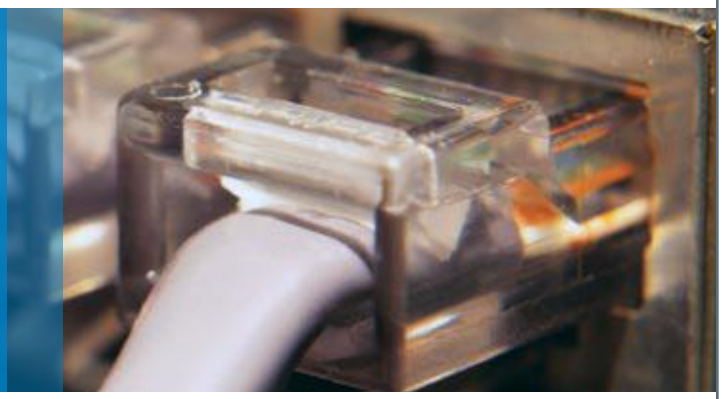
Lumension SECURITY™

EC Suite.com

EC Suite.com Adopts Lumension Security's Positive Security Model to Proactively Remediate Vulnerabilities, Prevent Malware, and Protect against Data Threats



Background

EC Suite.com is an e-commerce solutions provider based in Tempe, Ariz. The 320-employee company offers innovative and integrated e-commerce, digital storefront, hosting, IP transit, CDN (content delivery network) and content protection solutions, including a Windows Media DRM service and SecuredApp application and video game protection for downloadable digital content.

The Challenge

The IT security staff at EC Suite.com is charged with protecting the company's proprietary information and systems. "The very nature of our business demands that we proactively address all potential security concerns, including both external and internal threats," said William Bell, Director of Security. "If our systems are compromised, our clients' sensitive information becomes vulnerable."

Bell and his staff were particularly concerned with viruses, worms, spyware and other forms of malicious code—especially as hackers continued to discover more clever ways to disguise attacks and exploit zero-day vulnerabilities. Another major security concern for Bell and his staff was removable storage media. By plugging a cell phone, PDA, USB memory stick or other device into a corporate PC, laptop or server, an employee could easily pilfer sensitive information or inadvertently introduce malware.

To combat malware, EC Suite.com deployed traditional anti-virus and anti-spyware on its desktops and servers. While these solutions sufficiently blocked known threats, Bell realized that were not the most effective for dealing with unknown, emerging malware designed specifically to subvert blacklisting technologies.

"Traditional security systems protections such as AV and anti-malware are too reactive to rely on alone," said Bell.

"Our philosophy is that our security should be able to stay ahead of threats rather than just reacting to them," said Bell. "If a virus or other piece of malware slips past your defenses, it can run amok and wreak all kinds of havoc. Traditional solutions simply didn't offer the level of protection we were looking for, especially against zero-day threats and the more sophisticated viruses that propagate using removable storage media."

Solution and Benefits

With multiple companies under the EC Suite.com umbrella, there are no large departments with homogeneous system configurations within the company. And yet, with the help of Lumension's vulnerability management and endpoint security solutions, Bell and his staff were still able to construct a multi-layered security approach that worked across the entire organization.

In mid-2006, Bell was introduced to the Sanctuary endpoint security management suite. Sanctuary flips the traditional security model on its head by enabling administrators to create an automated whitelist of allowed applications and devices. All forms of malicious code, all unwanted software and all unauthorized devices are denied by default. Any device or executable that is not on the approved whitelist simply will not work on a Sanctuary-protected corporate endpoint.

Bell received approval from management to deploy Sanctuary on the 320 EC Suite.com systems, and immediately began seeing results. "Before implementing Sanctuary, we were replacing three to five computers every week. After rolling out the product, we replaced 72 percent fewer comput-

ers and there has been an overall decrease in the number of help desk tickets," said Bell. "The reason for this dramatic decrease is that the most common reasons to replace a computer were related to spyware or other viruses, so that immediately stopped because Sanctuary did not allow any malware to run on a company machine."

In early 2007, EC Suite.com added to its security arsenal by implementing PatchLink Update and PatchLink Developers Kit. PatchLink Update provides rapid, accurate and secure remediation for all major applications and operating systems, enabling Bell to proactively manage threats by automating the collection, analysis and delivery of patches and remediation. Bell uses PatchLink Developers Kit for security configuration management, which allows Bell to code his own customized patches, a process that is especially useful when a critical vulnerability is discovered for which a patch has yet to be released.

Bell also uses PatchLink Developers Kit to roll out applications and application packages onto the Sanctuary whitelist for rapid deployment. "The two products work well together, and I am looking forward to implementing Lumension's fully integrated solutions to make our security management processes more efficient as well as more effective."

"We believe in defense in diversity," said Bell. "Sanctuary is our security blanket against any possible zero-day attacks which covers about 90 percent of our security needs. On top of that, patching and remediation is the best way to assess risk and eliminate vulnerabilities before an attack occurs. This multi-layered approach helps us identify and remove vulnerabilities while maintaining a consistent baseline of security. This positive approach to security keeps our digital assets safe. In large organizations, it may take a month to roll out every necessary patch. With Lumension's PatchLink Update, Sanctuary and PatchLink Developers Kit, I can quickly deploy patches—including those I script myself—with the insurance of a 'big brother' protecting our patch cycle."

Lumension SECURITY™

Lumension Security
15880 N. Greenway-Hayden Loop, Suite 100
Scottsdale, AZ 85260
480.970.1025 / www.lumension.com