The future of network security is here

Rise of the Smart Firewall
White Paper

Published: March 2013
Introduction: The Future of Network Security is Here

William Gibson, famed author of the cyberpunk thriller, “Neuromancer,” and coiner of “cyberspace,” has been fond of saying,

“The future is already here — it’s just not very evenly distributed.”

Gibson’s forward-looking observation can apply to the current state and future of network security. The network security solution of the future, the Unified Threat Management (UTM) physical or virtual appliance, is already here—its adoption has just been unevenly distributed until now.

While the UTM concept has existed for at least 10 years, the evolution and capabilities of today’s foremost UTM solutions poise it to become, if it is not already, the cornerstone of your network security environment well into the future.

In this paper, we provide a brief introduction to today’s UTM, and more importantly, provide IT administrators and business professionals with a clear, common-sense way to evaluate UTMs versus other technologies, as well as how to differentiate UTM solutions from vendor to vendor.

Toss out any preconceived notions you may have formulated that point solutions or Next-Generation Firewalls (NGFWs) are for large enterprises and UTMs are for mid-sized enterprises and small businesses. Recent advances in hardware acceleration combine with core UTM strengths, allowing best-in-class UTMs to deliver secure performance, manageability, visibility, and reporting that is unparalleled by the combination of any other devices.

In fact, WatchGuard’s comprehensive range of security services elevate last year’s “next-generation firewall” to a whole new level, adding more layers of protection and enhanced capabilities to complement traditional Application Control and IPS—while delivering better security and performance. The best of the new wave of UTMs, or smart firewalls, deliver powerful defense-in-depth for growing enterprises and small businesses, protecting against both known and unknown attacks—providing maximum security while minimizing impact on network performance.

Security for 2013 and Beyond

Network security poses one of the most preponderant challenges confronting organizations today. Spyware, spam, viruses, Trojans, web exploits, and blended threats evolve and spread with alarming speed and regularity. Notoriety-seeking hacktivists steal and release sensitive information to humiliate governments and businesses across the world. Hacker toolkits abound over the web, so even an unsophisticated malefactor can access and repurpose sophisticated code, such as that used in Stuxnet and other state-sponsored attacks.

Moreover, the emergence of new business enablement technologies exposes new attack surfaces. We see it with the growth in IP networks and proliferation of web 2.0 applications, devices (BYOD), and web technologies in the workplace. We see it with increasing reliance on cloud-based infrastructures (SAAS,

PAAS, IAAS). Along with the exciting potential to cultivate work efficiencies and business opportunities, these technologies also generate more potential headaches for IT administrators.

Without question, ordinary, overstretched IT staffs everywhere find themselves regularly facing security challenges, which just a few years prior, were still relegated to the stuff of sci-fi.

We don’t need to enumerate for you the consequences of inadequate or mismanaged security—you hear about it, read about it, and see it every day in the news, from auditors, in company or industry meetings. To remain viable and competitive, organizations of all sizes need to be diligent and forward-looking in protecting data, intellectual property (IP), and their reputation. This means transcending what is merely required as a baseline by regulatory bodies and providing solutions that truly solve the security problems and vulnerabilities that put your business in jeopardy.

**Firewalling Evolves into More**

In this fast-evolving era of blended threats and new spheres of work and technologies, firewalling is just one requirement of a multi-faceted perimeter defense appliance. For these reasons, businesses of all sizes are increasingly turning to UTMs-- multilayered solutions that combine firewalling with other vital security features. UTMs centralize security controls in a single device, improving the IT organization’s control and simplifying management of network security.

Traditionally, firewalls have, at minimum, performed the same basic function of analyzing incoming and outgoing data packets against a list of rules that define what traffic to allow and what traffic to block. However, as we will discuss, different firewall and UTM solutions are from being equal, or commoditized.

Most older-generation firewalls rely primarily on "stateful inspection" technology, while the addition of deep packet inspection technologies is embraced by many of today’s premier vendors. WatchGuard has even developed a Proxy technology that blocks all but “known good” traffic, yielding a measurable increase in security. WatchGuard leads the way with an agile, forward-looking UTM platform, able to secure the business needs of today and accommodate the unknown threats and business security challenges of tomorrow.

![WatchGuard XTM solutions](image)

*Figure 1: WatchGuard XTM solutions guard against port and protocol-specific threats, and also apply intelligent visibility and security at the application layer.*
What is a UTM?

“As always, during times of rapid change in an environment, in this case the rise of targeted attacks and state sponsored hacking, there are point products that are the first to provide a response. But industry dynamics force the established vendors to add the capabilities of the point products. And customers, overwhelmed by the need to manage multiple solutions from multiple vendors, gravitate towards established vendors that can provide comprehensive protection in a managed platform,” Richard Stiennon, author of “Surviving Cyberwar” and frequent Forbes magazine contributor.2

Coined by IDC analyst Charles Kodology in 2003, the term, UTM, or Unified Threat Management applies to multi-function firewalls that combine many security technologies into one easy-to-manage appliance. Today’s UTM appliances typically consolidate firewall and VPN capabilities along with URL filtering, spam blocking, intrusion prevention, gateway antivirus, application control, and a centralized management, monitoring and logging function. Traditionally, these discrete functions were handled by multiple point solutions. The multilayered security approach of UTM appliances provides broad protection against all kinds of network threats.

UTM Combines Multiple Perimeter Services into One Box

Figure 2: Point solutions arise to solve a challenge at a moment in time. The premier UTM solutions integrate the best and most vital point solutions. The result?--consolidated management, reduced cost, and better security as layers of UTM protection work smartly together.

What is a Next-Generation Firewall (NGFW)?

Next-Generation Firewalls (NGFW) are a subset of today’s UTM appliances, or stated another way, UTMs comprise a superset of NGFWs. As first described and defined by Gartner Research, an NGFW, at a minimum, is a firewall with deep packet scanning and that integrates Intrusion Prevention Service (IPS) and application control capabilities with the firewaliing.3

---

3 Gartner, Inc., Defining the Next-generation Firewall, October 2009
Is an NGFW Different from a UTM?

While pure-play NGFW vendor Palo Alto Networks and some others may insist that a Next-Generation Firewall is an entity, altogether distinct from a UTM, that relies on a “revolutionary” underlying architecture—when it comes down to it, every Unified Threat Management Security Vendor, whether it be WatchGuard, SonicWall, Fortinet, Palo Alto, or others has its own proprietary security architecture. There is overlap in the security challenges these many UTM vendors strive to tackle, but each vendor executes on a slightly different path based on their core philosophies, pillars, and legacy technologies. In fact, the secure throughput of WatchGuard’s smart firewalls surpasses that of pure play NGFW vendors.

Figure 3: The salient different between NGFWs and UTMs?--NGFWs offer a limited feature set, while the best UTMs extend protection by seamlessly integrating additional complementary layers—without taking a hit to network performance.

While UTM security vendors may seem to offer a similar checklist of core technologies and features (firewalling, IPS, etc.), as we will later expound, when evaluating vendors, recognize that there is enormous disparity between UTM solutions in the following areas:

- Quality of the features/capabilities
- Security performance, or UTM performance
- Manageability and ease of use
- Flexibility
- Value

Why Unified Threat Management?


Viruses, worms, Trojans, rootkits, DDoS and cross-site scripting attacks are no less relevant today, however, the sophistication and scope of attacks continues to increase. For instance, today’s botnets
typically coordinate a range of blended attacks leveraging millions of zombie computers to exploit zero-day vulnerabilities. APTs (Advanced Persistent Threats), typically generated by rogue states or bands of cyber criminals, employ multi-vector techniques that persist until they penetrate the network, or can map the targeted environment for future attacks, as in the case of Flame (also called sKyWIper) and miniFlame. Today’s blended threats require blended security solutions. No single “point solution” provides adequate protection—only a Unified Threat Management solution with intelligent architecture can provide reliable, comprehensive security.

2. **Centralized Management and Compliance Reporting**

Having separate security systems means different management consoles to learn and configure for each system. Because the management paradigms of these systems are typically discrete, it can be onerous and time-consuming to verify that the different security policies on each system work together and provide adequate protection. Log information from each system will be stored in different formats in separate locations, further complicating detection and analysis of security events.

Whether you are an IT expert or a security novice, a UTM solution that centralizes management, monitoring, and logging provides indispensable ease of use for configuring and managing your security. A UTM solution makes it easier to build coherent security policies, simplifies administration tasks, such as log file management, while lowering operational costs.

Additionally, centralizing management and reporting makes it easier to collate and report on information that is imperative for compliance with industry (CIPA, HIPAA, PCI DSS, etc.), state, and federal regulatory mandates.

3. **Unified Threat Management Solutions Are Typically Far More Cost-effective**

Cost-effective solutions allow you to do more with less. Integrating multiple security capabilities into a single appliance means that you can purchase, use, and manage fewer standalone appliances, and thus, reduce your overall cost. Aside from the bundled price advantages, organizations find it easier to have fewer vendors to deal with for purchasing, support, and ongoing maintenance.

According to Gartner Research, unified threat management can roughly halve the annual network security spending—and over the lifetime of the product, the savings can be considerably more. Gartner also points out that the lack of systems integration between standalone products can be costly in terms of the administrative complexity needed to stay on top of it. Thus, the ability to administer one unified solution versus multiple standalone products not only simplifies management, but delivers considerable savings throughout the course of the product lifecycle.

**Evaluating the Best Security Solution: Why Some UTMS are Created Better than Others**

1. **Range and Quality of Layered Security Technologies**

At a glance, many UTM vendors seem to market a comparable checklist of features and services—yet vast differences exist between the performance, quality, and capabilities of these features from vendor to vendor. The less mature or “good” the security at each layer, the higher the risk of exploit.

---

**Home-Grown Vs. Best-in-Class Technologies**

The most prevalent approach among UTM vendors is to rely primarily on homegrown technologies for their gateway AV, URL filtering, application control (if they have any), anti-spam, and other security services. However, WatchGuard leverages a different approach, which we believe makes our UTMs “best-in-class” by design.

While Fortinet, SonicWall, Palo Alto, and others struggle to develop the many diverse security technologies in-house, WatchGuard partners with the category leaders in each specialized technology sphere—meaning WatchGuard customers get mature, highly vetted, best-in-class security technologies from AVG, Websense, BroadWeb, Commtouch, Kaspersky, and other leading technology specialists.

If you are going to consolidate a security feature typically provided by a point solution into a UTM—we believe that the UTM security feature should be of comparable efficacy to truly deliver best-in-class security. WatchGuard understands and accepts that no single company will ever be able to adequately research and develop the best technology for each discrete security problem. A shortcoming of the homegrown approach to multilayered security, is that these UTM vendors end up producing a watered down security solution at each layer. We believe this practice contributes to the reluctance of some organizations to choose a UTM solution for their security.

No other network security vendor incorporates the best-in-class mantra to the extent that WatchGuard does, nor does any other company match WatchGuard’s effectiveness at seamlessly integrating the partner security service into the user interface (UI).

WatchGuard’s best-in-class approach means our customers do not have to make security tradeoffs in order to benefit from consolidating security services and management and reduced cost. Layer-by-layer, a WatchGuard XTM multi-function firewall provides superior security over what competitors’ combination of in-house technologies can possibly muster.

![Figure 4: In-house (home-grown) Vs. Best-in-Class UTM Security Services. WatchGuard customers get best-in-class AV, URL Filtering, Anti-Spam, IPS and App Control powered by elite partner technologies.](image-url)
Other standard WatchGuard security capabilities include:

**HTTPS Inspection** on both incoming and outgoing traffic that inspects not only packet headers, but also payload (body content). An XTM firewall can inspect traffic for anomalies, re-encrypt the data, and pass it along to the user. The user’s communication remains confidential, while the network has an additional layer of protection from encrypted threats.

**VoIP Security** -- Fireware XTM, the operating system powering WatchGuard’s smart firewalls, comes standard with Application Layer Gateways that intercept and inspect VoIP-related protocols such as H.323 and Session Initiation Protocol (SIP). Fireware XTM allows you to hide your network topology, prevents directory harvesting, and has the ability to deny calls compressed in certain codecs.

**Security for Virtualized Environments**: As Neil MacDonald of Gartner Research has said:

“...Unless you put virtualized security controls—virtual sniffers, virtual firewalls, all the same controls you’d use on a physical server, inside that network, you don’t see what’s going on.”

WatchGuard XTMv solutions bring the visibility and security capabilities of XTM hardware appliances to virtual environments, specifically VMware and Hyper-V deployments.

For more in depth analysis and evaluation of the quality of security services between vendors, check out the white paper: [Defining, Evaluating, and Designing Best-in-Class Network Security](http://www.cio.com/article/492605/Server_Virtualization_Top_Five_Security_Concerns).

2. **UTM Performance**

A high performance packet throughput device, even one with custom ASIC processors, can fall over when a full suite of unified threat management tools are enabled. Many security vendors who freely tout their raw throughput numbers are not so quick to publicize their UTM throughput numbers--- the performance of the firewall once all the UTM security services are turned on. Once you activate the UTM security functions—such as those necessary for PCI DSS compliance (AV, IPS, etc.)— the performance evaporates in many competitor firewalls—even for those supposedly single pass “Next-Generation Firewalls”.

WatchGuard engineered its XTM firewall appliances with security performance in mind—and it shows. We believe this validates the investment spent in re-architecting our XTM solutions several years back, giving WatchGuard customers a flexible solution that delivers tightly integrated security technology demanded by businesses that want dependable, cutting-edge security without sacrificing network performance. The result?--WatchGuard’s UTM performance is up to 3 times faster than UTM performance of corresponding models from Fortinet, Sonicwall, Cisco, and others.

---

Figure 5: Hands down, WatchGuard XTM solutions trounce comparable Fortinet, SonicWall, and other competitor products in throughput performance when UTM security services are enabled.

*Note: Fortinet does not publish UTM throughput but advises customers wishing to run multiple security services to size based on the lowest performance number—typically Ant-Virus throughput, which is shown for Fortinet here.

If you are using a firewall for security (as we expect that organizations do), UTM performance is the only firewall performance metric that matters. WatchGuard firewalls trounce competitors in UTM performance. And or those that try to market NGFWs as fundamentally different from UTMs because of a supposedly more integrated, “single pass” architecture, note WatchGuard handily outperforms traditional/pure play NFW vendors in head to head comparisons when IPS is activated.
Figure 6: WatchGuard Firewall performance with IPS-enabled beats competitors in the same product class by leaps and bounds, even pure-play NGFW vendor, Palo Alto. On top of that, WatchGuard solutions deliver substantial cost-savings.

Don’t be fooled by “packet filter only” performance numbers. What matters most is the throughput that you get when full UTM security services are running. In that analysis, WatchGuard is #1. Only a purpose-built UTM, such as those designed by WatchGuard, can deliver comprehensive security and blazing performance, without succumbing to latency issues.

3. Centralized Management and Ease-of-Use
Despite the considerable media attention lavished on dramatic “zero day” security flaws, consensus opinion among security experts holds that firewall misconfigurations are perhaps a primary ingredient in data compromise events. In fact, Gartner speculates that firewall misconfigurations—as opposed to flaws in the firewall—play a factor in up to 95% of breaches. 6 We see it all too often with competitor solutions—poorly integrated management processes needlessly introduce complexity to administration. Improperly configured gear undermines security.

---

A core focus of WatchGuard engineering is to make our security solutions as easy as possible for administrators of all skill sets to manage. WatchGuard provides state-of-the-art centralized management capabilities and innovative ease-of-use technologies, features that help administrators:

- dramatically cut down on errors
- quickly hone in on problem areas
- save hours of time
- and rapidly enact policy changes and firmware updates across hundreds of XTM appliances.

Rival security vendors charge a premium for features that merely parallel WatchGuard’s standard management package, included with purchase. With WatchGuard, administrators can manage all security services and feature sets through a single pane of glass. Administrators can also choose and switch between using client-based, web, and command line interfaces.

Moreover, WatchGuard has pioneered a number of innovative, ease-of-use technologies that render traditionally onerous administration relatively hassle-free. For instance, the ability to create secure VPN tunnels using WatchGuard XTM's simple drag and drop feature routinely saves administrators hours. WatchGuard RapidDeploy, a cloud-based configuration capability, enables XTM firewall appliances to securely configure themselves in the field—dramatically reducing deployment time and costs for MSSPs and distributed retail environments.

WatchGuard’s commitment to streamlining management, consolidating controls, and developing powerful tools that simplify administration of traditionally sophisticated tasks, means even IT generalists can enable and manage best-in-class security for any environment.

4. Reporting and Visibility

Network visibility and security go hand in hand—and when it comes to achieving regulatory compliance (PCI DSS, HIPAA, CIPA, etc.), auditability is required. So, why would a security vendor not include visibility and reporting tools? Yet, many vendors, including Cisco, CheckPoint, SonicWall, and Fortinet, charge extra for these capabilities, often requiring purchase of a separate product just for reporting.
Figure 7: Hostwatch, one of many visibility and reporting tools WatchGuard provides—at no extra cost, delivers real-time visibility of your XTM devices and network—letting you take instant-action.

WatchGuard real-time and historical visibility and reporting tools truly illuminate your network, allowing you to quickly hone in on problem areas, troubleshoot issues, and make policy changes on the fly.

No standard reporting package surpasses WatchGuard’s offering of over 65 free reports. With WatchGuard, you get advanced real-time and historical visibility and reporting as well as policy management tools and pre-packaged compliance reports (PCI DSS, etc.) included at no extra cost—which is the way we think it should be.

5. Flexibility

Security vendors differ conspicuously in the flexibility of the solution they market to customers. For instance, some UTM products can only add security services by physically bolting on software cartridges, or blades. Such an architecture only provides a limited number of slots for which to add in security services, forcing you to tradeoff one security function for another when enabling UTM capabilities.

We believe lack of flexibility is a serious shortcoming of many of the competitor firewall solutions on the market. Many UTM/NGFW vendors have taken a short-sighted route of designing a security appliance to tackle only the threats of the current day. These UTM/NGFW vendors have essentially married their architecture to a distinct, but limited range of features. In contrast, the WatchGuard XTM architecture
reflects forward-looking engineering—the result is a flexible, purpose-built solution with the versatility to integrate the next-generation of vital technologies as they emerge.

_Elegant Engineering. Flexible Security Architecture. Smart Protection._

Hailed industry-wide for their inherent flexibility, WatchGuard XTM (Extensible Threat Management) solutions are built around the concept of “extensibility”, which means capable of extending or adding on to. The unique, modular architecture of WatchGuard XTM smart firewalls can rapidly integrate new “must have” technologies to diffuse and repel novel threats and securely harness new business-enablement technologies.

On the hardware side, WatchGuard appliances can rapidly leverage advancements in chip boosting technologies to deliver higher performance to customers. Competitors who engineer and manufacture their own hardware platforms carry a much higher cost in each product, and are able to bump their performance only every few years as they rev their hardware. Because WatchGuard's smart firewalls are built on industry-standard platforms, we can avail ourselves of our partners’ huge investment in boosting their performance. For example, Intel's recent advances in platform performance made it possible for us to offer our customers a 3x – 4x performance boost in our latest hardware offerings with little impact on price.

![Diagram](image.png)

**Figure 8:** The WatchGuard XTM smart firewall platform is a forward-looking, modular architecture built on industry standard platforms and designed to flexibly integrate the best security technologies that hit the market. The result—best-in-class security, best-in-class manageability, and best secure throughput performance in each product class.
Reflecting its elegant design principles, multilayered security from WatchGuard requires no extra parts or software blades. WatchGuard customers can select, at any time, to activate or de-activate the best-in-class security services that meet their organizations’ needs. For instance, a school IT administrator may only desire firewalls, application control, and web-content filtering on their XTM, while a business may opt to activate all security services for their WatchGuard XTM deployment.

With WatchGuard, flexibility also extends to ownership. Through firmware updates and software upgrades, our customers can boost security services, subscriptions, and capabilities on the fly, without ever having to swap out hardware—further extending the life of the appliance.

Additionally, WatchGuard strives to ensure that XTM appliances have the greatest degree of network systems interoperability. This way, regardless of the network topology mix (Cisco, Juniper or other), WatchGuard XTM appliances will provide maximum interoperability.

WatchGuard XTM appliances can be configured for optimal deployment for any network or business environment, delivering the agility, security, and performance that businesses need to compete.

**WatchGuard XTM – The Ultimate Solution for Defense-in-Depth Security and Network Performance**

The future of security is here. We believe the UTM platform will increasingly be the cornerstone of network security for forward-looking organizations of all sizes. Separate point solution devices will never be integrated enough to dynamically see and appropriately react to the overall threat pattern.

While different UTM vendors strive to solve many of the same security challenges, each vendor approaches product development with different philosophies. So, while there is overlap in the types of security offered from vendor to vendor, there is enormous difference with regards to:

- Quality of the features/capabilities
- Security performance, or UTM performance
- Manageability and ease of use
- Flexibility
- Value

WatchGuard XTM solutions are elegantly engineered, forward-looking, **smart firewalls** with unrivalled layers of protection that cooperatively and dynamically detect, block, and report on malicious traffic while passing benign traffic through. WatchGuard’s commitment to providing best-in-class security at each layer by leveraging the technology of leading pure players, means there is little reason to continue throwing money and resources into standalone products, when you can get all the functionality of multiple point solutions, peerless flexibility, powerful centralized management, and much more with a WatchGuard Smart Firewall.

And, with WatchGuard’s relentless focus on simplifying administration and pioneering innovating ease-of-use technologies, over-burdened IT staffs have never had a better partner.
Figure 9: WatchGuard is the reigning value-leader in the UTM/Smart Firewall space, providing best-in-class security, flexibility, and management at an unsurpassed value.

For More Information
For more information, visit the WatchGuard website, contact a WatchGuard reseller, or call 1 (800) 734-9905 in the United States and Canada.