs define permitted traffic. Cons: Disappointing reporting limited to alerts, diagnostics and errors.	**B-** Provides enterprise performance in addition to compliance-worthy application security. Pros: Straighforward administration model, automated policy creation. Cons: Difficult policy creation interface, very limited monitoring, alerting and reporting.	**A-** An excellent choice for data protection as well as application security. Pros: BreachMarks tagging to identify sensitive data, information-rich dashboard. Cons: Policy controls could be stronger against unknown attacks.	**B** Solid application security, but disappointing management GUI.. Pros: Useful recommendations facilitate Adaptive Learning process to reduce false positives. Cons: Weak reporting offers few options; lackluster dashboard.	**B+** Offers a variety of excellent traffic control features in addition to securing applications. Pros: Administrative controls are up to the task of managing complex traffic management features. Cons: Disappointing reporting tools considering wealth of available information.	**A-** A well-designed product that delivers comprehensive protection out of the box and is easy to use. Pros: Impressive protection through powerful combination of security techniques. Cons: Configuration requires more manual intervention than we'd like.

data simulating credit card information with BreachMarks, our exploitable shopping cart application lit up our alerts. At first, we allowed the private information to traverse the firewall to verify Breach's claims that it provides detailed records about any compromised information. This lets companies verify exactly what records have been illegally accessed.

MEETING THE NEW THREATS

All of the appliances we reviewed provide effective application layer protection; all scored well against the diverse attacks we threw at them. But we found significant enough differences depending on your organization's requirements. Imperva presented the strongest all-around offering, followed closely by Breach Security. Both were strong across the board. F5 and Barracuda Networks are strong choices, faltering only in their monitoring, alerting and reporting categories.

The scope of our testing was limited to a single appliance placed in front of a couple of Web servers. However, when working with these products it becomes apparent that they were designed to protect clusters of servers, if not entire server farms hosting Web-facing applications. Though network management features weren't part of our evaluation criteria, these may be important factors in your choice of an application firewall appliance.

Application firewalls represent next-generation digital security. As these technologies mature, and working in conjunction with traditional network firewalls, IDS/IPS and malware scanners, it is hoped they will reduce the threats faced by an increasingly Web application-driven society.›

Technical editor Sandra Kay Miller is a frequent contributor to Information Security. *Send comments on this article to feedback@infosecuritymag.com.*

AUTHENTICATION

Secure Computing SafeWord 2008

HotPick INFORMATION SECURITY®

REVIEWED BY SANDRA KAY MILLER

SafeWord 2008

www.securecomputing.com

Price: **Starts at $99 per user; includes token, server license and first year support; $4,995 for optional Enterprise Solution Pack**

Passwords are no longer effective for remote access to critical applications. Increasingly, organizations are turning to two-factor authentication.

SafeWord delivers identity management and access control for Windows systems using tokens that generate secure single-use passcodes that cannot be stolen or hacked, to complement existing remote access infrastructure such as VPNs.

It supports a variety of remote access products including those from Citrix, Cisco, Check Point, Nortel, Juniper, F5, Aventail and any other RADIUS-based VPN.

Configuration/Management A

There are two configuration options—via Active Directory or using the SafeWord 2008 Management Console, which is one of the components of the optional Enterprise Solution Pack (ESP). ESP offers a variety of useful features including SecureWire Access Gateway (an SSL VPN with unlimited users), protection for Windows login, and MobilePass, which generates the same passcodes as the physical token through mobile devices.

The basic installation of SafeWord Server, the management console and the Auto Updater Agent were straightforward, simple port settings for the authentication engine, administrative service and database, host addresses and key signing.

AD offered the easiest and quickest setup. We needed only to open AD to launch SafeWord. The Management Console operates independently through the Windows program groups. Users can be imported directly from AD or a third-party database.

We tested the Alpine model token, which comes with a lifetime guarantee. You can get a premium token with numeric keypads for added PIN-based protection.

Lost or damaged tokens can rapidly be decommissioned, replaced and reassigned. Emergency passcodes can be generated as well.

Testing methodology: We tested SafeWord on Microsoft Windows 2003 Server, managing with both Active Directory and with the SafeWord 2008 console. We also evaluated the optional add-on module, Enterprise Solution Pack.

Reporting and Logging B

With regulatory compliance driving many security purchases, SafeWord covers the bases with extensive logs for administrative actions and authentication.

To make log files more manageable, we were able to configure how frequently log files would be transferred from the database into an archive file for more efficient storage. However, to view an archived log, the file must be loaded back onto the database. Reports can be created through the tools option on the admin server. Log data can be exported into third-party report generators or Microsoft Excel spreadsheets for custom graphs, tables and charts. While the data sets for the templates were easy to assign, the actual report generation into spreadsheet format didn't work very well, splitting data into multiple sheets instead of into a single master table.

Effectiveness A

SafeWord's flexibility in securing user access provides a variety of ways for organizations to effectively control remote access through various multifactor authentication scenarios. Users have a choice between several methods including a combination of synchronous (event- or time-based), asynchronous (challenge-response), memorized, appended, CHAP-encoded and dynamic passwords. Multiple users can also share a single token, but each will have a different password.

Any organization with a significant mobile workforce armed with smartphones and PDAs should seriously consider purchasing the optional ESP for the MobilePass feature, which generates authentication codes on mobile devices in lieu of hardware tokens.

Verdict

SafeWord 2008's package is an attractive option for organizations wanting to add cost-effective, yet strong, two-factor authentication.

CONFIGURATION MANAGEMENT

Enterprise Configuration Manager 4.9

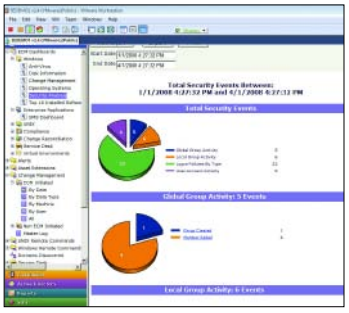
HotPick INFORMATION SECURITY®

REVIEWED BY MIKE CHAPPLE

Configuresoft

www.configuresoft.com

Price: **Starts at $995 per managed server and $40 per managed workstation**



Since we last looked at Enterprise Configuration Manager (ECM) about three years ago, Configuresoft has improved its value to enterprises seeking to survive in a complex regulatory compliance environment. ECM provides a centralized view into the configuration of managed servers and workstations, and the ability to initiate changes.

Policy Control A

ECM ships with a variety of compliance templates that you can modify to suit enterprise-specific requirements. You can also create exceptions.

You can monitor and manage a variety of system configuration elements, including disk usage, file system attributes, registry entries, installed software, local and domain accounts, service accounts and logging policies. It can also monitor application settings for SQL Server and Internet Information Services (IIS). New in this release, ECM includes help desk integration for Remedy.

ECM automatically tracks changes in the environment and can distinguish between changes made through the ECM interface and otherwise (for example, by a locally logged-in administrator). The change management workflow allows administrators to reconcile changes as authorized, out-of-band or noise.

Configuration/Management B

The two-tiered architecture comprises a centralized collector with an integrated SQL Server database and agents to gather information and report to the collector.

ECM can discover Windows hosts by accessing an Active Directory domain controller and automatically license the systems and push out the client software.

Unix/Linux servers require entering host information manually or file import. Agents are installed manually.

The Web-based portal has four tabbed sections available to users based on role: Console, Compliance, Reports and Administration. The interface is smooth and responsive, but there's a steep learning curve.

ECM's user account management integrates seamlessly with Active Directory, allowing you to leverage existing authentication and authorization infrastructure.

Testing methodology: We tested ECM in a Windows Server 2003 environment running under VMware Workstation.

Effectiveness A

ECM continues to deliver on its core promise: the ability to monitor and modify the configuration of managed systems in an extremely granular fashion. Our tests verified that the agents gather and report configuration information effectively. Additionally, we were able to issue configuration commands to managed systems through the ECM Portal. For example, we used ECM to kill processes and modify registry entries.

The Windows Remote Command interface allows you to execute arbitrary VBscript commands on managed systems and includes predefined scripts that accomplish common tasks.

The new version also provides support for monitoring VMware ESX virtualization servers.

Reporting A

ECM ships with a number of built-in, management-friendly dashboards complete with graphics for operational status reports. These dashboards track security log events, change management, antivirus status, installed software package and compliance with standards.

You can also create custom reports using a wizard.

One of the most important new features is the ability to enforce continuous compliance requirements through the use of alerts to notify you if a system's configuration varies from compliance requirements.

Verdict

ECM is one of the best configuration management products we've seen. If you're able to accommodate the product's steep price tag in your budget, it's a fantastic solution for monitoring and maintaining compliant system configurations in the enterprise.

DATA LOSS PREVENTION

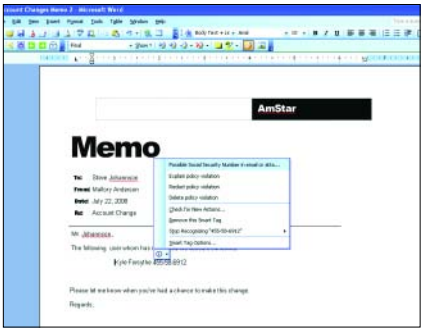
Workshare Protect Premium 6.0

REVIEWED BY ADAM HOSTETLER

Workshare

www.workshare.com

Price: **Starts at $49.95 per client**



Workshare Protect Premium 6.0 seeks to eliminate the malicious or accidental leakage of sensitive corporate data.

Workshare is client software that allows you to assess document risk, preserve content integrity and prevent disclosure of sensitive or confidential information. It installs several utilities and also integrates with products such as Microsoft Office and Lotus Notes.

Policy B+

The Policy Designer allows Workshare to be customized for your environment. Overall, it's well thought out, making it easy to create new policies. For example, we crafted a policy that searched for the word "confidential" in all text and HTML documents. You determine the files that are searched, such as Office, RTF, text, HTML, zip, XML and PDF. You can also create regular expressions (regex) to search for any standardized data such as account numbers. Several other criteria can be matched including looking in hidden data such as small text, hidden text, white text, etc.

Rules can be applied to Workshare "channels," the messaging protocol through which information is distributed—client email, Active Content Channel (in Office documents), removable devices and mail servers.

The actions and channels allow you to define how and where the information can be sent or stored. Our sample rule searched for "confidential," allowing it to be used in documents, but not allowing users to email it to anyone outside the corporation. The Workshare routing feature allows you to define who can and cannot be sent sensitive emails.

Auditing Tools B-

Workshare's greatest strength is its tight integration with Office. Workshare actively searches for policy violations in real time and tags violations.

Workshare allows the user to see what specific policy is violated, allows redaction of the violation or allows it to be ignored, depending on policy. For instance, when Workshare flagged our Social Security number violation, we redacted the number. Default policies search for profanity and other offensive terms.

Other tools, such as Trace Endpoint and Batch Clean, are run manually by the user.

Trace Endpoint runs all the current policy checks against files on the client system, and against email in the inbox. We used Trace Endpoint to scan a directory we made with files containing personal information. Trace Endpoint was able to identify all of the confidential information we defined in the rules.

After the scan is run, a report is available that details all of the violations and files in which they occur. The file can be saved to Excel or PDF format or printed. Data has to be removed manually from the offending files.

Batch Clean provides an easy way to clean multiple files of meta data such as usernames, comments, hidden data, macros, etc. Meta data can be useful to an attacker profiling your corporation for social engineering attacks. Batch Clean removed all the offending data from our test files but leaves no record of its action.

We would have liked to have seen centralized reporting and alerting for the various tools.

Verdict

Workshare Protect Premium provides a cost-effective tool to contain data leakage. It's not too intrusive, and helps educate employees. Companies looking for a more comprehensive data loss prevention solution may want to investigate Workshare Protect Network as well. ›

Testing methodology: We ran Workshare Protect on Windows XP with Microsoft Office 2003. Both default policies and policies created by the reviewer were used during the test.

DATABASE SECURITY & COMPLIANCE

DbProtect

REVIEWED BY JAMES C. FOSTER

Application Security, Inc.
www.appsecinc.com
Price: **$3,000 per database per year**

With most Web applications leveraging a back-end database, the importance of securing and monitoring your critical databases has never been higher. Application Security's DbProtect offers a one-two punch that scans databases for vulnerabilities and monitors them in real time for potential intrusions and compliance-related issues.

DbProtect consists of two software components. AppDetectivePro is a network-based database and application-specific vulnerability scanning tool for patch and hotfix levels, configuration, compliance and policy weaknesses. AppRadar is an application-layer intrusion detection system that can reside on or near databases to monitor for attacks.

Installation/Configuration B

After DbProtect's infrastructure is designed and implemented, the configuration is relatively straightforward. Most of the configuration for the scan engines and intrusion sensors can be accomplished through the Web GUI. Sensor agents can be installed locally on the database servers or on a network server. We recommend you run tools to baseline the database performance before and after the installations. The vulnerability scanning components are agentless.

You will need to reach out to your DBAs to get the connection and user account information for a current Microsoft SQL Server 2000 database, required as DbProtect's data repository.

Testing methodology: We tested DbProtect on MS Windows 2003 Server with an MS SQL 2000 back end against Oracle, Microsoft SQL Server, Sybase ASE and IBM DB2 UDB.

Reporting B

DbProtect's Web-based dashboard and reporting capabilities are solid, but lack full correlation of reports between the AppDetectivePro and AppRadar components. Several canned reports and filters allow you to quickly view report and risk statistics as well as trends. It would be nice to see more interactive components and high-end graphics, but all of the technical data is available.

Out of the box, DbProtect has an impressive list of supported regulations, including PCI DSS, HIPAA, GLBA, SB 1386, SOX, Basel II, ISO 27001/17799, DISA STIG, FISMA, NIST 800-53, PIPEDA, Canada's Bill 198 and MITS.

The DbProtect platform offers reports in several types to include PDF, HTML, XML, CSV and text, but does not yet offer customizable technical reports.

Management/Monitoring B

DbProtect can monitor and run vulnerability scans on Microsoft SQL Server 2000 and 2005, Oracle, Sybase ASE and IBM DB2 UDB/MF, and run vulnerability scans for MySQL, Lotus Notes/Domino and Oracle Apps Server. However, AppDetectivePro and AppRadar must be managed through separate interfaces.

Vulnerability scans are created via a central console and saved as scheduled jobs. Vulnerability scanning activities are divided into four overarching groups: discovery scans, pen tests, audits and reports. A typical configuration would allow organizations to schedule discoveries daily and pen tests weekly. Our pen testing identified several HTTP and server-related issues in addition to multiple cross-site scripting and SQL injection bugs.

The intrusion detection components allow you to create a series of attack or alert policies, which can be modified by risk levels for particular signatures, and to include or exclude alerts for individual or groups of signatures. The dashboard displays real-time alerts, color coded by level of risk. Alerts can be sorted, grouped and filtered based on a range of criteria, and, best of all, the refresh rate is customizable, which will help organizations trying to meet SLAs. The alerts can also be integrated into third-party systems such as SIMs or help desk systems via an SNMP output stream or writing to a text log file.

Verdict

DbProtect's combination of real-time monitoring and assessment capabilities is a strong solution for critical applications that face compliance and security risks.

DATA DISCOVERY

DD300

REVIEWED BY GREGG BRAUNTON

Deepdive Technologies
www.deepdivetech.com
Price: **$18,000**

To protect the important data on your network, you have to be able to identify what information you care about, locate it and report. Deepdive's DD300 appliance helps you manage this daunting task with its powerful search capabilities.

Setup and Discovery B+

The DD300 interface is a modern .NET Win32 application that installs in seconds. Built on proprietary Linux and hardware ASICs, the DD300 plugs passively into any network and readily accepts a DHCP address. Configuration walks you through all initial network settings. It can be up and running in minutes.

You can do network discovery or specify known targets. The DD300 will report all network file shares advertised on any host. Discovery is benign, using a standard RPC call requesting available shares. It's also quick, but enumerating the shares on the hosts does take time.

We conducted our test discovery on a local subnet using the range of IP address option. The resulting enumeration of the shares is displayed in the familiar tree layout.

Indexing B+

Indexing is as easy as discovery and is accomplished in a single pass—simply check the hosts you want. You can select single or multiple hosts, even specific folders and subfolders.

At selection time, the DD300 will prompt you to mount the shares. There's some waiting if you are mounting dozens of shares.

The indexing configuration wizard takes you logically through a comprehensive sanity check to ensure you index only content you are interested in. To speed indexing, common .dll, binary and system files are excluded by default.

Testing methodology: We set up test file servers and workstations with data files across dozens of shares.

Searching A

The DD300 search capabilities are so robust and dynamic you'd be hard-pressed to come up with any form of structured or unstructured data that can't be found. You want SSNs? DOB? Address, state, ZIP formats? Need to search .pst files for emails with certain content or keywords? No problem.

The query can be enhanced by enabling different search features. Stemming recognizes an equivalence between multiple grammatical forms, such as "library" and "libraries." Phonics, synonyms and "fuzzy" searching features find close matches.

The results show number of query hits, file name and type, network path, date created and date last modified.

In testing, our SSN search resulted in dozens of file matches in Excel spreadsheets, PDFs, and a PowerPoint file with an embedded chart.

One disappointment: We'd like to see NTFS file permissions as opposed to the document metadata because most documents are blank or inaccurate. This would help identify that data owner(s) for reporting or investigative purposes.

Reporting C+

Reporting is not a strong point, although Deepdive has made some strides in providing a basic reporting function that's quick, easy and an effective communication tool for use with management.

The source information for reporting is taken directly from the column fields selected when viewing the results (number of query hits, file name and type, network path, etc.). So, you may need to revisit the columns you selected on the results view so the pertinent information you want is available to report on.

Reports can be exported to Excel or PDF, but the files are awkward and not succinctly formatted.

Verdict

From discovery to indexing to searching and reporting, the DD300 is a versatile, intuitive and feature-rich data discovery device.

For an extended online version of this review, see this month's issue on SearchSecurity.com.

DATABASE SECURITY

SecureSphere Database Gateway

REVIEWED BY JAMES C. FOSTER

Imperva

www.imperva.com

Price: **Starts at $35,000**

Imperva's SecureSphere Database Security Gateway offers a unique combination of automated monitoring and proactive auditing for protecting your databases. Its configuration flexibility, a product strong point, allows you to protect against insider abuse, external attacks and comply with regulatory requirements.

SecureSphere includes more than 350 security tests to identify security issues such as unpatched database software, default user accounts, and vulnerable database objects and configuration issues to mention a few.

Installation/Configuration A

SecureSphere can be implemented in either passive offline mode, or inline via transparent bridging. An additional Management Gateway is available to help manage multiple appliances. Inline, it can protect databases from attacks and unauthorized access via a comprehensive suite of signatures and analysis techniques.

Physically installing a single appliance is straightforward. Passive mode only requires configuration of a mirror port on a network switch. Inline mode requires no changes other than plugging in Ethernet cables.

No database administration or engineering experience is required during the installation; all you need is an IP address and the database type (Oracle, Microsoft SQL Server, DB2, Sybase and Informix are supported).

One of the most impressive features is Imperva's Dynamic Profiling technology, which discovers database structure, users, executed SQL queries and stored procedures. With minimal additional human logic, the appliance creates an activity baseline, which is leveraged to determine anomalous behavior.

Testing methodology: We tested a SecureSphere Database Security Gateway G4 appliance in a lab that contained Microsoft SQL Server 2005 on Windows Server 2003, Oracle 9i on Windows 2000 Server, and Oracle 10g on Sun Solaris 8 and 9.

Management /Monitoring B+

The optional MX Management Server allows you to manage multiple appliances, create centralized reporting and log events from a single location. The hierarchical, object-based policy structure enables enterprises and ASPs to manage and audit hundreds to thousands of databases. SecureSphere can integrate its logs via SNMP, syslog, email or direct database access for consumption and correlation by SIEMs, ticketing systems or enterprise tools like HP OpenView.

A real-time dashboard provides system status and tactical information on security events. We were able to monitor attacks and access being blocked in real time via policies we created. For example, we stated that users could not log in to the database from external IPs that were not part of the VPN Group. The email alert followed with a "block" action worked as advertised.

Vulnerability Assessment B+

SecureSphere offers passive and active vulnerability assessment technologies. Active assessments require database credentials to retrieve information from the target database: configuration errors, unsafe practices, OS versions, appropriate user privilege levels, etc.

Our testing revealed platform configuration issues such as default installation accounts and weak password policy settings as opposed to software vulnerabilities.

Passive assessments analyze captured traffic to understand how the database is being utilized. It can identify issues such as account sharing.

Reporting B

SecureSphere ships with a variety of canned reports that provide summary information, trends or technical details. Additional compliance and application reports for SOX, PCI, HIPAA, SAP and Oracle E-Business are also included. You can also create new views or reports and quickly search the stored data. This is useful if you're trying to track the use of a particular source or user.

Verdict

SecureSphere is an impressive enterprise-ready product for large organizations. ›

DATABASE SECURITY

Hedgehog Enterprise 2.2

REVIEWED BY JAMES C. FOSTER

Sentrigo

www.sentrigo.com

Price: **$2,400 per database server CPU**

Eight years after the release of Microsoft SQL 2000, we're still looking for help from bolt-on security product vendors to harden and protect critical production database servers. Sentrigo's Hedgehog Enterprise 2.2 is designed to monitor and protect against known and unknown database threats.

Installation/Configuration A

The Hedgehog installation was quick and painless. It took approximately 30 minutes to get the basics of a single instance up and running. This included the server, used for centralized management and reporting, and one sensor running on SQL Server 2005.

Agents provide functionality that network-only-based solutions lack. For example, they can monitor and protect against local attacks and malicious use. They also can access server memory for payload inspection; network appliances typically go inline and protect outside the box. You have to deploy agents manually or with a third-party product.

Management/Monitoring B

Hedgehog has a robust yet intuitive Web-based user interface that enables security administrators and engineers to protect databases in a matter of hours. It leverages role-based access permissions at the user and group level.

Testing methodology: We tested Sentrigo Hedgehog Enterprise 2.2 on a Windows 2003 Server in a lab environment with the product monitoring databases for both active threats and user activity for Microsoft SQL Server 2005.

Within the interface, you can assign permissions by roles. The users assigned to a role then inherit those permissions. There are more than 30 types of granular permissions.

LDAP integration is included by default, to enable you to tie into Microsoft authentication.

Rule creation is about as good as it gets. Provided you understand databases and SQL statements, a four-minute Flash demonstration gives you all the information you need. You can create simple rules to trigger alerts against attacks or suspicious users. In addition, you can create a custom query that is executed on a target database when an associated rule is matched. For instance, if a user is found violating a policy, then you could automatically revoke that user's permissions to a protected database. Other valuable options include terminating that user's session or quarantining him.

Hedgehog comes packed with virtual patching capability, allowing you to prevent known database attacks through a series of identification rules and prevention triggers.

Hedgehog can use a number of output interfaces, such as email, syslog, Windows log file, CSV, Hedgehog internal log file format, and/or its two-way SNMP or XML API engines. These facilities give you a mechanism for collecting or integrating alerts and logs into a SOC, SIEM or log management product.

Three compliance wizards come bundled with 2.2: PCI, SAS 70 and SOX, which walk you through a series of configuration options to meet requirements.

Hedgehog supports Microsoft SQL Server 2000, 2005 and Oracle 8.1.7 or later.

Reporting B

Basic monitoring can be done through built-in dashboards, which have alert filter shortcuts to swiftly check the last 10 minutes, hour, day, week and month.

While the alerts should be monitored in near real time via the dashboards or a third-party product such as ArcSight or HP OpenView, executive and incident reports also add value. Canned reports come in PDF and HTML. Hedgehog's custom report engine allows you to slice and dice any of the data.

Verdict

You cannot buy a better database security solution for the money. Sentrigo's Hedgehog security suite installs quickly and can be leveraged for monitoring real-time external threats and malicious internal user activity.›

DATA SECURITY

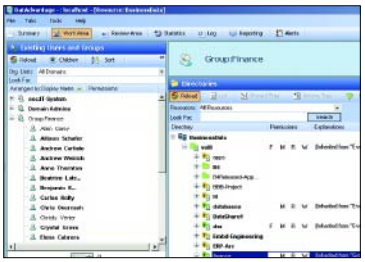
Varonis DatAdvantage

REVIEWED BY BRAD CAUSEY

Varonis

www.varonis.com

Price: **$22,000 for up to 250 Active Directory users**



Dealing with the growing challenge of unstructured data and its governance has been a struggle since the earliest use of file servers. Described as a large set of unorganized files and information, unstructured data presents a large security risk to companies of all sizes. Varonis DatAdvantage addresses this universal problem, giving IT departments the ability analyze, manage and secure all forms of unstructured data.

Configuration/Management B

Setup was fast and straightforward. All of the components can run from a single server, and for most environments, that will suffice. The analytics server requires IIS and MS SQL 2000.

DatAdvantage sends software "probes" to enumerate data that will be returned to the analytics engine. The analytics server is responsible for compiling information from Active Directory (AD) and the file systems. It correlates file system objects, access control lists (file system permissions), and the users or groups. This information is stored in the database and displayed in the management tool.

DatAdvantage analyzes file systems and their ACLs, collects information on data usage patterns and tracks the integrity of each file system object. Although it is modeled with an Outlook 2003 look and feel, working inside of the management software can get pretty tricky, especially when chasing very specific data. You can hide certain panes within the interface, allowing a cleaner look and feel.

Testing methodology: Our lab included a single Active Directory domain with users and groups for access assignment. The volume on the file server used for testing contained live data from a production environment.

Policy Control A

DatAdvantage has the unique ability to make recommendations on changes to permissions based on usage patterns and group memberships. Thus, you'll want to run it first in evaluation mode, so it can record how data is being accessed across each file system.

We were able to see what users or groups probably don't need access to specific resources. You can test changes in a sandbox to evaluate their impact.

Varonis mitigates the thorny issue of tracking and auditing changes made via multiple interfaces through product history, change monitoring and history timelines. Product history allows you to review changes and commands issued within DatAdvantage. Change monitoring tracks file system events and constantly checks and rechecks permissions.

Effectiveness B

DatAdvantage solves a number of challenges to managing standing file system objects, including the ability to determine data ownership based on access frequency. Identifying what data belongs to who is otherwise nearly impossible if the ACLs don't directly indicate it. Because DatAdvantage goes beyond the ACL, it can also perform usage auditing, allowing you to detect anomalies as users break their normal access patterns.

Arguably the most important tool is data integrity monitoring, watching for actions such as the deletion or modification of files and folders. You can use the detailed logging to find specific activities.

Reporting B

There are a number of canned reports offering a wide range of research and summary styles of information. They can be customized based on a number of criteria, though we'd like to see the ability to build reports from scratch. Reports can either be run as ad hoc query or scheduled to be run in the future. There are no compliance-specific (SOX, PCI-DSS, GLBA, HIPAA, etc.) reports, which we would like to see in a product of this type.

Verdict

There aren't very many players in this market space, and DatAdvantage is definitely a top contender, with its ability to deeply analyze file systems and access patterns to make recommendations on changes. ›

ENDPOINT SECURITY

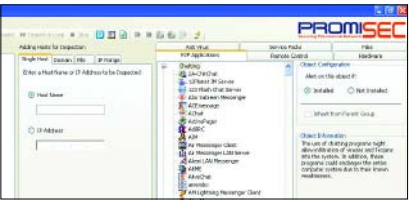
Spectator

REVIEWED BY MIKE CHAPPLE

Promisec

www.promisec.com

Price: **Starts at $20,000 for 500 clients**



The endpoint security market is flooded with solutions ranging from costly appliances to distributed software agents. Promisec's Spectator offers a nice compromise, providing a flexible, centrally managed tool that uses a combination of remote registry access and remote procedure calls to collect data and perform administrative actions.

Policy Control A

Spectator allows you to inspect host systems for an impressive variety of items. You can check hardware settings, checking, for example, whether the system has a modem, multiple NICs, removable media or synchronization software indicative of a portable hardware device. Spectator also checks compliance with security polices by verifying the presence of antivirus software from 18 manufacturers and the Microsoft service packs.

Spectator's real strength lies in monthly database updates of P2P and remote control applications signatures. At the time of our review, Spectator was able to detect 342 P2P file sharing and 455 IM applications, and 146 remote control packages. The management interface allows you to scroll through applications and choose those whose presence or absence you would like Spectator to alert on based on the application (AIM, PC Anywhere, etc.) or category (P2P, remote control).

Spectator allows you to create user-defined policies based upon specific Microsoft hotfixes, applications, registry entries, file names/types and processes/services.

Configuration/Management B

We ran into a few glitches configuring our first client, as we had to reconfigure the security settings on the client operating system to allow inbound file sharing access and remote registry access from the Promisec server. Promisec's technical support group resolved the issues.

Spectator offers a number of options for selecting hosts to scan. In addition to specifying hosts by name or IP address, you may import a list of hosts from a text file, specify a network range or select Active Directory OUs.

The Spectator console provides a dashboard-style view of scan results, including client name, last logged-on user and policy violation(s). Administrators may remediate violations by clicking on the vulnerability.

Effectiveness B

We intentionally created several policy violations on managed systems. We installed software that conflicted with our "alert on presence" policy, opened unauthorized file shares and installed software that was not included in our authorized baseline. Spectator identified every violation.

When we tested its ability to perform remote remediation of policy violations, Spectator closed file shares on managed endpoints. However, it failed to uninstall one of three software packages that weren't included in our established application baseline.

Spectator offers several remediation options: Force the automatic uninstall of software, enable alert notifications and start antivirus software that is not running. In addition, Spectator integrates with Check Point FireWall-1 to automatically block noncompliant systems, and Tivoli Monitoring Server, which provides monitoring reports.

Reporting B-

Spectator can create an HTML executive summary report that includes scan statistics, details on problematic hosts and policy objects and a summary. You can also export data to comma-delimited text files, filter report results and create differential reports.

You cannot, however, create customized reports within Spectator; you'll need to export to third-party software for that.

Verdict

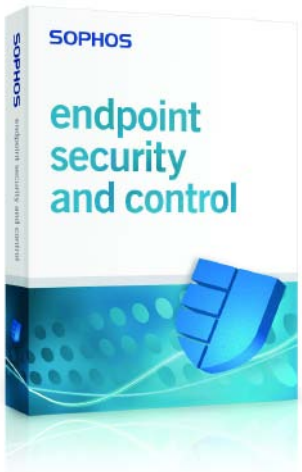
Spectator is a solid product for monitoring endpoint policy compliance, especially for organizations that do not wish to incur the overhead of installing, maintaining and running endpoint agents.›

Testing methodology: We tested Spectator in a Windows XP environment running under VMware Workstation..

ENDPOINT SECURITY

Sophos Endpoint Security and Control 8.0

REVIEWED BY SANDRA KAY MILLER



Sophos

www.sophos.com

Price: **Starts at $43 per user annually**

Sophos Endpoint Security and Control can easily replace a number of individual security products aimed at endpoint protection. In addition to antivirus, it delivers antispyware, HIPS, firewall, application and device control, and network access control (NAC) under centralized management.

Installation/Configuration B

Installation of the enterprise console and NAC server is straightforward. The console dashboard offers comprehensive access to managed computers, updates, alerts, policies, protection and errors.

However, we encountered several irritations trying to install the client software directly from the console, requiring us to resort to hands-on installation. For example, you need administrative rights on a PC and have to uninstall previous versions on older Windows machines. There's plenty of documentation to get past these issues, but they create a lot of extra work.

Policy A

The policy tree provides instant access for all functions. We set granular polices for different operating systems and Windows versions. Under AV and HIPS, we quickly set up detailed scanning options and exclusions specific to each platform. The Cleanup tab let us assign specific actions to known viruses and spyware, and suspicious files. Sophos provides an extensive list of application types that allowed us to move commonly known applications from being authorized to blocked.

There are also options to limit the use of devices such as CD/DVDs, floppies and removable USB drives.

Host firewall policies were standard fare, including rules for blocking and allowing different types of protocols, applications and processes.

NAC provides separate policies for managed and unmanaged computers.

Logging and Reporting C

With few options for customization, this was the weakest aspect of the product. Event logs and alerts are set up individually for each component, but while they are excellent for AV and HIPS, they're weak for application control and firewall.

Under AV and HIPS, we set up alerting for multiple events, including virus/spyware detection and cleanup, suspicious behavior, suspicious files, adware and PUAs (potentially unwanted applications). The application control and firewall lack specific event notification and had weak logging. Reporting is limited to generic reports generated through drop-down menus and radio buttons. There were no options for automated reports or having them disseminated via email.

Effectiveness A

Sophos has long been a leader in the antimalware space, with superior scanning engines and a research division that stays on top of emerging threats.

We were particularly pleased with the way Sophos goes beyond traditional signatures and basic heuristics to identify unidentified malware and unwanted files, code and behaviors. Suspicious file detection examines characteristics such as how the file was packed, whether it's making any calls to specific HTTP sites, and if there are embedded URLs in the code

Sophos passed all of our security tests, thwarting malware, spyware, exploits, intrusion attempts and the installation of unauthorized applications and devices.

Verdict

Sophos Endpoint Security and Control effectively covers all the bases for security on endpoint devices.

For an extended online version of this review, see this month's issue on SearchSecurity.com.

Testing methodology: We installed the enterprise console and NAC server on a Windows Server 2003 machine and tested with a variety of client endpoints, including multiple versions of Windows, Mac OS and Linux using a variety of active malicious code and adware/spyware.

ENDPOINT SECURITY

Trend Micro Worry-Free Business Security 5.0

REVIEWED BY SANDRA KAY MILLER

Worry-Free Business Security 5.0

www.trendmicro.com

Price: **Starts at $59.32 per user (one-year license for 51-250 seats)**

Trend Micro Worry-Free Business Security (WFBS) delivers comprehensive client/server protection for small businesses against a variety of Web threats for Microsoft Windows 2000/XP/Vista, Small Business Server 2003/2008 and Exchange Server.

Installation/Configuration A-

WFBS was a snap to install, configure and administer, stepping us through the configuration for the Security Server and agents to be deployed on client machines.

Compared to enterprise-class security applications, WFBS didn't require extensive network setting inputs.

The client/server security and remote messaging agents were created equally fast and simply. Client agents can be installed remotely via login scripts or downloaded from an internal or secured website.

The Vulnerability Scanner can scan the network and automatically deploy agents to unprotected systems.

We logged in to the Web Console through a browser connection. An SSL connection to the Security Server is optional, which we thought introduced unnecessary risk.

The Web Console was just about the most uncluttered security product interface we have ever encountered—eight menus are instantly accessible with a single mouse-click.

Testing methodology: We tested Worry-Free Business Security on Windows Small Business and Exchange servers connected to a variety of Microsoft Windows endpoints, including desktops and wireless laptops.

Policy B

Policy creation is straightforward. Policies include the usual choices found in antivirus/antispyware, firewall and behavior monitoring applications. There are also settings to secure wireless connections and client privileges. The default scanning policies provide real-time scanning for incoming and outgoing traffic, automatic cleaning for infected files and deletion for malicious code that cannot be otherwise disabled.

Logging and Reporting B+

WFBS can automatically generate a variety of useful reports aimed at IT and management. For instance, we were able to provide statistical analysis of security events for a security administrator as well as content filtering reports, informing managers which employees attempted to visit prohibited websites or send/receive inappropriate email.

The Outbreak Defense menu logged detailed information regarding infections and cleanups. Potential vulnerabilities based upon known threats were also identified. To quickly find a specific event or type of events, WFBS includes a Log Query screen that allows results to be exported to a CSV or text file.

Effectiveness A-

WFBS can be effectively handled by an administrator or small IT department.

The Live Status menu let us view the health of our environment through color-coded buttons for specific threats as well as clients requiring updated agents.

WFBS effectively scanned and protected all of our servers and client machines from a multitude of common threats, including viruses, spyware/adware, spam, infected URLs, phishing and malicious Java and ActiveX applets.

Using only the default settings, WFBS provided adequate security for messaging. The only problems we encountered were with large and compressed files that appeared to hang up the system.

We found the Web Repudiation feature that scans Web pages for malicious code prior to being displayed particularly useful in preventative network and system health.

WFBS also includes a basic firewall, which is adequate for use with mobile laptops.

Verdict

WFBS is an easy and affordable way for smaller organizations to cover all security bases.›

ANTIMALWARE

Webroot Antispyware Corporate Edition with AntiVirus

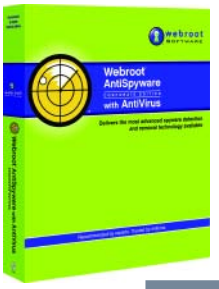
HotPick INFORMATION SECURITY®

REVIEWED BY SANDRA KAY MILLER

Webroot

www.webroot.com

Price: **Starts at $28.26 per seat**



Recognizing the growing challenge of managing multiple point solutions to combat the convergence of spyware and malware, Webroot has integrated the Sophos antivirus engine with the centrally managed version of its spyware product to produce Webroot AntiSpyware Corporate Edition with AntiVirus to provide continuous protection from online threats.

Configuration/Management A

We were impressed with the interface, which makes it easy to find regularly used settings and information.

Installation was straightforward, requiring installation of a MS SQL Server database prior to the Webroot Server. Clients can be installed on endpoints through the administration console, an MSI file for third-party delivery, log-on script or Active Directory Group Policies.

The intuitively designed administration console provides easy access to the excellent status dashboard, offering quick displays on top threats and infections, client administration and system settings for enabling Smart Shields on clients, Sweeps (scans), detection options (quarantine, delete), notification (alerts, errors and updates via email), updates and reports.

Updates, Sweeps and polling can be set up to run at different times among client groups to reduce impact on the network.

Testing methodology: Webroot AntiSpyware Corporate Edition with AntiVirus was deployed in a Microsoft-based environment with a variety of Microsoft endpoint operating systems (Vista, XP, 2000) on the network, including remote machines to simulate mobile users.

Policy Control A

Webroot offers granular controls—globally or by group—for more than a dozen types of Smart Shields that address common threats and vulnerable areas including memory, Internet communication, Windows Messenger Service, alternative data streams and ActiveX.

We set up white lists for commonly flagged items such as legitimate ActiveX controls, rootkit applications, browser toolbars and startup applications.

We were able to assign what was scanned and how often. We could also control how much a memory or file scan could affect CPU usage. This is very useful for slower, older machines.

Reaction options include simple logging, quarantining then deleting after two, seven, 30 or 365 days, or deleting right away. Spyware is broken down into five categories (adware, cookies, system monitors, Trojans and informational), each with policy options.

Reporting A

Webroot's reporting has taken leaps forward—granular, flexible and customizable. It weighs threats to create risk assessment scores for individual systems. For instance, viruses, Trojans and monitoring code such as keyloggers are assigned a higher value than adware and tracking cookies. Administrators can quickly see which workstations are infected with malicious code.

Webroot's extensive array of report templates includes threat blocking, quarantining and cleaning, and trends; you can customize information based on workstation, groups and type of threat.

Effectiveness B

Corporate Edition offers comprehensive protection. We launched multiple infections initiated through a variety of vectors using commonly encountered spyware and malware, including keyloggers, rootkits, Trojans, backdoors, worms, hijackers and adware.

Behavioral analysis is off by default to improve speed. Without this feature, Webroot failed to detect approximately 20 percent of the threats, especially polymorphic spyware, adware and rootkits. Once it was enabled, detection rose to nearly 100 percent.

Verdict

Webroot AntiSpyware Corporate Edition with AntiVirus is a comprehensive antimalware defense.

FIREWALL MANAGEMENT

AlgoSec Firewall Analyzer 4.0

REVIEWED BY BRAD CAUSEY

AlgoSec

www.algosec.com

Price: **Corporate license starts at $4,300, auditor license at $1,400**

Managing firewalls across an enterprise becomes increasingly difficult as organizations grow. Between the increase in use of distributed applications and needs for Internet connectivity, firewall rules can become complex and confusing, ultimately leading to misconfigurations and security holes.

AlgoSec's Firewall Analyzer (AFA) simplifies all aspects of firewall management, allowing you to discover and correlate redundant and conflicting ACL entries in routers and firewalls across the enterprise. Change management and regular audits are simplified tenfold, without modifying or interrupting production devices.

Configuration/Management B-

Installation is simple. We downloaded an installation file from the customer login page along with instructions and prerequisite information.

AFA can be installed on Red Hat Enterprise Linux and OpenSUSE, but not Windows. Before installation, you must create a dedicated user account and install JRE. Apache is automatically configured with SSL.

The only real issue we have with AFA management is that its dual interfaces force admins to go back and forth between them, which can be cumbersome. The local Linux interface provides user management, configuration options and overall management of the software. The Web-based interface is used more for day-to-day operations and reporting.

Testing methodology: Our lab included a single OpenSUSE 10.1 server with the AFA software installed. A number of sample configurations were used from various sources such as Cisco and Check Point firewalls. Configurations were analyzed individually and in groups to determine aggregate accuracy.

Effectiveness A

AFA's main role is to audit and evaluate firewall policies and configurations in the form of offline or exported configuration files, providing a complete audit without impacting the firewalls. You can import these configuration files directly through firewalls, the management interface or manually, by copying the configuration file. AFA supports Check Point Software Technologies, Cisco Systems and Juniper's Netscreen firewalls, as well as Cisco routers.

The audit engine is remarkable, using mathematical algorithms that calculate every possible packet that could traverse the firewall. This technique covers all external IP addresses, internal IP addresses, ports and protocols. All possible combinations are tested in every direction and on any interface.

Audits produce reports that contain data such as how a given rule or set of rules creates a risk. These risks are then rated, and can be investigated by drilling down to gain an in-depth understanding and suggested remediation. In our testing, for example, AFA detected a combination of rules that allowed UDP port 137 (NetBIOS) between our DMZ and internal network, and a recent change in a TFTP rule that opened the DMZ to inbound and outbound connections.

Reporting A

Reporting is mature and flexible. The executive summary report provides a high-level view of the firewall(s) with findings listed by risk level. This is excellent for aggregating rules on multiple firewalls to determine collective risk. You can also see reports that detail each rule and why it creates a specific risk. The rules and layout are presented in the native firewall format, making interpretation easy.

The change history report simplifies change management, providing an ongoing view of all changes, mitigated risks and new risks. The compliance report gives a top-down view of firewalls analyzed as they apply to a given need.

Verdict

AFA will greatly simplify firewall troubleshooting, management and compliance.›

FIREWALL

Netgear FVS336G ProSafe Dual WAN Gigabit Firewall

REVIEWED BY JOEL SNYDER

Netgear
www.netgear.com
Price: **$425**

The latest ProSafe series firewall brings together nearly everything Netgear offers in the security space, including firewall, IPsec and SSL VPN, neatly packaged into a small-office friendly device, with no fan and an internal power supply. For deployments needing a minimum of security rules, the FVS336G offers broad features at an attractive price.

Ease of Use A-

Netgear's ProSafe user interface has been honed from years of development in more than a dozen products, making basic setup and configuration of the FVS336G very easy. Our starting configuration took less than 10 minutes, and almost everything we tried was easy to understand and quick to do. For example, we wanted to test the dual-WAN capability of the FVS336G; Netgear provides two ways of using two WAN interfaces, load balancing and failover. Each option worked fine, and the user interface was intuitive.

We also had a good user experience in testing the SSL VPN client (up to 10 simultaneous users are supported). Windows and Mac users were able to connect, log in and deploy the client software without reading the manual or encountering confusing buttons. We also had no problems building a site-to-site VPN (up to 25 tunnels are supported), thanks to the VPN wizard and good default settings.

Testing methodology: We evaluated the FVS336G by connecting it directly to the Internet and placing test systems on the inside interface. We then tried to implement three different security policies for firewall and SSL VPN.

Security Features C

The FVS336G is not for the network manager who wants a fine-grained security policy. Although there are some features, such as time-of-day policies, the FVS336G is for the network manager who wants to allow all traffic out, block inbound traffic and be done with security configuration. This is true on both the firewall and VPN sides of the product. As a two-zone firewall (inside and outside), the policy set is simple, which should meet the needs of most small offices.

We found the logging to be poorly thought out and implemented. Log messages either overwhelmed with trivia or failed to capture the information needed to audit traffic. Policies such as NAT are global to the entire firewall—it's either on or off, making anything but the most basic deployments problematic.

The SSL VPN was a particular disappointment. With a default "permit all" policy that can't be changed, we found that trying to control access once someone logs in over the SSL VPN is impossible. Moreover, when we tried to put in an SSL VPN policy that didn't simply grant broad access, we ran into bugs in the way policies are evaluated, giving less security than the policy indicated. We also found bugs in enabling remote management, but fortunately the error was in the direction of greater security—remote management could not be enabled.

The FVS336G is not a UTM firewall, but it has limited UTM features, including content filtering by keyword and domain, as well as blocking of ActiveX and Java controls.

Performance B+

Our performance testing showed the FVS336G with a throughput of about 37 Mbps, less than Netgear's advertised rate of 60 Mbps, but still plenty fast even in dual-WAN deployments using DSL or cable modem connections. Netgear advertises slightly lower performance for IPsec (16 Mbps) and SSL VPN (10 Mbps) traffic.

Verdict

Although the FVS336G is not a gigabit performer, the street price of $265 to $300 (the list price is $425), along with a lifetime warranty and free software updates, make this a good and economical choice for the small business with modest security needs, including easy-to-use SSL VPN remote access.

NETWORK FIREWALL

PA-4050

REVIEWED BY PHORAM MEHTA

Palo Alto Networks

www.paloaltonetworks.com

Price: **$60,000**

Unlike traditional firewalls that identify applications only by protocol and port number, Palo Alto Networks' next-generation PA-4050 uses packet inspection and a library of application signatures to distinguish between applications that use the same protocols and ports, and to identify potentially malicious apps that use nonstandard ports.

Installation/Setup B+

Although the PA-4050 offers a command-line interface, the Web GUI is much simpler, at least for the initial setup. The appliance can be run in three modes: virtual wire, Layer 2 or Layer 3.

Virtual wire, best known as transparent mode or inline mode, is the default configuration and does not require many changes. In Layer 2 mode, the appliance, which is equipped with 24 interfaces—16 10/100/1000 and eight SFP ports—can act as a firewall and address switching needs. This is useful for networks divided into multiple VLANs, each with their own security requirements. Layer 3 is most like the traditional firewalls that operate on the network layer.

Controls A

The policy rule interface has a very familiar look with a couple of extra parameters. In addition to the typical source/destination zone/IP/service fields, administrators can also set application rules as an added control, such as P2P, IM and multimedia apps that use dynamically assigned ports or well-known ports such as port 80 or 443.

Additional options provide real-time threat prevention with add-on components such as antivirus, antispyware, vulnerability protection, URL filtering and file blocking profiles. User/group-based firewall rules can be customized through Active Directory integration. Maintaining a 5 Gbps throughput with all options running sets the PA-4050 apart from other firewalls.

Testing methodology: We tested the PA-4050 by using well-known and custom P2P and IM applications to send and receive traffic through the firewall along with attacks, suspicious URLs and worm downloads.

Effectiveness B+

The App-ID accurately identifies applications, irrespective of the ports used. This enables enterprises to address security evasion tactics such as the use of nonstandard ports, dynamically changing ports and protocols, emulating other applications, and tunneling to bypass existing firewalls.

The PA-4050, which can decrypt SSL traffic without revealing data content, identifies the protocol structure and the overall traffic pattern to flag anomalies. The signature engine identifies the exact application based on more than 450 definitions, with occasional updates downloaded manually.

Administration/Monitoring B

The customizable dashboard displays general device information and up to 10 of the most recent entries in the threat, configuration and system logs. Real-time on-box logging, in addition to the graphs, can be filtered on 17 different fields, including source/destination, user/group, application and usage. In addition to tracking user and traffic activities, the log viewer provides visibility into administrative changes to the firewall. Traffic logs can be sent remotely to a syslog server or as email notifications.

The application command center provides a detailed multilayer graphical representation of the application activity at any given time.

Also, about 25 predefined reports provide a good summary of all the major activities, threats and traffic patterns. Reports cannot be exported to PDF, XML or any other format.

PA-4050 supports high-availability configuration, and Palo Alto's central management system, Panorama, can be used to manage multiple devices.

Verdict

Palo Alto's application-centric approach, add-on threat prevention components and real-time graphical reports make the PA-4050 a coveted security solution for organizations requiring high firewall throughput, while consolidating security devices.

FIREWALL

SonicWALL NSA E5500

REVIEWED BY JOEL SNYDER

SonicWALL

www.sonicwall.com

Price: **$9,995**

SonicWALL's new E-class firewall appliance, the NSA E5500, packs a much-needed performance jump to the unified threat management (UTM) firewall. (The E6500 and E7500, faster systems running the same software, are also available.)

Basic Firewall Features B+

As a firewall, the NSA E5500 sat up and paid attention in class. It uses a zone-based firewall as a base, with different interfaces bound to different zones. Although you can't skip the zones and go pure IP firewall (one of the few gaps), the firewall is intuitive and easy to configure.

If the E5500 falls down anywhere it's in the complexity when you start configuring the firewall and turning on all the available features, such as wireless guest services, remote access VPNs and user-based firewall rules. For larger configurations, these rules tend to multiply and obscure the actual security policy.

The firewall also suffers from confusing feature-itis. For example, there's a check box that says "Enable support for Windows Messenger," but you don't get enough information to decide whether checking that box is a good idea.

Advanced Firewall Features A-

The NSA E5500 has a variety of optional features, including Web content filtering, gateway antivirus, signature-based intrusion prevention, and malware detection and blocking.

The E-class appliances feature the CPU power of the multicore Cavium Networks Octeon to handle UTM performance hogs such as antivirus.

Testing methodology: We installed the NSA E5500 in our production network, putting a subset of users behind it and testing each of the UTM and application layer firewall features. We also integrated the NSA E5500 with two SonicWALL SonicPoint 802.11a/b/g access points.

The UTM feature list is relatively standard, but the implementation is full-featured. For example, you can select from three content filtering engines—SonicWALL's own, Websense, and third-party RBL services, such as Spamhaus for spam filtering.

Another plus is stream-based antivirus scanning, providing coverage across all data streams, including P2P and IM.

All UTM features (except for content filtering) are enabled on a per-zone basis, with a single policy in each area applying to an entire zone, which doesn't provide much granularity.

SonicWALL has added an application firewall to apply extra application layer controls to Web browsing, file transfer and email streams. Once traffic matches one of the application firewall objects, the network manager can apply any of a number of actions, such as blocking the SMTP or FTP traffic or redirecting a Web browser to a different page.

The application firewall is still a toolkit. It needs fine tuning, bug fixes and additional functionality.

VPN B-

The NSA E5500 has basic site-to-site and remote access VPN features. However, although SonicWALL has bought two SSL VPN companies, it hasn't integrated any SSL VPN into its firewall appliances.

Network managers developing multisite VPN configurations will want to skip the Web-based GUI, which lacks the tools and coordinated policy for such deployments. SonicWALL's separate Global Management System makes the task of taking care of site-to-site VPNs much simpler.

Wireless A

The NSA E5500 does not have embedded wireless adapters, but it can be linked to SonicWALL's SonicPoints 802.11a/b/g thin access points. The appliance provides a fast, cost-effective way to securely add high-end wireless capabilities, along with some wireless intrusion detection and RF management features.

Verdict

The NSA E5500 is a leap forward in firewall and UTM performance for SonicWALL. The solid basic firewall and advanced UTM feature set provide the coverage and features midsized organizations need. Enterprise managers will find the application layer firewall and VPN features useful, with room for improvement.

FIREWALL MANAGEMENT

Tufin SecureTrack 4.1

REVIEWED BY BRAD CAUSEY

Tufin Technologies

www.tufin.com

Price: **Starts at $10,000 for base appliance and software**

Enterprise firewall management is a headache. An ever-growing labyrinth of access control lists, complex change management over geographically distributed organizations, plus audit and compliance requirements make it tough to bring under control. SecureTrack 4.1, a comprehensive firewall operations management solution, helps cut the job down to size, especially for Check Point Software Technologies firewalls.

Configuration/Management B-

SecureTrack is available as a software package or an appliance. For our evaluation, we utilized the software version that runs on either CentOS version 4 or Red Hat version 4.

The Web-based GUI is intuitive, and where possible, the rules interface strives to give the look and feel of each type of firewall. For example, it mimics the Check Point interface when viewing and managing firewalls from a SmartCenter NG system, which is nice, but we'd like the ability to switch to a standardized view of rules across all platforms.

You can use SecureTrack to manage Check Point, Cisco PIX and Juniper firewalls, but, in the current version, most of the key features are limited or nonexistent for the latter two.

A straightforward wizard is used to add a firewall to the system. SecureTrack passively pulls down the configuration and status of each firewall. You can view the rules and policy information side-by-side, so reviewing changes and other pertinent information is easy.

Testing methodology: Our lab included a single instance of SecureTrack on Red Hat, two Check Point firewalls and one Cisco firewall. Rules were imported from production environments.

Policy Control B

Although you can view firewall policies within SecureTrack, you have to use the respective Check Point, Cisco and Juniper native firewall interfaces to make changes or update configurations. We'd like to see a tool that can analyze and actively manage multiple types of firewalls for heterogeneous environments.

You'll spend most of your time in the Compare and Analysis interfaces. The Compare view allows you to see current rules, objects and global properties, offering a side-by-side comparison of current and previous versions. This is also where you can browse and drill down into firewall objects and properties, including any changes made. The revisions component is useful and allows you to view changes incrementally.

The Analyze tab allows you to make simple and effective queries, providing quick insight into any rule set. When you use the comparison and analysis tabs together, you can find conflicting and high-risk rules. Overlapping rules or gaps in rule sets between firewalls can lead to an unpredictable or insecure configuration. This risk assessment capability goes a long way toward helping you mitigate these issues.

Reporting B

SecureTrack has a number of features that provide value beyond simple reports, especially the ability to have reports emailed on a set schedule. Reports are fully customizable and include rule usage, rules and policy changes, and even node-specific object changes such as user membership, and OS modifications. Rule usage shows what firewall rules are triggered most, revealing unused or unnecessary rules.

These reports can be filtered by date, firewall, or nearly any other specific criteria. In addition to the canned reports, compliance and regulatory reports can be defined manually with custom policies that identify problem rules.

On the downside, the rule usage feature is currently not available for Cisco and Juniper firewalls.

Verdict

Tufin has done a very good job of creating a centralized management solution, primarily for Check Point firewalls deployed in distributed environments. It should have broader application with enhanced Cisco and Juniper support, planned for the next release.›

IDENTITY MANAGEMENT

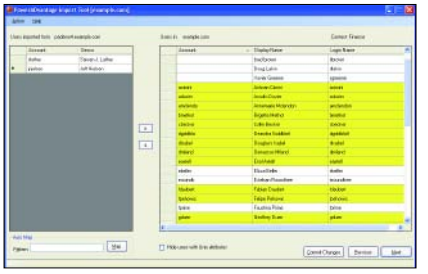
Symark PowerADvantage 1.5

REVIEWED BY PETER GIANNACOPOULOS

Symark

www.symark.com

Price: **$290 per Unix/Linux server, $45 per workstation**



Centralized directory services such as Active Directory are key to identity management initiatives, but one of the stumbling points has been integrating non-Microsoft platforms into the authentication infrastructure. Symark PowerADvantage eases integration of Unix/Linux and AD authentication.

Platform Coverage B+

PowerADvantage allows Unix hosts to become member servers of an AD forest and leverage AD's centralized user management and authentication capabilities.

All major enterprise Unix and Linux platforms are supported. Other Linux platforms such as Fedora are likely to work, provided they have relatively modern Kerberos and LDAP implementations.

Installation/Configuration A

Installation consists of a Windows-based service on the AD domain controllers and an agent with associated libraries on the managed Unix/Linux hosts. The Windows components do not require the schema to be modified, but do create some Symark-specific objects within AD.

Installation is a breeze: a straightforward MSI install on Windows and a tarball under Unix, which includes a text-based install script that walks you through the setup.

Normally, setting up Kerberos/LDAP on Unix hosts can be tricky, since each platform implements the protocols slightly differently with different flavors and locations of configuration files. Symark addresses this, abstracting Keberos/LDAP protocol implementation quirks on many Unix implementations, easing the headaches of configuring protocols on a given platform.

Testing methodology: We installed the PowerADvantage Windows components on a Windows 2003 SP2 domain controller running in Windows 2003 Native Mode, and agents on Unix clients.

Management B

PowerADvantage adds a tab to the standard Properties screen of both AD User and Group objects, which allows access to all the PowerADvantage-specific attributes required to get the users authenticating on the Unix hosts. It can be managed from the Unix or the Windows side.

Our testing focused on managing from AD. PowerADvantage uses the concept of contexts to manage Unix hosts with the same login configurations (username, primary group, home directory and shell). Contexts are mainly used to compartmentalize unique user and group attributes.

Once the contexts are created, admins can add users and groups from AD to the Unix hosts and use them to secure file system data as if they were local user accounts. PowerADvantage gives you the ability to map existing user/group IDs to AD accounts and import existing local Unix accounts to AD.

There are some rough spots, mainly around integrating smoothly with the Active Directory MMC console. For example, we found ourselves jumping back and forth between Symark's management console and the Active Directory Users and Computers MMC.

Unix GPO support is limited to managing various PowerADvantage settings on the hosts that will be authenticating against AD. A successful large-scale integration depends on other related components functioning properly (e.g., Kerberos auth will fail if KDC DNS entries are incorrect or if system time skew is too great), so it would be great to be able to centrally manage DNS and NTP settings on the Unix hosts.

PowerADvantage provides basic reporting that can keep the administrator informed on day-to-day activity.

Verdict

Symark does a great job streamlining a lot of underlying complexity and will get you rapidly standardized on AD. After our testing was completed, Symark was close to a new release that includes improved SSO for Kerberized applications and better GPO support.

For an extended online version of this review, see this month's issue on SearchSecurity.com.

INCIDENT RESPONSE

Mandiant Intelligent Response 1.0

REVIEWED BY PHORAM MEHTA

Mandiant

www.mandiant.com

Price: **$86,500**

Incident response remains a very manual process, rife with inaccuracies and inefficiencies. Mandiant, a trusted name in the incident response services arena, has created Mandiant Intelligent Response (MIR), an appliance that automates most of the time-consuming tasks.

Installation/Configuration B

MIR is an agent-based client/server architecture, with a controller appliance to collect and store information from agents on suspect machines (currently only for Windows; *nix coming soon). The administration console is the primary interface for managing incidents, from collection of evidence to analysis and examination.

Setting up the appliance is not simple, although the documentation is comprehensive and walks through each step. Installation requires creating agent installation sets, including generating and exporting SSL certificates. It also requires making sure that the discovery file used by the agents to find the controller during initial registration has the correct IP address.

Ease-of-Use/Effectiveness B+

IR teams face a stiff challenge collecting critical information such as running processes, network ports, suspected files, and memory and disk images as quickly as possible. MIR automates this process while preserving the integrity of the evidence.

To run a data collection audit you create a new audit script by dragging and dropping the target host(s) from the asset list into the input pane and selecting the audit modules (acquire file, acquire memory or entire disk image, listing of files, process, services, network ports or registry hive) to be executed.

The results viewer pane shows the overall progress of the jobs and the result files as they are being populated. Tabbed browsing makes it easier to open multiple windows for configuring jobs and viewing results.

Depending on the modules selected and the power available, audit jobs can take anywhere from a couple minutes to more than an hour. You can then run one of four analyses: time skew, time line, document difference or document intersection.

Individual records can be labeled with a custom label for future reference without having to search the results again. IR teams will appreciate the ability to add notes that can contain links to search results or entire documents.

MIR features an open format and easy integration with most open source forensic tools. For example, disk and memory images can be exported in standard formats for analysis. Audit and analysis documents are stored in an easily understandable XML schema.

Although MIR 1.0 takes a huge first step toward automating incident response, there are a few usability and operational issues typical of first releases. For example, you have to drag and drop each host for an audit, and there's no warning of inadvertent duplicate host entries before running the audit twice on the same host. Errors and warning messages are believed to be caused by conflicts with certain Microsoft patches.

Reporting B+

MIR stores evidence in the Advanced Forensic Format (AFF), which is considered an acceptable format for chain-of-custody for digital evidence.

The controller indexes audits, case notes and object metadata for fast and accurate searches by the very well-engineered search function, which accepts single words, phrases and regular expressions.

Case notes can be used for note-taking, report writing and linking to stored information, allowing you to quickly reference host audits, analysis results, etc. They can be exported into multiple formats, including XML.

Verdict

Despite a few first-release wrinkles, Mandiant has created a useful tool for large enterprises struggling to address their incident response needs.›

Testing methodology: MIR 1.0 was evaluated in a test lab with a few Windows XP and Windows 2003 machines. The test covered network-based as well as local acquisition modes.

INVESTIGATION MANAGEMENT

V-Flex

HotPick INFORMATION SECURITY®

REVIEWED BY BRAD CAUSEY

Vantos

www.vantos.com

Price: **More than $100,000 for three different product configurations**

Investigations are a considerable challenge. Complexity, evidence management, tracking resources and even data correlation pose serious issues. Vantos V-Flex not only manages an investigation, but nearly completes it.

Configuration/Management A

Setup was almost too easy. Vantos delivered a preconfigured appliance based on information we provided about our network. You can start centralizing the management of your investigations immediately through the intuitive Web interface. To fully realize the benefit of the product, however, you'll need to do some additional work.

This is where having Vantos onsite, at no extra cost, is extremely helpful. One of V-Flex's most useful features is that you can automatically query thousands of different systems across the organization for case-related data, as long as you set them up as a data source. Any system that supports a JDBC connection is able to feed into the V-Flex platform.

There are three types of accounts: administrator, investigation management and various investigator accounts. Individuals cannot have more than one role, though an investigator can be assigned to more than one probe by investigation managers.

Policy Control A

One of the most difficult issues in investigation management is that no two companies have the same policies and procedures. This is where Vantos really hit the jackpot. Using "playbooks," each company can create an investigation lifecycle that is unique for each type of investigation it handles: insider security breach, HR violation, physical intrusion, external hack, and more. This means your investigations will be consistent.

As you follow a particular playbook, each step is completed, each type of evidence is centrally stored, and each report will look the same, no matter who investigates.

When the investigation manager assigns a new case, the analyst is notified and a list is created based on the playbook defined for that type of investigation. The analyst follows each step, delegating or closing them until the investigation is complete. You can create blank investigations or customize playbooks.

Effectiveness A

V-Flex's effectiveness is defined by its combination of unique features. A walkthrough of a simple data loss investigation in our lab will illustrate.

The manager assigns the case, which is pushed to the investigator. The investigator logs in, opens the playbook and begins working. The relevant database sends its logs to a log management system that has been integrated with V-Flex, so the investigator retrieves information via a simple query. The suspect is identified through these logs and integration with LDAP. The suspect's badge access history, phone call logs and CCTV surveillance are retrieved via simple queries to each respective system. Within 45 minutes you know who they are, what data they took, where it went, on what brand of USB flash drive it was stored, and—using V-Flex's correlation and analytics engine—whom they were working with.

Reporting A

V-Flex reporting is everything you would want it to be, with nine canned reports. We found the Evidence Integrity Report especially interesting. You choose a hash, such as SHA1, and the report lists each item in the evidence locker for that case, and its associated hash. This is invaluable for audits or establishing and verifying chain of custody. Unlimited custom reports can be created using XSLT through the Web interface.

Verdict

V-Flex is an outstanding product for an underserved market. Your investigations will be consistent, thorough, centrally managed and less resource-intensive. Vantos has hit this one out of the park.

Testing methodology: Our lab included a mock-up of an enterprise organization. This included a central logging system, VoIP phones, CCTV and a Windows domain with various resources. Sample investigations were used to walk through playbooks and evaluate the product.

Review how we grade at searchsecurity.com/grading_criteria.

IT COMPLIANCE

NetChk Compliance

REVIEWED BY ADAM HOSTETLER

Shavlik Technologies

www.shavlik.com

Price: **Starts at $43.75 per workstation/year**

Regulations and industry mandates are putting increasing pressure on businesses to ensure that all critical systems meet required guidelines. NetChk Compliance helps automate the compliance process, working off a solid baseline of accepted requirements. It provides control by actively managing system and security settings and allows the IT manager to identify and mitigate risks.

Installation and Configuration A

Installation was a snap; all that is required is to run a common Windows installer. There are some requirements, such as current versions of .NET, MDAC, MSJET and MSXML, but the installer checks for them and installs them as needed.

Within minutes, NetChk is set up and ready to go with default settings.

Functionality and Ease of Use B+

The recommended baseline scans for almost 270 separate checks, including checking account settings (password policy, lockout) and service settings. We scanned an XP machine using Shavlik's recommended baseline configuration, as well as SOX/ISO and NIST/FISMA guideline standards.

Testing methodology: We tested NetChk Compliance in our lab environment with a variety of Windows versions, including Windows XP, 2003 and 2000.

Starting the scan for the local machine was as simple as choosing a few drop-down menus. The checks took about a minute, and NetChk presented a summary report; it was obvious our default Windows XP install did not fare well against the recommended baseline checks. The report displays the type of information available, machine name, checks and results (when you dig into it), and a scan summary.

Clicking on Compliance Summary in the information frame allows you to see results for each check—whether your machine passed or failed. It's also possible to view account information, with privileges and password age displayed. And clicking on your machine name brings up a more detailed version of the compliance summary—our test machine was not in compliance with many of the account settings, password length, lockout threshold, and the administrator account had not been renamed.

Based on results, you can allow NetChk to change the settings on your system for many of the checks. We had NetChk remediate our settings and rescan. Upon rescanning, the machine passed almost all of the checks. Most of those that still failed require manual correction. Not a huge issue, but we'd like to see complete automated remediation in future releases.

Shavlik NetChk is not limited to scanning the local host, of course. You can scan remote hosts without an agent, grouping them by domain, organizational units, or by IP addresses/range. After setting up a group and giving them credentials, select policies and scan them much like the local host.

Policies aren't limited to Shavlik's baselines. Using NetChk's wizard, you can create custom compliance checks using a wizard to scan registry entries, service rights, user rights assignments, etc.

Reporting B

Shavlik NetChk Compliance can generate 14 different reports covering machine, settings and policy results. Reports can be exported to HTML, PDF, TIF, CSV, text and Excel format. Reports are brief—basically a summary with a pass-fail list of selected compliance checks. The policy dashboard provides an easy to read graphical display, which we found effective in conveying the overall compliance status of the network.

Verdict

Reasonably priced, NetChk could make a good fit for any organization looking to ease regulation compliance. ›

COMPLIANCE Controllers

We look at three GRC products and the distinct ways these tools can help organizations navigate the complicated regulatory game.

BY ED MOYLE AND DIANA KELLEY

Photograph by JOHN KUCZALA

decade ago, regulated industries were the rare exception; today, the industry that isn't regulated is the exception. In fact, most firms have multiple sets of regulatory requirements they need to address.

As the regulatory burden increases, businesses are finding themselves in an increasingly complex ecosystem of governance—we audit our contractors and clients to ensure their compliance to our security requirements, and the firms we service audit us.

As we implement security controls related to compliance, as well as controls contractually required of us by our clients, we put into production an ever more complicated laundry list of security controls to manage. Making risk decisions in this hive of controls, regulation and contractual obligations is nigh onto impossible.

IT governance, risk and compliance (GRC) tools promise to help us meet these challenges. They promise to help us make smarter risk decisions, manage our compliance efforts and govern everything about our security program, from security awareness to technical controls.

GRC is the latest information security buzzword, but marketing hype is doing a disservice to this array of products that address an organization's policy governance, risk management and compliance needs. Most deliver only part of the picture they promise, and every tool in this market has its own focus, areas of maturity and strategies for solving the same business challenges.

To help you figure out what approaches might be right for your organization, *Information Security* took a close look at three GRC products that are very different in focus, coverage and technology: Archer Technologies' SmartSuite Framework 4.1, Symantec's Control Compliance Suite 8.60 and Modulo's Risk Manager 5.0

Our goal was to create tests that address the promise of GRC while not favoring any particular technical strategy for getting there. We wanted to test the heart of GRC, the products' ability to:

- Author, distribute and map policy and controls to the governing regulation, as well as to keep track of exceptions to those policies/regulations (compliance)
- Assess the proper technical and non-technical operation of controls, and to mitigate/remediate areas where controls are lacking or not operating properly (governance)
- Assist in quantification, analysis and mitigation of risk within the firm (risk)

Purchasing a GRC product is difficult, so we designed a flexible testing approach tied to real-world deployment scenarios to account for the range of corporate requirements, the expansive nature of the products and their varying levels of maturity. To do this, we foremost wanted to create a set of hypothetical scenarios that simulate how most organizations would typically use and deploy GRC products. We drew on real-life experiences and pain points to create regulatory, oversight and technical challenges, such as any organization might face, and how the products might solve these challenges in a typical deployment context. Specifically, our goal was to test the "promises" of GRC *(see "'Promising' Products," below)*.

Analyzing business risk is tough enough, but regulatory requirements add a layer of complexity that is fueling the market for specialized tools.

COMPLIANCE

We evaluated how these GRC products might facilitate compliance efforts by determining how they can help organizations understand, record and document where and how they meet specific regulatory requirements. How do they help you author policy, map regulatory requirements to policy, and, in turn, map specific technical controls to that policy? We also looked at the ability to create highly granular policies. For example, can you map a specific technical control on a particular server all the way back to the driving requirement for that control?

We created test policies and attempted to link those policies to both the regulatory requirements as well as technical controls used to implement the governing policy. In other words, can you actually use the tool to track compliance activities, track the implementation of technical controls specifically required by the regulation, and track the operation of those controls in the field.

RISK MANAGEMENT

Analyzing business risk is tough enough, but regulatory requirements add a layer of complexity that is fueling the market for specialized tools. Think of your own environment, where the data required to determine what risk applies to a particular set of devices, applications or processes is probably spread throughout the company.

For example, in order to understand what risk applies to a legacy system that doesn't support a particular control, you need to know what the system does, how it's used, what compensating controls might be in place and what systems are dependent on it. Typically, that means getting data from the business, IT, external parties (such as service providers) and the compliance department.

A tool that can automate this process and preserve the information gathered in a central repository is essential to conduct formal risk analyses. To this end, we looked at the ability of the products to help gather data about particular systems/processes and their relative risk, evaluate that risk and put it in context. A key related area is the products' ability to record and track areas of the firm where technical controls could not be implemented, as well as features that analyze the level of risk associated with those exceptions.

TECHNICAL CONTROLS

Finally, we considered how products manage the many technical controls that firms might be interested in from a compliance and governance perspective. We assumed from the get-go that different products would have varied ways to monitor controls. For example, a product might use an agent on the remote host to periodically poll the device, and/or import data from other sources, such as vulnerability assessment tools to gain information about the status of system and application controls. The bottom line: Does the product provide enough information and the right kind of information to be of real use?

'PROMISING' PRODUCTS

Mapping GRC's claims to your company's requirements.

BUSINESS DRIVER	GRC "PROMISE"
Multiple overlapping regulations	Regulatory framework construction allows multiple regulations to be mapped to one set of controls
Demonstration of regulatory compliance to management/ auditors	Mapping of policy to controls and regulatory requirements allows you to keep track of compliance activities
Difficulty managing numerous controls across multiple environments	Monitoring tools for technical controls; ability to record what controls are implemented at what locations (and to satisfy what requirements)
Complexity of business makes risk evaluation difficult	Ability to assign risk based on criticality of components and sensitivity of stored data. Ability to correlate changes in environment and controls to overall risk
Burdensome tracking of policy exceptions including exception expiration	Ability to track policy exceptions, owners of components in exception scope
Inefficient, complicated or expensive security program management	Ability to automate workflow for security program tasks such as exception approval, policy authorship and incidents

ARCHER SMARTSUITE FRAMEWORK 4.1

From Archer SmartSuite's central administration console, administrators can create and manage users, assign roles to users, and configure the installed modules.

Archer focuses primarily on the non-technical aspects of GRC. The core of the product is a central framework within which a customer can use various modules that target the issues that an information security practitioner might experience within a regulated industry. For example:

- Policy Management addresses the need of information security practitioners to author, organize and publish policy.
- Vendor Management provides tools to manage vendor relationships and track adherence to contractual obligations.
- Incident Management allows you to manage the workflow associated with a security breach.

In navigating and using SmartSuite, we found the Archer community to be head and shoulders above what you typically get with a vendor knowledge base or other support portal.

There's no installation to speak of, as the recommended customer interface is a Web portal for an ASP-type service offering. (Customers can also choose to host the product.)

Admins use their interface to create users and groups, modify roles, permissions and security parameters of the system, manage content, or change the appearance of the portal. However, the real magic happens within the customizable interfaces for the installed modules.

Archer's Strengths

Policy management is a real strong suit. To test how SmartSuite would be used in an actual organization, we wanted to create policy we could tie to the regulatory requirements of our hypothetical company.

However, we didn't need to. Archer ships with a stock policy that is pre-mapped to a large number of regulatory frameworks. Given Archer's roots in the financial services sector, we were not surprised to see some relatively specific requirements such as FTC 16 CFR Part 314 (GLBA) and the FFIEC Information Security Booklet. We were, however, pleasantly surprised to also find more general guidance, such as COBIT and ISO 17799 (although they still need to update the numbering), as well as specific guidance for other regulated industries, such as HIPAA for healthcare and PCI for retail.

Although the stock policies are quite comprehensive, most firms will need to modify them to reflect their own requirements. We found this process a bit counterintuitive. The editing function allows you to directly modify the policy supplied by Archer, but you're better off avoiding that and using Archer's somewhat kludgy alternative.

The problem is that Archer's periodic updates to the stock policy (as well as the mapping to the regulatory frameworks) will overwrite any custom changes you make to the stock policy directly. Archer recommends that instead of modifying its policies, you create a new policy statement with customized text, link it to the stock policy, and update your firm's views to display the new statement. The stock statements live on—just out of view of the users.

The upshot is you will need to periodically revisit your custom policy to ensure that it reflects updates, such as changes to regulatory requirements.

Nevertheless, exceptions are easy to create and relatively straightforward. You simply select a control to associate with the exception and enter information along with compensating controls to address the issue. The workflow allows exceptions to go from user entry to information security review and keeps track of approvals and timeframe for expiration.

The risk management feature is straightforward. You assign risk to entities entered via the asset module and score them according to a number of different risk vectors. For example, we used the asset module to create a new application and assigned an initial business criticality weight as well as risk profile (high, medium or low.) From there we were able to apply questionnaires to the asset to determine how it performed relative to items of interest, such as whether cryptography was employed.

These questionnaires targeted specific controls that have an impact on the overall risk of the application and include factors like vulnerabilities, cryptographic controls, access control, and so on. The responses to the questionnaires fit directly into the overall risk ascribed to the application. The workflow ensures that appropriate personnel review the submission and are alerted if it is completely non-compliant.

In navigating and using SmartSuite, we found the

Archer community to be head and shoulders above what you typically get with a vendor knowledge base or other support portal. The community allows users to interact with each other, ask questions of the Archer engineering team, and receive extensive training on use and configuration of the product.

Archer's Weaknesses

While the product was very strong in policy and risk management, the more technology-centric pieces are not as automated as the other products. There's no autodiscovery function—you add assets by submitting a spreadsheet. While this will satisfy the needs of many organizations, larger firms with extensive asset inventories may find this process error-prone and difficult to maintain.

Monitoring technical controls is also less automated than some of the competition. Archer provides instructions on how to create linkages between automated vulnerability assessment tools (e.g., Qualys), but automated vulnerability assessments may not give you the whole picture. There's little out-of-the-box integration of additional tools, such as other vulnerability assessment scanners, IPSes, SIEMs, etc., but you can use the flexible API to allow custom data consumption applications to be written using feeds from files/databases, etc.

One nice feature lets you correlate information from a number of threat publication sources, such as Verisign iDefense and Symantec DeepSight, in addition to custom entry of threat data.

SYMANTEC CONTROL COMPLIANCE SUITE

Symantec's Control Compliance Suite Response Assessment Module allows users to create questionnaires for use in assessing specific security requirements (for example, vendor governance).

While Archer is heavy on policy management, Control Compliance Suite 8.60 (CCS) has a deep focus on the management and monitoring of technical controls, providing quite a bit of functionality to assist in tasks like network discovery, automated validation of host technical configuration, and so on.

The software can be installed in standalone or enterprise mode, depending on whether you intend to host the database on the same box as the information server or use a different box for the database. Additionally, enterprise mode is required if you intend to make use of the Web portal integration with Microsoft IIS. We installed the product in enterprise mode, as this allowed access to the Web portal and supported a remote database and remote data collection.

Symantec's Strengths

At first, we were a bit skeptical about the policy creation interface (not the prettiest interface we've ever seen), but using it to write policy was straightforward despite the initial awkwardness.

We were able to author policy, import existing policy from Microsoft Word documents and approve publication to the CCS Web portal. The tool supports a policy authorship workflow in much the same way Archer does, allowing us to defer publication until approval and to keep a recorded archive once a new version is created.

One feature that really stood out was the flexibility provided to map policy to the compliance frameworks and regulations CCS provides.

Surprisingly, we found ourselves missing the kind of stock policy supplied by Archer. Symantec has a number of sample policies (templates), but we found that importing our own policies or creating new policies from scratch using the policy import and creation tools took less time than customizing the templates.

One feature that really stood out was the flexibility provided to map policy to the compliance frameworks and regulations CCS provides. The mechanism is a mapping editor that's reminiscent of the relationship manager feature of Microsoft Access. Though it took us a while to figure out how to use it, the mapping editor provides tremendous flexibility in making connections between policy, framework and regulatory items. The ability to see these relationships visually had a definite "cool factor." Of course, while this is a flexible approach, it requires a bit of manual interaction to maintain. An enterprise seeking to make heavy use of the policy portion of this tool would require more ramp-up time to get ready for full deployment.

CCS is very strong on technical controls. The product ships with a large number of technical standards packs that can be used as a benchmark against which to compare devices that it is aware of.

The standards packs draw on familiar source material, such as NSA configuration guides and the CIS configuration benchmarks.

The technical information-gathering feature supports a very large number of devices for remote profiling. CCS can use an agent or agentlessly retrieve data across a diverse range of platforms, such as various Windows versions and multiple flavors of Unix and Linux.

The product also ships with many benchmark standards to evaluate against, to ensure that appropriate patches are applied and that appropriate configuration steps are taken.

The technical information gathering supports a very large number of devices for remote profiling.

CCS also ships with network mapping capability that allows automatic discovery of devices, which can then be imported into the risk management and asset management view.

We expected CCS to perform very strongly in technical controls validation, but were unprepared for the product to perform equally well in policy and risk management. We were pleased to see the range of technical standards and regulatory frameworks that the product ships with: multiple versions of COBIT (both 3 and 4), FDA regulations, FISMA, HIPAA, NERC (North American Electric Reliability Corp.) guidance and NIST SP 800-53 were all included.

Symantec's Weaknesses

While CCS is heavy on governance and technical compliance, we found the risk piece difficult to use. Technical risk is assessed directly within the CCS console via evaluation of technical security controls; for the less technical areas, the product leverages customized questionnaires.

CCS allowed us to import Symantec's questionnaires using content packs or create our own. We used the tool to create an ad hoc vendor evaluation, and found the process painful.

Each questionnaire is represented as a tree view to which questions are added. Questions can require single or multiple-choice answers, or written responses. Creating a questionnaire required us to manually enter a large number of customized answers (the templates, which were fine for yes/no questions, rarely supplied the answers we needed).

Once the questionnaire was complete, we used a wizard to assign weights to each of the questions and answer choices. All told, the process took us about an hour to create a 20 questions. If you're planning to make extensive use of this functionality, we recommend using the content packs that supply stock questionnaires rather than creating customized questionnaires from scratch.

METHODOLOGY

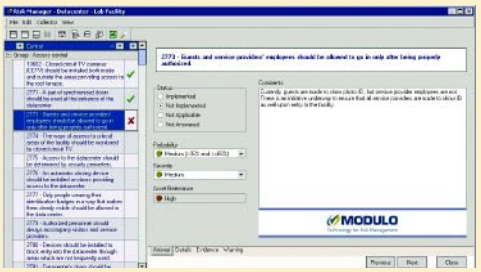
EVALUATING GRC PRODUCTS

We targeted the following functionality as part of this analysis:

FEATURE	PROCESS
Policy creation, publication and tracking	Created custom policy. Used publication, workflow and document management (version control, approval, revision tracking, etc.) features.
Compliance framework creation	Mapped custom and existing policy to the included regulations and/or frameworks provided within the tool. Tested the ability of the products to add new requirements such as information security terms and conditions or other contractual requirements.
Exception tracking	Created exceptions mapped to specific policy, controls and/or regulations. Tested workflow related to exception approval and exception lifecycle management.
Controls management	Tested the ability of the product to track and manage technical, administrative or physical controls deployed to support defined policy and regulatory requirements.
Risk assessment	Used the products to assess risk related to technical controls and coverage of regulatory and/or policy by deployed controls.
Risk management and calculation	Used features to manage risks identified through risk assessment–for example, to aggregate risk areas, to associate technical risk to specific controls, etc.
Reporting and dashboards	Used reporting and dashboarding features for assessments, control coverage and risk.

TEST BED We used a laboratory environment consisting of a closed Windows domain consisting of a Microsoft Windows 2003 Server domain controller, a Microsoft Windows 2003 server and a Microsoft Windows XP Professional SP2 client. VMware Workstation 6.0.3 was used to simulate a combination of operating system configurations such as might exist on a homogenous enterprise network, including Microsoft Windows XP, Microsoft Windows 2000 Professional and Debian Linux 4.0.

MODULO RISK MANAGER 5.0



The integration console allows Modulo Risk Manager to import information from Active Directory, from an XML file, or from a spreadsheet (for example, an asset spreadsheet).

Many vendors in the GRC space try to take the "boil the ocean" approach by being everything to everybody. Not Modulo. It doesn't have the compliance-framework creation and policy-centric features of Archer, or the technical control validation capabilities of Symantec. Instead, Modulo's aptly named Risk Manager focuses almost exclusively on the risk aspects of the GRC equation. The functionality within the other areas of GRC serves only to support the risk management mission.

Modulo's aptly named Risk Manager focuses almost exclusively on the risk aspects of the GRC equation and provides functionality within the other areas of GRC solely to ultimately tie them back to risk.

Risk Manager does not have a Web front end (although you can submit questionnaires via the Web), and relies on a number of client-side applications to implement various features.

The installation process gave us quite a bit of trouble initially. Insufficient RAM on the first few lab machines we attempted to install caused the installer to fail (the test machines had double the memory requirements specified in the manual). However, with some coaching from the Modulo engineers—followed by a hardware upgrade beyond the recommended requirements—we completed the installation.

Modulo's Strengths

Risk Manager allows enterprises to categorize themselves into one or more "organizations" that are represented by a tree view in the client. It auto-populates this view by importing information from a variety of sources, such as Active Directory, asset spreadsheets/databases and manual entries.

Its real power lies in its ability to categorize every asset in the organization—processes, applications, technical components and facilities—associate a risk level to each, and keep track of the controls that are implemented on an asset-by-asset basis. The tool also facilitates keeping track of personnel associated with the assets and threats to it.

Risk information is collected using one or more questionnaires applicable to different assets, based on their categorization. For example, data centers can be assigned one or more data center-specific questionnaires to appropriate personnel. Risk Manager gathers information about all the assets in a particular scope and quantifies the associated risk, keeping track of controls' status on an asset-by-asset basis.

You can link evidence with particular answers as well. For example, to support a response to a questionnaire about authentication, you can attach evidence in the form of policy, an export of the appropriate group policy objects governing password characteristics, and so on.

This ability to associate evidence with questionnaires should please auditors, who require proof of a particular control, rather than simply validating that a governing policy exists.

Auditors will also appreciate the ability to generate remediation plans for particular assets based on the results of the questionnaires. The remediation guidance provided for each of the assets in scope is concise, yet thorough.

Risk Manager facilitates governance of vendors and external relationships in a way the other products do not. For example, Risk Manager ships with the ability to perform a risk assessment using the Financial Institution Shared Assessments Program Standardized Information Gathering questionnaire. It also allows you to create "perimeters" (nodes on the organizational tree) for vendors and third parties. While the other products can be configured to do similar things, native support for FISAP out of the box is a real plus for organizations who use Risk Manager in an auditing context.

Other questionnaires can be assigned to assets within the vendor perimeter. This enables you to keep track of assessments performed of a particular vendor, the evidence collected during the assessment, the vendor's compensating controls, etc.

Modulo's Weaknesses

Risk Manager has a few rough edges. First and foremost, the lack of a fully functional Web interface is a significant drawback. While questionnaires can be submitted over the Web, a portal view of the application (including a Web-enabled dashboard) was a sorely missed feature and would provide quite a bit of benefit.

Additionally, installation was challenging; the application has very specific installation prerequi-

sites, and any failure of the installation process (due, for example, to lack of a prerequisite, insufficient memory or a populated database instance) resulted in an error message that required technical support to interpret.

Further, the product appears to be difficult to customize. For example, some of the built-in databases (such as the threat database) are static, precluding user customization.

ONE SIZE DOESN'T FIT ALL

Each of the products we looked at interprets governance, risk and compliance in a different way and has a feature set tailored to its vision. Archer emphasizes regulatory compliance, most useful for the compliance or security group in a heavily regulated industry. Modulo focuses on risk management, which is of special value to the auditor or consultant out in the field validating organizational compliance to controls. Symantec focuses on technical control validation, most useful to information security technical personnel.

But in order to know how the vendor interprets the GRC vision, you must look beyond the marketing. All of these products are marketed similarly; they get coverage from analysts in the same reports and they're lumped together in the industry press. But they're really very different.

What does that mean to the industry? Maybe we should start segmenting the GRC market to reflect the fact that these products aren't the same. What does it mean for GRC vendors? Maybe it's not a threat if your product doesn't do exactly the same thing as the other guy's product. And what does that mean for the consumer? It means you need to be extra careful before you buy: Make sure your vendor's vision of the market aligns with yours, and that the product you're buying does what you think it will.

Each of the products we looked at interprets governance, risk and compliance in a different way and has a feature set tailored to its particular vision.

Ed Moyle is founding partner of SecurityCurve and a manager with CTG's information security solutions practice. He is co-author of Cryptographic Libraries for Developers. *Diana Kelley is founder and partner at SecurityCurve.*

LOG MANAGEMENT

LogRhythm

REVIEWED BY GARY MOSER

LogRhythm
www.logrhythm.com
Price: **Starts at $20,000**

LogRhythm is a cross-platform log management program that provides a multitude of functions to manage audit files and IT security management processes. It's well crafted to meet IT industry trends aimed at increased enterprise efficiency, security and governmental/industry compliance standards.

Configuration/Installation B+

While the configuration of data sources initially seemed a daunting task, the installation documentation guided the process in a step-by-step format that was easy to follow and manageable.

However, actually deploying log management in an enterprise is hardly plug-and-play, and prospective buyers with complex IT infrastructures may want to consider onsite installation and training.

LogRhythm is a cross-platform tool, with out-of-the box configuration settings to bring in data for many sources, including Linux syslog, Cisco NetFlow, Snort, Blue Coat Web proxy, and all ODBC-compliant databases.

LogRhythm also supports application logs, such as Apache, IIS, DNS and DHCP.

Dashboard B+

We were impressed with the configurable dashboard, with plenty of options to monitor network activity in a real-time, visual interface. The display is set up to show near real-time activity in a graphic format in operations, security and audit panels.

The dashboard can be configured to display pertinent critical data based on any aggregated data variables. Further log management functions are started from the main console, with clearly defined dropdown menus.

Testing methodology: We tested a LogRhythm appliance connected to a lab environment with multiple syslog sources.

Monitoring/Analysis A

LogRhythm's aggregator can be configured to collect data at variable intervals to minimize bandwidth concerns. Queries can then be run on the aggregated data to drill down to find specific information. Setup wizards facilitate step-by-step development of queries and reports.

LogRhythm is remarkably configurable, which enables rapid development of queries to correlate, filter and find data quickly. Its ability to filter and correlate data provides a fantastic forensic analysis tool, which can be finely tuned to examine any details users need to look at, cross-referencing multiple sources.

For example, we were able to quickly see anomalous activity on our network by examining trends in login failures and after-hours activity, easily focusing our search to identify specific users.

The ability to save complex queries for future use will prove especially efficient in fast-paced IT data centers, particularly for incident response situations, where time is a critical factor. The graphic presentation of the data queries was impressive, one of the best we've seen, painting a clear picture of large and complex data sets.

The custom alarm rule setting function provides in-depth functionality in categories of classification, events, login and service rules. Varying thresholds and time requirements can also be set, like number of events before an alarm is triggered, and how often to report. Alarms can be delivered via email, SNMP or in the console.

Reporting A

Reporting is outstanding for its range of templates, output formats and exceptional graphic displays.

The reporting functions provide templates to meet most commonly used industry compliance standards for data collection and auditing purposes, such as PCI, SOX, GLBA and HIPAA. The output formats included Crystal Reports, which enables a host of additional options. The graphics formats visually depicting the data correlation were particularly impressive at summarizing trend data in easy-to-digest format.

Verdict

LogRhythm is an outstanding and affordable log management tool, with many uses to fit any enterprise IT management tasks, and particularly useful in forensic analysis.

MOBILE SECURITY

Credant Mobile Guardian 6.0

HotPick INFORMATION SECURITY®

REVIEWED BY SANDRA KAY MILLER

Credant Technologies

www.credant.com

Price: **Starts at $85 per user**

The latest version of Credant Mobile Guardian (CMG) offers a unified Web-based management portal that lets administrators discover, secure and monitor endpoints, regardless how they touch the enterprise network.

Installation/Configuration B

Be prepared to dedicate some time to install and deploy its components in large, distributed environments to ensure for efficient scalability. Even our basic installation consumed a significant amount of configuration time.

The Gatekeeper component listens for synchronization between mobile devices and workstations, performs automatic discovery of mobile devices, distributes updates, policies and encryption keys, and performs monitoring, reporting and application control. Agents enforce policies, regardless of connection status.

The Enterprise Server is managed through a browser-based interface that works equally well on Internet Explorer and Firefox. Integrating with Active Directory provided a speedy designation for individual users and groups.

Installing client software on workstations was straightforward, but the agent deployment on our Windows Mobile device required several attempts.

Policy Control A

Defining policy by user, groups and devices was much easier. The Web-based policy editor's tabbed environment is broken down by mobile device platforms, and Gatekeeper offers pages of comprehensive options, including login attempt thresholds, number of characters required in passwords, etc.

Our policies worked flawlessly on endpoints, regardless of their network connection status. For example, when we attempted to replace the SD card in our smartphone with an unauthorized card, we were no longer able to access network resources. Equally impressive was the granular control over connection types, including infrared, Bluetooth and Wi-Fi. Whitelist/blacklist functionality let us control applications policies.

Overall Security A

By far the strongest feature of CMG is encryption—your choice of AES 128 or 256, Blowfish and Triple DES. We designated automatic encryption data in a variety of mobile device and workstation scenarios, all transparent to the end user.

In case of lost or stolen laptop, we could issue a command that would instantly destroy the data and/or encryption key on the device as soon as it is connected to the Internet and automatically polls the Gatekeeper for updates. You can also designate similar actions upon a predetermined number of failed logins. One feature in particular caught our eye—the In Case of Emergency button that could be installed on the login screen. This offered non-authenticated access to the device user's contact information in the event of an emergency or if a good Samaritan wanted to return a lost device.

Intelligent Encryption allows administrators to designate different layers of encryption based upon user data, application data, system files and external media.

Logging/Reporting A

CMG's logging and reporting offers robust insight into what's happening on devices throughout the network.

Through the Web interface, we could check on the status of the Enterprise Server, Gatekeepers, Policy Proxies, Shields, encryption and users, along with a full accounting of devices discovered by the Gatekeeper.

We particularly like the fully searchable log files, allowing us to quickly pin down a specific event.

Verdict

CMG is a robust endpoint security solution that can meet the demands of large and small enterprises.›

Testing methodology: We deployed Mobile Guardian on Microsoft Windows Server 2003 with Active Directory and managed a variety of devices, including workstations, mobile phones/PDAs with wireless network connectivity, and portable media such as flash drives and SD cards.

Review how we grade at searchsecurity.com/grading_criteria.

IT COMPLIANCE

GoldKey Secure USB Token

REVIEWED BY JOEL SNYDER

GoldKey

www.goldkey.name

Price: **Starts at $132 per user token**

The GoldKey Secure USB Token works with Windows and Macintosh operating systems to provide a secure place to stash encryption keys for virtual disks. By keeping encryption keys on a small, removable USB token, GoldKey simplifies the task of locking away important information on laptops and encourages good security behaviors.

GoldKey takes on one of the most difficult tasks in hardware-supplemented encryption by providing a manageable hierarchy of master keys, group encryption keys, and the ability to duplicate tokens.

Performance A

We had no problems in our tests of GoldKey USB on Windows and Mac laptops. Everything worked as advertised without any problems or bugs.

One of the main concerns about encrypted virtual hard drives is the impact on system performance. We tested a GoldKey encrypted virtual disk against one using the operating system's native encryption system (both Windows XP and Mac OS X), as well as a local laptop drive. On our ThinkPad laptop running Windows, the GoldKey disk was about 50 percent faster than a drive encrypted using Windows tools, and about the same speed as the local 7200 rpm laptop drive. On a MacBook Pro, GoldKey was 75 percent faster than the native OS X encryption, although about 60 percent slower than the local 7200 rpm laptop drive. Windows users should see little performance impact in modern laptops.

Testing methodology: We used MacBook Pro and IBM ThinkPad X61 laptops to test the GoldKey USB key. We encrypted volumes and used them for day-to-day operations for a week. In addition, we used simple benchmark tools to compare performance of GoldKey USB, native O/S hard drive and native encrypted file systems.

Management B+

One of GoldKey's unique features is the ability to use group encryption keys as well as personal encryption keys. A virtual disk may be encrypted by one member of a team, with full access by other members in the same group. GoldKey provides a basic management tool that makes management of groups and group memberships easy.

GoldKey also supports master and grand master keys, as well as the ability to duplicate tokens. Together, these tools help eliminate one of the greatest fears of encrypted data: permanently losing the key. While GoldKey's mechanisms won't scale up to a Global 100 enterprise and don't integrate with the corporate directory, they are easy to use and simple enough for fairly large deployments.

However, be aware that GoldKey doesn't have any online magic to access controls. You can't remotely revoke privileges to read or write a volume from someone, and if someone loses an encrypted volume and token, and writes down the password to the token, whoever finds all three will have full access to the volume. GoldKey doesn't protect you against rogue employees, just forgetful ones.

Other Security Functions C

While testing GoldKey, we kept hoping it would do more than it does—but it doesn't. Features such as auto-lock of laptop and encrypted drives when the token is removed are present, but they can't be centrally controlled or locked. Other common features, such as automatic timeout to require reauthentication, aren't available. While you can email around GoldKey-encrypted volumes, there is no real integration with any application other than the file system.

Verdict

While GoldKey is far from a do-everything desktop security solution, it handles the problem of key management for encrypted volumes very well.

MOBILE SECURITY

GuardianEdge Data Protection Platform

REVIEWED BY SANDRA KAY MILLER

GuardianEdge Technologies

www.guardianedge.com

Price: **Starts at $182 per user**

The GuardianEdge Data Protection Platform addresses the challenge of securing data wherever it resides, with centrally managed security on computers, mobile devices and portable storage. It offers hard disk and removable storage encryption, device control, advanced authentication and smartphone protection.

Installation/Configuration B

The Server and Manager Console software provides framework to create custom application deployment packages for clients through wizards, including policies for hard disk and portable storage encryption. Granular device, port and access control leverages Active Directory.

The management console has a basic Microsoft Windows design with a hierarchical tree. GuardianEdge also installs a Microsoft Management System snap-in as a management console option.

Policy Control A

GuardianEdge offers flexible policy control; we were impressed by the complete ease with which policies were created and modified through multiple channels.

Policies are deployed to clients through AD Group Policy or a third-party tool for distributing software. Implementing and editing policies was easy, in contrast to the obscure and tedious methodologies on many similar products. GuardianEdge provides granular control over ports, devices, storage and wireless adapters, as well as specific logging, alerting and encryption controls.

Testing methodology: We deployed GuardianEdge Server and Manager on Microsoft Windows Server 2003 with Active Directory and tested using a variety of devices running Windows 2000, XP and Vista.

Client-based policy enforcement includes an anti-tampering feature that we were unable to circumvent.

Overall Security B-

Although GuardianEdge provides all the endpoint control security features found in competing products, it's limited to Microsoft systems.

It covers all the bases of endpoint device protection, including defense against hardware-based keyloggers, autorun blocking for executables stored on portable media, and tight controls for physical and wireless ports.

Data shadowing allows all information accessed by a specific port or device to be recorded.

The device control component's audit feature let us quickly discover specific items on our network. We set up filters to identify machines with wireless adapters on the entire network, by network segment or by individual computers, then created an inventory spreadsheet.

Encryption covers all the bases for security, compliance and usability, including a self-service password recovery feature. GuardianEdge supports AES 128 and 256, multifactor authentication and kernel-level authentication prior to booting from an encrypted hard disk.

However, neither hard disk nor removable storage encryption functioned well on our Vista test systems.

Logging and Reporting B+

GuardianEdge delivers comprehensive logging and reporting without any extra snap-in or software.

Responding to regulatory requirements, some companies have become overzealous in their logging; this is one product you don't want to do that with. Given the wide range of security GuardianEdge covers, it's easy to become quickly overwhelmed by logging everything.

Administrators can keep track of policy-controlled events through the Windows System Event Viewer, reports created through the Windows Group Policy Management console or through a Client Monitor Watchlist.

Extensive support for Windows snap-ins creates a familiar environment for administrators to quickly integrate logging and reporting into standardized distribution channels, such as SNMP.

Verdict

GuardianEdge delivers easy administration, acceptable security and automated logging for Microsoft clients.

For an extended online version of this review, see this month's issue on SearchSecurity.com.

SIEM

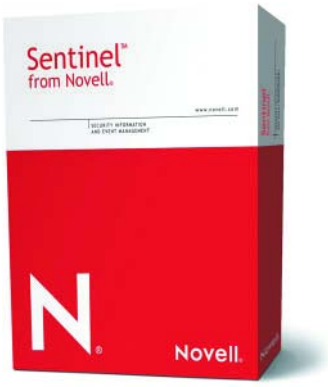
Sentinel 6.0

REVIEWED BY BRENT HUSTON

Novell

www.novell.com

Price: **Starts at $65,000**



Novell, which acquired Sentinel, its entry into the SIEM market, from e-Security last year, offers a robust product that is getting better with each revision.

Setup B

Sentinel has many parts, and could take quite a bit of work to set up in a large environment. The setup isn't necessarily painful, but there are steep system requirements, which may not be an issue for enterprises.

In a large environment, Novell recommends each component be installed on a separate machine for maximum performance. Setting up collectors, which gather data from devices and convert it to the Sentinel event log format, takes some work, but it pays off in the end in the breadth of device support.

For test purposes, we installed them on the same machine. Sentinel supports a variety of platforms, such as Linux, Solaris, Windows and databases, including Oracle and Microsoft SQL Server.

Management/Monitoring B+

Control Center is the front end to the brains of the operation, and where most of the time will be spent analyzing data and events. Sentinel manages to display copious data in a logical GUI.

Nonetheless, Sentinel's interface can be somewhat intimidating at first, because you have to deal with so many pieces and so much data. It's tab-based, with a navigation toolbar on the left that changes depending on the tab you are in.

For example, Active Views looks at and investigates events in real time; Correlation is where you create rules that tie together event triggers, adding intelligence to event flows; Incidents displays events entered by analysts or alerts triggered by correlation rules.

The iTRAC tab is a workflow tool, tracking incident response processes through event resolution. The Analysis tab handles historical reporting, and the Adivsor tab takes data from VA scanners and IDSes. In addition, this is where you can pick up guidance for remediation.

All of these parts worked quite effectively together, allowing us to see events come in, identify those that appeared to be suspicious and then track and investigate them as the case requires.

The correlation tool was surprisingly easy to use, with a built-in wizard to allow the creation of rules, including more complex chains of triggers. For example, we would set up a simple rule that triggered when there were four failed logins in two minutes. Then we created more interesting combinations reflecting things like IDS events and root login attempts.

We built a simple workflow to track incidents, but be cautioned that workflows can be very complex in the large IT environments in which tools like this are employed. Depending on your organization's requirements, you can integrate Sentinel with external scripts to interact with third-party systems, such as Remedy and HP OpenView.

A major enhancement since the e-Security acquisition is the ability to track users as well as devices, an important trend in enterprise SIEMs for security and compliance auditing.

Reporting B

Reports are handled by Crystal Reports, a powerful and popular tool. Sentinel comes with Crystal Server as well as Developer, so you can modify and create your own reports.

Sentinel's reporting leaves no event data unseen, and is highly configurable.

Verdict

Sentinel is aimed at very large enterprises, and this is where it is best suited. It can be an extremely powerful tool, if used to its potential, with many features to help automate and analyze all of your enterprise's logs and events. ›

Testing methodology: For lab purposes, all of the components were installed on one machine. Windows Server 2003 was used, as well as SQL Server 2005 standard edition.

SIEM

RSA enVision

REVIEWED BY NATHAN GRANDBOIS AND BRENT HUSTON

RSA

www.rsa.com

Price: **Starts at $25,900**

EnVision is a powerful and manageable tool that enterprises can easily leverage to reduce the resource requirements of the security team for event analysis, incident handling and baseline compliance reporting.

It possesses a strong mechanism for gathering data from myriad devices and applications around the enterprise and performing parallel processing, correlation and analysis.

Installation and Configuration A

Software configuration was a snap, and RSA includes onsite time with its engineers as part of the sale.

Configuration and log delivery mechanisms are typical of this type of tool. Any system or network administrator with a modest level of experience should be able to get enVision working with any device or application in the enterprise.

We had no problems setting up a variety of platforms and applications in our lab.

The appliance is well equipped with RAID, multiple power supplies and powerful cooling units. It's a bit louder than some server devices we have tested in the same size range, but this is trivial once it's installed in your network room.

Ease of Use B

That nuisance aside, the Event Explorer interface is clean and extremely powerful. Building rules to trigger alarms based on various parameters, and creating special "watch lists" and other customizations is quite easy. The documentation and help mechanisms gave us any additional insight we required. Watch lists are a way to filter events based on certain strings and lists of like values. We were impressed with the level of drill-down detail on the one hand, and the ease of understanding that the reporting engine and high level reports provided for upper management on the other (a real time-saver for administrators).

Our only real complaint is that the GUI does not adhere to normal Windows shortcut standards. For example, one of the most annoying problems we encountered was that instead of refreshing the screen, the F5 key would silently end our session and log us out. RSA should update the key maps to adhere to Windows conventions.

Testing methodology: The lab consisted of multiple machines, with focus in the Windows environment. Data was generated by a utility provided by RSA, and multiple syslog devices within the lab.

Capability A

EnVision's real power is in its ability to perform complex correlation and alerting. The correlation engine does a great job of helping administrators identify important alerts, so organizations don't waste time and money assigning resources and people to investigate false positives. Once you learn to trust the tool's analyses, your event management practices should improve in a serious way.

We were easily able to drill down, analyze and identify events that related to each other and formed the basis of a serious compromise attempt, while sorting out the normal noise.

We were impressed with the ease of integrating into the product database logs and other event sources, such as firewall, IDS/IPS and alternative operating systems. We were pleasantly surprised at how easy it was to create effective monitoring for an average e-commerce website installation that we modeled in our lab. It took our team less than four hours to establish a comprehensive view of the site and be able to effectively monitor the security and events.

Reporting B

Reports, which are created through an easy-to-use interface, can be run ad hoc or scheduled. Report generation is fairly straightforward, with a number of built-in reporting packages available, including SOX, PCI DSS, HIPAA, GLBA and SAS 70.

Verdict

EnVision is quick to install, easy to configure, and will bring most organizations a deeper, more complete view of their environments.

NETWORK DEVICE TESTING

BPS-1000

REVIEWED BY ED SKOUDIS

BreakingPoint Systems
www.breakingpointsystems.com
Price: **Starts at $185,000**

Before enterprises deploy new network equipment, they need to make sure they can handle a barrage of traffic, including exploits and attacks.

BreakingPoint Systems' BPS-1000 is designed to test network equipment under gigabit loads of legitimate and exploit traffic to measure performance, traffic leakage, packet dropping and stability.

Test Comprehensiveness A-

The BPS-1000 is unique in supporting tests at various layers of the protocol stack, all in one package.

Other tools focus on testing a device at one layer, such as the ability to switch Ethernet frames (Layer 2) or evaluate how network equipment routes packets (Layer 3) and handles malformed headers (Layer 3 and up). Others simulate large numbers of TCP sessions (Layer 4) or complex application mixes (Layer 7). Still others launch exploit traffic through a network device to see how it detects and blocks attacks (again at Layer 7).

The BPS-1000 also includes traffic replay capabilities to spit out packets from a capture file, modifying elements of the headers, including IP address and TCP sequence numbers. Playback can be sped up or slowed down to see how the device deals with changes in the rate of incoming traffic.

However, the tool is architected to test network equipment only, not end-system targets. Based on a sender-receiver architecture, the tool is designed to send packets and determine what makes it through a network device. Unlike other security testing products, the BPS-1000 is not designed to attack end systems and determine which particular packets caused them to crash.

Testing methodology: We configured the BPS-1000 to send data through a switch, a routing system and a network-based IPS device, using a mix of test traffic that included legitimate TCP sessions, exploit traffic and malformed packets.

Security Testing Capabilities B

The BPS-1000's security testing capabilities are outstanding, but also where expanded functionality would be most useful. The tool includes hundreds of different "strike" packages, each capable of launching a different exploit. Further, testers can use several dozen obfuscation and encoding techniques for the strikes to dodge packet-inspection technologies like firewalls and network-based IPS tools, representing the most comprehensive exploit and evasion testing technology on the market today.

However, while you can run through a series of tests to see how a mix of traffic affects the target network device, you can't iterate step-by-step by changing specific fields or set break points during a given test. This forces you to conduct tedious manual hunting to discover which elements caused a crash or error condition.

Setup and Configuration B+

Configuring tests is straightforward. Each type of test traffic you choose is represented as an icon on a graphical display of a data center rack. You can tweak a test by simply clicking on the appropriate icon and altering its settings. The BPS-1000 also includes a variety of Quick Tests to evaluate Ethernet traffic handling, IP routing, TCP session support and exploit blocking. It also supports TCL-based code for custom tests (Ruby, Python and Perl scripts will be supported in future releases).

The GUI is intuitive and flexible, but suffers from issues typical of a first release; some dialog boxes lack a cancel button, and some of the drag-and-drop features for grouping strikes require very careful dropping in a small subsection of the GUI.

Reporting A

Numerous reporting options are available, including PDF, HTML and XLS formats. The system auto-generates well-organized reports that include a synopsis, success criteria (as defined by BreakingPoint), pie charts of traffic types, and graphs of transmitted and received packets sorted by application type.

Verdict

The BPS-1000 offers comprehensive, fast and flexible testing, the best we've seen for generating exploits and evasion tactics.

SYSTEM/DEVICE TESTING

Mu-4000 Security Analyzer

REVIEWED BY ED SKOUDIS

Mu Security

www.musecurity.com

Price: **Starts at $40,000; $300,000 with all modules—protocol mutations, published vulnerability and DoS—and gold support**

The Mu-4000 is a traffic generation, testing and test-monitoring tool focused on creating network attack patterns and illegitimate traffic, and measuring their impact on target machines. Since *Information Security*'s last analysis of the Mu-4000 in December 2006, Mu Security has significantly increased the capabilities of its flagship product, adding new testing capabilities and monitoring options.

Test Comprehensiveness B+

The Mu-4000 offers a vast number of different tests, including mutated traffic, published vulnerabilities and DoS attacks. The mutation engine is a top-notch commercial fuzzer, iterating through patterns of attack traffic, launching billions of different combinations of packets to find zero-day vulnerabilities in target software. Mu's published vulnerability analysis feature generates traffic for known attack vectors and flaws, including hundreds of buffer overflows and related problems.

The new DoS test suite allows testers to launch dozens of different DoS attacks, choosing from multiple protocols, including TCP, UDP and ICMP, with specialized payloads. When configuring DoS attacks, Mu supports ramp-up and ramp-down rates for traffic, letting an organization see if the target systems recover appropriately or are damaged or unstable.

Testing methodology: We configured the Mu-4000 to send a variety of packet mutations, published vulnerability attack vectors and denial-of-service attacks through a switch, router and network-based IPS device against a vulnerable target system running a variety of services, including Windows File and Printer Sharing, and a Web server.

Security Testing Capabilities A

Mu offers one of the best fuzzing engines available and a comprehensive set of published vulnerabilities.

The system watches for service availability and response time during an attack, using a variety of instrumentation and monitoring options, including checking for system availability, service responsiveness, system log monitoring and more. When a fault is encountered, the Mu Analyzer supports stepping through groups of traffic and individual packets to determine which combinations of settings caused the problem.

Setup and Configuration B

Given the increased types of tests and greater flexibility, creating a custom test involves numerous steps setting up the appropriate protocols, choosing from a myriad of options, and configuring the appropriate monitoring and instrumentation of the target device.

The GUI is organized to walk you through the various steps for configuration, but building custom tests is not for the faint of heart. To help, Mu has added the ability to create test templates, XML files that simplify creating and customizing an attack scenario.

All of the options for a given test can be saved as a template and exported from one Mu-4000 and imported into another. In addition, Mu ships dozens of prebaked complex test templates in the product, with new templates released periodically.

The documentation is voluminous, but well written and illustrated, walking users through the complex setup and explaining the report format well.

Reporting A

Mu's reports are easily understood, providing overall graphical representations of the test traffic generated, and the responsiveness of the target system under attack.

The Mu-4000 generates executive summary reports and assigns a letter grade based on faults and performance issues. Detailed metrics include not only service or system crashes, but also response time problems and the particular attack traffic that caused each problem.

Verdict

The Mu-4000 offers comprehensive security testing, providing deep insight into how systems will fare under a barrage of attack traffic of all types.

VIRTUALIZATION

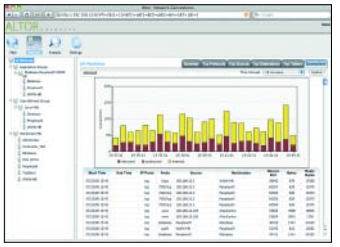
Virtual Network Security Analyzer (VNSA) 1.0

REVIEWED BY PETER GIANNACOPOULOS

Altor Networks

www.altornetworks.com

Price: **Starts at $1,500 for Altor Center Enterprise and $500 per agent**



The explosive growth of virtualized x86 environments challenges security vendors to adapt their appliance/server mentality to a radically different computing environment and rethink approaches to network segmentation, intrusion detection and traffic monitoring.

Altor Networks seeks to address this problem with Virtual Network Security Analyzer (VNSA). VNSA and the unreleased Virtual Network Firewall (VNF) are intriguing, but not yet ready for prime time.

Installation/Configuration A

Altor is clearly aiming at enterprise-level VMware deployments and requires a VMware Virtual Infrastructure 3 (VI3) install. Installation is simple and consists of creating a port group in promiscuous mode on the virtual switches you wish to monitor (to allow network sniffing by the VNSA appliance), and setting up a VM with the complete Altor VNSA application. You can install the VM by unpacking a complete image from a standard zip archive or downloading an Open Virtual Machine Format file directly from within Virtual Center.

You then assign the VNSA NICs to the preconfigured promiscuous mode port groups, and power on the VM to perform basic network configuration. This takes minutes and is a perfect example of how virtual appliances should be packaged and distributed.

Testing methodology: We installed VNSA in a VI3 environment consisting of ESX 3.5 hosts and a Virtual Center 2.5 console. The ESX hosts were running a mix of Windows 2003, SuSE Linux and Windows XP VMs.

Management B+

VNSA agents are installed on the hosts supporting the monitored virtual switches and forward collected data to the Altor Center master server. Once the VM is running, the Altor Center Web application can be configured to access Virtual Center.

Altor Center queries Virtual Center for all registered VMs and populates its internal database with the information. It uses this information when tracking and analyzing vSwitch activity. The Altor Center Web UI is very well laid out and intuitive.

Monitoring B+

VNSA agents monitor vSwitches and report activity to Altor Center. Traffic is broken down by protocol, source/destination, etc., and can be sorted and analyzed in a variety of ways. Suspicious activity, such as port scans or user-defined, high-risk protocols can be highlighted.

The interesting aspect of this monitoring is the ability to recognize and track communications between VMs and tag them as application partners. For example, you could determine which Web server VMs are talking to a back-end database server and decide whether or not it was approved traffic.

The documentation says this information can then be used by VNF, which, according to the Altor website, is scheduled for release later this year.

Effectiveness D

The absence of VNF is the VNSA's Achilles' heel: You can't really do anything meaningful with the very valuable data it collects. You can't allow/disallow communication between identified partners or generate alerts.

VNSA keeps a historical database of activity that can be queried ad hoc via Altor Center, but any such reporting must be done directly via the Web GUI in real time.

This leaves a lot to be desired for large VMware environments with numerous groups requiring varying levels of access and reporting, particularly for regulatory compliance. There is a definite need to provide management with dashboard-style "are we compliant?" reports.

Verdict

Altor has significant work to do—adding acceptable enterprise-level reporting and enhanced alerting/IDS.›

For an extended online version of this review, see this month's issue on SearchSecurity.com.

SSL VPN

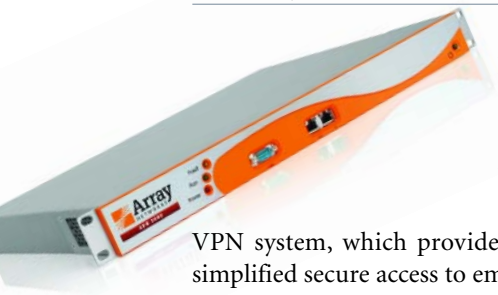
SPX2000

REVIEWED BY ADAM HOSTETLER
AND BRENT HUSTON

Array Networks

www.arraynetworks.net

Price: **$4,995**



Array Networks' SPX2000 VPN appliance is a full-featured VPN designed for small- and medium-sized businesses.

It's a cost-effective SSL VPN system, which provides users with flexible and simplified secure access to email, file shares and chosen applications. The SPX2000 is a plug-and-play solution that enables quick and efficient configuration of VPN parameters and provides a high-performance "in-office" experience for an increasingly mobile workforce.

The SPX 2000 stacks up well against the competition, competitively priced with up to 500 concurrent connections, which is more than most SSL VPN appliances that are designed for the small- and medium-sized business market.

Setup and Management B

Setting up the device does not take much effort, but could be simpler, especially for people who don't have a background in Cisco-like interfaces. However, we completed the first part of the device setup without looking at documentation.

The first step requires connecting to the device via serial cable and using a terminal program (such as Windows HyperTerminal).

Having Cisco terminal experience will make this part easier. Once the interfaces are configured, you're able to log in to the Web application to continue the configuration.

We would have found it very helpful to have an LCD screen and controls on the front of the appliance that could configure the addresses, then complete the rest of the setup through the Web interface.

The Web GUI is set up well, and we found it quite easy to figure out, thanks in large part to built-in PDF help documents, which are available through the interface. The only issue we encountered with the GUI was that it would sometimes become unresponsive, requiring us to log in again. We weren't able to track down the issue, but it was an annoyance.

Many companies will like having Array Networks' embedded NAC-like function, which verifies the integrity of the endpoint, including antivirus software, personal firewall, service pack, and patch/hotfix policies. Needless to say, this adds some of the complexity that comes with the territory, but is an attractive feature for companies looking to implement NAC capability.

Function B+

Setting up a "virtual site" for client connections is easy, but there are many options available. We were pleased to see many authentication methods are supported, including RSA SecurID, RADIUS, LDAP, Active Directory and a built-in local database. We used AD, which was easy to set up.

There's enormous flexibility through the use of virtual sites, which can be configured to access different resources within your organization, such as different business units, offices and departments. For example, you may have one virtual site that connects to human resources, and another separate site that connects to various IT groups.

The policy options are extensive. Virtual sites can use different authentication methods based on policy that requires weaker or stronger controls, so one virtual site could require AD, another RADIUS. You can have multiple methods for each site as well. Granular user access can be defined through the "AAA authorization" function.

There are also several ways to access resources via the virtual sites. Simple Web access, file access (CIFS and NFS), mail services, thin client (using Citrix or other thin client technology) and a Layer 3 SSL VPN are available. There is a client for Windows as well as Linux for the Layer 3 VPN client. All of the access types were simple to set up, and they all work well.

Verdict

The reasonable cost and relative ease of use provide a mix that will work well with most any small- or medium-sized organization.

Testing methodology: We tested the SPX 2000 with Windows XP and Windows Vista clients.

WEB SECURITY

Network Composer

REVIEWED BY JOEL SNYDER

Cymphonix

www.cymphonix.com

Price: **$1,095 to $27,995, depending on model**

Network Composer is a security and visibility appliance focused on controlling and monitoring end user traffic passing through the network perimeter to the Internet. We tested the DC10, Cymphonix's smallest appliance, supporting 250 users.

Administration/Management B

Network Composer classifies users (or systems) into groups, to which it applies rules. Rules can include application blocking and traffic shaping, as well as antimalware threat protection and URL-based content filtering.

It strikes a good balance between too much flexibility and ease of use, with a strong set of default policies and groups. For example, it defines seven groups, ranging from "deny access" to "monitor only," in which you can move users and systems, all with predefined access control policies.

Groups can be defined based on the normal IP and subnet definitions you'd expect, or user information stored in Active Directory, which requires a small client on each workstation.

The Web-based management system requires Internet Explorer and refuses to run with Firefox. Deployment is simple, because Network Composer sits transparently between the end user network and the perimeter firewall.

As long as you stick with the 14 built-in categories, such as "Web filter and anonymous proxy guard" or "Web filter plus IM plus SSL filter," setting things up for control and management is easy.

We pushed a little harder into customizing existing policies and ran into a poorly designed GUI (with some bugs) that discourages the effort. We also found some design limitations around VLANs, which are not supported, and large networks, because only static routing is supported.

Testing methodology: We put the DC10 into a live network between a group of 150 DSL users and the Internet in monitor-only mode for one week and evaluated the network visibility aspects of the product. Then, we ran specific tests to evaluate the security protection capabilities of the DC10.

Security and Control C+

Network Composer did a great job of catching viruses and malware from our library of recent samples, as long as we downloaded using HTTP over port 80.

In normal protection mode, Network Composer misses threats on non-standard ports and for other protocols, such as SMTP and FTP. However, if we put the Network Composer into strict blocking mode, it identified non-standard HTTP and blocked it—viruses or not

A nice feature is the ability to scan HTTPS traffic, but look for those high-end models with encryption acceleration if you want to use this feature. Network Composer can intercept SSL-encrypted traffic and splice together two connections to enable it to decrypt and scan traffic. This all depends on the system manager giving Network Composer a digital certificate.

Control features include the standard gamut of URL filtering (with the option to add your own block list and pass lists) and detection of other filtering avoidance techniques such as anonymous proxies, as well as traffic shaping and specific application blocking.

Visibility A

Network Composer shines in its ability to give visibility into network traffic. It slices and dices by user and user group, by application, usage level and threat. It gives amazing visibility into traffic and usage, such as where your Internet bandwidth is going, what people are saying via IM and what applications are running,

Network Composer provides this information through its Web-based dashboard, for real-time information and drill-down, as well as through a reporting system that lets you run short-term or long-term reports whenever needed. A library of common report templates comes preloaded, or you can define your own reports.

Verdict

Network Composer is well suited to organizations looking to gain strong visibility into network traffic, and to supplement an existing firewall and antivirus tools.›

For an extended online version of this review, see this month's issue on SearchSecurity.com.

WEB SECURITY

Finjan Vital Security NG-5000

REVIEWED BY SANDRA KAY MILLER

Finjan

www.finjan.com

Price: **Starts at $22,340 for 1,000 users, one-year subscription**

There have been a variety of changes since we reviewed Vital Security in September 2005. It sports a much improved GUI, with streamlined navigation and configuration wizards. Web filtering engines provide stronger detection, offering a choice between Websense and IBM Proventia.

Installation/Configuration A

Following the excellent documentation, we initialized the appliance through a shell command line interface, choosing to do host management, scanning and reporting on the same box. The appliance can be used as an ICAP server to work with caching proxies.

The improved Web-based GUI offers a clean tabbed layout for managing users, policies, logs and reports, and administration. The help tab provided quick access to an extensive knowledge base. We really like the dashboard, which offers one-click access to quickly assess the overall status of traffic on the network.

Policy A-

We love the choice between simplified and advanced security policies. Vital Security ships with several predefined security policies—basic, medium, strict, emergency and X-ray.

The first three are part of the simplified security policy. The emergency policy is attached to a panic button that would lock down traffic in the event of a severe Internet virus outbreak. The X-ray policy allowed us to test policies prior to going live.

Advanced security policies let us create much more granular rules and conditions regarding how active content is handled, but we found it challenging to correctly place our rules in the cascading security policies tree so they performed correctly.

There are multiple options for handling flagged content. The most lenient is to allow it. We could also temporarily block content through the coach option, which flashed a warning message to the end user. You configure a custom message for blocked content.

Alerting, Logging and Reporting B-

Although Vital Security provides extensive logging capacity—more than enough to satisfy compliance requisites—the reporting features were weak. The generic report templates lacked good customization capabilities.

While there is extensive alerting for system, application and update events via email and SNMP, we would have liked to see similar capabilities for serious policy violations or blocked event thresholds.

Logging properties allowed us to determine from what devices logs would be gathered. We could enable and configure syslog data, which could easily be sent to a SIM/SEM, and archiving options for location and scheduling. Report data can be stored only on a weekly or monthly basis.

Effectiveness A

Vital Security offers the ability to repair HTML security issues while providing access to content. For example, it stripped out ads leading to URLs hosting known spyware, leaving access only to legitimate content.

Relying on leading antivirus engines (Sophos, Kaspersky Lab and McAfee), Finjan's signature-based protection delivered full coverage against all of our malicious code samples. Vital Security also utilizes behavioral analysis to identify and block zero-day threats and virtual patching for common applications with known vulnerabilities. Websense and IBM Proventia provide effective and granular URL filtering.

Vital Security's rollback capability allowed us to set up an automatic backup schedule to securely transfer our policies and system settings.

Verdict

Finjan Vital Security is a scalable security solution that can effectively protect networks of all sizes from the increasing pressure of Web-based crimeware and enforce corporate Internet policy.

Testing methodology: We tested Vital Security on an Internet-facing network and subjected workstations to a variety of attacks.

For an extended online version of this review, see this month's issue on SearchSecurity.com.

WIRELESS NETWORK SECURITY

HotPick INFORMATION SECURITY®

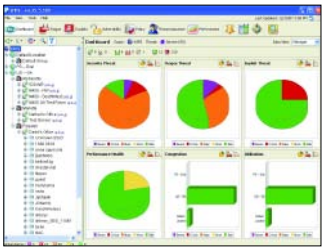
AirDefense Enterprise 7.3

REVIEWED BY SANDRA KAY MILLER

AirDefense

www.airdefense.net

Price: **Starts at $7,995**



There have been numerous updates since we last examined AirDefense Enterprise in March 2006 (Motorola recently announced it will acquire AirDefense). Notable improvements for this wireless intrusion detection/prevention tool include support for Power over Ethernet (PoE) for its sensors, an improved user interface, overhauled reporting and new features such as WEP cloaking, advanced forensics, spectrum analysis and a centralized console to manage appliances.

Installation/Configuration A-

The startup wizard led us through system settings, network structure, user account creation, policy definition, configuring alarms, automated event classification, notification and identifying access points. This was the easiest deployment method, as the documentation for the server and administrator is weak.

You can also restore a saved configuration or perform manual configuration.

Administration is much improved, thanks to distinct management roles. We created administrators, who handle configuration/management; managers, who have administrator rights except for editing logs and adding users; network operators, who deal specifically with network operations, including alerts and alarms; and guests, with limited manager/network operator functions.

Administration roles can be limited through domain-based partitioning, which restricts access to different networks, groups and devices. Users can be authenticated locally through the AirDefense server or through remote RADIUS or LDAP servers.

Testing methodology: We tested the product by deploying the appliance and wireless sensor on an 802.11 network utilizing 802.11a, b and g devices.

Policy A

AirDefense Enterprise includes a comprehensive set of default policies. Custom policies are easily configured through the Policy Manager, from which we could quickly view the associations, behaviors and protocols (a, b, g) of all locations, groups and devices.

There are four basic policy types: configuration, performance, vendor and channel. The first three apply to access points and the fourth to the sensors. The channel policies are the most powerful, offering granular control over when specific channels are allowed on the network.

Logging and Reporting A

Extensive logging and reporting provides access to real-time information and historical data in syslog format.

Web Reporting is suitable for the manager role, with access to standard report templates, previously published reports and frequently run reports.

Administrator and network operator roles have much greater control over content with the Report Builder, which can be used to create reports from scratch or templates.

Effectiveness A

Three new features (optional modules) stand out.

Advanced Forensics covers troubleshooting network anomalies and digs deeper into security-related events.

The Spectrum Analysis tool provides background and dedicated spectrum scanning through the sensors. We were able to locate and identify sources of interference from other wireless networks, as well as non-network devices such as microwave ovens.

Live View offers a real-time observation of sensors, APs and users—data, connections, devices and frames—as well as graphical charts for at-a-glance analysis.

WEP cloaking protects organizations that still use that vulnerable encryption protocol. WEP cloaking generates "chaff" frames to confuse common sniffing and WEP-cracking applications.

The wireless traffic detection sensors are a huge improvement, as the model we tested solely utilizes PoE.

Verdict

AirDefense is a comprehensive, cost-effective solution for protecting and troubleshooting WLANs.

For an extended online version of this review, see this month's issue on SearchSecurity.com.