Unlocking the Promise of UTM-Enabled Network Protection

What small, midsized, and distributed enterprises need to know to get the most from Unified Threat Management

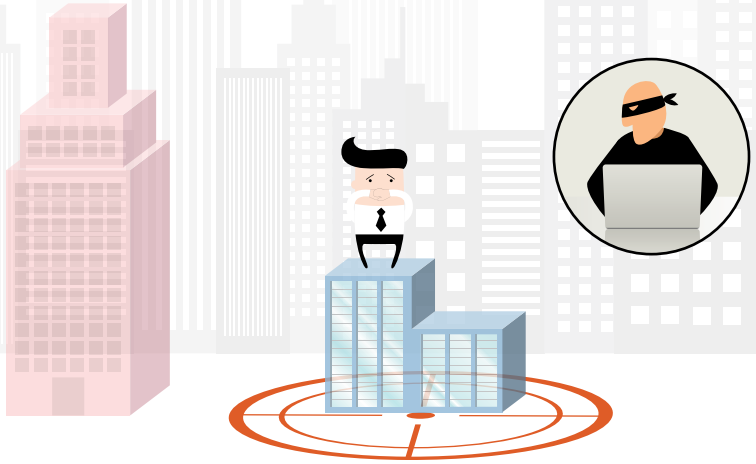
Based on a Frost & Sullivan Executive Brief Sponsored by WatchGuard Technologies

The Threats Are Enterprise-Grade. Your Budget Isn't.

Despite the headline-dominating data breaches in large, global businesses, cyber-threats pose a greater risk to midsize businesses. Why? Large enterprises typically have the resources to recover from a cyber-attack. For a midsize business, however, the financial damages and lost customers due to a data breach can be overwhelming.

At the same time, midsize businesses present the optimal blend of valuable assets and limited defenses that appeal to financially motivated hackers. These businesses are especially lucrative targets if they partner with large organizations. Cyber-criminals infiltrate partner networks and use this foothold to launch attacks against otherwise unreachable systems, as in the case of the Target and Home Depot breaches.

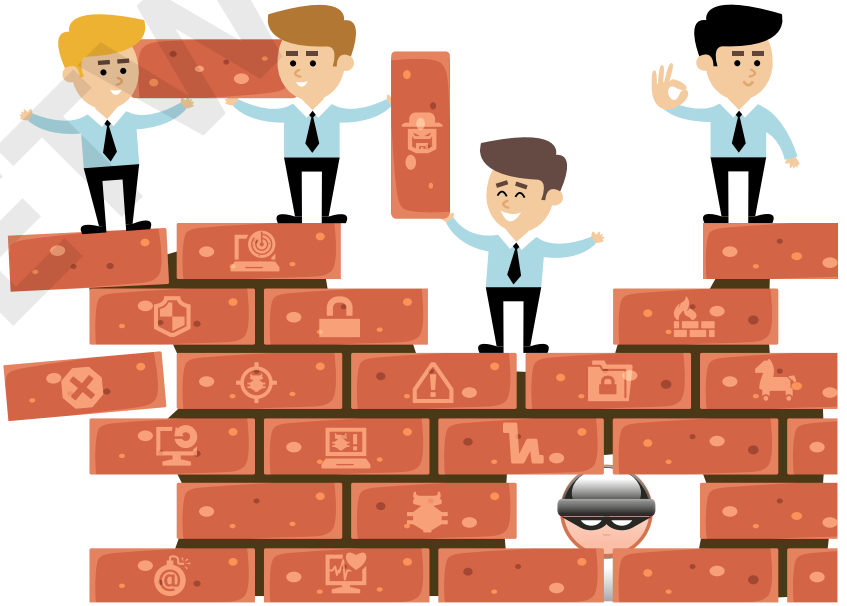
Large enterprises typically have the resources to recover from a cyber-attack.



For a midsize business, however, the financial damages and lost customers due to a data breach can be overwhelming.

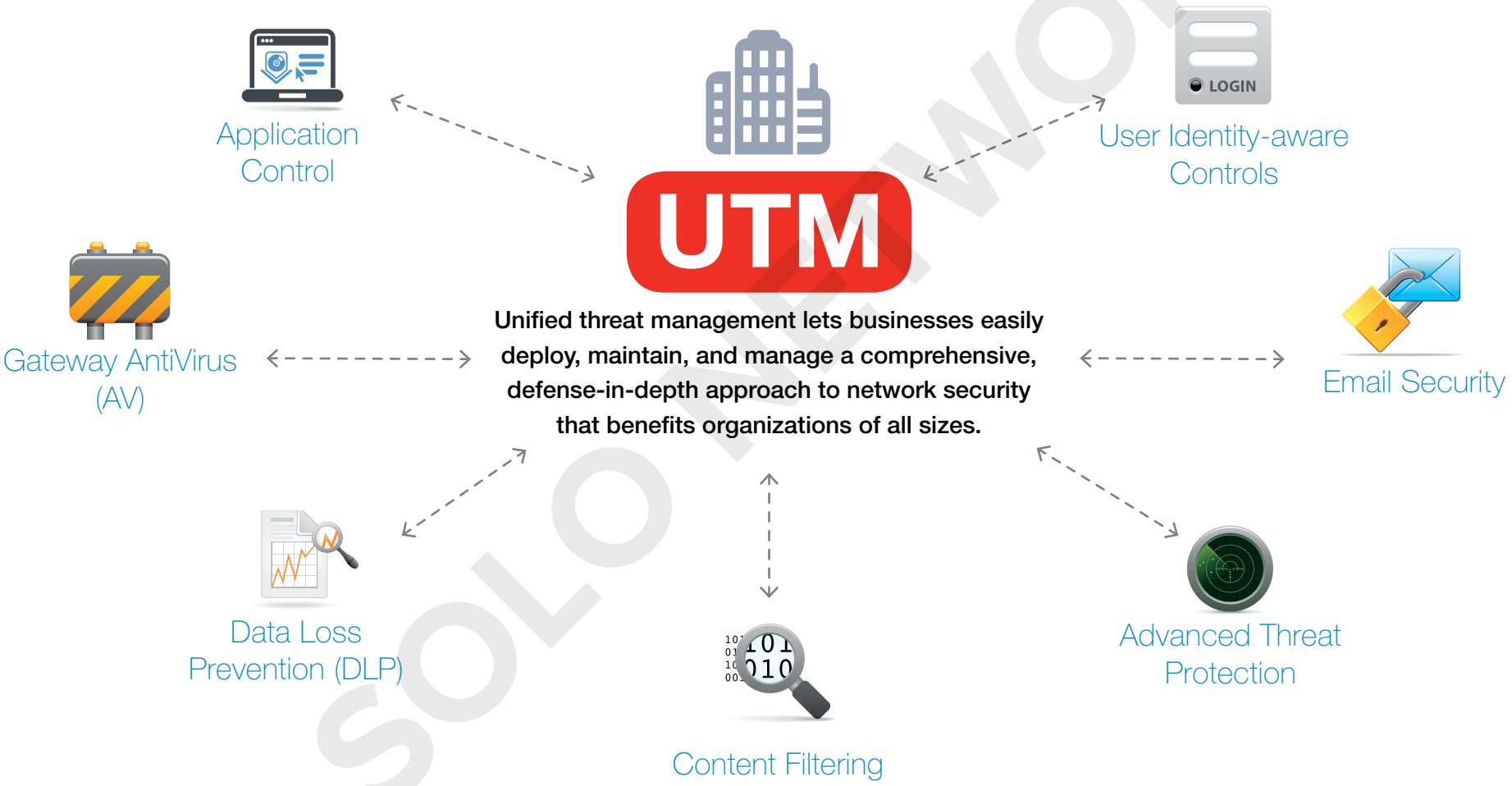
Midsize Businesses Take a Piecemeal Approach to Security

While many midsize businesses have multiple network security point products, they often can't afford to implement and maintain what becomes a complex, disjointed strategy. Unfortunately, this piecemeal approach leaves security gaps. In comparison, Unified Threat Management (UTM) appliances offer high value by consolidating multiple network security technologies in a single appliance. But to unlock UTM's full value, the device must be architected for scalability and engineered to meet the constantly changing nature of cyber-threats and networks—and must operate without degrading network performance.



Unified threat management (UTM) solutions offer a powerful alternative to midsize organizations that are challenged to defend against enterprise-grade cyber-threats with limited budgets and 'piecemeal' results.

UTM vs. Multiple Point Products



Network Performance Limits the UTM Value Proposition

On paper, the UTM value proposition for midsize businesses is compelling. In practice, however, the performance degradation with full UTM-enabled protection has caused many midsize organizations to turn off essential security functions in order to maintain network performance levels.[1] Moreover, businesses are quick to disable the most essential protections such as IPS, an important security technology for all organizations.[2]

Underpowered UTM solutions force businesses to make security compromises that leave them inadequately protected. Management may not even be aware of the gap, believing that the security purchased is actually being implemented. This camouflaged security gap may be especially acute in businesses with smaller IT and security staffs.

Testing firm Miercom found that enabling IPS decreases throughput performance by as much as 45% and full UTM by 90%.

While businesses claim that security considerations drive network planning, the reality is that any security technology that hampers network performance is simply switched off.

Businesses Take a Crawl-Walk-Run Approach to UTM

A flexible UTM solution lets businesses subscribe to UTM functions piecemeal or invest in the full bundled subscription and enable functionality as needed. This allows them to quickly deploy the security technologies they need and expand their deployments as security requirements change.

Typically, the full UTM subscription is the most cost-effective option, but customers rarely utilize all the functionality at their disposal, possibly due to the dedicated security products they already have in place. For example, a business may not enable the content filter included in their UTM license if they already have a dedicated solution deployed. However, the business can still reap the benefits of consolidation by switching to the UTM-provided content filtering when the point product license expires.

Customers rarely utilize all the functionality at their disposal, possibly due to the dedicated security products they already have in place.

What's Holding Back UTM Adoption?

What's Holding Back UTM Adoption?

Security Inspections Have a Cumulative Impact on Network Performance

Security inspections introduce an added layer of processing for UTM devices. A stateful firewall only inspects packet header data, with a fairly low impact on network performance—along with minimal protection. More robust UTM functions such as IPS and gateway AV provide much-needed protection by inspecting the packet contents for malware and exploits, comparing against known attack signatures and vulnerabilities, and performing behavioral analysis.

As a result, UTM inspections take more time, and can also throttle network performance. This problem is amplified as network traffic increases. The UTM solution must scan for more malware, scan more ports, perform more URL filtering, and send more and different types of files to the advanced threat sandbox when necessary.

UTM inspections take more time, but can also throttle network performance.

What's Holding Back UTM Adoption?

SSL Inspection Is a Necessary Defense

Online threat actors are known to use encrypted Web traffic as an attack vector to bypass inspection mechanisms. For example, hackers target popular social media sites and applications such as Facebook, LinkedIn, and Twitter, which are increasingly using HTTPS to alleviate privacy concerns among their users.[3] Hackers that target social networking applications gain direct access to users and benefit from an encrypted connection that is shielded from security inspections.

Inspection of SSL-encrypted traffic is a processor-intensive function of decrypting traffic, inspecting packets, and encrypting the traffic again. A UTM appliance is a logical place to perform this inspection as decrypted packets can be inspected against multiple security systems such as IPS, gateway AV, and DLP, rather than performing the SSL decryption process multiple times as required by a disparate point-product strategy.

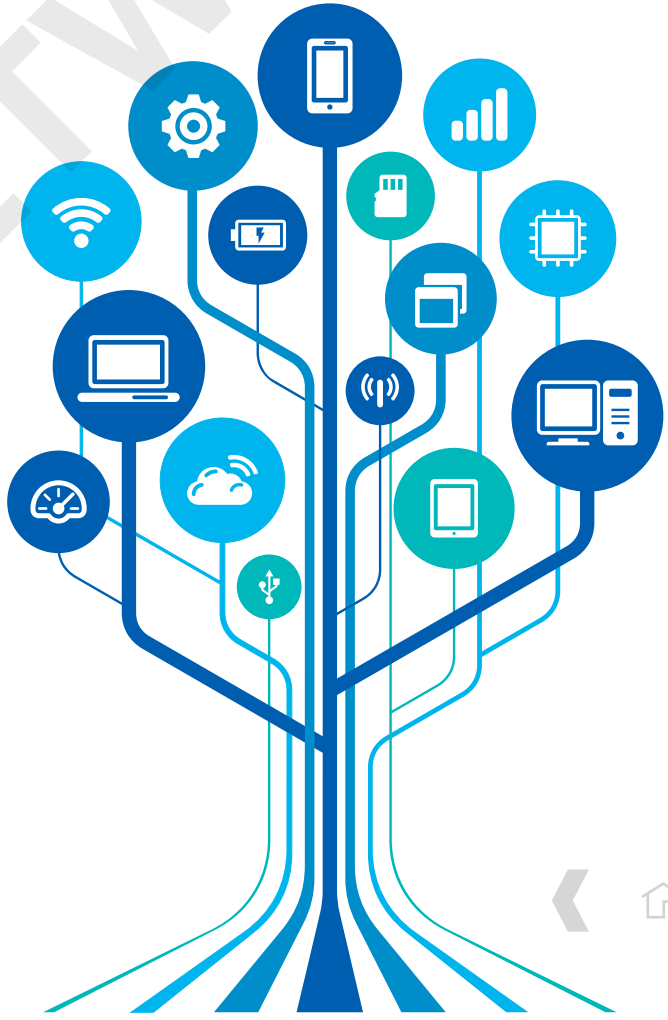
Inspection of SSL-encrypted traffic is a processor-intensive function of decrypting traffic, inspecting packets, and encrypting the traffic again.

What's Holding Back UTM Adoption?

Network Demands Are Rising at a Meteoric Rate

High-bandwidth and demanding applications that require low latency, low jitter, and high packet delivery rates—such as streaming video, Voice-over-Internet-Protocol (VoIP), file sharing, and online conferencing—challenge the limits of business networks.

The proliferation of these high-bandwidth applications also places greater demand on network security. UTM solutions are further challenged to inspect a greater number of channels as applications such as VoIP, teleconferencing, and instant messaging dynamically open multiple ports that threaten the stability and quality of these communications.



The WatchGuard Approach to UTM Protection

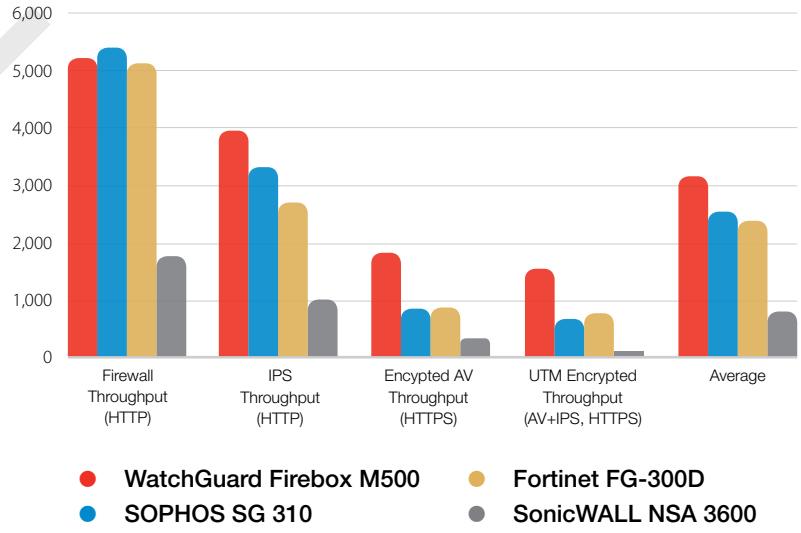
The WatchGuard Approach to UTM Protection

Total System Performance

WatchGuard takes a holistic approach to UTM, optimizing total system performance rather than a single security service. This systems-centric approach was at the heart of WatchGuard's decision to build its UTM product on general microprocessor platforms. The latest WatchGuard UTM products feature Intel Core microprocessors with built-in Advanced Encryption Standard New Instructions (AES-NI) technology. That enables hardware-based acceleration of key inspection processes, resulting in a significant increase in product performance. WatchGuard UTM solutions support high availability and clustering to ensure reliable network performance by combining multiple UTM appliances to share the processing load.

WatchGuard UTM Throughput Comparison (in Gbps)

The performance of competing UTM solutions diminishes drastically when using full UTM functionality compared to WatchGuard UTM.

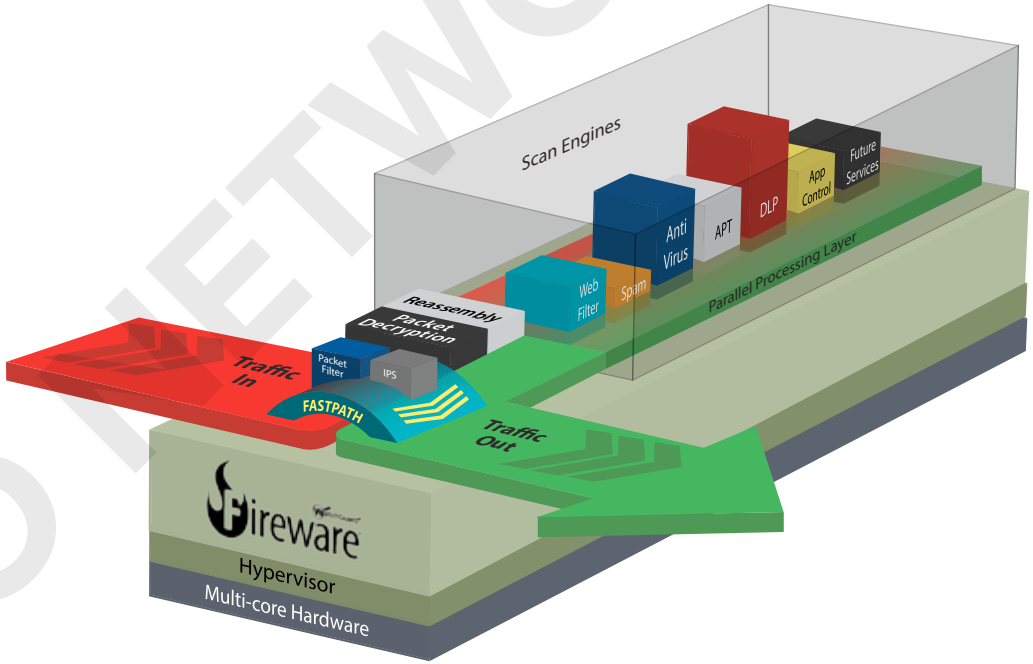


Source: Miercom and WatchGuard Technologies.

The WatchGuard Approach to UTM Protection

Highly Efficient SSL Inspection

WatchGuard UTM solutions act as a proxy between users and encrypted Web sites, decrypting HTTPS traffic, applying security logic, and performing additional checks, then encrypting the traffic in the firewall before passing it to the destination. This strategy avoids the need for SSL decryption multiple times in different network security appliances. In recent tests by Miercom, the WatchGuard Firebox M500 Firewall inspected encrypted traffic at speeds that outperformed the competitor average by 149 percent.[4]

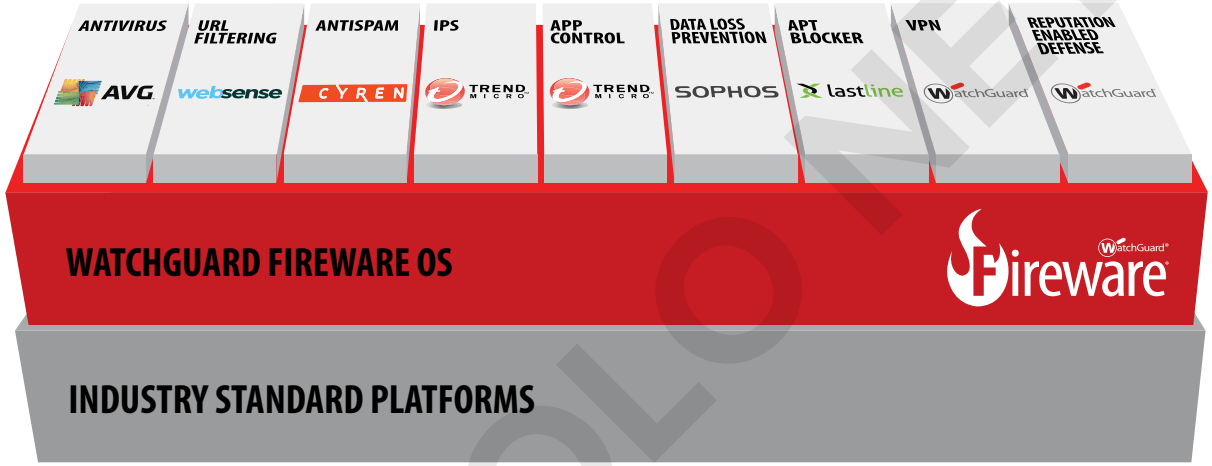


WatchGuard's efficient UTM appliance decrypts secure packets before running them through multiple security scanning engines, for significantly faster performance than competitors.

The WatchGuard Approach to UTM Protection

Future-Proof Platform

Furthermore, WatchGuard continues to develop new products and platforms for businesses that need to secure their networks now and in the future. The focus on high-performance products is important for WatchGuard, as it enables the company to expand the definition of UTM further in response to changing cyber-threats.



The modular design of the Fireware® operating system allows WatchGuard to continuously deliver the most effective security technologies available.

How to Future-Proof Your UTM Security Strategy

The changing nature of applications, technologies, and threats complicates the security planning process for any business. The traditional approach to managing these risks is to invest in new security products, but an incremental security investment practice leads to appliance sprawl, with a growing number of devices to manage, numerous monitors to watch, and minimal tolerance for false alarms. UTM consolidates otherwise disparate security technologies into one appliance with a single management console.

Here's how to future-proof your UTM security strategy

1. Focus on UTM Performance instead of Firewall Performance
2. Carefully Analyze Third-Party Testing
3. Consider UTM Features for Maximum Scalability

How to Future-Proof Your UTM Security Strategy

1 Focus on UTM Performance Instead of Firewall Performance

Vendors often promote the performance of their UTM products when used as a stateful firewall, but this inspection is inadequate on its own. Selecting a UTM solution based on stateful firewall performance is like purchasing a car based on how it idles on a car lot. While this rating allows vendors to promote impressive product statistics, businesses should make comparisons based on full UTM performance.

Network Performance Specifications To Consider

- ☐ At a minimum, look for the network performance specifications for UTM products when deployed as a stateful firewall, firewall with IPS enabled, and fully enabled UTM.
- ☐ The most complete analysis includes additional metrics such as network performance with virtual private networking (VPN) or gateway AV enabled.

How to Future-Proof Your UTM Security Strategy

2 Carefully Analyze Third-Party Testing

Third-party testing often compares UTM capabilities when deployed as an IPS or in other dedicated security roles. Even though UTM products are not designed for a single-function capacity and may not test well compared to specialized point products. UTM solutions are best tested and compared in full protection mode, as they were designed to operate.

UTM Network Performance Considerations

- ☐ Should products that offer additional capabilities (such as advanced malware detection) be penalized with lower performance statistics compared to a UTM product lacking this valuable technology?
- ☐ At what point is new security technology included in the UTM definition?
- ☐ Does the UTM have headroom to address unanticipated security needs with new services in the future, from both a hardware performance and product architecture perspective?

How to Future-Proof Your UTM Security Strategy

3 Consider UTM Features for Maximum Scalability

UTM solutions should be designed for modularity so that new security features can be added with minimal impact to network performance. UTM products that combine old software code onto a single appliance can impede network performance and require multiple management consoles and reporting systems. The UTM solution as a whole should be greater than the sum of its individual components.

Important Scalability Considerations

- ☐ Look for a "single pane-of-glass" management console that provides visibility across all integrated security tools and locations.
- ☐ Ask about clustering capability that distributes the network load across multiple appliances for load balancing, scalability, and redundancy. Even for midsize businesses that do not want to invest in multiple appliances now, this functionality helps future-proof current investments.
- ☐ Consider whether you can acquire the security technologies that are needed now, and easily deploy new security capabilities and advanced features as budgets, threats, and network needs dictate.

Download the Frost & Sullivan Executive Brief: Fulfilling the Promise of Unified Threat Management (UTM): Unlocking Full UTM Enabled Network Protection, sponsored by WatchGuard Technologies.

About Watchguard

WatchGuard® Technologies, Inc. is a global leader of integrated, multi-function business security solutions that intelligently combine industry standard hardware, best-of-breed security features, and policy-based management tools. WatchGuard provides easy-to-use, but enterprise-powerful protection to hundreds of thousands of businesses worldwide. WatchGuard products are backed by WatchGuard LiveSecurity® Service, an innovative support program. WatchGuard is headquartered in Seattle, Wash. with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.

Notes

1 McAfee Security vs Network Performance Research, SpiceWorks Voice of IT Panel, July 2014, available at http://www.mcafee.com/hk/resources/reports/rp-mcafee-security-vs-network-performance.pdf.

2 The 2013 (ISC)2 Global Information Security Workforce Study, Frost & Sullivan, 2013, available at https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/2013-ISC2-Global-Information-Security-Workforce-Study.pdf.

3 The Business Risk of Social Media in the Workplace, Frost & Sullivan, March 2014, available at https://www.frost.com/q289714227.

4 Report TB141118, Miercom, 2014, http://www.watchguard.com/docs/analysis/miercom_report_112014.pdf

505 Fifth Avenue South
Suite 500
Seattle, WA 98104
www.watchguard.com

North America Sales
+1.800.734.9905

International Sales
+1.206.613.0895