



The Washington Savings Bank Cuts Recurring Costs with eEye Blink Endpoint Protection

The Challenge: Finding Cost-Effective, Manageable Endpoint Security

The Washington Savings Bank (TWSB) was unhappy with its endpoint security. Headquartered in Bowie, Maryland, TWSB has five banking branches, approximately 130 employees and 110 client devices to protect.

“Because of high risks and regulations, IT for even the smallest bank is extensive,” said Bruce Smith, Vice President of Information Systems, TWSB. “We have a small IT staff of three people, and keeping up with security was consuming too much of our time.”



Customer:

The Washington
Savings Bank

Fast Facts:

Headquartered in
Bowie, MD

5 branches in
Southern Maryland

110 end devices

\$450 million in assets

Key IT challenge:

finding lower-cost endpoint protection with additional integrated features beyond AV, including antispysware protection, intrusion prevention, and vulnerability scanning

www.twsb.com

TWSB had been using Symantec Enterprise Antivirus. When it came time to renew their license, Smith balked at the steadily climbing renewal price and decided to investigate whether TWSB could get more for its security dollar.

Additionally, the bank is required to meet stringent compliance standards including the use of an intrusion prevention system to guard against malicious internal network activity. Hardware based IPS systems offered by other companies were well beyond the reasonable price point of a bank this size.

Selection Criteria:

Cutting Costs while Adding New Security Features

Like many organizations with legacy security products, TWSB had layer upon layer of security; however, none of it was integrated. End-user PCs had separate antivirus and antispysware, while they lacked other features such as endpoint firewalls, intrusion prevention, and policy control. The bank had a perimeter firewall, but more and more employees wanted to work from home or as they travelled.

While reducing costs was critical, integrating disparate client-side security features was even more important. “Symantec was adding features, but its security suite was getting incredibly bloated. It had a huge footprint and was very expensive,” Smith said.

TWSB had a list of features they wanted integrated into endpoint security, such as antispysware, a client firewall, intrusion prevention and detection, zero-day protection and policy-based rules. “We also wanted other features that would make our lives easier, such as centralized policy control and reporting,” Smith said.

A technology consulting firm (Miller Technology Solutions) that TWSB worked with suggested that they consider eEye Digital Security.



The Solution: eEye Blink Endpoint Protection

eEye Blink Endpoint Security is a comprehensive software suite that offers zero-day protection, centralized management and behavior-based, rather than signature-based, protection – all at a much lower price than competing solutions.

Blink protects client devices by identifying behaviors, not signatures. Offering integrated multi-layered endpoint protection, Blink is a single lightweight client that replaces multiple security agents, against known attacks, zero-day exploits, and all other attack vectors.

One of the features that impressed TWSB was Blink’s System Protection. As a financial institution, TWSB is a prime target for cyber-criminals. If they were to rely on signatures alone, they would be vulnerable to new attacks for which there were no security signatures.

After some cost analysis and testing, Smith was convinced that Blink was the answer. After testing Blink for a short time in a pilot group of 12 computers, he and his IT team quickly rolled it out to the entire organization.

“After the pilot, the rollout to all of our branches was painless. eEye automated the deployment and updating process, so it was really just a simple administrative job,” Smith said.

Blink: Easier on End Users and IT

Any reliable approach to security tries to shield end users from as many security decisions as possible – without forcing IT to react to multiple false alarms. Symantec often forces end users to make security choices they may not be informed about, such as whether or not to permit registry changes, and it is notorious for compromising end-device performance because it consumes too many memory and CPU resources.

Symantec also places a significant burden on small IT staffs, which have to consult multiple user interfaces for separate products, while also having to constantly monitor for updates, patches and non-compliant end devices.

Blink’s small, consolidated footprint on end devices boosted client-side performance for TWSB, while its integration of a slew of security features into a single console made life much easier for IT.

eEye’s Blink offers a single portal for client-side security management; while eEye’s REM Security Management Console provides the same benefit for IT. Designed for enterprise scalability, REM provides a single point of visibility into and a centralized point of control over enterprise networks.

Key Benefits:

- Zero-day protection
- Quarantining of suspicious machines
- Policy creation and enforcement
- Antivirus protection
- Intrusion Prevention
- Integrated antispysware protection
- Visibility into endpoints
- Centralized security management
- Reporting and auditing



eEye Digital Security®

To learn more, please visit www.eeye.com or call 866.282.8276





Blink also allows TWSB to take a policy-based approach to security. "Having control over policies is important as more and more users work remotely," Smith said. TWSB can vary policies by branch, user role or a user's physical location, helping to mitigate many of the risks associated with remote computing.

Moreover, IT can update policies over the web, meaning changes can be made instantly with little or no disruption for end users.

ROI and Ongoing Cost Savings

While TWSB didn't do a detailed, formal ROI study, it has already saved money by switching to Blink.

"I did a short analysis," Smith said, "and Blink, with its many additional features, was about the same price as Symantec's antivirus and antispysware alone." (When TWSB's license was up for renewal, Symantec had updated their antivirus software to include antispysware.)

Since deploying Blink, TWSB continues to save. "In terms of labor, I'd guess we are saving at least 8 man hours a month," Mr. Smith said. He also noted that much of Blink's advantage is not quantitative. "For a staff as small as ours, the less hands-on a product is, the better. With Blink, you can set it and forget it. Blink gives you ease of mind. It probably also saves me three nights of sleep per month."

Coping with Compliance

IT professionals in the financial sector must cope with an alphabet soup of regulations, including SOX, GLBA, PCI and a litany of FFIEC regulations. "Most of my job revolves around compliance. I deal with internal audits and federal regulators all the time," Smith said.

"We had a checklist of features we wanted integrated into our endpoint security, including antispysware, a client firewall, intrusion prevention, vulnerability scanning and policy-based rules.... Blink, with its many additional features, was about the same price as Symantec's antivirus and antispysware alone."

***- Bruce Smith,
Vice President of Information Systems,
The Washington Savings Bank***

Other Key Benefits:

Automated notification when problems occur

Streamlined incident response

Vulnerability scanning

Transparent to end users

Centralized security management that provides a single point of visibility into and control over the network

Centralized reporting simplifies compliance efforts



eEye Digital Security®

To learn more, please visit www.eeye.com
or call 866.282.8276



With Blink, TWSB can demonstrate that they've taken steps to meet regulations. "Having something considered best of breed in the industry goes a long way with regulators. I can say to them, 'we have protections in place,' and I have a single security console I can refer to in order to prove it."

TWSB is hoping to automate much of the compliance process as it gets more familiar with Blink and starts to leverage more of Blink's feature set. "We're not quite there," Smith said. "That's not a knock on Blink. We just haven't had the time internally to take advantage of all of Blink's features yet."

eEye's Integrated Threat Management Suite:

Retina Network Security Scanner provides multi-platform vulnerability management. Retina identifies known and zero-day vulnerabilities and provides security risk assessment, enabling security best practices, policy enforcement, and compliance with regulatory audits.

Retina Web Security Scanner rapidly and accurately scans large, complex web sites and web applications to tackle web-based vulnerabilities, ensuring privacy, security integrity and compliance.

Blink delivers multi-layered endpoint protection in a single, lightweight client that replaces multiple security agents, protecting against known exploits, zero-day attacks, and all other attack vectors.

REM simplifies the security management of complex networks. Designed for enterprise scalability, REM provides a single point of visibility into and a centralized point of control over enterprise networks.

Retina On Demand simplifies the entire vulnerability management process by allowing an organization to rapidly deploy Retina Security Management Appliances within an environment and manage all of the job scheduling, reports, and results through a hosted version of REM. There is no need to setup servers, configure databases, or even install any software to benefit from Retina On Demand. eEye has created true black-box technology that can be plugged into any environment and managed via the Internet for a hands-free approach to vulnerability management and regulatory compliance.



eEye Digital Security®

To learn more, please visit www.eeye.com
or call 866.282.8276

