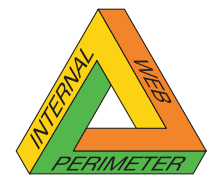


Centralizing Security:

Why unified security architecture is the best defense



Intelligent Security

Check Point protects every part of your network—perimeter, internal, Web—to keep your information resources safe, accessible, and easy to manage.

Contents

- Introduction 3
- What's out there 4
- The going approach 5
- A unified architecture 6
- Check Point's take 7
- Conclusion 8

INTRODUCTION

In today's fast-paced Internet age, it's no secret that enterprises must balance increasing demands for access to information with the need to protect the privacy and integrity of the data itself. The equation is simple: as soon as network administrators install a new system, they must find a way to secure it. Because so many enterprises have so many systems, security technologies have proliferated like wildflowers. Firewalls, virtual private networks (VPNs), antivirus filters, intrusion detection and prevention tools—you name it—most enterprises have them in droves. Some network administrators report they have so many security technologies that they're not even sure which ones they've got.

Generally, security solutions protect one of four areas of the network: the network perimeter, the network core, the Web, or the endpoints. As network administrators install more and more of these piecemeal solutions to protect assets, managing all the devices becomes challenging if not impossible. How do they know one device can communicate with another? How do they know all the devices are installed with the latest security protections? How can they maintain the panoply of devices without spending the entire IT budget for the year? Administrators who take the reactive approach ask themselves nagging questions like these every single day.

Beyond management, another challenge is compliance with federal regulations that govern the way enterprises collect, store, and audit mission-critical information. Regulations such as the Health Insurance Portability and Accountability Act of 1996, the Gramm-Leach-Bliley Act of 1999, and the Sarbanes-Oxley Act of 2002 all require companies to focus on reporting, hiring audit firms to make sure information is accurate, and installing complicated IT infrastructures that prove financial and private customer information is secure. To do this, enterprises first must control their data, and then they must control the act of securing it.

Most important, enterprises must mitigate risk and maximize security in a way that ensures business continuity, maintains budgets, and achieves operational efficiencies across the board. A smorgasbord of point solutions is a costly, time-consuming, and inefficient way of handling security skirmishes. Instead, the challenge calls for a new security management model that weaves disparate security elements into a single, centralized security architecture that is easy to install, easy to manage, and easy on the budget. Think of network defenses like an army: With threats and other security risks increasing every day, the best defense is unified security architecture.

WHAT'S OUT THERE

Just as the best products are those with clearly defined markets and customers, the very best security strategies are those carefully designed to fight specific threats. The threats of today are nothing new: viruses, Trojans, worms, and malicious software continue to reign supreme on the list of what threatens the security of an enterprise. According to IDC's Enterprise Security Survey 2005, more than 57 percent of 473 respondents stated that various forms of malware comprise the greatest threat to their enterprises. Spyware was a close second on that list—not surprising when one considers recent reports that these threats tripled over the course of 2005.

Although network administrators have identified these threats as preeminent, they still occur frequently. In the same IDC study, nearly 40 percent of respondents reported successful attacks on their systems, and 50 percent of the 160 companies with more than 1,000 employees reported at least 11 successful attacks. Figures from the InformationWeek U.S. Information Security 2005 report support this data, indicating that two-thirds of the 2,540 IT professionals surveyed said that their companies were targeted by a virus at some point between August 2004 and August 2005. Pick any other report and you'll find similar stats. The numbers don't lie.

Adding insult to injury, threats today are bigger and badder than ever. Just as networks have gotten more complex, so too have the tools used to destroy them. The newest class of attacks is constantly evolving, making it difficult for enterprises to stay one step ahead of potential problems. Case in point: worms and other attacks that not only target network components and the firewalls, but also look to exploit vulnerabilities in operating systems, Web applications, and other programs running on the network. Another problem is what is known as the "Day Zero" proliferation effect of viruses, whereby a piece of malicious code can traverse the entire world in less than 24 hours.

Threats from outside a network aren't the only problems. A recent report from Gartner indicated that IT designed to prevent intrusion from the outside doesn't necessarily keep confidential data inside the enterprise. The study estimates that 84 percent of high-cost security incidents occur when insiders send confidential data outside the company. To prevent this, enterprises must invest in safeguards that prevent the transmission of confidential data outside the network. These types of systems exist, and are designed to help enterprises comply with federal reporting regulations. The downside: They are expensive and, like other security products, have proven to be difficult to manage.

THE GOING APPROACH

To date, enterprises have responded to these escalating threats by investing in a wide array of specialized security solutions. Taken individually, these products are designed to secure an enterprise in one of four major areas: the network perimeter, the network core, the Web, and the endpoints. At face value, the products work—firewall products stop threats at the perimeter, antivirus software stops threats on endpoints, and so on. Collectively, however, this piecemeal approach to network security always seems to be one step behind.

Why? For starters, few of these products—especially those from different vendors—can communicate with each other to prepare for the latest threat. Secondly, each security product requires different management interfaces to define and manage security policies, complicating a process that should be easy given what's at stake. Next, as the network perimeter continues to expand, enterprises must allow secure access for new constituents, using a range of devices such as PDAs and laptops that might not have appropriate endpoint security precautions. With so many users accessing the corporate network from so many different spots, there's simply no way to make sure everyone is secure.

To address this challenge, many companies have introduced integrated security appliances or Unified Threat Management (UTM) appliances. Typically, UTM appliances combine firewall, intrusion prevention, and antivirus, but they can also include anti-spyware, URL filtering, and other content security technologies. This development has greatly simplified the problem of managing point solutions in the enterprise. However, many solutions still lack extensive integration even though they reside on the same device. Also, managing multiple UTM appliances along with other aspects of security such as endpoint protection continues to be a challenge.

Many organizations are realizing that true UTM goes beyond a single integrated device and requires a high degree of management integration of all security components utilized across the entire organization, including centralized updating of security protections and centralized reporting. Today's increasingly complicated security threats have driven up the complexity of security, leaving many administrators struggling to keep pace. The 2005 IDC study indicates that 40 percent of surveyed enterprises cited lack of resources as their biggest overall security management challenge. With so many security technologies and so little time, right now is when administrators must have a unified security architecture to meet the ever-increasing challenge of maintaining a successful security posture.

A UNIFIED ARCHITECTURE

The benefits of unified security architecture are plentiful. For starters, a unified architecture tackles security across the four most critical layers of network security: the network perimeter, the network core, the Web, and the endpoints. Second, a single architecture is compatible with all security devices on a network, no matter which vendor made them or where on the network they sit. Perhaps most important, unified security architecture offers a single interface to manage all security devices including endpoints, facilitating network management for overworked administrators who previously had not been able to keep up with the overwhelming number of security devices in an enterprise.

This single console not only makes management easier, it also helps administrators implement and enforce security policies and make sure their network has all of the latest protection against threats. Because administrators can control the system from one single spot, once they upload the latest security signatures they can deploy them to every device on the network with the click of a mouse. As the Tolly Group noted in a February 2005 white paper, a centralized management capability that does not require command-line interaction on a device-by-device basis can save hours of administrator time—a reality that adds to the total cost of ownership (TCO) of security equipment overall.

Another bonus of the unified security architecture is closer monitoring of security event management, providing network administrators and chief Internet security officers (CISOs) with end-to-end visibility to validate and audit security effectiveness. This comes in handy for two reasons: First, because it's always good for administrators to see what's happening on their networks, but second, because a system that records every security event meets perfectly with the requirements of federal reporting requirements. Using unified management solutions, network administrators can solve the compliance issue without investing big bucks in a cumbersome system that doesn't scale. In the process, they also make the network safer.

Unified security architecture also is better than strategies of years past because it incorporates endpoints, ensuring that security policies on laptops, PDAs, and other mobile devices are consistent with overarching network security policies so unsecured endpoints do not compromise network security. Finally, having an easy-to-learn, unified approach to security enables network administrators to cut the time they spend training other security professionals on monitoring the enterprise network in their absence, freeing up security personnel to perform other mission-critical tasks and saving money down the road.

CHECK POINT'S TAKE

No vendor delivers unified security architecture as sophisticated as the NGX platform from Check Point Software Technologies. The Check Point approach is a security platform that enables enterprises of all sizes and organizational structures to reduce the cost and complexity of security and ensure that their security systems easily can be extended to adapt to new and evolving threats. The NGX platform is a major upgrade to the core technology underlying Check Point's market-leading VPN, firewall, and management solutions. It delivers new features and extended functionality to more than 20 Check Point products, including VPN-1® Power™, VPN-1 UTM, Check Point Integrity™, Connectra™, Eventia Reporter™, InterSpect™, and SmartCenter™, to name a few.

The NGX platform delivers unified enforcement and management across the four most critical layers of network security: the network perimeter, the network core, the Web, and the endpoints. Specifically, some of the platform's features include:

- Unified security management that reduces overhead by allowing administrators to define, manage, and update policies on the network perimeter, network core, Web applications, and endpoints centrally from a single SmartCenter console
- An integrated SmartDefense™ Services console that enables network administrators to update Check Point enforcement points globally, and apply defenses for new protocols, applications, and threats without service interruptions
- Expanded intelligent inspection technologies that secure the network, Web applications, and endpoints from threats to ensure the confidentiality of business data
- Protection of Voice over Internet Protocol (VoIP) traffic in every area of the network
- Support for multicasting applications in a dynamic network environment
- Advanced VPN capabilities such as dynamic routing, which allows enterprises to manage large and complex networks more efficiently with fewer resources
- Reporting features through Eventia Reporter that provide expanded reports to integrate log data and help network administrators make sure their security devices are meeting federal reporting regulation standards
- Unified logging, tracking, and monitoring, providing total visibility to security systems across the network

The unified security architecture of Check Point's NGX platform stretches across the entire network, providing security and oversight to every component of an enterprise. All Check Point products share this technology, meaning security is consistent in every layer of the network. With one security architecture running through one management console, the platform lowers IT costs by eliminating the need for separate management log-ins, servers, and reports. What's more, because all Check Point applications and devices are linked to the same system, the platform offers increased visibility for real-time detection of security problems and anomalies, as well. Put simply, the unified security architecture of Check Point's NGX platform is network security at its most secure.

CONCLUSION

With the unified security architecture of its NGX platform, Check Point Software Technologies offers industry-leading security and management capabilities that enterprises need to facilitate secure access to network assets. Check Point provides all the capabilities necessary for security across the four most critical layers of network security: the network perimeter, the network core, the Web, and the endpoints. With a tightly integrated security and management architecture, the NGX platform supports the centralization of security management, implementation of common security policies, and distributed deployment of the latest and greatest security signatures.

Perhaps more important, NGX architecture offers closer monitoring of security event management, providing network administrators and CISOs with end-to-end visibility to audit security effectiveness for compliance with federal laws. Management tools included within the NGX platform also reduce the learning curve for new administrators and simplify the ongoing management effort, making significant contributions toward Check Point's ability to offer a competitive TCO for Internet security as a whole. No longer must enterprises maintain an armada of point security solutions. Today, the all-inclusive approach to unified security architecture makes every network more secure.



About Check Point Software Technologies

Check Point Software Technologies Ltd. (www.checkpoint.com) is the worldwide leader in securing the Internet. It is the market leader in the worldwide enterprise firewall, personal firewall, and VPN markets. Through its NGX platform, the company delivers a unified security architecture for a broad range of perimeter, internal, and Web security solutions that protect business communications and resources for corporate networks and applications, remote employees, branch offices, and partner extranets. The company's ZoneAlarm product line is one of the most trusted brands in Internet security, creating award-winning endpoint security solutions that protect millions of PCs from hackers, spyware, and data theft. Extending the power of the Check Point solution is its Open Platform for Security (OPSEC), the industry's framework and alliance for integration and interoperability with "best-of-breed" solutions from more than 350 leading companies. Check Point solutions are sold, integrated, and serviced by a network of more than 2,200 Check Point partners in 88 countries.

CHECK POINT OFFICES:

Worldwide Headquarters:

3A Jabotinsky Street, 24th Floor
Ramat Gan 52520, Israel
Tel: 972-3-753 4555
Fax: 972-3-575 9256
e-mail: info@checkpoint.com

U.S. Headquarters:

800 Bridge Parkway
Redwood City, CA 94065
Tel: 800-429-4391 ; 650-628-2000
Fax: 650-654-4233
URL: <http://www.checkpoint.com>

©2006 Check Point Software Technologies Ltd. All rights reserved. Check Point, Application Intelligence, Check Point Express, the Check Point logo, AlertAdvisor, ClusterXL, Cooperative Enforcement, ConnectControl, Connectra, CoSa, Cooperative Security Alliance, Eventia, Eventia Analyzer, Eventia Reporter, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, IMsecure, INSPECT, INSPECT XL, Integrity, InterSpect, IQ Engine, Open Security Extension, OPSEC, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureKnowledge, SecurePlatform, SecuRemote, SecureXL Turbocard, SecureServer, SecureUpdate, SecureXL, SiteManager-1, SmartCenter, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, Smarter Security, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Power, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, VPN-1 XL, Web Intelligence, ZoneAlarm, ZoneAlarm Pro, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 6,496,935, 6,873,988 and 6,850,943 and may be protected by other U.S. Patents, foreign patents, or pending applications.

May 17, 2006 P/N 502114



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.