

A blurred background image showing a person's hand pointing at a laptop screen. Overlaid on the image is a semi-transparent circular gauge with numerical markings from 0 to 7.0.

Trend Micro Enterprise Security

Immediate Protection. Less Complexity. 

 Lower Security Risks
and Costs by
Minimizing the Time
to Protection

A Trend Micro White Paper | January 2009

I. ENTERPRISE CONTENT SECURITY THREATS

The enterprise threat landscape has dramatically changed with the proliferation of a new generation of content security threats. Today's cyber attacks harvest sensitive corporate data and expose companies to the risk of losing revenue, employee productivity, customer relationships, and market reputation. As the headlines prove, targeted threats are hitting companies faster and in larger quantities than ever before.

With this new generation of attacks, the focus has shifted from notoriety and publicity to profiting from threats that steal data and resources. Profit-driven cybercriminals lurk behind most web threats, creating a new generation of spam and malware based on a powerful underground economy. Enterprises are direct targets for cybercriminals, seeking to profit from the stolen data or resources of enterprises. Cybercriminals have also become more sophisticated, delivering faster more insidious attacks. In addition, the volume of threats has dramatically increased. Spam now comprises up to 95 percent of all email and, according to AV-Test GmbH, security vendors collected 1,738 unique threat samples in all of 1988, which grew to 177,615 samples in 1998 and then to over 5 million by 2007.¹

II. CHALLENGES TO CREATING A DEFENSE

Enterprises are spending billions of dollars deploying “best-of-breed” security products, often layering multiple products, in an effort to create a solid defense against the next generation of content security threats. Plus, government and industry regulations and new technology trends—such as the mobile workforce, virtualization, Web 2.0, and third-party collaboration—increase complexity, risk, and cost. To address these problems, enterprises have implemented a wide range of security products—many of them narrowly focused on one security issue. Managing the complexity of point-product sprawl with constant deployment, administration, and support often poses greater problems than the threats themselves.

These changes make mastering enterprise IT security more difficult today than it has ever been before. The 2008 InformationWeek Strategic Security Survey determined that the biggest security challenge is managing the complexity of security. The study also found that 69 percent of businesses believe they are more vulnerable to risks this year than last year because of the increased sophistication of attacks.² Enterprises need a solution that closes the window of vulnerability, while also reducing management complexity—this combination addresses all of the key enterprise security challenges.

III. NEED FOR A NEW PROTECTION PARADIGM

Conventional security solutions cannot combat the new generation of faster, stealthier threats. Most security solutions rely on periodic pattern file downloads that cannot keep up with the volume and speed of today's threats. This reactive approach relies on the discovery of a threat, the creation of a threat signature, and the deployment of the

“Trying to distribute thousands of attack signatures per day to millions of endpoints in a timely manner is not a viable approach. Trend Micro's innovative strategy enhances its detection network to also prevent attacks from even reaching customer endpoints and enterprise networks.”

Ogren Group, August 2008

TREND MICRO ENTERPRISE SECURITY

pattern file. In addition, as the number of threats increase, so does the size of the pattern file that has to be downloaded. This entire process can take hours, if not days, creating a significant window of vulnerability. As more time elapses in identifying and resolving threats, risks and costs increase.

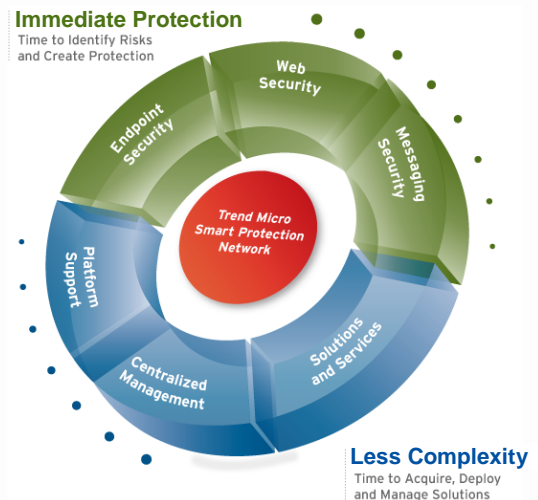
Today's higher threat exposure causes enterprises using conventional content security products to significantly increase costs just to maintain a defense. However, in the future, conventional security solutions will not only be costly and risky, they will be completely unsustainable. Threats are expected to continue to increase exponentially. Pattern files will grow too large to provide an adequate defense and the time and infrastructure needed to deploy them will be impractical, if not impossible. The content security industry needs a new protection paradigm—a solution that minimizes security latency, closing the window of vulnerability.

Better protection should also be easier to manage. A common pain point for security executives is the level of complexity inherent in enterprise security and the time and resources required to keep an enterprise secure. Time is money. But the time it takes to protect the network can also impact more than the bottom line. Enterprises cannot risk delays when it comes to securing private data, business resources, and company reputation. Enterprises need a better approach.

IV. TREND MICRO ENTERPRISE SECURITY

Trend Micro™ Enterprise Security is a tightly integrated offering of content security products, services, and solutions designed to help enterprises stay ahead of content security threats. To offer the best defense with proactive protection, Trend Micro believes there are two critical time challenges to address. First, it is critical to minimize the time it takes to protect the enterprise from new and unknown threats by speeding up the time it takes to identify threats, create protection, and put that protection in place. Second, it should take less time to manage security with a better solution that minimizes complexity while providing effective protection.

Trend Micro Enterprise Security addresses both of these content security time challenges and does so more effectively than any other security vendor in the marketplace by providing immediate protection with less complexity. First you get immediate protection that improves automatically—closing the window of vulnerability. Second, this tightly integrated security provides less complexity and minimizes the time it takes to acquire, deploy, and manage content security. Trend Micro Enterprise Security gets there first—before cybercrime can infiltrate businesses and impact resources.



V. TREND MICRO™ SMART PROTECTION NETWORK

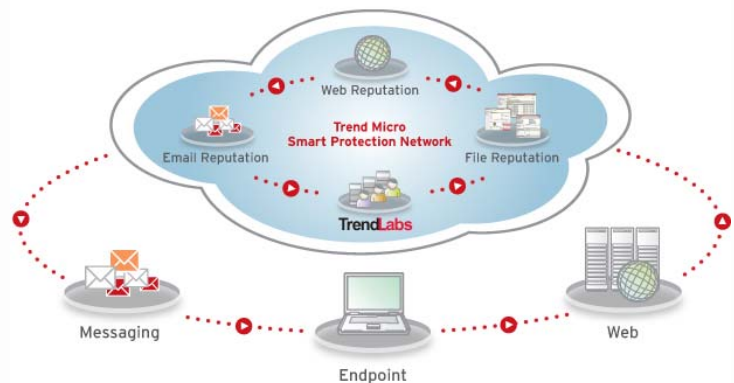
Trend Micro Enterprise Security is able to deliver immediate protection with less complexity because all solutions are powered by the unique Trend Micro™ Smart Protection Network. This innovative approach delivers security that is smarter than conventional methods—blocking the latest threats before they reach the organization to prevent threats from impacting networks and damaging businesses. The Smart Protection Network uses cloud-client architecture that combines in-the-cloud technology and light-weight client infrastructure to quickly and automatically protect information wherever and however an enterprise's employees connect—from home, within the company's network, or on the go.

Smart Protection Network automatically coordinates information from in-the-cloud threat correlation, behavior analysis, feedback loops, and global threat intelligence to dynamically update the web, email, and file reputation databases. This up-to-the minute data is immediately available to the thin-client technologies in Trend Micro products at the customer site.

INTEGRATED REPUTATION DATABASES

Web Reputation

As a critical element of the Trend Micro Smart Protection Network, Trend Micro™ Web Reputation technology guards against web-based threats before they endanger a network or a user's PC. Web Reputation assigns a relative reputation score to domains and individual pages within these domains. Web Reputation then conducts malware behavior analysis, monitoring network traffic to identify any malware activity originating from a domain or web page. Access to malicious web pages is then blocked based on reputation ratings.



Email Reputation

Email is often the entry point of many web attacks. Trend Micro™ Email Reputation blocks up to 80 percent of email-based threats before these threats reach the network or the user's PC. Email Reputation validates IP addresses—or computer addresses—against both a reputation database of known spam sources and a dynamic service that can assess email sender reputation in real time, even blocking spam from botnets when they first emerge. In addition, if Web Reputation determines that a web page contains malicious content, Trend Micro antispam will identify any email containing a link to that web page as spam.

File Reputation

The Trend Micro Smart Protection Network also assesses the reputation of specific files, including files downloaded from websites and email attachments. As cybercriminals move a malicious file from website to website to avoid detection, a reputation may not yet be assessed for each web page that contains this file. But the file's reputation will be triggered wherever the file is found. Trend Micro™ File Reputation checks the

reputation of a file against an extensive database before permitting the user to download it to their system. To continually update the database in real time, File Reputation instigates a data crawl of each file hosted on a web page or attached to an email and conducts an assessment, assigning a reputation to any new files.

CORRELATING THREAT INTELLIGENCE

All reputation databases are updated constantly and share data to provide significantly better protection than would be possible using any of these databases by itself. If any one attack element gets a bad reputation, it is automatically blocked across all threat delivery methods—providing immediate protection at every point of attack. This approach safeguards against all components of a content security threat—spam sources, embedded links, dangerous attachments, and malicious websites.

Not only do the reputation databases share threat intelligence, they also work together to determine if a threat is present. The Smart Protection Network uses behavioral analysis to correlate combinations of threat activities to determine if they are malicious. By correlating different threat components and continuously updating its threat databases, Trend Micro has the distinct advantage of providing immediate and automatic protection from email, web, and file-based threats.

Trend Micro is unique in owning all the security technologies used in this correlation process with a number of patent-pending technologies designed to protect customers from web threats. Trend Micro maintains one of the world's largest, most reliable reputation databases with over 5 billion dynamically rated websites, spam sources, and files every day.

BENEFITS OF A CLOUD-CLIENT ARCHITECTURE

With the Smart Protection Network, not only is threat information correlated, it is also delivered through a cloud-client architecture that enables enterprises to access this information much faster than traditional methods of protection. Conventional content security relies on pattern file updates which are not fast enough to keep an enterprise safe—particularly in today's threat environment. A cloud-client architecture is much faster because it houses immediately accessible threat intelligence in the cloud. Trend Micro can update the reputation databases in real time and enterprises can quickly access this information as needed—no longer waiting for periodic downloads of static pattern files to be protected.

THREAT INTELLIGENCE FEEDBACK LOOPS

Trend Micro is in a distinct position in the security industry—not only does Trend Micro have a vast global customer base, the threat information from those customers is leveraged to gather immediate threat intelligence. Each new threat identified via a single customer's routine reputation check becomes part of a feedback loop that will automatically update databases around the world, blocking any subsequent customer encounters of a given threat. These built-in feedback loops provide continuous communication between Trend Micro products and Trend Micro threat research centers and technologies.

VI. BENEFITS OF TREND MICRO ENTERPRISE SECURITY

COMPREHENSIVE CONTENT SECURITY

Trend Micro Enterprise Security, powered by the Smart Protection Network, creates a unified defense throughout the network with web, messaging, and endpoint security. Up-to-the-minute content security provides complete protection against any attack as well as a comprehensive platform for the integration of future information security technologies. Tightly integrated, centrally-managed security enables seamless inter-product collaboration to guard every network endpoint. Trend Micro Enterprise Security products and services minimize the time it takes to identify risks and secure your network.

REDUCED COMPLEXITY

Trend Micro Enterprise Security not only provides immediate protection, it also provides less complexity through a unified defense that simplifies security management. Unlike conventional security, Trend Micro's cloud-client architecture in the Smart Protection Network reduces the complexity of deploying pattern files by housing threat intelligence in the cloud and blocking content security threats before they even reach the enterprise. The light-weight client architecture and fewer threats on the network take a load off infrastructure resources. With less burden on the network, costs and management requirements are reduced.

- **Holistic Solutions.** While many other security vendors are narrowly focused on securing specific points within the network infrastructure, Trend Micro's international product development teams have designed complete content security solutions that combine integrated, best-of-breed technology with maximum flexibility. Purchasing full solutions from Trend Micro, instead of single point products also offers less complexity by providing one point of purchase, maintenance, and support.
- **Flexible Platform Options.** The flexible platform support of Trend Micro Enterprise Security allows customers to select the solution that best fits their network environment. Trend Micro's enterprise solutions are offered on software supporting over 20 operating systems, Software as a Service (or SAAS), appliances, and software virtual appliances. These platform options optimize and integrate with enterprise network environments, making IT security more efficient.
- **Centralized Management.** In addition, centralized management across these solutions further simplifies configurations and reporting to make managing enterprise security easier and faster. Unlike the multi-vendor best-of-breed security in place at many enterprises, Trend Micro lowers Total Cost of Ownership by providing a comprehensive security solution with shared management tools and technologies that easily integrate into the existing IT infrastructure.
- **Protects Evolving Business Models.** Trend Micro also understands the security requirements for new technologies trends, including protecting mobile workers, Web 2.0 technologies, virtualization, as well as other new and emerging technologies that will support businesses in the future. Trend Micro's cloud-client architecture delivers constantly-updated threat intelligence from minute zero and keeps roaming users protected from web threats when both on and off the network.

All of this adds up to a uniquely cohesive framework of offerings that collaborate to provide the industry's best security with less complexity. Trend Micro recognizes the value of time, and will partner with organizations to save them time, allowing enterprises to focus on other high priority initiatives.

VII. WHY TREND MICRO

Trend Micro has been singularly focused on content security since its founding 20 years ago. With over one billion U.S. dollars in annual revenue, over 1,000 threat researchers—and over 4,000 employees—around the world, Trend Micro has the size, the speed, and the unique in-the-cloud core technology infrastructure required to handle today's enterprise content security. No other security vendor can match the strengths Trend Micro offers enterprises. That is why thousands of enterprises around the globe continue to put their trust in Trend Micro.

“This increasing scale simply breaks the old model as it demands constant signature updates, massive local pattern matching databases, and growing system resources. Trend Micro Smart Protection Network is a new type of security model that is spot on and a view of things to come for threat management.”

Enterprise Strategy Group, July 2008

As the speed of threats increases, so do risks and costs. Enterprises are looking for security that is scalable, manageable, and capable of reliably staying ahead of new threats. Only Trend Micro offers the unique combination of immediate protection with less complexity. Powered by the innovative Smart Protection Network, Trend Micro Enterprise Security delivers immediate protection that improves automatically, closing the window of vulnerability before damage is done. Trend Micro also dramatically reduces the time to acquire, deploy, and manage security. With Trend Micro Enterprise Security, enterprises minimize their time to protection, reducing business risks and costs.

For more information please call or visit us at.
www.trendmicro.com/go/enterprise
+1-877-21-TREND

VIII. REFERENCES

1. AV-Test. “Considerably more viruses, worms and other malware than ever.” Data compiled by Andreas Marx (listed in articles in the AV-Text news archive 11 January 2008). Retrieved from: <http://www.av-test.org/index.php?menu=2&sub=Newsarchiv&lang=0>
2. InformationWeek Analytics. “2008 InformationWeek Strategic Security Survey.” Mike Fratto. June 2008.

©2008 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, and TrendLabs are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. [WP01_TMES-6_081121US]