LOGIN/FOTOLIA

COMPUTER WEEKLY IT SECURITY CASE STUDIES

WINNERS OF THE EUROPEAN USER AWARDS FOR SECURITY

Winning security use cases in the Computer Weekly European Awards

Warwick Ashford takes a look at the security technology and strategies that made the winning entries stand out from the crowd

Case study: How Bromium helped US supermarket chain solve security challenge virtually

Winner of Best Technology and Best of Show

A large US supermarket chain has implemented an innovative endpoint security technology to secure point of sales systems running legacy applications to save additional development or patching costs.

Bromium's vSentry endpoint security software applies virtualisation expertise to isolate and secure every untrusted network task within its own tiny virtual machine or microVM.

According to Bromium, it is impossible to detect all the possible attacks or monitor all the possible forms of suspicious behaviour. However, the firm maintains it is possible to protect endpoints using highly granular virtualisation in combination with hardware-enforced isolation.

In this proactive approach to security, vSentry assumes all internet tasks are untrusted and automatically puts each task into its own microVM, which is destroyed when the task is completed.

If an attack occurs within any of these tasks, the malware remains contained and isolated inside the microVM, unable to escape and access any system or network resource. Because vSentry is completely transparent to the user – even during a malware attack – there is no affect on user experience or performance, according to Bromium.

This approach, the security firm claims, de-couples protection for the first time and provides 100% protection against all malware attacks as it does not use any "detection" technologies.

To validate this claim, research organisation NSS Labs completed an independent security validation exercise on vSentry. The results, published in February 2013, stated that vSentry protected endpoints from every attack, including 166 embedded exploits delivered through email and drive-by attacks.

VSentry also protected targets against 15 advance attacks using the Metasploit penetration testing toolset that incorporated advanced obfuscation and evasion techniques in an attempt to bypass protection.

Bromium's vSentry assumes all internet tasks are untrusted and automatically puts each task into its own microVM, which is destroyed when the task is completed

Cyber attack protection and alerts

Speaking on condition of anonymity, the director of information security for a large US-based supermarket chain says the company implemented vSentry in the face of malware designed to avoid detection.

"This compelled us to examine solutions with novel approaches to solving the problem," he says.

According to the supermarket chain, network-based detection tools would not be able to provide the adequate visibility or control to deal with this type of malware. Similarly, there were certain attack types that the other endpoint security controls could not mitigate or were operationally burdensome.

"We were also looking for technology that would prevent the most sophisticated, targeted attacks, not just produce forensic data after they were

ComputerWeekly
EuropeanUser Awards

successful and eventually detected," says the director of security.

The threat intelligence provided by Bromium's Live Attack Visualisation and Analysis (LAVA) system is one of the pillars of an improved security framework that the company is implementing to achieve greater visibility and alerting for malicious activity.

"The exceptional benefit that vSentry provides is that the isolation-based approach first protects the systems from targeted attacks, then alerts us of the threat – after it has already been mitigated," he says.

This reduces the noise and number of alerts to investigate as well as having a measurable savings around the operational cost incurred to remediate those machines and associated lost productivity.

There are three main business benefits of vSentry, according to the supermarket's director of security:

- The systems running legacy applications could be secured with no additional development or patching cost.
- The number of malware infections and the associated time it takes to remediate them has been almost non-existent.
- The intelligence gained from malware captured with LAVA on only a small number of vSentry hosts protects the entire environment.

> "The exceptional benefit that vSentry provides is that the isolation-based approach first protects the systems from targeted attacks, then alerts us of the threat – after it has already been mitigated"
>
> Bromium customer

Case study: How the IASME information assurance certification gives SMEs the edge

Winner of the Private Sector category

IT consultancy Purple Frog Systems believes its gold certification to the IASME information assurance standard for small to medium enterprises gives it a competitive edge.

Many of the firm's customers are large corporations looking for help in data warehousing, data mining and building business intelligence dashboards. But clients such as these typically want proof of a rigorous audit process. As part of the tender process, they often want to know how suppliers will handle their data and what security measures are in place.

"It can be difficult for SMEs to win work with this type of client," says Hollie Whittles, director at Shropshire-based Purple Frog Systems.

Corporations and SMEs alike increasingly require suppliers to demonstrate they are competent, professional and do not pose a risk. "Operating in a highly competitive market, we wanted to demonstrate that we took information security seriously," says Whittles.

Purple Frog Systems recognised that having an independent certification would benefit the business and went through the AccreditUK certification process. While this is an independent mark of quality for SME IT suppliers to show they have the right business processes in place and are competent, it offers no assurances on sensitive data.

"Because we handle a lot of sensitive client data, we wanted to do more in this area to prove to our corporate customers and their auditors that we can handle their data securely," says Whittles.

Information security standards

Initially, Purple Frog Systems considered the ISO 27001 international standard for information security, but this standard was too complex and costly for an organisation of its size.

Through AccreditUK, the firm was introduced to the IASME information assurance standard for small to medium businesses, which was a much better fit. "IASME was the best affordable solution to us as an SME," says Whittles.

IASME started as a Technology Strategy Board part-funded project managed

ComputerWeekly EuropeanUser Awards

by The National Computing Centre, and involving the University of Worcester and information assurance consultants.

IASME addresses the complexity and relevance of applying ISO 27001 information security controls to SMEs by identifying an intermediate level of controls and developing entry-level certification for SMEs.

The IASME certification enables SMEs in a supply chain to demonstrate their level of cyber security and that they can properly protect their customers' information. The certification process is provided through accredited assessors and is moderated by IASME as a mark of excellence to demonstrate the level of assurance attained by the organisation.

IASME certification process

The scheme was piloted with a number of SMEs in the Midlands in 2011. Purple Frog Systems became one of the first to receive a Gold Award under the scheme.

"The IASME process was very thorough and encouraged us to document everything that was in our heads," says Whittles. "We knew what our disaster recovery plan was, but we hadn't written it down."

As well as recognising good practice in information assurance, IASME also provides a good framework for continuous improvement for SMEs.

"The benefits of IASME include peace of mind to ourselves, and also to our clients, that our information security policies are fully up to date and that there are no loopholes," says Whittles.

When going to tender, the IASME accreditation also means Purple Frog Systems can easily demonstrate its procedures and guarantee that its processes comply with requirements.

"It is hard to evaluate whether we would have won contracts without having IASME, but we feel that it adds another string to our bow and is something that sets us apart from our competitors," says Whittles.

Large organisations that rely on SMEs in their supply chain increasingly require them to prove they operate according to information assurance best practice.

Apart from providing a competitive edge, the standard is also useful tool to help SMEs improve their data protection capabilities.

Wider benefits of IASME certification

SMEs form a large part of the national information infrastructure of the UK. Regulatory bodies, including the Information Commissioners Office, expect evidence that SMEs are taking information security seriously. The EU is stepping up requirements for information security.

IASME certification aims at providing enterprise-class security to SMEs, which are at the heart of the UK economy, says Clive Longbottom, analyst at Quocirca.

"By doing so, not only are problems minimised within this core group, but they can also interact with large enterprises as peer, secure partners," he says.

IASME is preparing for the expected push for better cyber security down the supply chain by training small businesses to become assessors for the IASME certification process. It is also developing non-technical advice for better cyber security on its website and working with other groups to spread the benefits of good information security.

> "The benefits of IASME include peace of mind to ourselves, and also to our clients, that our information security policies are fully up to date and that there are no loopholes"
>
> Hollie Whittles, Purple Frog Systems

Case study: How Solihull council saves time and money with bring your own device programme

Winner of the Public Sector category (entered by Good Technology)

At least one in five local authorities in the UK is looking into the idea of allowing staff to use their own devices at work, mainly due to demand from employees.

ComputerWeekly EuropeanUser Awards

Solihull Metropolitan Borough Council in the Midlands rolled out a secure bring your own device (BYOD) programme, but found it achieved efficiency gains and cost savings in the process.

As for all organisations going this route, the main challenge for the IT team was the safeguarding information and data security while giving staff the flexibility to use their own devices.

Being a local authority dealing with sensitive information on residents, the council had to ensure that any systems it deployed adhered to the strict security requirements set by the government's information assurance advisor CESG.

To achieve its goals without risking security, the council's IT team developed policies for BYOD and "your own device at home" (Yodah), underpinned by two main security technologies that enable employees to access systems from a device of their choice.

For laptops and home PCs the council is using virtual private network (VPN) appliances from Juniper Networks. For smartphones and tablets the council uses an enterprise mobile device management (MDM) system from Good Technology.

As a backup for when devices fail, council employees can access the systems they need to do their work on any available machine through a Citrix system.

While VPNs are fairly established as a means of enabling secure remote access, Good Technology was the only solution open to the council for smartphones and tablets, according to Solihull Council project manager Alan Colson.

By encrypting sensitive data and keeping it in a secure container on the device, it was separated from personal data. This enabled the council to allow employees to use their device of choice, while keeping the sensitive data secure and not requiring continual authentication, he says.

Allowing the greater choice of devices led to an improvement in the ICT's reputation in the council, says Colson.

"By empowering employees to work how and where they wanted to, on a device that suited them, the IT team went from being the department of 'no' to the department of 'go'," he says.

More than 375 council employees have already gone live with BYOD, which is nearly 15% of the organisation's eligible workforce.

Staff continue to drive the process, with five people added to the scheme every week.

Cutting public sector costs

In today's economic climate of public sector cuts, the council says Yodah is also able to attain notable fiscal benefits as a result of supporting BYOD.

"People are returning council-issued phones and laptops and using their own devices instead, so there is a saving straight away," says the council's head of IT, Steve Halliday.

Detractors of BYOD schemes say this approach will automatically result in a spike in support costs, but Solihull Council has not encountered that problem, he says: "We decided to adopt the approach of monitoring the situation and managing problems if they arose, but we are not seeing that."

Social media support

As part of the BYOD initiative, the IT team has set up a social media site where staff can pose questions and provide answers on any issues they face, without resorting to IT support services.

"This enables a kind of 'support your own' approach," says Halliday, but the roll-out has been relatively smooth and traffic has not been substantial on the site. In addition, if devices fail, employees are able to go back to suppliers to get problems resolved.

The second saving from BYOD comes from increasing productivity. "Many users are effectively adding two hours to their work day, which is a gain of 25%," he says.

> "By empowering employees to work how and where they wanted to, on a device that suited them, the IT team went from being the department of 'no' to the department of 'go'"
>
> Alan Colson, Solihull Council

ComputerWeekly EuropeanUser Awards

In addition to providing choice and a richer user experience, Halliday says the initiative has also led to quicker and more efficient decision-making.

Yodah continues to be popular with employees, and IT's reputation is at an all-time high, he says.

Solihull Council has a winning approach, according to Quocirca analyst Clive Longbottom. "It deals with a hot topic (BYOD) and also flexible working in allowing employees to work from home, and shows how an inclusive model for information security can work," he says.

Case study: How Symantec helped an NHS trust cut security costs by a quarter

Winner of the Supplier of the Year award

The Royal Liverpool and Broadgreen University Hospitals NHS Trust has cut its security costs by a quarter through its partnership with security supplier Symantec.

In the face of decreased public spending and increased cyber threats, the trust reviewed its legacy multivendor security strategy to improve data protection but reduce costs at the same time.

The review sought to consolidate suppliers, simplify processes and enable a more co-ordinated approach to data security.

The trust decided to deepen its relationship with Symantec, having already rolled out the firm's enterprise vault storage and backup products.

The trust looked at several technologies, says James Norman, director of information management and technology at the trust.

"But the blend of potential cost savings, the quality of the integrated security technologies and Symantec's excellent market reputation all pointed to the company being the right partner to work with," he says.

To help the trust achieve its goals, Symantec suggested its business-led initiative aimed at helping public sector organisations reduce software expenditure by 25% while achieving a high level of security.

"Symantec was able to advise on the best way to cut costs without impacting services," says Norman.

> "The blend of potential cost savings, the quality of the integrated security technologies and Symantec's excellent market reputation all pointed to the company being the right partner to work with"
>
> James Norman, Royal Liverpool and Broadgreen University Hospitals NHS Trust

Protecting data and educating users

Under the Symantec 25 programme, the trust deployed Symantec's Data Loss Prevention and Symantec Protection Suite.

As a healthcare provider, patient confidentiality is critical, says Norman.

"The recent high-profile media reports of both inadvertent data loss and malicious data leakage incidents further heightened the need to find a provider who could provide optimal protection against data theft or loss, while simultaneously enabling better data sharing and access to services," he says.

Having cut IT security costs by a quarter, the project enabled the trust to improve its ability to identify, monitor and protect its data.

The project has also enabled the trust to educate its 4,500 users on the risks of unguarded technology and prevent staff from sending unencrypted sensitive information via email.

"Ultimately, improved IT security practice will provide enhanced IT compliance and avoid enforcement action by the Information Commissioner's Office for any data breach," says Norman.

Improved productivity with mobility

In addition to cutting costs and improving data protection, the trust wanted to improve productivity by enabling staff to access patient and clinical data when at the bedside.

ComputerWeekly
EuropeanUser Awards

However it was imperative to comply with legislative requirements for secure processing of patient data. It was also key for IT management to be streamlined, making it easier to use and administer as well as reducing the cost of managing IT security.

As a result, the trust implemented Symantec's Mobile Management system (MMS) for secure mobile working.

Rolling out the MMS means 4,500 medical staff now have instant access to healthcare history, medical images, medical notes and more, at a patients' bedside, says Norman.

"Staff can work more efficiently and productively, helping the trust save valuable time and money, and resources can be used more effectively and enables faster decision making," he says.

The MMS also gives staff access to access to email, calendars and the electronic patient healthcare record, while securing the devices and data.

Data moves with consultants and patients

This includes enforcing access controls, maintaining a separation between healthcare data and personal data and providing a central point of control.

"We wanted our consultants to make immediate decisions aimed at enhancing the quality of patient care and improving outcomes, so our strategy was to allow the data to move with them," says Norman.

"When a patient moves between wards the data goes with them, letting the medical staff work more efficiently, freeing up more time for consultative advice."

Norman says the trust wanted to standardise its technology portfolio. "Symantec offered the best products and the seamless integration with our existing technology, to take the trust into the next dimension of healthcare data security: both mobile and static," he says.

Andrew Rose, principal analyst security and risk at Forrester Research says Symantec's breadth of coverage and customer-focused strategy mean that it can make a good partner and provide real business benefit. ■

> "Symantec offered the best products and the seamless integration with our existing technology, to take the trust into the next dimension of healthcare data security: both mobile and static"
>
> James Norman, Royal Liverpool and Broadgreen University Hospitals NHS Trust

ComputerWeekly
EuropeanUser Awards