

PLUS: UTM Should NOT = Unnecessary Threat Management

# INFORMATION **S**ECURITY<sup>®</sup>

## CONTROLLING PRIVILEGED ACCOUNTS

Regulatory requirements and economic realities are pressuring enterprises to secure their privileged accounts. Applied correctly, technology can help offset the risks.

### ALSO:

Time to push DNSSEC over the deployment and political hump



# contents

## FEATURES

### 13 Controlling Privileged Accounts

**ACCESS CONTROL** Regulatory requirements and economic realities are pressuring enterprises to secure their privileged accounts. Applied correctly, the technology can help offset risks. **BY MARK DIODATI**

### 20 Has the Time Come?

**EMERGING THREATS** DNSSEC brings PKI to the Domain Name System and prevents dangerous cache poisoning attacks. Implementation difficulties and political battles, however, keep it from going mainstream. **BY MICHAEL S. MIMOSO**

### 29 UTM Should NOT = Unnecessary Threat Management

**NETWORK SECURITY** Buying the right unified threat management appliance means knowing what—if anything—you actually need beyond a firewall. **BY NEIL ROITER**

### 7 PERSPECTIVES

#### Wrestling Match

Data protection and compliance teams battle for resources but need each other to succeed.

**BY RANDALL GAMBY**



## ALSO

### 3 EDITOR'S DESK

**Hey Google: Do the Right Thing** **BY MICHAEL S. MIMOSO**

### 9 SCAN

**ISP Shutdown Latest Cat-and-Mouse Game with Hackers**  
**BY ROBERT WESTERVELT**

### 11 SNAPSHOT

**Light at the End of the Tunnel?**

**38 Advertising Index**



# Database security and compliance made simple.

More Global 1000 companies trust Guardium to secure their critical enterprise data than any other technology provider. We provide the simplest, most robust real-time database security, and activity monitoring solution for:

- Protecting Oracle EBS, PeopleSoft, SAP and other sensitive data.
- Preventing SQL Injection attacks.
- Enforcing change controls & vulnerability management.
- Blocking privileged users such as outsourced DBAs from accessing sensitive data.
- Automating compliance reporting & oversight.

For more information, visit [www.guardium.com/ISM](http://www.guardium.com/ISM)

© 2009 Guardium. All rights reserved.

**Guardium**<sup>®</sup>  
SAFEGUARDING DATABASES™



# Hey Google: Do the Right Thing

BY MICHAEL S. MIMOSO

Security's leading thinkers ask Google to turn on HTTPS by default for Gmail, Docs and Calendar.

## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### PRIVILEGED ACCOUNTS

### DNSSEC

### UTM

### SPONSOR RESOURCES

**GOOGLE'S CREDO** is "Do no evil." Some of the best security minds in the industry are imploring Google to do the right thing when it comes to the security and privacy of its free email and productivity application offerings.

In case you missed it, 38 security thinkers and researchers wrote an 11-page letter to CEO Eric Schmidt [<http://files.cloudprivacy.net/google-letter-final.pdf>] asking him to enable HTTPS encryption on Gmail, Google Docs and Google calendar by default. That list of 38 is a roll call of security pioneers and current thought leaders, everyone from Gene Spafford, Steve Bellovin, Bill Cheswick and Bruce Schneier to white hats RSnake, Joe Grand and Jeff Moss. They point out that Google's current insecure default settings put the privacy of its cloud-based services users at risk.

"Anyone who uses these Google services from a public connection (such as open wireless networks in coffee shops, libraries, and schools) faces a very real risk of data theft and snooping, even by unsophisticated attackers. Tools to steal information are widely available on the Internet," the letter says.

Already, researchers have successfully developed tools to steal authentication data stored in cookies that are by default sent without encryption to and from Google's servers. Researcher Mike Perry's Cookiemonster <http://fscked.org/projects/cookiemonster> debuted at DefCon two years ago as did Robert Graham's Hamster Wi-Fi cookie stealer <http://erratasec.blogspot.com/2008/01/more-sidejacking.html>. Both tools swipe unencrypted authentication data found in cookies and allow the attacker to pose as the victim.

Google has known about these flaws for close to two years now and has released a configuration option that, should a user choose, turn on HTTPS. The group of 38, however, dares you to try to find it in the Settings option of Gmail, for instance (Hint: there are 13 settings on the General screen; HTTPS is the last one and it's under Browser Connection).

## Four Things Google Needs to Do

The 38 security experts who co-signed a letter to Google CEO Eric Schmidt made four recommendations:

1. Place a link or checkbox on the login page for Gmail, Docs, and Calendar, that causes that session to be conducted entirely over HTTPS. This is similar to the "remember me on this computer" option already listed on various Google login pages. As an example, the text next to the option could read "protect all my data using encryption."
2. Increase visibility of the "always use https" configuration option in Gmail. It should not be the last option on the Settings page, and users should not need to scroll down to see it.
3. Rename this option to increase clarity, and expand the accompanying description so that its importance and functionality is understandable to the average user.
4. Make the "always use https" option universal, so that it applies to all of Google's products. Gmail users who set this option should have their Docs and Calendar sessions equally protected. »

Furthermore, there are no encryption options for Docs and Calendar, and the letter intimates that users may think the Gmail protection extends to the other services. Encryption has to be on by default across the board.

“A large body of scientific research shows that users overwhelmingly retain default options; thus, unless the security issue is well known and salient to consumers, they will not take steps to protect themselves by enabling HTTPS. To deliver on Google’s promises about privacy and security, the company should shift the default option to the more protective HTTPS setting,” the letter says.

The letter also slams Google for not better informing its users the risks of sending their docs and cookies in the clear, and also points out that the performance hit from turning on encryption is negligible. Oh by the way, did you know that Google has turned HTTPS on by default in its Google Health, Voice and AdWords and AdSense offerings?

That’s what makes their decision not to do so for Docs, Gmail and Calendar so baffling. Web 2.0 apps are supposed to be business enablers, but if individuals and/or businesses start losing personal or corporate information via this avenue, the value proposition of Web 2.0 starts looking pretty thin. Two articles in this issue of *Information Security* take a deeper dive into Web security: “Controlling Privileged Accounts,” looks at the need for privileged access control; and “DNSSEC: Has the Time Come?” looks at some of the advantages and hang-ups around adding security to DNS. Check them out.

In the meantime, do the right thing Google; turn on HTTPS by default, listen to the best minds security has to offer and follow their recommendations (*see “Four Things Google Needs to Do,” p. 3*). They know their stuff. •

---

*Michael S. Mimoso is Editor of Information Security. Send comments on this column to [feedback@infosecuritymag.com](mailto:feedback@infosecuritymag.com).*

## TABLE OF CONTENTS

---

### EDITOR'S DESK

---

### PERSPECTIVES

---

### SCAN

---

### PRIVILEGED ACCOUNTS

---

### DNSSEC

---

### UTM

---

### SPONSOR RESOURCES

---

---

**YOU DON'T  
NEED MORE  
SECURITY.  
YOU NEED  
BETTER  
SECURITY.**

---



CA Security Management software streamlines your IT security environment so your business can be more secure, agile and compliant without upsizing your infrastructure. All with faster time to value. Greater efficiency starts with more efficient IT.

*That's the power of lean.*

Learn more at [ca.com/security/value](http://ca.com/security/value)

# COMING IN SEPTEMBER

## 2009 Readers' Choice Awards

*Information Security* and SearchSecurity.com surveyed more than 1,300 readers to determine which products are best at protecting data and networks. Readers only voted on products they had deployed in their company so this listing may help you simplify your information security product buying decisions.

## Encryption Fact and Fiction

While encryption is very effective for certain security problems, it is not a panacea for all security needs. In this feature, Adrian Lane, partner of Securosis, will discuss the practical considerations for encryption, and what to consider when meeting compliance and security goals. We will look at common pitfalls many customers face, and examine trade-offs.

## Easing the Burden of SOX

The cost of Sarbanes Oxley compliance for thousands of smaller public companies is disproportionate, both in terms of percentage of revenue and cost per employee, as opposed to large enterprises. This article will look at how to approach SOX compliance in a midmarket organization, who internally needs to be involved and what resources are at your disposal.

### TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### PRIVILEGED ACCOUNTS

### DNSSEC

### UTM

### SPONSOR RESOURCES

# 7 SECURITY AWARDS

## IT'S TIME TO RECOGNIZE THE INDUSTRY'S BEST

*Information Security* magazine and SearchSecurity.com will again honor innovative security practitioners in seven vertical markets this fall with the fifth annual Security Seven Awards. The awards, to be announced this fall in the pages of *Information Security*, will recognize the efforts, achievements and contributions of practitioners in financial services, telecommunications, manufacturing, utilities, government, education and health care.

While vendor executives are not eligible, we're inviting you to nominate the industry's most innovative practitioners. Nominees must have made a noteworthy contribution to their organization or the security community in areas such as, but

not limited to, research, policy and process development, product development, standards work and community contributions. Individuals must have made an impact on the advancement of, research of, application of and management of information security technologies, policies and practices.

Last year's winners were: Guardian Life Insurance's Mark Sokol; Stanford Hospital's Michael Mucha; Purdue University's Gene Spafford; Rogers Communications' Martin Valloud; the California Office of Information Security and Privacy Protection's Mark Weatherford; Gaylord Entertainment's Mark Burnette; and Motorola's Bill Boni.

Download the nomination form at [www.searchsecurity.com/securityseven](http://www.searchsecurity.com/securityseven) and email it to [securityseven@infosecuritymag.com](mailto:securityseven@infosecuritymag.com).

**NOMINATION DEADLINE: July 25, 2009**



# Wrestling Match

*Data protection and compliance teams battle for resources but need each other to succeed.* BY RANDALL GAMBY

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

PRIVILEGED ACCOUNTS

DNSSEC

UTM

SPONSOR RESOURCES

**IN TODAY'S SECURITY-CONSCIOUS ORGANIZATION**, there is a split between two competing security camps: the policy-driven governance, risk and compliance (GRC) group and the technology-driven data protection group. In the "ring of protection," the GRC camp and data protection camp are locked in a veritable "Smackdown," wrestling for the same buckets of resources and funding for their projects. Ultimately, however, both sides need each other to succeed.

Data protection tools like DLP examine, block and report on unauthorized transmission of data which protects an organization against loss of sensitive and confidential information. In many organizations, they're being deployed as a stop-gap measure while security managers develop and/or refine their long term protection strategies. But how do you configure a DLP service without proper security standards already in place? Vendors may offer "best practice" sets of configuration data, but be cautious: While they can be used as examples of the information needed to configure a DLP service, they generally don't provide an effective set of standards that fit an organization's data protection requirements.

On the other side, GRC activities create the foundational standards that drive security deployments such as data protection. But how do you know they're effective without the feedback data protection tools provide? Surveying managers and workers who handle sensitive data is one way to get feedback, but it's time consuming and not always accurate.

When GRC and data protection activities are both effective and are not in competition with each other, they create an ongoing cycle which benefits both as illustrated:

Business and security requirements + key security events = security standards → local execution → configuration information → data protection and reporting → standards effectiveness feedback → business and security requirements → {cycle begins again}.

So the configuration of a good data protection service relies on good GRC standards and an effective set of GRC standards rely on good DLP services to provide feedback on their effectiveness. While both GRC standards and data protection services are needed, most companies don't have the time or energy to dive into them at the same time. So how does a company decide where to start? Here are some key considerations:

- **Does the organization have a working, clearly defined security standards development process?** This process should take into consideration the organization's business and security requirements and prioritize the results according to the

## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

#### SCAN

#### PRIVILEGED ACCOUNTS

#### DNSSEC

#### UTM

#### SPONSOR RESOURCES

top security and industry or regulatory compliance issues that most affect the organization. The resulting standards should then be communicated down to the local business managers for execution. However, if the organization doesn't have a clearly defined process, then short term, this lack of direction will undoubtedly benefit from technological services like DLP. These services will block, as best as possible without a configuration mapped to the business' security standards, unauthorized access to sensitive information at the business' security boundaries until the process can be formally initiated.

- **Is the organization heavily regulated or constantly "under cyber attack" from outside entities?** Businesses that are under the scrutiny of outside entities, whether legally or illegally (such as large online retailers who are constantly bombarded by cyber attacks), have to be able to monitor the effectiveness of their information boundaries. In this case, deploying tools like DLP is mandatory, even with a lack of security standards.

- **Who owns security?** Is the enterprise managed centrally or is it distributed? Are there political ownership obstacles for security? Centrally managed organizations typically can create good GRC standards that are applicable across the entire organization. But distributed management models can run into political and control issues and usually have to rely on locally generated standards to manage security. This leads the local lines of businesses to protect their limited amounts of sensitive data with locally deployed data protection services.

- **What is the "resource to area of coverage" ratio?** While this isn't necessarily a quantitative number, if you have a limited number of security personnel and large geographic areas or end user populations, strong standards or strong tools will have to be put into place depending on your resources' capabilities. Businesses with limited resources tend to deploy tools first to augment their security team's activities.

So as you examine your business to see which camp you're in, you must look critically at the effectiveness of your GRC standards and data protection efforts. Short term, funding and efforts should be directed at maintaining the stronger components while shoring up the weaker ones. In the end, the standards and services must be in balance to securely protect your information. •

---

*Randall Gamby is an independent security analyst who has worked in the security industry for more than 15 years. He specializes in security/identity management strategies, methodologies and architectures, and has a security and identity management blog at: <http://randallgamby.wordpress.com>. Send comments on this column to [feedback@infosecuritymag.com](mailto:feedback@infosecuritymag.com).*

Analysis | MALWARE

## ISP Shutdown Latest Cat-and-Mouse Game with Hackers

*While the 3FN.Net shutdown had limited impact on cybercriminals, it signaled that the private sector and the government are serious about illegal activity.*

BY ROBERT WESTERVELT



**WHEN THE FTC SHUT DOWN** California-based ISP Pricewert in June, it was only a temporary victory for the U.S. government in the war on cybercrime. Still, the action signaled an important notice to cybercriminals around the world: the feds are watching.

The shutdown of Pricewert, also known as 3FN.net and APS Telecom, occurred on June 5 and spam and phishing campaigns dipped for several days, according to several antispam vendors. But while the ISP went dark, disrupting one of the largest and most active spam botnets known as Cutwail, the blow to cybercriminals was shortlived at best. Experts say those in control of the command-and-control servers likely had a contingency plan in place, acting quickly to regain control of their zombie computers to resume spamming runs and other more nefarious activities.

“What happens is you take out one of the big boys and somebody will take over those customers and start spamming for them,” says Matt Sergeant, senior antispam technologist for Symantec’s MessageLabs.

Despite the ISP shutdown, global spam levels went unchanged in June at 90.4% of all email, according to statistics provided by MessageLabs, which tracks global spam levels. Spam from botnets accounted for 83.2 percent of all spam in June.

Some say the 3FN.net shutdown actually calls into question the ability of law enforcement to have a major impact on cybercrime and of the private sector to effectively police itself. Short-term gains were made late last year when two upstream providers shut down Web hosting service provider McColo, which was notorious for hosting botnet command-and-control servers. ICANN also took action, de-accrediting ISP EstDomains. Several spam bots were disrupted, but months later they either recovered or were replaced by other botnets.

### TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

PRIVILEGED ACCOUNTS

DNSSEC

UTM

SPONSOR RESOURCES

**TABLE OF CONTENTS**

**EDITOR'S DESK**

**PERSPECTIVES**

**SCAN**

**PRIVILEGED ACCOUNTS**

**DNSSEC**

**UTM**

**SPONSOR RESOURCES**

The problem is that the cost to rent a botnet for a single spam campaign is ridiculously cheap, Sergeant says. It takes about \$10 to send 1 million spam email messages.

Still experts say the shutdowns are significant because they send a signal to cybercriminals that governments and those in the private sector are taking illegal activity seriously. They also disrupt other cybercriminal activities. Investigators discovered websites serving up child pornography, malware-laden websites used to conduct drive-by attacks and malicious traffic identified as part of click fraud campaigns. Ultimately, the shutdown increases costs for those who control botnets by interrupting their business activities, says Pete Lindstrom, director of research at Spire Security.

“The value in this is in setting the precedent and making sure that the message is out there that folks doing the wrong thing can be caught and they might be punished,” he says. “It’s not ever going to reduce the amount of spam or significantly reduce the number of botnets. It’s almost impossible.”

But perhaps the next step is to figure out a way to disinfect zombie computers without trampling on a victim’s privacy. The technology is available, but it’s been controversial. Last year, researchers at TippingPoint discovered a way to issue whatever commands they chose to the thousands of bots in the Kraken arsenal, including the ability to order them to self destruct. The possible legal, ethical and technical issues forced them to resist action.

Surely, the security industry will continue to innovate, developing new defenses and services that disrupt cybercriminals. Companies will continue to invest in new security technologies just as cybercriminals will continue to be one step ahead. In other words, this cat-and-mouse game isn’t going away any time soon, says Mary Landesman, a senior security researcher at Web security services vendor ScanSafe Inc.

“When the cost of doing business with criminals is higher than the cost of doing business legitimately,” she said, “then they’ll start doing business legitimately.”

*Robert Westervelt is news editor for SearchSecurity.com Send comments on this article to [feedback@infosecuritymag.com](mailto:feedback@infosecuritymag.com).*

**The problem is that the cost to rent a botnet for a single spam campaign is ridiculously cheap, Sergeant says. It takes about \$10 to send 1 million spam email messages.**

# SNAPSHOT

## Light at the End of the Tunnel?

**THE FINANCIAL SERVICES SECTOR**, which saw the worst of the downturn last year, is starting to see some glimmers of hope when it comes to security expenditures. Still, cybercriminals are taking advantage of the uncertain times and stretched security staffs. —*Information Security staff*

# 45%

Percentage of respondents that expect their security projects on hold to be re-approved in the next six months.

SOURCE: SearchFinancialSecurity.com survey conducted in May; 175 respondents

# \$700,000

Thieves hacked iTunes recently, setting up a fake artist account to use stolen credit card numbers to buy their own music, pocketing more than \$700,000.

# \$5-\$100

Amount for batches of 1,000 malware-infected PCs on the the Golden Cash botnet.

### TABLE OF CONTENTS

#### EDITOR'S DESK

#### PERSPECTIVES

#### SCAN

#### PRIVILEGED ACCOUNTS

#### DNSSEC

#### UTM

#### SPONSOR RESOURCES

OVER-HEARD



**SOX was hastily and badly drafted...If SOX was really effective, would we have seen the subprime crisis in corporate America?**

—Former Securities and Exchange Commission Chairman HARVEY PITT, who once led the implementation of the Sarbanes-Oxley Act (SOX)

# The one security blanket you won't be embarrassed to take to work.



CISA wins *SC Magazine's* Best Professional Certification

CISM named finalist for *SC Magazine's* Best Certification Program

## ISACA® Certifications

ISACA certifications increase your value to employers and clients.

Being a CISA®, CISM® and/or CGEIT®:

- ▶ Counts in the hiring process.
- ▶ Enhances your credibility and recognition.
- ▶ Boosts your earning potential.

Secure Your Career: Get Certified.

Visit [www.isaca.org/infosemag](http://www.isaca.org/infosemag).



# Controlling Privileged Accounts

Regulatory requirements and economic realities are pressuring enterprises to secure their privileged accounts. Applied correctly, technology can help offset the risks.

BY MARK DIODATI



**IN THE WRONG HANDS,** privileged accounts represent the biggest threat to enterprises because these accounts can breach personal data, complete unauthorized transactions, cause denial-of-service attacks, and hide activity by deleting audit data. Privileged accounts, such as the UNIX root, Windows Administrator accounts or accounts associated with database ownership and router access, are required for platforms to function. Moreover, they are required for “break the glass” emergency access scenarios as well as more mundane day-to-day tasks.

While important, they are notoriously difficult to secure because they don't belong to real users and are usually shared by many administrators. However a down economy increases the risk of disgruntled workers abusing the access, making it more important than ever to have a system in place to control privileged access.

What's more, control of privileged accounts is at the top of the auditor's findings list, and is an essential component of compliance mandates associated with Sarbanes-Oxley (SOX), the Payment Card Industry Data Security Standard (PCI DSS), the

## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### PRIVILEGED ACCOUNTS

### DNSSEC

### UTM

### SPONSOR RESOURCES

Federal Energy Regulatory Commission (FERC), and HIPAA. If those mandates aren't enough, many business partners are asking for a review of controls associated with privileged accounts as part of their Statement on Auditing Standards (SAS) 70 reviews.

Let's take a look at the technology and strategies that are available to help organizations can get better control over their privileged accounts.

## Privileged Account Management Tools

Privileged account management products can help mitigate the risks associated with elevated access. These products can help close out audit findings, assist in meeting compliance mandates, and increasingly enable an organization to pass its SAS 70 reviews.

Clearly, privileged account management products have met a need in the enterprise: the product class has experienced explosive growth in the past three years, with the number of customers doubling every year. The number of organizations that have deployed a privileged account management product now exceeds 2,000.

Privileged account management products control access to accounts via two mechanisms. The first mechanism forces the administrator or program to check out the account password and the second mechanism changes the account's password frequently on the target platform. These products also provide some workflow capabilities for approval and follow-up after giving emergency access to a privileged account.

**CHECKOUT METHODS.** Traditional identity management provisioning systems are not up to the task of managing privileged accounts because they lack checkout methods. But privileged account management tools provide two password-checkout methods: interactive and programmatic.

In an interactive checkout, system administrators use the privileged account to access target platforms. Typically, the system administrator authenticates to the privileged account management product via a Web browser session. Once authenticated, the system administrator retrieves the specific account password, then uses the password in an interactive session such as Windows Terminal Services, Secure Shell, telnet, or a SQL client.

Programs also need access to privileged account credentials. Examples of programmatic access include: shell and Perl scripts for the startup, shutdown, and maintenance of target platforms including databases and application servers; services controlled by Windows Control Manager; and configuration files for database and LDAP account connection information. These access methods have traditionally required the embedding of the privileged account management password. The embedding of this password is a significant security risk, because anyone with access to the script or configuration file can steal the password and

### TABLE OF CONTENTS

#### EDITOR'S DESK

#### PERSPECTIVES

#### SCAN

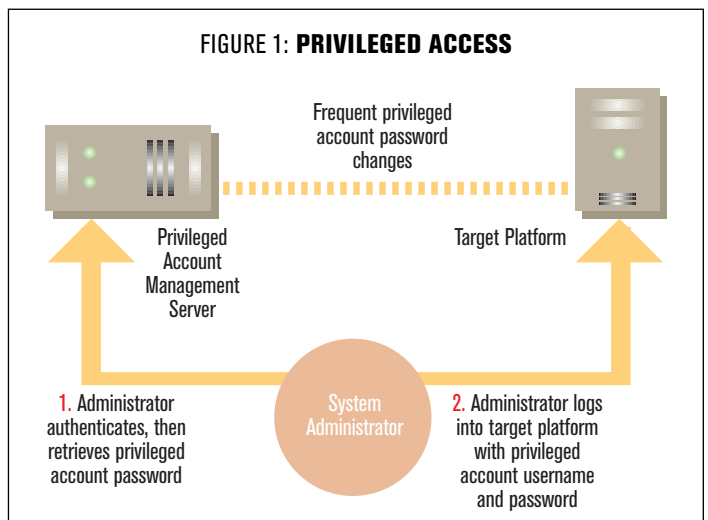
#### PRIVILEGED ACCOUNTS

#### DNSSEC

#### UTM

#### SPONSOR RESOURCES

FIGURE 1: PRIVILEGED ACCESS



use it maliciously.

Privileged account management products have tools to help remove the embedded password, and programmatically retrieve it as needed. Programmatic retrieval requires the installation of privileged account management middleware on the target platform. This software enables the program to retrieve the account password in real-time. In some cases, a Secure Shell client residing on the target platform can be used in lieu of middleware.

The interactive access method is by far the easiest

to secure, and most organizations tackle it first. The protection of accounts via the programmatic access method requires an inventory of all the places where the account password is stored, then replacing it with execution code that retrieves the password on the fly. Shell scripts and Perl files are relatively easy, but other programmatic access methods can require considerable work.

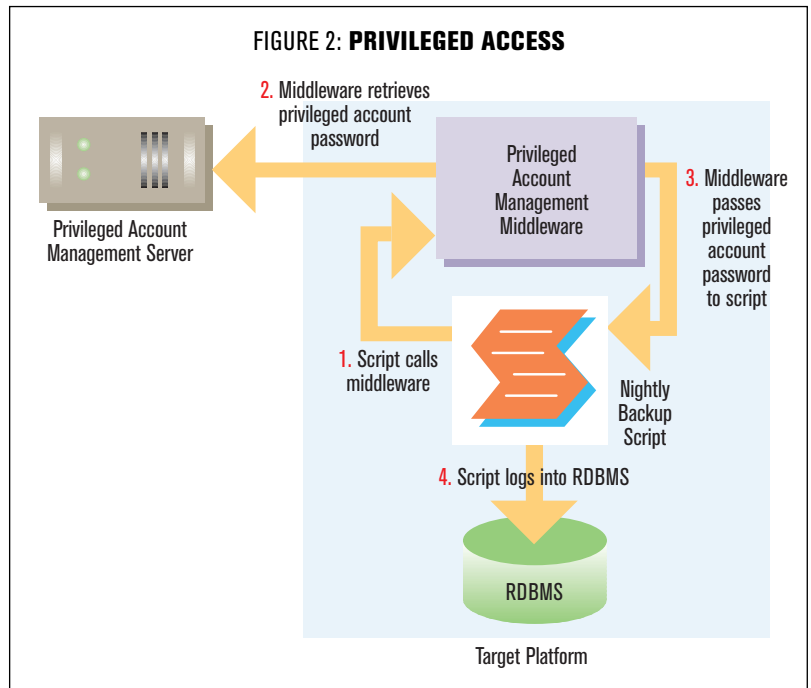
In particular, account passwords embedded in configuration files—for example those associated with application servers—are more difficult because the privilege account management product cannot control when the configuration file is read. Some of the vendors are addressing difficult programmatic access methods like application servers with modules specific to the application server. While tackling programmatic access requires elbow grease, companies that ignore the embedded privileged account passwords do so at their peril; in most cases these accounts can be used for interactive sessions by intruders.

**PASSWORD CHANGE FREQUENCY.** When controlling access by routinely changing an account's password on a target platform, privileged account management products provide organizations with several options, including:

- Never (not recommended but may be required for antiquated target platforms)
- Frequently (configurable, but the range is generally between one to 30 days)
- Per session (otherwise known as the exclusivity option)
- On demand

Most companies opt to frequently change most of the account passwords. Deployments in early stages typically change the password less frequently, for example every two weeks. As deployments mature and an organization gets more comfortable with the privileged account management product, passwords are changed more frequently; daily changes are common.

For very sensitive systems, some businesses implement the exclusivity option. With this



## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### PRIVILEGED ACCOUNTS

### DNSSEC

### UTM

### SPONSOR RESOURCES

option, the system administrator must “check in” the password when done with the session. The benefit of the exclusivity option is that it provides tighter accountability because the checkout can be closely associated with subsequent actions executed by the privileged account. After the system administrator checks the account in, the product randomizes the password. The password randomization effectively means that no system administrator knows the password until it is checked out again. When the next system administrator checks out the account password, she has “exclusive” access to the account. All subsequent activity can now be correlated to this system administrator. Most organizations reserve the exclusivity option for very few high security systems because of its operational limitations: only one user can access target platform via the account at any given time.

The on-demand password change mechanism is becoming increasingly important in these economically turbulent times. When a system administrator’s employment is terminated, timely revocation of access to privileged accounts is essential. The on-demand password change effectively locks the terminated administrator out of sensitive systems, because he no longer has knowledge of the account passwords.

**PRIVILEGED SINGLE SIGN-ON (SSO).** Single sign-on is a recent feature added to privileged account management products. The system administrator accesses the target platform via the privileged account management product’s workstation client software or proxy server. Both mechanisms provide single sign-on because the system administrator is transparently logged into the target platform. Behind the scenes, the privileged account management software retrieves the password and logs the user onto the system via the session protocol (for example, telnet, Secure Shell, and Windows Terminal Services). Enhanced security is an additional benefit because the system administrator does not have knowledge of the account password.

**PROGRAMMATIC PASSWORD CACHING.** Highly distributed production environments such as

## Privileged account management vendors.

Cloakware

Cyber-Ark

e-DMZ Security

Lieberman Software

Passlogix

Quest Software

Symark

## Vendors whose products can delegate UNIX privileges.

CA

Centrify

FoxT

IBM

Novell

Quest

Symark

\*Sudo, a free software program

# Vendors

large retail corporations are at a disadvantage if the account management password cannot be retrieved due to network issues. Additionally, some target platforms use the account password frequently during processing, and the constant retrieval of the privileged account password would bring processing to a grinding halt. Some of the privileged account management vendors have responded by providing the ability to cache the account password on the target platform. Caching introduces additional security risks, relative to retrieving the privileged account password dynamically. However, caching is a much better alternative than leaving the password embedded in files. The account password will be more difficult to steal because it will not be resident in the file, and the password will be changed more frequently.

## Important Considerations

While privileged account management tools can help organizations deal with a tricky security problem, they should be integrated with SIM and identity management systems to be truly effective. In addition, enterprises should leverage any platform privilege delegation capabilities, which reduce the need to give access to privileged accounts in the first place. Important systems also should be physically secured to help reduce the risk of intruders bypassing logical security controls.

**SECURITY INFORMATION MANAGEMENT.** The auditing of privileged account passwords is an essential component of successful compliance initiatives. Most organizations want the ability to determine who checked out the account and when the account was checked out. All of the privileged account management products possess this capability. Additionally, most of the products can forward audit events to the Windows Event Log or a syslog collector.

To obtain full auditing benefits, a privileged account management product usually needs to be integrated with a Security Information Management (SIM) tool. While privileged account management products will happily log all account checkout events, that's only part of the picture. Checkout events need to be correlated with the subsequent actions taken with the privileged account. Some correlation may be possible via Windows Event Log or syslog, but organizations will benefit by spending the extra time integrating the privileged account management tool with an existing SIM tool. In some cases, the product will integrate directly with the SIM tool; in other cases the integration is achieved via syslog or the Windows event log.

**IDENTITY MANAGEMENT.** The integration of a privileged account management product with a provisioning system provides two benefits. The first is timeliness; the provisioning system can make real-time updates to who can access the accounts. The best example is the timely removal of access to all sensitive systems when an administrator's employment is terminated. Another example is removing access to sensitive production resources when the administrator changes job function or location. The other benefit is better security; the provisioning system's role management capabilities can restrict access to privileged accounts to authorized system administrators. For example, only system administrators in Chicago can access the accounts

The auditing of privileged account passwords is an essential component of successful compliance initiatives.

associated with the systems in Chicago.

Most of the privileged account management products have integration with the large identity management vendor provisioning systems. In some cases, an LDAP-based directory server can be used as a conduit between the provisioning and privileged account management systems when formal interoperability does not exist.

**PRIVILEGE DELEGATION.** Target platforms that can delegate privilege to real users can diminish but not eliminate the need for a privileged account management product. For example, the Microsoft Windows platform has good capabilities in assigning privilege rights to users, without giving access to the Administrator account. In general, UNIX platforms have delegation capabilities, but this varies by platform. Many organizations use UNIX security products to delegate privilege and therefore reduce the need for accessing the root account.

Some platforms, such as network routers, don't possess the necessary delegation capabilities. For these platforms, the best option is the use of a privileged account management tool coupled with a SIM product.

**PHYSICAL SECURITY.** Of course, in controlling privileged access, don't forget about physical security. Physical security almost always trumps all logical controls. Ensure that only authorized personnel can access the "raised floor" (that is, the data center) where the target systems physically reside. In some cases, people have general access to the data center, but should not have access to specific systems. In this case, consider a locked cabinet inside the data center.

To be sure, controlling privileged access is an issue that organizations cannot afford to ignore. Failing to secure privileged accounts could mean failed audits and worse, a data security breach with devastating consequences to the business.

---

*Mark Diodati, CPA, CISA, CISM, has more than 19 years of experience in the development and deployment of information security technologies. He is a senior analyst for identity management and information security at Burton Group. Send comments on this article to [feedback@infosecuritymag.com](mailto:feedback@infosecuritymag.com).*

## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### PRIVILEGED ACCOUNTS

### DNSSEC

### UTM

### SPONSOR RESOURCES

**Protecting your most valuable assets.**



**Source**  **Consulting**

**[www.source44.net](http://www.source44.net)**

# HAS THE TIME COME?

DNSSEC brings PKI to the Domain Name System and prevents dangerous cache poisoning attacks. Implementation difficulties and political battles, however, keep it from going mainstream. BY MICHAEL S. MIMOSO

There's a certain Energizer Bunny quality to the Domain Name System. It just goes and goes and goes, usually without much maintenance. Problem is, while it's hassle-free, DNS usually isn't very secure.

Last July, researcher Dan Kaminsky exposed DNS' worst-kept secret. His now famous cache-poisoning bug turned DNS—best known for translating human readable domain names into IP addresses that servers understand—into center stage of the computer security world. The little protocol that could was quickly the biggest problem on the Web. Suddenly, it was relatively easy for attackers to redirect requests to malicious websites where phishing attacks or SQL injections awaited.

## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### PRIVILEGED ACCOUNTS

### DNSSEC

### UTM

### SPONSOR RESOURCES

**TABLE OF CONTENTS**

**EDITOR'S DESK**

**PERSPECTIVES**

**SCAN**

**PRIVILEGED ACCOUNTS**

**DNSSEC**

**UTM**

**SPONSOR RESOURCES**

And aside from an ambitious patching effort, coordinated by Kaminsky, and pulled off by a gaggle of vendors including Cisco, Microsoft, the Internet Systems Consortium (ISC), and others, there was little in the way of a permanent fix.

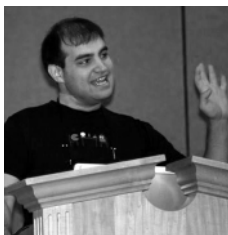
His bug not only kicked off a firestorm of publicity and new disclosure debates, but it cast a glaring light on DNS' shortcomings. It also renewed interest in DNSSEC, or DNS Security Extensions, which are a set of protocols that essentially introduce PKI to the Domain Name System.

DNSSEC is the cure to cache poisoning attacks in the DNS. No one argues the point. It won't fix all the security woes in DNS, but it does check one of the biggest threats to e-commerce and trust on the Internet. Implementing DNSSEC, however, is another matter. Not only does it require a significant infrastructure overhaul for large enterprises and service providers running DNS servers, but a host of political battles are keeping DNSSEC from reaching critical mass.

"DNSSEC is interesting not because it fixes DNS," Kaminsky says, acknowledging that until his bug was made public last July, the DNS protocol wasn't widely well understood; people knew that it just worked. "DNSSEC is interesting because it allows us to start addressing the core problems we have on the Internet in a systematic and scalable way."

## **POLITICS AND SIGNING ROOT AND TOP-LEVEL DOMAINS**

DNSSEC is not new. It's been around for the better part of 15 years, but every single iteration of DNSSEC has run headfirst into oblivion; beaten down by complexity and scalability issues. DNSSEC promises to protect the Internet against cache poisoning attacks such as Kaminsky's (it does not guarantee confidentiality, nor does it protect against denial-of-service attacks). Attackers can poison a DNS cache by exploiting a flaw in the system that prevents a DNS server from validating a website request. Incorrect entries are cached instead and served to others trying to reach that website. Those users are then sent to the attacker's site where the user is infected by malicious code



**"DNSSEC is interesting because it allows us to start addressing the core problems we have on the Internet in a systematic and scalable way."**

—DAN KAMINSKY, security researcher

or tricked into giving up personally identifiable information.

DNSSEC counters that possibility by implementing digital signatures and encryption to DNS lookups. Each lookup adds four new resource record types to a request, according to the dnssec.net website [<http://www.dnssec.net/>]: a resource record signature; DNS public key; delegation signer; and Next Secure, or NSEC. DNSSEC verifies whether the respective keys match the information on the sender's DNS server. If not, the request is dropped.

If it sounds complicated, it is.

But that doesn't lessen the need for it, according to many. In fact, the DNSSEC movement is gaining momentum. Most recently, the .org top-level domain was signed with DNSSEC, joining the .gov TLD, which was signed earlier this year. Sweden's .se top-level country code domain has for years been signed, as have some banking

domains in Brazil. DNSSEC, however, won't reach Jon and Kate proportions of critical mass until the .com domain is signed, as well as the Internet's 13 root zone domains.

"You need root signed, you need .com signed; bottom line," Kaminsky says. "That is not a situation that can remain in the long term. [Signing] .com is huge, and it's a major technical challenge to figure out how to sign it."

VeriSign controls the .com and .net domains, as well as two server clusters that make up root domains. IANA (Internet Assigned Numbers Authority) manages IP address allocation and manages the root zone. IANA, a subset of ICANN, decides what goes into the root zone, DNSSEC included, and works closely with VeriSign which manages the server clusters that produce daily zone files that are passed along to name server operators.

VeriSign announced in February that it would sign .com with DNSSEC by 2011. VeriSign declined to be interviewed for this article. Many expect the signing of .org and .gov with

## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### PRIVILEGED ACCOUNTS

### DNSSEC

### UTM

### SPONSOR RESOURCES

## NEXT STEPS

# PIR Moves Cautiously with .org Domain Signing

**The Public Interest Registry plans up to a year of beta testing DNSSEC on the .org domain.**

The Public Interest Registry (PIR) [<http://www.pir.org/>], which manages the .org domain—the latest top-level domain signed with DNSSEC—says the move is a foundational element that will enable the development of secure applications and enhanced trust on the Internet.

"DNSSEC, as an extension to DNS, is the best way to authenticate sites effectively," says Lance Wolak, director of marketing and product management for PIR. "It's the best method because it extends DNS' capabilities; DNS is proven by far to be a great platform to build apps, and remains today a very open and sound architecture."

The PIR announced on June 3 that the .org TLD had been signed, and for the next six months to a year it will beta test DNSSEC extensions. It is the latest generic TLD to be signed with DNSSEC, .gov was signed in February.

"We're going out in a careful, responsible manner with the .org zone and testing DNSSEC with test domains that are not connected to actual live sites," Wolak says. "We'll start with test domains, and then once we are satisfied, we'll move on to public facing domains and continue to broaden that circle of what testing."

The PIR, which chairs the DNSSEC Industry Coalition, applied last March with ICANN to sign the zone with DNSSEC; that application was approved in June 2008. Along with asking for help from coalition members, PIR also reached out to other registries, including Sweden, that had done DNSSEC rollouts.

"We felt it was important to share implementation plans with others of similar interest," says Lauren Price, coalition chair. "We've gone as far to share our implementation guidelines across registries. This is an industry-wide upgrade to DNS; it's important to have a level of consistency in how we roll it out." •

—MICHAEL S. MIMOSO

**TABLE OF CONTENTS**

**EDITOR'S DESK**

**PERSPECTIVES**

**SCAN**

**PRIVILEGED ACCOUNTS**

**DNSSEC**

**UTM**

**SPONSOR RESOURCES**

DNSSEC to further illuminate the need to shore up DNS security (*see "PIR Moves Cautiously with .org Domain Signing," p. 22*).

"Having the top-level domain signed is really important, but really, the most critical thing is having the root signed," says Ram Mohan, executive vice president and chief technology officer of Afilias, service provider for the .org domain. "Having the root signed ensures that you can have a complete, trusted chain in the entire ecosystem.

"Most of it has to do with how one looks at DNS. Today, DNS is incredibly vulnerable and pretty open to cache poisoning and the Kaminsky-type attacks in spite of all the patches," Mohan says. "If you don't fix the problem, I fear that in a short while, we're going to have attacks the size and scale we've never seen before. Signing the .org TLD is a symbolic and important milestone along the way."

While the technology challenges are steep, the political ones may be at a sharper incline.

"The amount of data at the root is small enough that signing it is no big deal," says Paul Mockapetris, the man who invented DNS in 1983. "The technology problems are trivial. The political problems are a mess."

Mockapetris, board chairman at Nominum, a network naming and addressing provider and original developers of BIND 9 and ISC DHCP3, has watched DNSSEC wallow in discussions around standards and political tugs of war. The crux of the political issue is control over the encryption keys that will sign the root. Who holds the keys? What crypto systems and algorithms will be amenable to all nations? Digital signatures that work in the U.S., may not be acceptable in Russia or in Asia Pacific. These are complicated questions all around.

"We need to figure out how to disperse authority and share control," Mockapetris says. "Having one authority based in one nation, you won't get long

term buy-in from everyone else. The problem with DNSSEC is that it is oriented toward having one party in charge, and they all think they should be." (*See "Call for Alternatives," p. 24*).

Mockapetris fears that while the Kaminsky bug forced ISPs and enterprises to patch a serious vulnerability, that people won't be resolved enough to send necessary money and resources toward DNSSEC without an extensive, tangible attack.

"My personal position is that in order to get DNSSEC to happen widely, you have to have a billion-dollar attack," he says. "Right now, the message is still 'there's a vulnerability out there.' But people are more concerned with other things. I don't think [DNSSEC] was designed to make it easy to deploy. People have been at this for 15 years in many versions. To some extent, they haven't been able to make hard compromises to make it easy deploy. That is part of the problem as well."

**"If you don't fix problem, I fear that in a short while, we're going to have attacks the size and scale we've never seen before. Signing the .org TLD is a symbolic and important milestone along the way."**

—RAM MOHAN, executive vice president and chief technology officer, Afilias

# A Call for Alternatives

Some researchers are hesitant about compulsory use of DNSSEC.

Not everyone is jumping on the DNSSEC bandwagon.

There are some holdouts who believe caution should be taken before diving headfirst into DNSSEC deployments.

"I think that DNSSEC is over-engineered and it's trying to impose PKI on DNS; there are advantages and disadvantages to that," says Ivan Arce, chief technology officer at Core Security Technologies. "If we use DNSSEC, it's not because it's the best thing, but because there is no other thing."

Arce raises concerns about complexity and the bloat of DNSSEC code intertwined with the political issues haunting deployments at the root and TLD levels.

"Part of this hesitancy around DNSSEC is that it heavily relies on crypto magic; when you have a security problem, sprinkle a little crypto on it, and it will be resolved," Arce says. "If you think about it, the paradigm it proposes is a thing of the past. PKI—it's very early '90s, and it didn't catch up. It requires a lot of code to implement it and a lot of operational overhead as well. It's also a business as well; there's money to be made on DNSSEC. I'm not saying it's not going to work, but I would rather see a more open discussion about alternatives."



Ivan Arce

DNSSEC requires an infrastructure overhaul, but not different than other overhauls enterprises are regularly faced with; the Kaminsky patch last year required a significant investment in time and resources to ensure it did not impact critical systems and applications.

"If there's a way to adapt the current protocol to enforce some basic security mechanisms and not boil the ocean to solve everything, I think that would be sufficient rather than changing the DNS infrastructure of the entire Internet," Arce says. "The point I'm trying to make is that we don't know how much discussion there has been about alternatives. Imposing PKI on that may solve some problems, but it's not a guarantee it will solve DNS security. There hasn't been an open discussion to do so."

In fact, the introduction of DNSSEC exposed a new security vulnerability known as zone walking. DNSSEC exposes private information about a network housed in the DNS. Attackers gaining access to this information would benefit from knowing the list of machine names in a particular zone; DNS is configured in such a way that users are not allowed to access this information. DNSSEC must be able to report when names are not found in a zone, therefore it must have access to the information.

The answer has been to use a protocol known as NSEC3 to obfuscate the contents of the domain, says Shane Kerr, BIND 10 program manager for the Internet Systems Consortium [<https://www.isc.org/downloadables/11>]. Kerr says NSEC3 is leading edge technology; the .gov domain was signed with DNSSEC earlier this year and also used NSEC3. Kerr says there were instances where users had difficulty reaching .gov websites because of it.

"It requires more computation on the server side for queries," Kerr says. "Normal DNSSEC looks up a name and if it doesn't exist, you get a pre-computed answer signed back that it does not exist. With NSEC3, it takes a crypto hash of that query. If you look up ABC.com, you would not get the pre-computed answer, but you'd get an MD5 hash back."

Paul Mockapetris, the inventor of DNS in 1983, agrees that DNSSEC doesn't necessarily have to immediately be used on a wide scale. With DNS now routing email, VoIP phone calls and many other types of network traffic, why not push DNSSEC toward specific applications?

"Nothing says with DNSSEC that the whole space has to be signed," Mockapetris says. "We can figure out how to sign all phone or RFID data, or your own intranet. Most don't understand that a lot of DNS data on the Internet, billions of pieces of information, five times more of that is private behind firewalls. Maybe DNSSEC could catch on in limited contexts, then as we get more tools and experience, it could go more mainstream. That's my hope for it."

Arce, meanwhile, says DNSSEC goes against the open nature of the DNS. By adding PKI, you're essentially transferring control over it from the DNS operator to whomever controls the encryption keys.

"DNS problems have been known for a decade. There has not been as much visibility with policy makers or IT managers, but security experts have known DNS is broken, and known that for more than a decade," Arce says. "It's good that someone is actually paying attention, however I think the solution is not just to react and force compulsory deployment of DNSSEC."

—MICHAEL S. MIMOSO

## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### PRIVILEGED ACCOUNTS

### DNSSEC

### UTM

### SPONSOR RESOURCES

**TABLE OF CONTENTS**

**EDITOR'S DESK**

**PERSPECTIVES**

**SCAN**

**PRIVILEGED ACCOUNTS**

**DNSSEC**

**UTM**

**SPONSOR RESOURCES**

## COMPLEXITY, SCALABILITY IMPEDE DNSSEC DEPLOYMENTS

Many large enterprises run their own DNS. Many companies outsource their DNS needs to a service provider. DNSSEC is gaining momentum in verticals such as financial services, telecommunications and the government with .gov. Deployments in the U.S. are expected to ramp up as products mature and help automate deployment and key management of DNSSEC.

Unlike DNS, which can essentially be set and forgotten, DNSSEC must be babysat. There are free and open source tools available for an enterprise that wishes to deploy DNSSEC manually.

“You have to generate keys; you have to insert the keys into a zone file, sign the zone and then push the signed zone to slave servers,” explains Mark Beckett, vice president of marketing for Secure64, a provider of zone signing and key management software.

When cryptographic signatures are generated, they are good only for a certain period of time. They must continually be re-signed and frequently (weekly or more frequently) regenerated. Key values must be changed and key rollovers done periodically.

“If you run your own DNS, you have a lot of options already. You can secure it tomorrow depending on how thorough you want to do it: you can go to extremes and buy a hardware security module to store keys, and develop procedures to secure keys,” says Shane Kerr,

BIND 10 program manager for the Internet Systems Consortium, which manages BIND, the most common DNS software in use today.

“For the average organization, you don’t need to be more secure with DNS than you do with Web pages. If you run SSL on a page, you probably want to look into DNSSEC as well and leverage existing procedures to have similar levels of security,” Kerr says. “It depends on the type of technology you use; if you run BIND, you can use DNSSEC out of the box; plus there are a number of commercial products you can buy that run DNSSEC.”

All of this adds operational complexity.

“It’s not just set it once and forget about it,” Beckett says. “This is a big break from the way we tended to manage DNS in the past. With DNSSEC it’s a much more active process.”

That means educating DNS operators and registrars, some of whom are not incented enough to pursue DNSSEC because they offer free DNS to customers, to understand the security issues and responsibilities associated with managing DNSSEC.

“Simplification is the key here,” says Afilias’ Mohan. “We hear complaints about how geekified DNSSEC is; keys, zone signing and key rollover. These are mind-numbing terms. What is the real benefit? That has been missed.”

“The situation was that this is another solution in search of a problem. The Kaminsky vulnerability defined the problem. We’ve got to get to the point where we clearly explain this solves DNS hijacking, not data integrity not data confidentiality, not phishing, not pharming. This ought to be a straight line. Everyone is going to have to face this problem of having their domain traffic hijacked. If we solve it with one good solution that works well, it’s DNSSEC,” Mohan says

Kerr says ISC’s next release BIND 9.7 aims to simplify DNSSEC use.

“For the average organization, you don’t need to be more secure with DNS than you do with Web pages.”

—SHANE KERR,

BIND 10 program manager, Internet Systems Consortium

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

PRIVILEGED ACCOUNTS

DNSSEC

UTM

SPONSOR RESOURCES

“Right now, the software implements all of the standards, but not in an easy-to-use way,” Kerr says. “One of big hurdles is that this is something you don’t want the average admin to have to configure. There’s a lot of work with UNIX command lines and ugly crypto strings that don’t fit on the screen. We’re hoping to make that simpler.”

Beckett says large service providers such as cable and broadband providers are asking specific deployment questions around DNSSEC. Some began piloting DNSSEC in the months following the Kaminsky bug disclosure and are trying to understand some of the operational issues around deployments.

“What I’m seeing is some of the bigger service providers actively looking for ways they can offer secure DNS services to their federal customers first of all,” Beckett says. “Some have broader horizons than that. Large cable or DNS providers are worried about consumers and how to protect them as more zones and domains become signed.”

### DNSSEC AS A BUSINESS ENABLER

Dan Kaminsky sees a bigger picture with DNSSEC.

He sees it as the cornerstone of Internet trust and the springboard for a new wave of products that scale across organizational boundaries in a secure way.

“The reality is that trust is not selling across organizational boundaries,” Kaminsky says. “We have lots and lots systems that allow companies to authenticate their own people, manage and monitor their own people and to interact with their own people. In a world where companies only deal with themselves, that’s great. We don’t live in that world and we haven’t for many years.”

Data in the Verizon 2009 Data Breach Investigations Report [[http://www.verizonbusiness.com/resources/security/reports/2009\\_databreach\\_rp.pdf](http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf)], released in April, indicates that 60 percent of hacks are due to authentication flaws, usually around passwords being stolen or ineffective. Still, passwords remain the most common authentication method because they work across organizational boundaries, and they scale well.

By putting DNSSEC into DNS, a system doing cross-organizational address management for 25 years, Kaminsky sees boundless opportunities for trust and business enable-

ment. (Read this interview with Dan Kaminsky, [http://searchsecurity.techtarget.com/news/interview/0,289202,sid14\\_gci1360143,00.html](http://searchsecurity.techtarget.com/news/interview/0,289202,sid14_gci1360143,00.html))

“DNS works. It’s the world’s largest PKI without the ‘K.’ All DNSSEC does is add keys. It takes this system that scales wonderfully and been a success for 25 years, and says our trust problems are cross organization and we’ll take best technology on the Net for cross-organizational operations and give it trust,” Kaminsky says. “And that if we do this right,

“DNS works. It’s the world’s largest PKI without the ‘K.’ All DNSSEC does is add keys.”

—DAN KAMINSKY, security researcher

we’ll be able to see every single company with new products services around the fact there’s one trusted root, and one trusted proven system doing security across organizational boundaries.”

Indeed, DNS does more than IP address translation. It routes email, VoIP traffic and even RFID traffic, for example. Kaminsky believes that DNSSEC will force companies to escape the current security paradigms that were designed for a single organizational boundary.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

PRIVILEGED ACCOUNTS

DNSSEC

UTM

SPONSOR RESOURCES

# “I did the basement and the first two floors. In 25 years since, people have been adding stuff on top of it.”

—PAUL MOCKAPETRIS, board chairman, Nominum

“How many people have bought products that worked great in the lab and for a few groups, and once they try to scale it out, oops it doesn’t work and you’ve gotta shelve it,” Kaminsky says. “I’m tired of that happening. I’m tired of systems engineered just enough to make the sale. I want to see systems scale larger than the customers they’re sold to.”

Kaminsky admits he wasn’t always backing DNSSEC. But the research he did on DNS following the discovery of his bug made him realize the levels of connectivity between organizations that DNS affords and how with a relatively simple attack he could access volumes of Web-based data simply by corrupting DNS. He wants organizations to break away from password-based trust models and absorb the one-time cost on DNSSEC, and realize that cost can be amortized across every Web-based project an organization takes on.

“People will deploy insecure solutions if it’s too expensive to deploy what is theoretically correct,” Kaminsky says. “DNSSEC is not an insignificant cost, but those costs can amortize across products that will be policy, compliance and revenue sensitive across an organization. We can eliminate 30 percent of the bugs Verizon saw. That’s huge. There’s ROI right there. Right now, we don’t have scalable ways to do this, therefore it costs money. If we fix this problem, money is saved. It’s called a business model, it’s a good thing.”

The Domain Name System Paul Mockapetris built 25 years ago [[http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14\\_gci1321713,00.html](http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1321713,00.html)] wasn’t meant to support all that it does today. Security, for one, he says, was left out on purpose with the expectation that as more engineers gained experience with DNS, more would be added on to it.

“I did the basement and the first two floors,” Mockapetris says. “In the 25 years since, people have been adding stuff on top of it.”

DNSSEC is one of those add-ons, and in the year since Dan Kaminsky’s bug, it has taken on new meaning and importance as organizations and engineers see the frailties of DNS exposed before their eyes.

“It’s been my opinion for a long time that DNSSEC is a good solution; it doesn’t solve every problem perfectly, but it does solve the small problems it attempts to fix,” says Afilias’ Mohan. “It’s a good solution for a defined problem of DNS hijacking.”

*Michael S. Mimoso is Editor of Information Security. Send comments on this article to [feedback@infosecuritymag.com](mailto:feedback@infosecuritymag.com).*

# what drives *your* approach to IT security?

Balancing business priorities  
and risks is key to a solid approach.

SystemExperts helps you build a comprehensive and cost-effective information security plan that makes sense for your company. Right now, our **ISO 17799/27002 Compliance Program** helps you to focus resources on your most important business risks and comply with regulations such as **Sarbanes-Oxley, FFIEC, HIPAA, PCI, and Gramm-Leach-Bliley**. Best of all, our approach works equally well for “Main Street” businesses and the Fortune 500 clients we’ve proudly served for years.

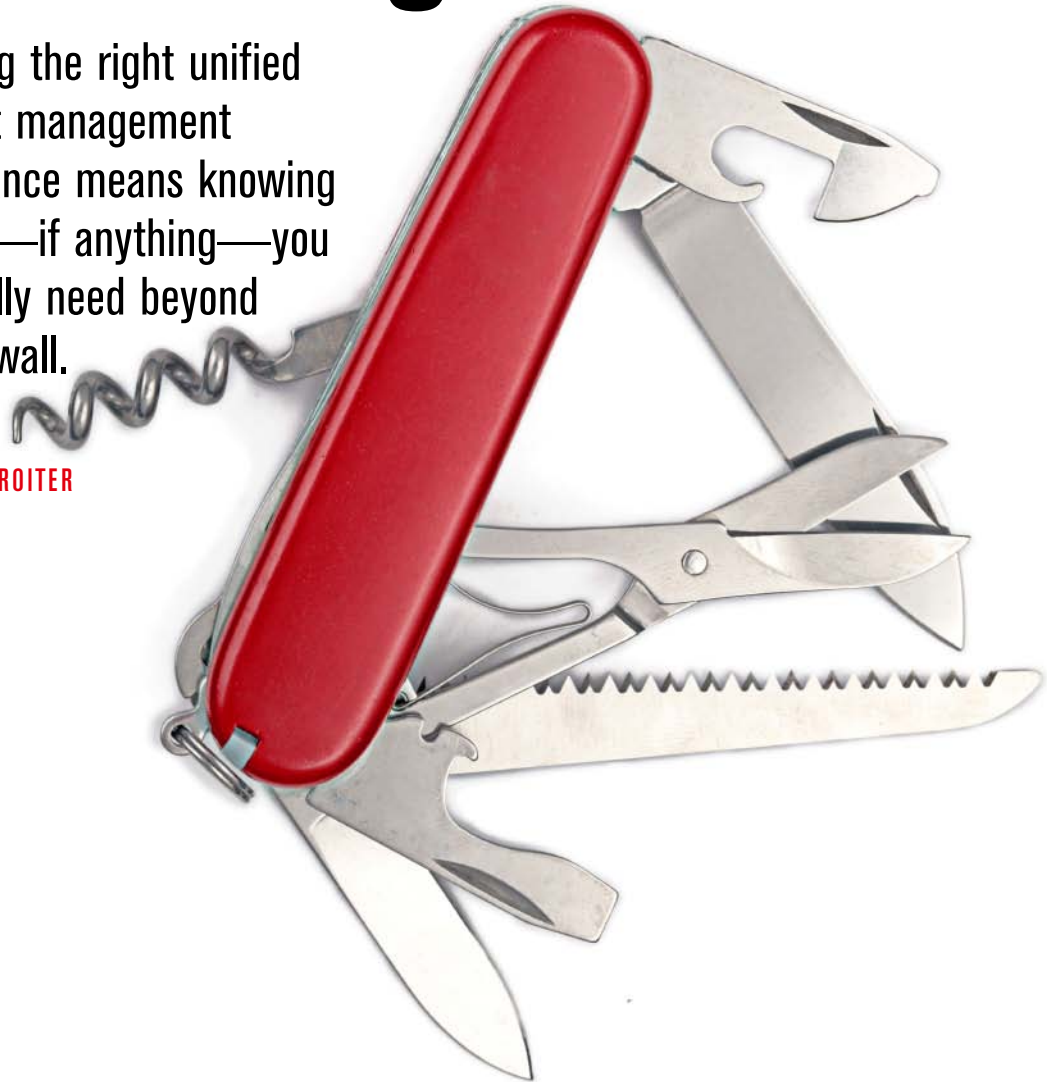
If you want a practical IT security plan that addresses your real business risks, contact us today at 888.749.9800 or visit our web site at [www.systemexperts.com/public](http://www.systemexperts.com/public).

- ISO 17799/27002 Compliance
- HIPAA and PCI DSS Compliance
- Application Vulnerability Testing
- Security Audits and Assessments
- Security Architecture and Design
- Identity Management
- Penetration Testing
- Security Best Practices and Policy
- Emergency Incident Response
- System Hardening
- Technology Strategy
- ASP Assessments

# UTM Should NOT = Unnecessary Threat Management

Buying the right unified threat management appliance means knowing what—if anything—you actually need beyond a firewall.

BY NEIL ROITER



**IF YOU ARE RESPONSIBLE** for security at a small- to mid-sized business, if your current firewalls aren't unified threat management (UTM) appliances, then your next ones will be.

With the possible exception of a few low-end SOHO firewall products, every vendor offers a range of firewall/VPN appliances with options to add gateway antivirus, intrusion prevention, antispam, URL filtering and other security functions on a single box.

"The UTM space has essentially replaced the firewall space; at the low end, there are no firewalls that are not UTM," says Joel Snyder, senior partner at consultancy Opus One. "If you talk about what people used to buy for a small business in the \$150-to-\$1,000 range, I don't think you can find one that doesn't have UTM capabilities."

## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

#### SCAN

### PRIVILEGED ACCOUNTS

### DNSSEC

### UTM

### SPONSOR RESOURCES

It can get confusing. Businesses are faced with complex choices: Extra security comes at a price, both in ongoing subscriptions and performance, so what do you really need and what are you prepared to pay for?

Most vendors offer an extensive line of appliances to accommodate traffic requirements and number of end users. Ready to choose? Not so fast. You'll take a performance hit when you start adding AV, IPS, and other security functions.

## Small businesses have big security needs

Small businesses were starting to wake up to changing security needs when *Information Security* first covered "turnkey appliances" in 2004. Some had no firewalls at all, or first-generation firewalls that no longer supported the business. IT managers shopping for replacements from established firewall vendors found young companies that could offer firewalls plus additional security features packed into a single appliance—all at an attractive price.

Soon, this was christened the UTM market, and, eventually, everyone in the network firewall business was pushing unified threat management. Today, some vendors are

pushing high-end appliances in what they claim is a nascent enterprise UTM market (*see "Is there an enterprise UTM?" p. 31*).

For smaller businesses faced with growing security requirements, UTM made it easier to buy and manage a lot of security tools in a single appliance. The alternative was more point products they could not afford. Or, worse yet, simply going with less security.

"Ten or 12 years ago, we had a firewall, but it wasn't a major piece of equipment—we thought, 'yeah, maybe we should get one,'" says Jason Omens of Seattle, Wash.-based marketing consulting firm BuzzBee, a WatchGuard

For smaller businesses faced with growing security requirements, UTM made it easier to buy and manage a lot of security tools in a single appliance.

UTM customer. "Now the number of threats has skyrocketed."

Omens has to be security conscious now, particularly because of the work BuzzBee does for Microsoft. Keeping precious intellectual property inside the organization is his biggest concern.

ZirMed, a Louisville, Ky.-based software-as-a-service provider for the healthcare industry, which has used SonicWALL UTM appliances since 2000, also raised its security profile as the years passed.

"It's not that we weren't focused on security—we had patient healthcare information to protect," says ZirMed CIO Chris Chirgwin. "But we've seen enactment of HIPAA, and since we added credit card processing, we fall under PCI. We've become a bigger business; now people want us to be SaS 70 audited."

Smaller companies can still have big security headaches. Law firm Sonnenschein Nath & Rosenthal LLP, an IBM ISS customer, is relatively small in employees numbers—but about 800 of them are lawyers, and the firm has a lot to protect.

"We produce hundreds of thousands of documents," says Adam Hansen, Sonnen-

## Is there an *enterprise* UTM?

**SOME HIGH-END** network firewall and UTM vendors say we're seeing the dawn of enterprise-grade unified threat management appliances. These, they say, are high-performance beasts that can process network AV, email security, Web security and perhaps other functions such as data loss prevention—in addition to network firewall, VPN and intrusion prevention in front of the data center without missing a beat.

While the rationale for UTM in the SMB world is adding affordable security on top of firewall/VPN in a single box, the argument in the enterprise is consolidation, as large companies look to save on capital expenses, management overhead, rack space and power.

Whether we'll see real UTM at the enterprise level is open to debate, but we are seeing IPS integrated into high-end firewalls with the muscle to keep traffic moving quickly enough for performance-sensitive applications.

"There are certain decision points where an organization reevaluates their security infrastructure," says Guy Guzner, Check Point Software Technologies director, security products. "There's a lot of restructuring of data centers, a lot of consolidation. When this happens, it gives us an opportunity to revisit some decisions that were made when integrated IPS wasn't mature."

But vendors, including Check Point, take this further. Guzner says that its UTM "software blade" approach is in the "early adoption phase" on its high-end Power-1line for things like gateway AV.

"The enterprise can realize an incredible ROI from a technology and cost perspective, says Anthony James, Fortinet vice president of products. "UTM gives them much more bang for the buck. They can move at the pace they want. They can replace a firewall at cost and add functions over time."

Greg Young, an analyst for Gartner—which prefers the term "multi-function firewall" to unified threat management—is more than cynical.

"There are lies, damn lies and UTM for the enterprise," he declares. "The physics works out, for doing inspection, so that you don't start running into problems until you hit the larger volumes of users, traffic and connections, and then the physics breaks down and then you really need separate products and processors for antivirus, for firewalling, for other deep inspections."

In effect, what vendors are talking about, Young says, are blades in a chassis, where the chassis becomes essentially a server rack. He cites Crossbeam Systems' blade architecture as a prime example.

He breaks the enterprise market into three silos: Next-generation firewalls, which include VPN and IPS; Web security gateways, which typically include URL filtering, and email security appliances.

Joel Snyder, senior partner at consultancy Opus One, takes a slightly different tack, defining Crossbeam as UTM, but otherwise agrees.

"I'm not saying there is one big UTM market," he says. "There are two: Crossbeam and everyone else that's SMB."

Enterprises *are* doing true UTM in the branch office, which have differentiated into separate product lines. The branch appliances generally don't need things like AV or antispam, because the mail is still centralized. But they do need other services, Young says, such as WAN optimization, and they will be managed by the same console as the enterprise firewall, because companies don't want to use two different consoles. For that reason, large firewall vendors tend to do well in the branch offices. ▸

—NEIL ROITER

### TABLE OF CONTENTS

#### EDITOR'S DESK

#### PERSPECTIVES

#### SCAN

#### PRIVILEGED ACCOUNTS

#### DNSSEC

#### UTM

#### SPONSOR RESOURCES

schein manager of information security. “Think about what lawyers print, what they transfer electronically. We protect information throughout its life cycle in whatever form it may take and be sorted.”

Also, firms like Sonnenschein need the extra layers of security UTM can offer because they tend to stick with standard, off-the-shelf products. “That’s great for support, Hansen says, “but not great in terms of mainstream vulnerabilities. The risk landscape is fairly broad. If they can run it through Word, we’re vulnerable.”

## Growing into UTM

Years ago, it was fairly simple to choose the right-sized firewall for your business. Your bandwidth pipe was limited and your was traffic predictable.

Today, your choice of UTM appliance is a factor of business needs and the security features you choose to purchase and turn on. It’s not just a purchase—it’s a commitment. ZirMed found that out as it upgraded from a firewall to full UTM, then to a bigger UTM appliance.

“First, we said, let’s embrace UTM—IPS, gateway AV, malware detection. Then we had to get more serious as we needed a chassis upgrade with considerably more horsepower,” says Chirgwin. The next upgrade came when “we needed more horsepower, simply for more bandwidth. As we were committed to UTM and brought on more customers, the firewall was getting close to being a performance issue.”

In general terms, you can plan to upgrade as your needs change, say every couple of years, or perhaps spend more initially to accommodate that growth down the line. BuzzBee’s Omens, for example, faced with growing traffic as more customers have network access and transfer big files over FTP, is about to upgrade from a T-1 line to 10 Gbps Ethernet without changing appliances.

“It handles our small business needs as we grow,” he says. “We want to be able to grow with what the company needs to do and know that these boxes can handle it.”

He also looks for features like external ports on an appliance to accommodate his environment. For example, he uses one of the Watch-

Guard interfaces to link to an external NAS, so that traffic doesn’t interfere with the internal network.

Even with planning, making the right choice isn’t easy.

“Bandwidth growth is terribly hard to predict,” says Gartner’s Young. After you invest in the capital expense, if your throughput strains the appliance, vendors are ready to help you trade up. “That’s how they make money.”

“You need to balance a box with more horsepower that doesn’t break the bank,” says eSoft CEO Jim Finn. “It’s a fine line vendors walk down, a fine line users walk down, and the bar continues to be raised.”

“You need to balance, a box with more horsepower that doesn’t break the bank. It’s a fine line vendors walk down, a fine line users walk down, and the bar continues to be raised.”

—JIM FINN, CEO, eSoft

### TABLE OF CONTENTS

#### EDITOR'S DESK

#### PERSPECTIVES

#### SCAN

#### PRIVILEGED ACCOUNTS

#### DNSSEC

#### UTM

#### SPONSOR RESOURCES

**TABLE OF CONTENTS**

**EDITOR'S DESK**

**PERSPECTIVES**

**SCAN**

**PRIVILEGED ACCOUNTS**

**DNSSEC**

**UTM**

**SPONSOR RESOURCES**

Opus One's Snyder advises caution as you walk that line. High speed cable and DSL have brought fat pipes to small businesses. If you go beyond firewall and VPN and add gateway antivirus, you'll not only be paying a recurring cost for the subscription, but you'll also bump up your capital expense for a more powerful appliance.

"The costs can be non-predictable," he warns, "because vendors don't like to give good numbers for performance."

The wrong choice can be costly. If you don't have a good case for gateway AV, you're wasting money on the subscription and the box. If you find your box isn't fast enough, you have to upgrade. Or turn of the AV.

"And then you've wasted money and time," says Snyder.

Snyder, who has done extensive UTM testing, has written that transaction rates can drop in half with IPS enabled, and fractions of that with AV and IPS combined in extreme cases.

The recommendation is to plan ahead for your future needs, so you don't need to upgrade in six months or a year if you decide to turn on AV and/or other security apps because your security requirements change. Perhaps your compliance auditor says you need to improve security at the perimeter. Maybe you've had a data breach or your IT staff is spending too much time cleaning up/reimaging infected computers? Or those complaints to HR convinces management that you need to control visits to porn sites.

What's more, your changing business needs also impact your selection.

As the economy improves and your business grows, you may hire more people, upgrade to a faster network or expand your online business. Save money and trouble ahead of time by testing the UTM appliance under stress on your network, and anticipate your needs to allow for growth.

**"The big thing was to get the VPN working. The other things, like gateway antivirus, are good to have, since we're too small to have interest in another appliance. As BuzzBee grows, we'd like to be preemptive."**

**—JASON OMENS, BuzzBee**

**UTM security options**

Most SMBs aren't in the market for a UTM. They are shopping for a better firewall, perhaps or more robust VPN.

BuzzBee's Omens went to a UTM appliance because he was having difficulty setting up a VPN using PPTP on his old firewall.

"The big thing was to get the VPN working," he says. The other things, like gateway antivirus, are good to have, since we're too small to have

interest in another appliance. As BuzzBee grows, we'd like to be preemptive."

"I don't believe most small business or even midmarket IT managers—think I want UTM versus I want a firewall, Snyder says. "But, the features are now so ubiquitous they are not surprised to see them. They hit a stumbling block of 'do I want them, do I have to pay, and does this help me in any way?'"

Antivirus and other security applications are what make UTM a UTM. As a result,

## TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

#### SCAN

#### PRIVILEGED ACCOUNTS

#### DNSSEC

#### UTM

#### SPONSOR RESOURCES

you need to consider the value to you versus the cost.

AV is probably number one on the list. Small businesses are accustomed to buying it for their PCs and servers. And they worry about malware, in part because they are finding their endpoint AV isn't sufficient—PCs and servers still get infected.

You pay a performance premium for turning on additional capabilities, particularly AV and IPS, which have to closely inspect traffic. You may not want everything or everything at one time, so set your sights on a low bundle price for the entire package. That way you can cherry pick and turn on a security service when you are ready or the need arises.

For example, you may not use URL filtering initially, but perhaps your HR department starts enforcing acceptable use policies, or wants to keep your employees off sites that eat up their work time. You may not feel you need network intrusion prevention now, but might when the business grows or you begin hosting Web sites.

Snyder again raises a yellow flag on IPS, saying the quality varies widely.

Don't expect any of these security apps to be as robust as stand-alone products or services, but they may be "good enough," or simply add a layer to your defenses at a reasonable price.

For example, antispam is a good addition if you are not using a stand-alone product or hosted service.

URL filtering is a good fit for UTM appliances, Snyder says—the firewall is a logical place to put it. The same goes for SSL VPN, which some UTM vendors offer as an option along with the more traditional IPsec. In either case, don't expect either to have the kind of granular policy and management controls of their full-featured counterparts.

A UTM version of URL filtering is likely to be pretty basic. It will work off a URL database, but will not give you dynamic evaluation based on content. Nor should you expect access control integration with your directory, or the ability to set exceptions for groups or individuals who have legitimate access to certain types of sites.

In addition, some new options such as data loss prevention are appearing. but again, manage your expectations.

"The DLP is very rudimentary; it's not full enterprise DLP," says Gartner's Young. "But if

**"The DLP is very rudimentary; it's not full enterprise DLP. But if your requirements are low, it's perfect."**

—GREG YOUNG, analyst, Gartner

your requirements are low, it's perfect."

So, if all you want to do is watch for credit card numbers or Social Security numbers, this is almost surely good enough DLP at the right price.

We're starting to see Web application firewalls (WAFs) in UTMs as well, but this seems like even more of a reach. WAFs have become very popular since they became an option for the application security requirement for PCI DSS. But WAFs aren't plug-and-play tools, and simply turning on this option in front of your Web apps will neither make you more secure nor PCI compliant. Plan to invest some care and feeding if you are going to deploy a WAF as part of your application security program and investigate the WAF's capabilities before you decide it will be a checkbox PCI solution.

# UTM Products

## REPRESENTATIVE LIST OF UNIFIED THREAT MANAGEMENT VENDORS AND PRODUCTS.

COMPANY	PRODUCT(S)	DESCRIPTION
Astaro Internet Security www.astaro.com	Astaro Security Gateway	Appliances ranging from low-mid-sized companies to 10,000 users. Firewall, IPSec/SSL VPN, AV, Web filtering, email security
Calyptix Security www.calyptix.com	Access Enforcer	Appliances for 10 to 100 users designed to work with Microsoft Small Business Server 2008. Firewall, VPN, AV/antispayware, antispam, Web filtering, IPS IM management
Check Point Software Technologies www.checkpoint.com	UTM-1, Power-1	UTM-1: 12 appliances ranging from 400 Mbps to 4 Gbps firewall throughput. Firewall, VPN, AV, IPS, Web filtering, antispam-email security. Power-1: High-end network firewall appliances up to 25 Gbps firewall throughput; same security options plus IM control, VoIP security, SSL VPN, and networking features such as load balancing, HA, clustering and QoS
Crossbeam Systems www.crossbeam.com	X-Series	Blade architecture for mixing and matching third-party firewall, VPN, IDS, antivirus, URL filtering, content filtering. C series: 380 Mbps to 6 Gbps firewall throughput; X-Series: adds load balancing, IPS, Web application firewall; two 10 Gbps and 10 1 Gbps ports
Cyberoam www.cyberoam.com	Comprehensive Internet Security System	SOHO up to 6 Gbps firewall throughput appliances featuring identity-based UTM with include firewall, VPN (SSL & IPSec), AV and anti-spyware, anti-spam, IPS, content filtering, bandwidth management
Cymtec www.cymtec.com	Sentry	Appliances for small offices, branch offices; firewall, URL filtering, AV, application control
DeepNines Technologies www.deepnines.com	Security Edge Platform (SEP)	Software-based UTM up to 1 Gbps; firewall, IPS, AV, content filtering
eSoft www.esoft.com	InstaGate	SMB firewall/VPN, Web and email security
Fortinet www.fortinet.com	Fortinet FortiGate	Appliance ranging from small businesses to the FortiGate-5000 series for large enterprises, service providers and carriers; IPS, AV, Web filtering, antispam, application control
Funkwerk Enterprise Communications www.funkwerk-ec.com	Packetalarm UTM	10-250 user appliances; firewall/VPN, IPS, AV, antispam
Global DataGuard www.globaldataguard.com	Global DataGuard All-in-One Security Module for Enterprise UTM	IDP, NBA, AV, NAC, content filtering in medium-to-large enterprise appliances
Halon Security www.halonsecurity.com	SX series	800 Mhz to 3200 Mhz appliances; firewall/VPN, AV, antispam, content filtering, Web access control, IDS
Juniper Networks www.juniper.net	SSG	160 Mbps to 1 Gbps firewall throughput; VPN, IPS, AV, antispam, and Web filtering
McAfee www.mcafee.com	McAfee UTM Firewall (formerly Secure Computing SnapGear)	25 Mbps to 180 Mbps SMB appliances; firewall/VPN, AV, IDP, URL filtering, email filtering
O2 Security www.O2security.com	SifoWorks	100 Mbps to 1650 Mbps firewall/VPN; intrusion prevention, antivirus, Web filtering
Panda Security www.pandasecurity.com	GateDefender	40 Mbps to 850 Mbps SMB appliances; Firewall/VPN, IPS, AV, content filtering, antispam and Web filtering
Reticorp www.reticorp.com	Reticorp RetiEdge	Firewall/VPN, IPS, AV
Smoothwall www.smoothwall.com	Smoothwall SmoothGuard	900 Mbps series appliances, firewall/VPN, Web filtering and VPN solutions with IDS, antivirus, antispam
SonicWALL www.sonicwall.com	SonicWALL E NSA, NSA, TZ series appliances	Wide range of 90 Mbps to 5.6 Gbps appliances; application firewall, IPSec/SSL VPN, AV, IPS
Untangle www.untangle.com	Gateway Platform	12 open-source security apps for SMBs
Vasco www.vasco.com	aXsGUARD Gatekeeper	Three gigabit interface appliances; firewall/VPN, AV, IPS, content filtering, antispam
WatchGuard Technologies www.watchguard.cm	Firebox X	50-1,000 user appliances; firewall/VPN, AV, antispam, URL filtering, IPS
ZyXel www.zyxel.com	USG100, 300	Firewall/IPSEC/SSL VPN for up to 50 users

### TABLE OF CONTENTS

### EDITOR'S DESK

### PERSPECTIVES

### SCAN

### PRIVILEGED ACCOUNTS

### DNSSEC

### UTM

### SPONSOR RESOURCES

If it fills the bill, however, says Young, you won't have to buy a stand-alone product or tinker with open-source tools.

UTM is here to stay. For organizations with up to 500, perhaps 1,000 employees, depending on the specific attributes of the business, it is the firewall of the present and at least the foreseeable future.

It's a winner for firewall vendors, Snyder says.

"The whole reason UTM exists is because of recurring revenue," he says. "The recurring revenue model is the salvation of firewall industry. That's why these boxes exist."

For SMBs, UTM offers a number of security services for the price of a single appliance to purchase and modest, though recurring subscription fees. If you're sure all you need is firewall and VPN, don't feel you have to buy the extra subscriptions, so you don't get stuck with added fees or a more expensive appliance than you really need. If you think you may need to turn on additional services in the foreseeable future and/or anticipate more users and traffic, make sure you buy appliances that will grow with your needs. ▸

---

*Neil Roiter is senior technical editor for Information Security. Send comments on this article to [feedback@infosecurymag.com](mailto:feedback@infosecurymag.com).*

## TABLE OF CONTENTS

---

### EDITOR'S DESK

---

### PERSPECTIVES

---

### SCAN

---

### PRIVILEGED ACCOUNTS

---

### DNSSEC

---

### UTM

---

### SPONSOR RESOURCES

---

WE'LL GET  
YOUR IT SYSTEMS  
TO TALK...



ARE YOUR NETWORK DEVICES HOLDING YOUR LOGS HOSTAGE?  
WHAT YOU DON'T KNOW CAN HURT YOU.

OPTICS FOR SECURITY INFORMATION MANAGEMENT IS AN AFFORDABLE AUTOMATED LOG MANAGEMENT SERVICE THAT CENTRALIZES, ANALYZES AND RETAINS LOG DATA AND HELPS YOU USE IT TO SUPPORT BUSINESS FUNCTIONS. SCALABLE TO 100% OF YOUR LOG DATA, SO YOU CAN REST EASY, GLASSHOUSE HAS GOT YOU COVERED.

FOR MORE INFORMATION CONTACT: [SECURITY@GLASSHOUSE.COM](mailto:SECURITY@GLASSHOUSE.COM)

[WWW.GLASSHOUSE.COM](http://WWW.GLASSHOUSE.COM)

 **GLASSHOUSE**

## ADVERTISING INDEX

**Guardium** ..... 2  
<http://guardium.com/>

- HOWTO Secure and Audit Oracle 10g and 11g
- Integrating Privileged Accounts with Existing Security Infrastructure

**CA** ..... 5  
<http://www.ca.com/>

- Learn how effective identity and access management can help you grow your business — with less risk
- You don't need more security — you need better security. CA IT Management Security Center. Click Here to Explore.

**ISACA** ..... 12  
[www.isaca.org](http://www.isaca.org)

**the Academy** ..... 19  
[www.theacademy.ca](http://www.theacademy.ca)

- Free infosec videos for security professionals from network admin to director of IT.
- Free information security videos for home users/end users.

**SystemExperts** ..... 28  
[www.systemexperts.com](http://www.systemexperts.com)

**Glasshouse Technologies** ..... 37  
<http://www.glasshouse.com/>

### TABLE OF CONTENTS

#### EDITOR'S DESK

#### PERSPECTIVES

#### SCAN

#### PRIVILEGED ACCOUNTS

#### DNSSEC

#### UTM

#### SPONSOR RESOURCES

## TECHTARGET SECURITY MEDIA GROUP



**EDITORIAL DIRECTOR** Kelley Damore

**EDITOR** Michael S. Mimoso

**SENIOR TECHNOLOGY EDITOR** Neil Roiter

**FEATURES EDITOR** Marcia Savage

#### ART & DESIGN

**CREATIVE DIRECTOR** Maureen Joyce

#### COLUMNISTS

Jay G. Heiser, Marcus Ranum, Bruce Schneier

#### CONTRIBUTING EDITORS

Michael Cobb, Eric Cole, James C. Foster, Shon Harris, Richard Mackey Jr., Lisa Phifer, Ed Skoudis, Joel Snyder

#### TECHNICAL EDITORS

Greg Balaze, Brad Causey, Mike Chapple, Peter Giannacopoulos, Brent Huston, Phoram Mehta, Sandra Kay Miller, Gary Moser, David Strom, Steve Weil, Harris Weisman

#### USER ADVISORY BOARD

Edward Amoroso, AT&T  
Anish Bhimani, JPMorgan Chase  
Larry L. Brock, DuPont  
Dave Dittrich  
Ernie Hayden, Seattle City Light  
Patrick Heim, Kaiser Permanente  
Dan Houser, Cardinal Health  
Patricia Myers, Williams-Sonoma  
Ron Woerner, TD Ameritrade

#### SEARCHSECURITY.COM

**SENIOR SITE EDITOR** Eric Parizo

**NEWS EDITOR** Robert Westervelt

**ASSOCIATE EDITOR** William Hurley

**ASSISTANT EDITOR** Maggie Wright

**ASSISTANT EDITOR** Carolyn Gibney

#### INFORMATION SECURITY DECISIONS

**GENERAL MANAGER OF EVENTS** Amy Cleary

**EDITORIAL EVENTS MANAGER** Karen Bagley

**SR. VICE PRESIDENT AND GROUP PUBLISHER**  
Andrew Briney

**PUBLISHER** Josh Garland

**DIRECTOR OF PRODUCT MANAGEMENT**  
Susan Shaver

**DIRECTOR OF MARKETING** Kristin Hadley

**SALES MANAGER, EAST** Zemira DelVecchio

**SALES MANAGER, WEST** Dara Such

**CIRCULATION MANAGER** Kate Sullivan

**ASSOCIATE PROJECT MANAGER**  
Suzanne Jackson

**PRODUCT MANAGEMENT & MARKETING**  
Corey Strader, Jennifer Labelle, Andrew McHugh

#### SALES REPRESENTATIVES

Eric Belcher [ebelcher@techtarg.com](mailto:ebelcher@techtarg.com)

Neil Dhanowa [ndhanowa@techtarg.com](mailto:ndhanowa@techtarg.com)

Patrick Eichmann [peichmann@techtarg.com](mailto:peichmann@techtarg.com)

Jason Olson [jolson@techtarg.com](mailto:jolson@techtarg.com)

Jeff Tonello [jtonello@techtarg.com](mailto:jtonello@techtarg.com)

Nikki Wise [nwise@techtarg.com](mailto:nwise@techtarg.com)

#### TECHTARGET INC.

**CHIEF EXECUTIVE OFFICER** Greg Strakosch

**PRESIDENT** Don Hawk

**EXECUTIVE VICE PRESIDENT** Kevin Beam

**CHIEF FINANCIAL OFFICER** Eric Sockol

#### EUROPEAN DISTRIBUTION

Parkway Gordon Phone 44-1491-875-386  
[www.parkway.co.uk](http://www.parkway.co.uk)

#### LIST RENTAL SERVICES

Kelly Weinhold  
Phone 781-657-1691 Fax 781-657-1100

#### REPRINTS

FosteReprints Rhonda Brown  
Phone 866-879-9144 x194  
[rbrown@fostereprints.com](mailto:rbrown@fostereprints.com)



INFORMATION SECURITY (ISSN 1096-8903) is published monthly with a combined July/Aug., Dec./Jan. issue by TechTarget, 117 Kendrick St., Suite 800, Needham, MA 02494 U.S.A.; Phone 781-657-1000; Fax 781-657-1100.

All rights reserved. Entire contents, Copyright © 2009 TechTarget. No part of this publication may be transmitted or reproduced in any form, or by any means without permission in writing from the publisher, TechTarget or INFORMATION SECURITY.