

THE THIRD IN A SERIES OF 4 >

A SECURE NETWORK-PROTECTION ARCHITECTURE

▶ **CORPORATE IT** departments have worked for decades to build strong defenses against outside assaults on their IT networks.

In recent years, however, such threats have become more sophisticated than ever before. No longer focused merely on hacking or denial-of-service attacks, a new breed of cyber-criminals is aggressively striking at the heart of corporate value, seeking to steal critical financial and other proprietary information that they can sell on the open market.

Unfortunately, current security solutions simply are not up to the task. Web links to malware-infected web pages go unrecognized by most existing IT security systems. Conventional intrusion detection and prevention systems likewise fail because malefactors transmit malware in small bundles that fly below the radar of activity-level monitors—bundles that are automatically reassembled once inside a network. And even data-encryption techniques are easily foiled by malware that steals users' passwords or else operates at run-time, making data theft a simple matter.

A FUNDAMENTALLY DIFFERENT SECURITY MODEL

Clearly, in the face of this host of challenges, it is time for a new enterprise IT security model, one that keeps data-stealing malware out of enterprise IT networks in the first place. The archetype for this new model is Trend Micro's "Smart Protection Network." Built around a next-generation, cloud-centric architecture, the Smart Protection Network is designed to block malware threats before they have the opportunity to

infiltrate corporate IT networks. And if data-sharing malware already has entered this environment, the Trend Micro Smart Protection Network prevents compromised data from being sent back out to malicious, Internet-hosted servers.

The Trend Micro Smart Protection Network thus offers a fundamentally different form of network security, acting like a powerful invisible shield that blocks potential malware threats no matter where they originate or what form they take. The Smart Protection Network maintains this barrier primarily through its unprecedented malware-recognition capabilities. Current IT security solutions fail in part because sophisticated malware can bypass their defenses by transmitting malware via otherwise innocuous emails, web links, or web sites. Through an array of "reputation" technologies, however, the Smart Protection Network peels back these layers of disguise to reveal malware for what it is.

BANKING ON REPUTATION

Three distinct reputation technologies are the cornerstones of the Smart Protection Network's malware-blocking capabilities. These technologies are:

▶ **Web reputation technology**, which analyzes and halts malicious web traffic from coming into or leaving corporate IT networks. This technology operates by assigning web domains a "reputation score" based on a web site's age, previous URL changes, and other factors that might indicate suspicious behavior. The technology then blocks any dangerous URLs or individually hijacked

pages within otherwise legitimate web sites. By excluding only specifically compromised pages, the technology reduces false positives while allowing access to web sites that companies need in order to be productive.

▶ **Email reputation technology**, which stops up to 80% of all email-based threats, including emails with links to dangerous web sites, before these threats ever reach the recipient. The technology works by validating IP addresses against a large and growing reputation database of known spam sources, as well as through a dynamic service that assesses email-sender reputation in real time.

▶ **File reputation technology**, checks the reputation of each file against an extensive in-the-cloud database before permitting user access. Since the malware information is stored in the cloud, it is available instantly to all users. The Cloud-client architecture offers more immediate protection and eliminates the burden of pattern deployment.

PUTTING THE ELEMENTS TOGETHER

The above are key elements of the most effective enterprise IT security system ever created. But it is how these elements work together that make the Smart Protection Network the security powerhouse that it is. We'll explore that topic in the final article in this series ♦



KAWASAKI MOTORS CORP., U.S.A.:
**Less Admin Time Spent
With Trend Micro Solutions**

**41% fewer infected
machines at
University of Windsor
thanks to Trend Micro**

Lakeridge Health
Taps Trend Micro,
Reduces Security
Management
Costs 10-15%

Georgia-Pacific
LLC touts Trend
Micro: "Right
Functionality &
Good Value"

page 3C

CUT COSTS UP TO 40%.*
Think better protection has to cost more?

THINK AGAIN.

*A recent, independent research study shows that Trend Micro™ Enterprise Security, powered by the Trend Micro Smart Protection Network™, can lower your management costs by up to 40%. That's because this next-generation, cloud-client security infrastructure enables a unique combination of solutions and services to stop threats before they reach your network, significantly reducing enterprise risk and productivity loss. Enterprises around the world are saving big and you can too. Run the numbers and see how the Trend Micro Smart Protection Network can help you reduce costs without compromising security.

▶ Try our free, online TCO impact calculator now at trendmicro.com/thinkagain



Securing Your Web World