WatchGuard Extensible Threat Management

An Overview of XTM

July 2008

Abstract

Unified threat management (UTM) spawned a new era of IT security. The promise of these integrated security appliances proved to be an exceptional and efficient way of securing commercial networks. However, businesses today face an inflection point, dictated by changing market trends and new technologies that demand more of today's UTM. Hence the need is for eXtensible threat management (XTM) solutions, the next generation of UTM appliances. XTM is predicated upon the substantive expansion of three elements: more security, greater networking capabilities, and more management flexibility. This paper provides an overview of these issues and the WatchGuard® Technologies perspective on "extensibility" and XTM.

Unified Threat Management (UTM)

Originally coined in 2003 by IDC analyst, Charles Kolodgy, the term *unified threat management (UTM)* represented a ground-breaking concept in having disparate security functions – firewall, intrusion detection/intrusion prevention (IDS/IDP) and gateway anti-virus (AV) – reside in a single, integrated network security appliance.

WatchGuard Technologies, a pioneer of firewall technology since 1996, was an early innovator of UTM solutions, and was one of the first to lead the industry with high performance UTM offerings. By January, 2008, WatchGuard offerings had far exceeded the foundational elements of UTM (firewall, IDS/IPS and gateway AV) to include a host of new security and network connectivity features, such as web-based content filtering and spam blocking, as well as both IPSec and SSL VPN capabilities.

UTM appliances quickly became a network security favorite for SMB, mid-market (SME), and enterprise branch office environments. UTM devices gained substantial ground in education, healthcare, and retail segments because they helped to address regulatory mandates, such as the Children's Internet Protection Act (CIPA), Health Insurance Portability and Accounting Act (HIPAA), and Payment Card Industry Data Security Standard (PCI DSS).

As the demand for UTM grew, so too did the industry and the number of respective solutions. By 2007, the UTM market had grown approximately 35 percent year-over-year, to reach $1.216 billion. By 2008, industry analysts estimate that sales of UTM appliances will surpass traditional firewall/VPN solutions. By 2010, sales of UTM devices are expected to exceed $2.5 billion.

WatchGuard confirms that analyst reports are on target, and that the UTM market continues to grow at a record pace. In particular, WatchGuard sees accelerated UTM market growth as appliances expand into new geographic regions around the world and move upstream into more enterprise and distributed environments. What is unclear right now is whether the current state of UTM offerings in the market is sufficient to fully meet future business demand and IT expectations.

Trends Affecting UTM

Clearly, UTM has moved from a concept to a business and network security reality. The growth and acceptance of UTM is undeniable. However, there are factors to suggest that UTM, in its current state, will not be sufficient to tackle the next generation of looming security threats, nor capable enough to meet the needs of savvy businesses that leverage new forms of technologies to be more productive and efficient.

New Threats

Threats are changing. The next generation of security threats will present unparalleled challenges and risks. The "black hat" community is not the band of miscreants that it used to be. What was once done to gain notoriety and underground fame among fellow hackers has now turned into big business, similar to organized crime syndicates. Data is valuable, and gaining control of web sites, servers, and personal computers can be lucrative.

WatchGuard sees the next generation of security threats to be more sophisticated and less conspicuous. Security threats are taking on new forms, morphing common annoyances such as spam email and mutating them into hybrid spam/phishing/malware payload-delivery vehicles. The traditional attacks on network ports and data networking protocols will change to attacks that exploit holes directly at the application layer.

Threats are becoming more stealthy and concealed, as well. Typically, when a threat reaches a broad enough audience, a "signature" can be developed to counter and neutralize the threat. Today, the writers of these attacks have learned that low profile attacks keep threats "under the radar," and hence, avoid detection and the eventual signature that will wipe them out. Likewise, other attackers have developed automated repackaging malware applications so that the malware changes every few minutes – effectively staying ahead of any anti-virus vendors' ability to produce a signature.

Changing Business Dynamics

Business is changing. Several factors are all converging to change the way businesses operate. Leading this, WatchGuard sees business mobility, the "millennial" generation, the "consumerization" of IT, Web 2.0+, and new technologies, such as virtualization and Software as a Service (SaaS), all creating new dynamics for network security and data protection.

Mobility, mobile workers, and remote office technologies accelerate business opportunities, but at the same time, create new venues for security risks. According to a recent survey conducted by Stanford University and Hong Kong University of Science and Technology, "92 percent of Fortune 500 respondents agreed that uncoordinated mobility initiatives lead to security risks and high integration costs. But 93 percent reported that mobility can provide a significant competitive advantage."[1] The traditional desktop is being redefined by mobile devices and mobile applications. As this happens, IT staff must address the inherent security risks that accompany this trend.

Likewise, the next generation of workers, the "millennials", mirrors the benefits and risks associated with mobility. The millennial generation is instrumental in adopting new technologies, particularly, IM, peer-to-peer, and social networking tools, yet shows lackluster awareness and even disdain towards the risks that go with these technologies. In a recent blog post titled, "IT Risk and the Millennials," Samir Kapuria talks about what could turn out to be one of the most pressing issues for IT. Kapuria points out, CIOs are trying to figure out how to cope with this generation.

[1] "The Mobility Manifesto: What enterprise mobility means and how to make the most of it" – Nokia Corporation

> "Millennials are used to freely downloading software from the Internet, such as Skype; using applications like Facebook; and bringing their iPods and laptops into the office—all of it blurring the lines between personal and work life."[2]

New Technologies

Relative to this is the "consumerization" of IT and Web 2.0 technologies. Designed to foster more collaboration, greater efficiencies, the sharing of information, and more productivity, the IT landscape of "consumerized' technologies (iPhones/iPods, USB drives), and Web 2.0 applications (mash ups, peer-to-peer and social networks) is also creating new security and information leakage concerns. It has been noted that some consumer-oriented applications, such as Facebook or LinkedIn,` are being used as contact managers or even as CRM substitutes. Businesses that rush out and adopt these new tools may also find themselves in uncharted security waters.

For example, the media recently reported on a popular online consumer game, World of Warcraft, and how malware associated with the game is stealing user passwords and account data. For a consumer, that is a serious threat. By analogy, if one applies this type of scenario to something like Second Life, which quickly morphed from a game into a business-to-business[3] vehicle for corporate events, sales, training, marketing, and demand generation, then we see how deleterious this type of malware could be if it could capture corporate passwords and corporate data. Bottom line is businesses have yet to experience the risks associated with consumer technologies and Web 2.0 applications in the work environment.

New business technologies are shaping security profiles. This ranges from VoIP to Virtualization. For example, virtualization is the general term used to describe the abstraction of IT resources. Virtualization hides the physical characteristics of computing resources from their users, be they applications or end users.[4] This includes making a single physical resource (such as a server, an operating system, an application, or storage device) appear to function as multiple virtual resources; it can also include making multiple physical resources (such as storage devices or servers) appear as a single virtual resource.[5] As businesses adopt virtualization, they must understand the security risks associated with it.

Software as a Service (SaaS) presents similar security challenges for IT staff. With industry heavyweights, such as Cisco, Google, and Microsoft, pushing for more IT services to be "in the cloud," questions arise of

---

[2] https://forums.symantec.com/syment/blog/article?message.uid=306119
[3] Using Second Life as a Business-to-Business Tool, Information Week (April 26, 2007) http://www.informationweek.com/blog/main/archives/2007/04/using_second_li_2.html
[4] Electronic Commerce: A Managerial Perspective, Turban, E., (2008)
[5] "The Pros and Cons of Virtualization," Business Trends Quarterly, Mann, Andi (April 21, 2008); "Virtualization 101," Enterprise Management Associates (EMA), Mann, Andi (Oct. 29, 2007)

who controls the data, how is it protected, which laws and regulations apply, how is it audited, and what recourse is available should something happen? Assuming that SaaS is an inevitable reality, businesses will need XTM solutions to ensure secure connectivity to the cloud, as well as to protect the integrity of applications and data interactions.

Likewise, as businesses deploy new technologies, they must address protection in new ways. For example, mobility and data in motion is changing the concept of how to secure the network perimeter. Protecting the end point device will be subjacent to protecting users and data as they move through networking, web, and messaging platforms.

Lastly, businesses and IT administrators will have to do more with fewer resources. A recent Goldman Sachs report stated that security budgets are down from previous forecasts. As global economic issues create turbulent markets, companies are expected to react by reducing IT expenditures.

All of these factors – the next generation of threats, changing business dynamics (i.e. mobility, "millennials," consumerization of IT, and Web 2.0 applications), and new business technologies – dictate how network security will operate in the future. WatchGuard believes that the UTM industry is at an inflection point, and that the current state of UTM appliances is insufficient to fully address these factors. Therefore, what business and technical decision makers will need is the next generation of UTM – XTM, or extensible threat management solutions.

Extensible Threat Management (XTM)

Extensible threat management (XTM) is the next generation of unified threat management (UTM), integrated network security appliances. As stated by IDC analyst, Charles Kolodgy, in SC Magazine (May 2, 2008):

> "IDC believes that UTM will remain the primary security solution for distributed environments, but within the enterprise it will evolve into an eXtensible Threat Management (XTM) platform. XTM platforms will take security appliances beyond traditional boundaries by vastly expanding security features, networking capabilities and management flexibility. Future XTM appliances should provide automated processes – such as logging, reputation-based protections, event correlation, network access control and vulnerability management. Adding to the networking capabilities will be management of network bandwidth, traffic shaping, throughput, latency and other features, including unified communications."

Based on this definition, WatchGuard foresees XTM as an extension of the UTM category. XTM will expand on what UTM has delivered, but will include additional substantive developments in three core areas:

- More security features
- Greater networking capabilities
- More management flexibility

WatchGuard Extensibility

Extensibility means having the ability to extend or add on to. This is what WatchGuard is innovating with its UTM family of security and connectivity solutions. The vision is to provide XTM solutions that deliver extensibility. WatchGuard's extensible components are:

- Extensible protection
- Extensible management
- Extensible choice
- Extensible ownership

Protection

Extensible protection derives from the unique WatchGuard approach to network security. WatchGuard utilizes a security scheme built upon its "intelligent layered security" architecture that incorporates myriad security technologies, including application proxy technology to defend against spyware, malware, viruses, outside attacks and other harmful events. This approach of extensible protection guards against port and protocol-specific threats, as well proactively protecting businesses at the application layer, thus creating an "application aware" defense posture.

Management

Extensible management addresses the need to incorporate more network and management capabilities. This includes integration of networking technologies, such as WAN optimization, active/active failover for high availability (HA), and management software that allows one-touch control over hundreds of WatchGuard XTM appliances. As well, extensible management includes having open, standards-based management hooks, thus allowing businesses to leverage and utilize existing management suites, such as HP OpenView, to seamlessly manage their XTM appliances as part of one console.

Choice

Extensible choice speaks to providing complete device flexibility. This means that WatchGuard XTM appliances will have the ability to be configured for optimal deployment in any kind of network or business environment. As well, this means administrators will have the ability to pick and choose security services that best meet their organization's needs. For example, a school administrator may only want firewall and web-content filtering on their XTM, while a business may opt for all security services, minus gateway AV, for their WatchGuard XTM deployment.

Ownership

Extensible ownership revolves around growth-oriented options that yield superior total cost of ownership (TCO) and return on investment (ROI). WatchGuard XTM solutions will continue to support a software upgradeable path, which allows users to upgrade security services, subscriptions and capabilities on the fly, without ever having to swap out hardware. Not only does this extend the life of the appliance, but gives owners more flexibility in determining how they utilize their security investment. As well, WatchGuard is working to ensure XTM appliances have the greatest degree of network systems interoperability. This way, regardless of the network topology mix (Cisco, Juniper or Extreme), WatchGuard XTM appliances will provide maximum interoperability.

The Business and Technical Cases for XTM

For business decision makers, XTM offers an ideal cache of reliable security and superior TCO. XTM allows businesses to utilize mobility, consumer technologies, Web 2.0, and other new business applications in a highly secure manner.

Because of the inherent flexibility found in XTM, these solutions will help businesses address the needs of regulatory compliance and future changes that are bound to come.

With greater networking and security capabilities, XTM solutions also eliminate the costly need to purchase and manage multiple routing and stand-alone security appliances. For example, small businesses that currently purchase low-end routers and then supplement them with firewall devices will be able to use a single XTM device for both routing and security. Likewise, instead of utilizing separate appliances, such as a spam firewall, web application filter, and IDS/IDP solution, with XTM businesses can utilize all of these services in one device. This makes the cost of XTM acquisition, as well as the cost of management, much lower than traditional best-of-breed, stand-alone appliances.

For technical decision makers, XTM offers greater management, real-time user control and superior security. As the network perimeter changes and users pass through network, web and messaging platforms, administrators will look to XTM appliances to provide “common reputation services” so that regardless of the device or location, the user and data are always protected. XTM will offer administrators new capabilities in “policy migration” as well. This way, as older appliances such as firewalls are replaced, newer devices can extend and enforce existing security policies.

Finally, technical decision makers who are not security experts will be able to rest assured, knowing that their networks are highly protected with proactive, XTM-based security. The intelligent layered security architecture from WatchGuard offers an unmatched array of security technologies, designed to protect against unknown, “zero day” threats.

Conclusion

XTM is the next generation of UTM, and it is predicated upon the substantive expansion of three foundational elements: more security, greater networking capabilities, and more management flexibility. From this foundation, WatchGuard adds to extensibility by offering: extensible protection, extensible management, extensible choice, and extensible ownership. Although the changing landscape of business dynamics and technology developments has created new efficiencies and accelerated business opportunities, these carry with them new forms of sophisticated threats and risks. The current state of UTM will not be enough to address these changes, hence the need for the next generation of UTM – WatchGuard XTM solutions.

For more information about WatchGuard XTM security solutions, visit us at www.watchguard.com, or contact your reseller.

ADDRESS:
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:
www.watchguard.com

U.S. SALES:
+1.800.734.9905

INTERNATIONAL SALES:
+1.206.613.0895

ABOUT WATCHGUARD

Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. Our Firebox X family of unified threat management (UTM) solutions provides the best combination of strong, reliable, multi-layered security with the best ease of use in its class. Our newest product line – the WatchGuard SSL – makes secure remote access easy and affordable, regardless of the size of your network. All products are backed by LiveSecurity Service, a ground-breaking support and maintenance program. WatchGuard is a privately owned company, headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. For more information, please visit www.watchguard.com.

Part. No. WGPE66567_072408