SearchSecurity.com E-Guide

# Best Practices for Integrated Threat Management

Slithering across today's threat landscape are stealthy, financially-motivated attackers who exploit vulnerabilities in endpoint devices. Too many of their attacks are sophisticated enough to avoid detection by traditional security solutions. And too often the targeted organizations, small and large alike, suffer disruption of business-critical services and discover too late that their data has been manipulated or stolen.

This expert E-Guide takes a look at the integrated threat management landscape and details some tips and best practices to properly deploy an integrated threat management solution. Find out how integrated threat management can help ease compliance burdens and what to look for in a threat management solution.



TechTarget
The IT Media ROI Experts

SearchSecurity.com E-Guide

# Best Practices for Integrated Threat Management

## Table of Contents:

# What integrated threat management delivers

By Carol Weiszmann and Susan Messenheimer

Server, desktop, and notebook computing environments—the endpoints of the enterprise IT infrastructure—have transformed the way we do business. But the price is complexity—increasingly intricate operating systems and browsers, fat office suites, specialized business applications that deal in more media than ever before.

All this has attracted the bad guys, who have of late been spreading malware and exploring client-side exploitation.

So, in addition to staving off network-based attacks, providers of information security solutions must respond to an evolutionary progression in endpoint threats. What began as DOS viruses a generation ago has sprouted into macro viruses, mass mailing viruses, spam, spyware, and, most recently, blended threats in which viruses, worms, trojans, spyware, botnets, zero-day threats, port attacks, keylogging, phishing, and spam have converged.

Slithering across today's threat landscape are stealthy, financially-motivated attackers who exploit vulnerabilities in endpoint devices. Too many of their attacks are sophisticated enough to avoid detection by traditional security solutions. And too often the targeted organizations, small and large alike, suffer disruption of business-critical services and discover too late that their data has been manipulated or stolen.

## A structured, proactive, centrally managed line of defense

In response to this endpoint complexity and the intensifying risks it engenders, security vendors are integrating the protection they provide to span the endpoint, vulnerability assessment, and risk management. Some do this by adding to existing firewall solutions. Others anchor broadened capabilities on their antivirus platforms.

Either way, this kind of integrated threat management—also referred to as unified threat management—establishes a structured, proactive, centrally managed line of defense from the operating system(s) to applications to the network that is able to address both known and unknown threats. This sort of integrated threat management solution generally is delivered via one or more appliances that include

- *A network-aware policy* engine that dynamically manages policies and configuration settings based on physical network location.
- *A centralized management console* to simplify policy enforcement, scan scheduling, audits, and generation of the detailed reports that ease analysis.
- *Vulnerability assessment* that defines, identifies, and classifies security risks and vulnerabilities in operating systems and applications as well as the network.
- *Intrusion prevention* that, via analysis of network traffic, identifies and blocks malicious data while allowing legitimate traffic to be processed—so both attacks from outside an organization as well as dubious internal activities are stopped.

- *Proactive host-based protection* against zero-day attacks, buffer overflow, and memory-based attacks.
- *System and application firewalls* to control the network activity of systems and installed applications.
- *Virus, spyware, phishing, and botnet protection* that checks each process and application before it's loaded, thus providing in-memory protection and disk scanning for computer viruses, worms, trojan horses, spyware, botnets, and blended threats.
- *Identity theft protection* to intercept attempts to deceive users with misleading HTML and XML in email and web pages.

## Fast deployment, lower TCO

Unlike point solutions, integrated threat management solutions ease deployment and management burdens precisely because they integrate so many previously discrete functions. eEye Digital Security's Integrated Security & Threat Management Appliances, for instance, can be deployed and scanning in as little as 15 minutes, thanks to its best-practice default settings and an automated, wizard-driven installation process.

Integrated threat management solutions lower total cost of ownership (TCO), too, by reducing administrative overhead—including management and help desk costs—and rationalizing security policy enforcement. And the best of these solutions are built for scalability, so adding new appliances is straightforward.

In addition, risks are mitigated because these appliances inherently provide layered defense, which results in fewer compromises, more consistent service continuity, and better compliance.

# How integrated threat management eases compliance risks

By Carol Weiszmann and Susan Messenheimer

Integrated threat management appliances are appealing for a variety of reasons, including quick deployment and lower cost of ownership. They also can help organizations cope with the compliance requirements that impact just about all businesses, large and small.

Regulations like Sarbanes-Oxley, which affect publicly-held companies, get most of the press. But there are plenty of regulations with security implications that hover over smaller businesses, including HIPAA (Health Insurance Portability and Accountability Act), California's SB 1386 data breach disclosure law, and even the Gramm-Leach-Bliley Act, which covers the likes of those who prepare income tax returns, debt collectors, consumer credit counseling and reporting agencies, and real estate transaction settlement services.

All of these—and plenty more—carry the force of law, and failure to comply can result in fines and even criminal charges as well as civil lawsuits. In addition, other standards that don't have the force of law—notably PCI DSS (Payment Card Industry Data Security Standard), which covers credit card transactions and is legally mandated only in Minnesota—nevertheless can impose fines or the loss of essential privileges on violators.

## Relief from compliance burdens

Because a company deploying an integrated threat management solution deals with one or two appliances rather than a parade of disparate point products, it gets significant relief from compliance management burdens.

Consider PCI DSS, which mandates that retailers ensure that credit card transaction data transmissions are securely separated from other network traffic. This must be done without impeding movement of other data or the ability to retrieve antivirus updates.

It's a tall order that's neatly fulfilled by an integrated threat management appliance that includes a firewall capable of segmenting network traffic and imposing different security rules for each segment—all while maintaining other key security functionality, such as continuous threat scanning, antivirus updating, and intrusion prevention.

An integrated threat management appliance can also log security data, collecting the audit information essential to maintaining PCI DSS compliance. This is immensely valuable, since one of the largest compliance costs comes from the need to gather and package data demanded by auditors.

What's more, security policies and events can be monitored and adapted to events from a central console. That capability can be especially important for smaller distributed businesses that can't afford to put an IT staffer in every location. With integrated threat management solutions, they don't have to.

## Built-in best practices

Another aspect of regulatory and standards compliance involves risk assessment. All organizations affected by

HIPAA, Gramm Leach Bliley, and FISMA (the Federal Information Systems Management Act, aimed at Federal agencies and their contractors), for instance, are required to assess their risks. However, the protocol for doing this, the National Institute of Standards and Technology's NIST 800-30, is complex and difficult.

Integrated threat management solutions that carry built-in best-practices configuration settings as a default can go a long way to helping companies assess their risks—and reduce them—without spending a lot of money on consultants.

What's more, the extensive reporting and logging capabilities built into an integrated threat management solution mean threats can quickly be identified and neutralized—and the log may become a crucial aid to post-event audits and investigations.

End-to-end security has become a necessity for all businesses, which is why security-oriented standards and regulations have become such an important part of IT. It's also why auditors look for strong, well-implemented security solutions that can monitor, detect, and remediate attacks of all kinds—known and unknown, from without and from within.

Integrated threat management solutions go a long way to making such end-to-end security practical and cost-effective.


## Professional-Grade Security Solutions for Demanding Technical Specialists

Integrated Security & Threat Management solutions from eEye Digital Security help IT Pros responsible for application, networking & desktop security automate internal security administration and eliminate complexity. Over 9,000 private and public organizations around the world use eEye security software, appliances, and advanced security intelligence services to:

- Protect critical information across all systems
- Enforce PCI, HIPAA, and other compliance initiatives
- Identify network vulnerabilities and manage threats
- Implement a consistent and comprehensive security strategy
- Eliminate the need for multiple endpoint security products

## Quality matters. Choose eEye.

To learn more, please visit www.eeye.com
or call 866.282.8276

# What to look for in an integrated threat management solution

By Carol Weiszmann and Susan Messenheimer

Since there's a limit to the practical number of host-based security products an enterprise can deploy and manage, vendors have taken another approach: integrate a variety of endpoint (i.e., server, desktop, notebook) defenses into a single suite, generally delivered in an appliance.

These integrated threat management solutions typically include

- *Protection against malware*
- *System and application firewalls*
- *Intrusion prevention*
- *Email and web filtering (identity theft protection)*
- *A centralized management console*

Integrated threat management solutions have become popular because they're effective. They reduce costs, thanks to a consistent cross-functional interface, consolidation of event logging and reporting, and simplification of network architecture—all of which eases management efforts.

So what considerations matter when it comes time to choose an integrated threat management solution?

## What matters most

There are some key capabilities to look for.

***How integrated?*** Look for integrated threat management solutions that bring disparate components into a consistent, well-managed whole.

***Management reach.*** As various kinds of security functionalities converge in one or a few appliances, things inevitably get complex. Integrated threat management solutions are doing a lot of work: parsing vast number of files for malware, monitoring numerous processes and operating system settings in search of questionable actions, sifting through countless packets as part of intrusion-prevention and the firewall. And all of this is orchestrated in adherence with policies that must adapt to changing conditions

So it's important that an integrated threat management solution be easy to set up, configure, manage, and update. That's why a well-organized, intuitive management console is essential. All the better if the solution includes vulnerability assessment capabilities that define and identify security risks across the enterprise and provides a network-aware policy engine that dynamically manages policies and configuration settings.

***Anti-malware.*** Look for solid anti-malware scanning. This should include scanning for viruses, worms, trojans, spyware, phishing, and botnets.

***Going dynamic and deep.*** Make sure the solution does dynamic rather than just static packet filtering, so the state of active connections is monitored and this information is used to decide which network packets to allow through the firewall. It should also do deep packet inspection, so it can examine the application payload of a packet or traffic stream using both signature-based and heuristic content analysis to determine the legitimacy of the data.

***Effective host-based intrusion prevention.*** Look for host-based intrusion prevention with the ability to detect and stop client-side attacks, including zero-day exploits.

***Scalability.*** Look for a solution that can handle adding new boxes to an existing deployment and can manage distributed appliances at regional branches.

**Performance and necessary functionality.** Think about the functionality that's really needed. With integrated threat management solutions, there's a tradeoff. Firewalls and intrusion detection functions tend not to be compute-intensive, but they're not very tolerant of latency. On the other hand, anti-malware and web filtering are latency-tolerant but also compute-intensive. When these two types of services are combined, latency-sensitive applications may suffer.

To get a sense of how a solution performs in the real world, look for performance tests that combine key functions.

---

**About the authors:** *Carol Weiszmann and Susan Messenheimer are partners at aimpublications.com, a content consultancy at the intersection of technology and business. They analyze and write about how key information technologies impact enterprise security, compliance, infrastructure, productivity, and profitability.*

# Resources from eEye Digital Security


Podcast on Integrated Security, Threat Management, and Endpoint Protection

Blink 4.0 Endpoint Security Product Datasheet

Blink Pre-Recorded Product Webinar & Demo

## About eEye Digital Security

eEye is pioneering a new class of security products: Integrated Threat Management. This next-generation of security detects vulnerabilities and threats, prevents intrusions, protects an enterprise's key computing resources, from endpoints to network assets to web sites and web applications, all while providing a centralized point of security management and network visibility. Products include: Retina Network Security Scanner, Retina Web Security Scanner, SecureIIS Web Server Security, Iris Network Traffic Analyzer, Blink Endpoint Protection, and Preview Security Intelligence Services. eEye's research team is consistently the first to identify new threats in the wild, and our products leverage that research to deliver on the goal of making network security as easy to use and reliable as networking itself. eEye protects 9,000+ organizations worldwide, including half of the Fortune 100.

www.eeye.com