Trend Micro’s End-to-End Vulnerability Management: A New Approach to Layered Security

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for Trend Micro
December 2010
# Table of Contents

Executive Summary ........................................................................................................................................1  
Systematic Threats Demand a Systematic Response................................................................................1  
The Reality is Often Different ..................................................................................................................2  
A Better Way .............................................................................................................................................2  
The Trend Micro Approach ........................................................................................................................3  
   An Innovative Partnership .......................................................................................................................3  
   A Greater Role for Host and Network Security in Vulnerability Management ....................................3  
End-to-End Vulnerability Management In Action ....................................................................................4  
   A Broader Approach ...............................................................................................................................4  
   Greater than the Sum of Parts ..................................................................................................................5  
EMA Perspective ..........................................................................................................................................5  
About Trend Micro and Qualys ..................................................................................................................6  
   Trend Micro Incorporated .......................................................................................................................6  
   Qualys Incorporated ...............................................................................................................................6
Executive Summary

The growing capabilities of applications and content delivery technologies have created entirely new architectures that have had nothing short of a transformative impact on IT. With this growth, however, have come new complexities—as well as new ways to exploit sensitive and valuable information resources. An explosion in system and application vulnerabilities has been met with new and sophisticated ways to attack these weaknesses and exploit information assets. This, in turn, has called into question many legacy approaches to security in the face of new risks and new threats.

It has become evident that traditional or “legacy” approaches to vulnerability remediation are insufficient to address the increasingly aggressive threat landscape. No longer can organizations wait until a patch is available to close a high-risk exposure already targeted by a zero-day attack. Organizations need more responsive strategies in order to deal with a fast-changing threat landscape and limit the risks exposed by high-impact vulnerabilities at every level of IT—from networks and systems to applications, and from the data center to the endpoint. These strategies must not only recognize the complexity and severity of vulnerabilities, but also the malware threats often associated with these security issues. They must also recognize the realities of IT as it is today, translating the concept of “defense in depth” into more realistic terms. In short, modern defenses must provide integrated or layered protection in response to today’s more sophisticated IT challenges—from both a security and an operations perspective.

In this paper, ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) analysts take a look at the factors driving this need, and how new approaches to mitigating vulnerabilities such as remediation via vulnerability shielding, also referred to as virtual patching or remediation, provide more practical ways to deliver end-to-end vulnerability management. The Trend Micro approach, in partnership with Qualys, is highlighted as an example of a more comprehensive approach to tackling this challenge, providing continuous assessments and shorter response times in the face of more complex vulnerabilities and threats.

Systematic Threats Demand a Systematic Response

Today’s attacks against IT security are more agile than ever. Custom malware reflects the highly developed state of craft among the malicious that has resulted in an alarming number of data security incidents. According to the 2010 Verizon Data Breach Investigations Report, an astounding 97% of the more than 140 million records compromised in the report caseload were breached through customized malware.¹

These attacks are the evolution of the multifunctional threats that first made their appearance a decade ago. Well-known early manifestations included blended threats and worms such as Code Red, Nimda and similar attacks. Multifunctional threats have since continued to mature in their sophistication over the years, applying new expertise shared within the crimeware community. Designed to work in a...

systematic way, contemporary attacks can target a range of vulnerabilities to achieve a number of objectives of value to the attacker. These may include capturing confidential information, unlocking visibility into sensitive environments, providing a stepping stone to more valuable targets, performing functions such as message relaying, or simply listening and waiting for an opportunity as part of a well-organized network of compromised hosts that can change its shape and definition with often surprising agility.

The Reality is Often Different

Defense, however, may rarely be as well coordinated. Vulnerability assessment, for example, is a common security management tactic—but it is often disconnected from vulnerability remediation and the interim security controls designed to mitigate attack risk. The sheer volume of vulnerabilities in many organizations makes it overwhelming in many cases to prioritize remediation based on asset type and vulnerability severity.

Disconnects between authenticated and unauthenticated scans may also drive a wedge in management strategy. External scans may reveal exposures, but insight into configuration details can only come from access to system internals. The typical tools for collecting this information are the agents of systems or security management, but these tools may have little or no integration with vulnerability scanning technologies, which can make it difficult to correlate the attacker’s view of an opportunity with the corresponding details of system configuration.

This insight is obviously essential to vulnerability remediation, which highlights a further disconnect in many strategies. Defenses are often broadly applied to cover whole environments, with a single system or appliance often deployed to protect an entire network—but there must be a one-to-one correspondence between a specific vulnerability and its resolution. This means addressing each vulnerability on each affected system that presents a potential risk exposure, which can be overwhelming for IT operations management.

Even when a vulnerability remediation strategy such as patch management is in place to deal with large-scale exposures, it may not be responsive enough. Software publishers or specific development teams will manage to their own schedules. And once released patches are made available, it may take days or weeks to evaluate before they can be deployed without fear of disrupting critical functionality. Meanwhile, attacks may be active in the wild—and in the case of zero-day threats, they are active before the vulnerability is even known.

These breakdowns may do more than increase or prolong security exposures. Multiple tools with little coordination can lead to needless redundancies as well as gaps that can drive up IT management costs without significantly improving security outcomes—if improving them at all.

A Better Way

If, however, vulnerability assessment and the tools of defense were better integrated, gaps could be closed that could improve vulnerability and threat correlation, provide more timely and actionable threat response, and enable more effective long-term remediation. These capabilities would not only improve the security posture, but would also provide a more efficient and cost effective approach to security and risk management.
The Trend Micro Approach
As one of the leading vendors of security products adopted by businesses and individuals worldwide, Trend Micro is well positioned to address the impact of these issues in actual practice. Trend Micro has also distinguished itself as a forward thinking vendor, with a strategy that has most recently included the broadening of its portfolio into areas where some of its most direct competitors have yet to invest, such as its Cloud-based Smart Protection Network and its Deep Security solutions for securing modern data centers, particularly where virtualization plays a significant role.

Today, Trend Micro is further extending its vision of security that recognizes the gaps in many current strategies, with a new and distinctive approach to end-to-end vulnerability management.

An Innovative Partnership
A highlight of this new approach is Trend Micro’s partnership with one of the leading names in vulnerability management. With its pioneering Software-as-a-Service (SaaS) model, Qualys became an early transformational force in the security market that changed the nature of vulnerability assessment for its customers. Trend Micro’s Vulnerability Management Services, powered by Qualys, provides an actionable platform that customers can use from day one, directly reflecting the view of the attack surface the adversary has. This capability is complemented with an on-premises approach that integrates directly with the hosted service to provide a comprehensive, centralized view of vulnerability assessment both inside and outside the enterprise.

The value of the internal view cannot be overemphasized. Today’s malware often directly targets enterprises users, often via spam or direct Internet attacks via the browser or Web applications, and leverages their privileges to gain access to sensitive internal information. The increased availability of detailed intelligence into the activities and interests of potential targets gives attackers a much wider range of tools for successfully penetrating the enterprise, contributing to the sophistication of attacks beyond technology alone. The success of these threats requires visibility into activity inside the enterprise, in order to determine where legitimate user privileges may have been exploited to compromise access to sensitive data.

This emphasizes the need for visibility at the level of individual systems, which are often the target of initial attack and the first point of entry for modern malware.

A Greater Role for Host and Network Security in Vulnerability Management
Authenticated scans are often used to gain this visibility inside targeted systems. Even when accessed via authentication, however, off-host scanning may not be able to deliver the depth of information that on-host management tools can provide. Configuration management systems may be engaged to provide this detail, but these tools cannot provide the defensive capabilities of anti-malware or host intrusion prevention. Nor do they have the more extensive support of security tactics such as global intelligence networks that reinforce today’s security management systems.

This highlights one of the most overlooked opportunities in security management: the ability to deepen vulnerability data with not only the insight, but also the defensive capabilities of other security technologies in an approach that complements visibility with actionable defense and remediation.
This is the opportunity that Trend Micro and Qualys are seizing with their partnership in end-to-end vulnerability management.

An example of how this partnership works in practice illustrates the value of the joint solution.

**End-to-End Vulnerability Management In Action**

When a new exploit appears in the wild, it is typically identified by threat management technologies such as Trend Micro’s Smart Protection Network, which incorporates feedback from its antivirus and intrusion detection systems. Malware pattern files are then quickly updated and distributed to Trend Micro threat defenses. Often, however, a threat may be released into the wild before the vulnerability it targets is known (a “zero-day” attack). Once the specific vulnerability is discovered, it is documented and added to the library of known vulnerabilities evaluated by vulnerability assessment tools.

This is where the Trend Micro and Qualys solutions begin to reinforce each other. Trend Micro’s host-based anti-malware and intrusion prevention systems, such as Deep Security, can share threat information as well as any status of current protections with Qualys vulnerability data, so that vulnerable systems can be immediately protected from attacks that target the exposure. Trend Micro intrusion prevention technologies can inspect network traffic for content that targets a known vulnerability, blocking it from reaching its destination and shielding the vulnerability from attack. This enables the Trend Micro system to deliver defense on multiple levels: threat management through integrated anti-malware and host defense, and protection for known vulnerabilities through the shielding or virtual patching techniques of Trend Micro intrusion prevention.

This protects specific vulnerabilities from exploit, even though a software patch may not yet be available for the issue. Once a patch becomes available, IT organizations can be more deliberate and careful in evaluating the impact of patching, since protection is already in place through the vulnerability shielding capabilities of vulnerability-aware Trend Micro defenses. This allows organizations to operate less in “fire fighting” mode, with greater latitude for exercising care in long-term resolution of critical vulnerabilities. Together, this lightens support burdens and reduces the risk of unexpected consequences from patching, which can help lower IT support costs.

**A Broader Approach**

Simple threats, however, are no longer the norm as they once were. Today’s more complex threats may have multiple components, assembled in a sequence directed by the attacker—or by the attack itself. This requires a deeper level of insight into threat behavior. This insight comes from multifunctional intelligence resources such as the Trend Micro Smart Protection Network, which examines multiple aspects of a potential threat, including referenced IP addresses or Web URLs, before malicious content such as spam or malware downloads reach their destination. This enhances the capabilities of Trend Micro threat defense in alignment with Qualys vulnerability awareness.

The Trend Micro solution takes the concept of layered security to an entirely new level in modern data centers, going beyond malware protection and remediation in physical systems alone. Trend Micro Deep Security also provides vulnerability shielding and defenses for virtualized environments, including agentless anti-malware. This includes the ability to defend individual virtual machines within a virtualized physical host, as well as defending virtual machines from other virtual systems, regardless whether on the same physical host, or on other hosts in the environment. Trend Micro Deep Security
inspects inbound packets for potential exploits against vulnerabilities and applies shielding rules to prevent attack. It also scans physical and virtualized systems for determinations of operating system, service pack and patch level, as well as installed applications and software versions. The Deep Security solution provides policy recommendations, threat defense, host protection, intrusion prevention and vulnerability shielding at each level, addressing a number of security requirements with a unified solution for modern data centers.

Trend Micro’s Vulnerability Management Services, or the Qualys aspects of end-to-end vulnerability management, go beyond the assessment of external host exposures. Scanner appliances can be placed inside protected networks, to provide insight into vulnerabilities within defended environments and securely coordinate assessment both inside and outside the enterprise. Vulnerability Management Services also provides vulnerability assessment for Web applications, addressing a far more substantial range of frequently exploited vulnerabilities, and broadening the scope of the comprehensive solution.

**Greater than the Sum of Parts**

These examples highlight how security solutions can provide greater value in combination than in isolation. Threat-aware defenses may not always identify vulnerabilities that require remediation—but when they are, they can deliver interim remediation in advance of more comprehensive pattern files or patches, even when an attack may not have yet been released into the wild. Once vulnerabilities are known, the capabilities of Trend Micro end-to-end vulnerability management in partnership with Qualys deliver protection that is both broad and deep, combining the breadth of Qualys vulnerability assessment capabilities with the depth of Trend Micro threat research and defensive resources such as vulnerability shielding. This provides more comprehensive remediation for actively exploited vulnerabilities, enabling IT organizations to prioritize long-term response more cost effectively, and deploy remediation with greater latitude for evaluating the impact of long-range techniques such as patching, software or system update, or reconfiguration.

**EMA Perspective**

Security has long been plagued by the silos of functionality that isolate—and ultimately cripple—effective defense. This leaves organizations more exposed to high-risk exploits than they should be. Gaps do more than heighten the risk of attack, however. Disjointed defenses also shift burdens into IT operations teams, when they must scramble to patch high-risk vulnerabilities as quickly as possible, with negligible prioritized “patch” guidance and limited regard for the impact of unexpected outcomes. As high a priority as security has become in the enterprise today, defense should deliver more.

---

Today, the risk of exposing gaps in defense are higher than they have ever been, and the stakes are only likely to escalate. Modern attacks—and attackers—are far more coordinated than many legacy defenses.

---

Today, the risk of exposing gaps in defense are higher than they have ever been, and the stakes are only likely to escalate. Modern attacks—and attackers—are far more coordinated than many legacy defenses. Indeed, attacks often directly exploit these gaps in defense, when threats outpace the ability
of organizations to respond, either in recognizing the coordinated nature of attacks, or in protecting critical vulnerabilities. Moreover, too many legacy defenses fail to realize the realities of modern IT. Virtualization is fast becoming the norm in many data centers today, yet “defense in depth” still too seldom applies to the virtual environment in many traditional approaches.

The partnership of Trend Micro and Qualys in end-to-end vulnerability management confronts these realities directly. It strengthens threat defense with vulnerability awareness, with the attacker’s perspective both inside and outside the enterprise. It complements the breadth of insight of both the comprehensive QualysGuard system and the Trend Micro Smart Protection Network, with depth at multiple levels of both physical and virtualized environments. This introduces a new level of realism to the concept of “defense in depth” in the face of equally coordinated—and far more malicious—attacks against today’s vital information assets.

Enterprises would be well advised to investigate this partnership in end-to-end vulnerability management for the synergies it delivers, particularly in the added value it offers to IT operations management in giving response teams greater latitude for evaluating long-term remediation through software update or configuration management. These benefits emphasize the advantage organizations can gain when security solutions capitalize on the all-too-seldom realized promise of coordinated defense that is greater than the sum of its parts.

About Trend Micro and Qualys

Trend Micro Incorporated

Trend Micro Incorporated, a global leader in Internet content security and threat management, aims to create a world safe for the exchange of digital information for businesses and consumers. A pioneer in server-based antivirus with over 20 years experience, Trend Micro delivers security that fits its customers’ needs, stops new threats faster, and protects data in physical, virtualized and Cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, Trend Micro’s industry-leading Cloud-computing security technology and products stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit www.trendmicro.com.

Qualys Incorporated

Qualys, Incorporated is a leading provider of on demand IT security risk and compliance management solutions — delivered as a service. Qualys’ Software-as-a-Service solutions are deployed in a matter of hours anywhere in the world, providing customers an immediate and continuous view of their security and compliance postures. The QualysGuard® service is used today by more than 5,000 organizations in 85 countries, including 45 of the Fortune Global 100 and performs more than 500 million IP audits per year.
About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise IT professionals, lines of business users, and IT vendors at www.enterprisemanagement.com or follow EMA on Twitter.

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. “EMA” and “Enterprise Management Associates” are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2010 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.

Corporate Headquarters:
5777 Central Avenue, Suite 105
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com