IDC
Analyze the Future

WHITE PAPER

Network Security Overwatch Layer: Smarter Protection for the Enterprise

Sponsored by: Trend Micro

Charles J. Kolodgy Christian A. Christiansen

November 2009

IDC OPINION

Despite determined efforts to secure their businesses from attacks by cyber criminals and others seeking to steal private and confidential data for financial gain, enterprises continue to experience a steady stream of high-profile breaches against established security infrastructures.

The reality is that existing enterprise security architectures continue to have gaps and vulnerabilities. Well-established best practices and countermeasures to thwart today's complex and sophisticated blended attacks fail to provide the highest levels of protection for many businesses. In IDC's 2008 *Enterprise Security Survey*, over 50% of participating executives were only somewhat confident or not confident in their security systems.

The consequences of a single breach in security can have severe and lasting effects on a business. The impact of an event can damage an enterprise's reputation and credibility. In turn, customer retention suffers. The direct financial impact of a security breach can be substantial. The costs of forensic analysis, employee downtime, and staff time and labor to remediate the effects of a breach are significant. According to the Computer Security Institute (CSI), on average, a single breach can cost a business in excess of $300,000. If the disclosure of private or confidential customer data is involved, levied fines can easily exceed the cleanup costs several times over.

IDC believes that multilayered security solutions offer enterprises a cost-effective and multifaceted alternative to enhance overall infrastructure security posture and improve customer and management confidence levels. By adopting an overwatch architecture with additional security layers that detect and remediate threats that have bypassed perimeter and content security, security managers can reduce the risks of breaches and infections associated with existing unknown security gaps and vulnerabilities. By advancing enterprise security with a multilayered security architecture combined with vendor-supplied security support services, businesses are able to clearly show their commitment to meeting and exceeding today's established best practices in security.

In addition, many enterprises that add an overwatch layer to address their security challenges will gain significant value. The overwatch security layer provides real-time and ongoing visibility into security posture with immediate information on when a security breach has occurred. Enterprises will close the existing day-zero security gap with proactive and automated remediation of a data breach — ultimately helping to ensure more comprehensive protection of corporate assets. Enterprises will be

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

relieved from the costly and time-consuming efforts of manually determining the state of their security posture and cleaning up successful infections.

IDC believes that Trend Micro's overwatch service offering, Trend Micro Threat Management Services, delivers an attractive, high-performance, and cost-effective security solution that promises to raise the bar for enterprises' best practice security requirements.

METHODOLOGY

The premises and opinions of this white paper are based on leveraging a combination of research sources, including IDC primary research as well as historical and current research efforts. In addition, IDC participated in briefings held by Trend Micro in order to gain an in-depth understanding of Trend Micro's Threat Management Services and business proposition.

IN THIS WHITE PAPER

In this white paper, we provide background on today's threat ecosystem with an overview of network security threats, the impact of the threats on enterprises, and the operational challenges faced by IT. We also describe Trend Micro's approach to helping businesses attain enhanced security through the Trend Micro Threat Management Services offering.

SITUATION OVERVIEW

The Evolving Threat Environment

If we lived in a static world, developing effective solutions for known attacks might be achievable over time. However, in today's complex cyber business environment, there is no static state. Too often, attackers are ahead of the curve, continually innovating effective attack strategies and schemes, while security professionals and enterprise IT continue to struggle to keep pace with malicious developments.

Today's enterprise threat environment has evolved and exploded into an assortment of blended attack vectors that effectively work in concert to breach existing security defenses. Because intruders are stealthy, they are able to take advantage of gaps in security to infiltrate and, in some cases, disable existing security systems. Despite concerted efforts to block these attacks as they attempt to enter, enterprise malware breaches continue to occur.

The need has never been greater for enterprises to advance security best practices by continuing to invest in, deploy, and maintain existing security solutions, including firewalls, email, Web, endpoint security, and IPS.

 ©2009 IDC

The Current State of Enterprise Security

The Security Vendor Perspective

Security vendors strive to provide new and innovative products and services that allow customers to rapidly deploy and provide optimal protection against today's continually evolving and sophisticated threat ecosystem.

Despite these ongoing efforts, traditional security solutions and approaches by themselves sometimes fall short in protecting enterprises against many of today's complex and zero-day attack forms. The reality is that due to existing unknown security gaps and vulnerabilities, current enterprise infrastructure security is not 100%.

To assist enterprise IT and security professionals in closing the gaps, security vendors have successfully innovated security solutions that close the window of vulnerability to new threats and demonstrate enhanced defense-in-depth security solutions for their customers. Trend Micro has responded to its enterprise customers' needs with its Threat Management Services overwatch security layer.

The Enterprise Perspective

Many of today's existing enterprise security infrastructures are the result of an incremental and evolutionary process. As a consequence, they generally comprise a series of point solutions, upgrades, and add-ons that are not seamlessly integrated, creating gaps in their overall security effectiveness. Supporting and maintaining these security solutions requires significant amounts of dedicated staff time, and because of the unknown gaps in security, they are vulnerable to attacks that too often lead to expensive cleanup efforts and/or the theft of a business' private, personal, and confidential digital information.

Security professionals understand that these gaps exist and represent risks for them. In IDC's 2008 *Enterprise Security Survey*, only 46% of surveyed participants said that they were very confident or extremely confident of their existing enterprise security. IDC believes that this finding demonstrates a noticeable level of management uncertainty and a lack of confidence in existing security systems. The source of this lack of confidence is largely due to the understanding that existing infrastructures do have security gaps. The absence of an integrated view of what is happening in security infrastructures results in little to no visibility into where and in what forms vulnerabilities exist.

Recognizing that unknown vulnerabilities do exist in security and having an awareness of defense-in-depth approaches to security, where layered security solutions are employed, many enterprises are looking to adopt a solution that provides both comprehensive visibility into the threats that have infiltrated their network and automated remediation.

Enterprise Challenges

Infrastructure Security Visibility

Network infrastructure visibility is a crucial component of an overall enterprise security posture. As discussed earlier, enterprise security infrastructures generally comprise a number of point security solutions. Achieving an overall integrated view of an enterprise's security activities and status is often a difficult and time-consuming task. Because each security component or, in some cases, component groupings produce individual logs and reports, they need to be patched together for review in order to gain a global enterprisewide view of network activities, attack attempts, or malware breaches leading to possible data thefts and damage to their internal security. This time-consuming process provides only a "patched-together" view of the network posture and, more importantly, does not provide continuous, real-time visibility into and reporting when active malware infections have entered the network at the time the breach takes place.

Lack of Skills and Planning

Enterprise network architectures are in a constant state of flux, and due to a lack of resources and knowledgeable security expertise, some businesses are unable to maintain ongoing security best practices that include proactive security planning and ongoing optimization.

Because today's security threats are so stealthy, it is often difficult to impossible to perform root cause analysis to determine how a breach or potential breach event occurred. Without actionable information produced by a root cause analysis, enterprises are unable to develop countermeasures for existing security gaps, and consequently, their businesses continue to be exposed.

Infection Remediation Costs

The costs associated with a single breach, including employee downtime and staff time and labor to diagnosis and remediate the effects, are significant. In the 2008 CSI *Computer Crime & Security Survey*, the average loss per respondent caused by various types of computer security incidents was determined to be $288,618. Dealing with "bot" computers within an organization's network reportedly cost an average of $345,600 per event. Dealing with either loss of proprietary information or loss of customer and employee confidential data cost an average of approximately $255,000.

The Need for an Overwatch Security Layer

Traditional, single-layered security architectures currently represent an enterprise's "best efforts" in securing its businesses from attacks and infiltrations. However, with only 46% of IDC survey respondents indicating that they are very confident or extremely confident about their existing enterprise security, there is significant room for enterprises to improve their security posture and management confidence levels.

 ©2009 IDC

New, multilayered security architectures are raising the bar in demonstrating "best efforts" to protect enterprises from attacks. These new approaches to enterprise security are now demonstrating their enhanced overall effectiveness when compared with existing and earlier enterprise security architectures.

In the new and enhanced security architecture, the existing in-line threat detection forms the first layer and the overwatch component forms the second layer. The second layer or pillar complements an enterprise's existing security infrastructure, preserving an enterprise's current investments in existing security solutions and services, and is independent of the existing deployed technologies, security brands, or form factors.

The new overwatch security pillar acts as an infection detection, containment, and remediation engine that is automatically triggered when a threat has bypassed detection by the existing "in-line" infrastructure and has infiltrated the enterprise network. The overwatch security layer uses data from a real-time reputation and behavioral correlation database to detect active data-stealing malware and other potential threats.

IDC believes that layered, in-line threat detection and threat overwatch architectures provide enterprises with a higher degree of security and are capable of addressing more of their security requirements when compared with legacy security infrastructure architectures.

The key benefits are real-time overwatch, infection mitigation, thorough remediation, and constant improvement. Real-time overwatch sees new instances of malware and other threats when they first arise around the globe. Enterprises will close the existing day-zero security gap with proactive and automated remediation of a data breach.

Overwatch is also synergistic with a customer's existing security solutions. Utilized as part of a multi-layered security approach, Threat Management Services extends investments in:

- Network behavior analysis by detecting "low and slow" malware attacks that may seek a few, carefully selected targets
- Security incident and event management by providing additional visibility into infiltrations that are undetected by conventional security
- Intrusion prevention systems by rapidly identifying new threats and malware that have evaded perimeter security measures
- Network access control by continually monitoring endpoint network activity beyond initial access checks.

TREND MICRO'S THREAT MANAGEMENT SERVICES

Trend Micro Threat Management Services

Trend Micro has taken the multilayered security approach to the next level of sophistication with its Trend Micro Threat Management Services network security "overwatch" service.

Threat Management Services provides an additional security layer that greatly strengthens an organization's security infrastructure by monitoring the network for active infections that have successfully infiltrated. Once the threat discovery occurs, in real time, the network overwatch layer intercepts the attack and performs automated containment and remediation.

Trend Micro's Threat Management Services solution layers into any existing security infrastructure, using noninvasive technology that analyzes network traffic up to the application layer for signs of embedded malware. The Trend Micro solution performs ongoing monitoring for any active malware activity that may be in the process of stealing personal, confidential, and proprietary data and information. The process does not introduce any traffic latencies.

Threat Management Services includes three packages that provide a critical network security overwatch layer for complete threat life-cycle management:

- Threat Discovery Services
- Threat Remediation Services
- Threat Lifecycle Management Services

Threat Discovery Services

Threat Discovery Services provides corporatewide traffic threat detection and analysis capabilities via a threat discovery appliance or any VMware-based system. It is deployed out of band at the network layer on the core switch, where it can monitor the stealth techniques being used by modern malware to provide 24 x 7 network monitoring and detection of hidden malware infections.

The threat discovery technology detects day-zero infections by leveraging Trend Micro Smart Protection Network and multiple threat analysis engines. By performing in-depth correlation analysis, the technology assembles network traffic packets into single streams. Single-session correlation is performed on the network streams, scanning the traffic for exploits and network worms and performing reputation scans on embedded files and URLs.

Threat Discovery Services also provides enterprises with increased visibility into a variety of information security risk factors across their network through a security dashboard as well as executive summary and custom reports, including:

 ©2009 IDC

- Business Risk Meters, which provide a summary of risks associated with detected threats
- Affected Assets, which report on groups and endpoints affected by threats
- Threat Statistics, which report on the types of malware in the network
- Infection Sources, which report on the sources of malware infection(s)

Threat Remediation Services

Threat Remediation Services builds on Threat Discovery Services and includes 24 x 7 monitoring by Trend Micro Threat Management Advisors who provide proactive early warning notifications and remediation advisory services to help diagnose outbreaks, determine containment measures, and provide remediation strategies.

Threat Lifecycle Management Services

Threat Lifecycle Management Services builds on Threat Discovery Services and Threat Remediation Services and includes automated threat remediation and root cause analysis with end-to-end threat analysis and management. In the event a suspected exploit is discovered in a network stream or a routine scan of the on-premise network, the threat mitigator technology will trigger processes to perform pattern-free cleanup and root cause analysis and produce remediation advisories.

The service includes an assigned Trend Micro Threat Management Advisor who offers customized corporate threat security management planning, outbreak drills, infrastructure business impact briefings, and recommendations on security best practices.

CHALLENGES: FIGHTING COMPLACENCY

Enterprise IT and security professionals are being challenged to defend against increasingly complex cyber attacks on their businesses. However, in most cases, they still rely on the tools of "yesterday" to get the work done. In many cases, due to the restraints of reduced security-oriented staff and limited and tight budgets, security managers continue to use what they have always used, even if it isn't totally effective. It is interesting to note that in IDC's *Enterprise Security Surveys*, the overall confidence of respondents in their enterprise security has fallen from 61% in 2004 to 46% in 2008; however, the types of security solutions have rarely changed. What has been changing are the threats. Some IT and security professionals are reluctant to embrace new and innovative security products and services that could improve overall security. Some don't want to address change because they don't immediately see the potential cost benefit or they are content to settle for doing what they have always done, even if that approach doesn't meet the existing threats.

CONCLUSION: GOOD-ENOUGH SECURITY ISN'T

Complacency, or the belief that "good-enough security" is all that is required, seems to be the mind-set of many. Consequently, IT professionals may have settled for security that isn't always effective. In the 2008 CSI *Computer Crime & Security Survey*, 50% of the survey respondents reported that they suffered virus-based security incidents. The survey results also show that one in five suffered a bot attack in 2008. Virus security incidents have been the number 1 attack item for four of the past five years, placing second in the other year. Interestingly, in the 2008 CSI survey, 97% of the respondents reported using antivirus software.

Enterprises cannot accept the inevitability of security breaches because any security breach results in considerable costs, from the direct loss of money with the loss of intellectual property to indirect costs required for cleanup, that can be avoided. Depending on type and scope, a breach can result in tens of thousands to millions of dollars in loss.

IT professionals are under more pressure than ever to deliver a valuable IT infrastructure. At the same time, the threat environment continues to become more complex. Given this duality, IDC believes that security professionals must find ways to protect their businesses with innovative security products and services that assist them in improving overall security without increasing complexity and security staff workload or breaking the budget.

Trend Micro's Threat Management Services provides a comprehensive view of the activities occurring in the network. The solution evaluation offers a unique network security assessment that provides organizations with tangible details on the value of adding an overwatch security layer for a current defense-in-depth strategy.

The overwatch security layer can uncover when a breach has occurred and, more importantly, immediately take action to intercept it and remediate it to ensure that it doesn't happen again. Typically, security solutions are designed to address a single or limited set of pain points but can miss the bigger picture. This permits attackers to create blended threats that are designed to evade standard single-point security solutions. Antimalware protection requires multiple layers of protection. Threat Management Services offers an approach to network security that assesses risk and provides insight on potential gaps within the current security environment.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2009 IDC. Reproduction without written permission is completely forbidden.