

Beyond UTM

*The Value of a Purpose-Built
Network Security Platform*

White
Paper



Unified Multi-Threat Security Solutions

FORTINET®

Introduction

Prevailing conditions relative to the regulatory, threat, and technology landscapes are changing the nature and scope of information security requirements. Providing comprehensive protection for computing systems and associated information assets is not just a good business practice, but in many cases it is now mandated. In addition, what constitutes “comprehensive” has expanded significantly in recent years. Just implementing a handful of perimeter-based, network-layer countermeasures is no longer sufficient. Today’s organizations must account for more points of entry into their networks, more types of resources that require protection, and substantially greater diversity of the threats seeking to exploit any weaknesses that may be present.

A corresponding implication then is that taking an approach to information security that is heavily dependent on point products is also no longer sufficient. Indeed, real-world experience has clearly demonstrated that given the conditions discussed above, the cost and complexity of such a strategy will quickly become overwhelming, not to mention counterproductive. Therefore, many organizations have selectively implemented and continue to consider unified threat management (UTM) devices as a means to restore balance to their overall security solution.

To be clear, there is little doubt that the reductions in cost and complexity and improvement in effectiveness that result from having a wide range of security capabilities available in a single device are advantageous. However, it should be equally clear that “actual results will vary”. After all, not all UTM technology is created equal. Gains will inevitably vary considerably from one product to the next based on a range of possible differences, such as: the source, quality, and comprehensiveness of the individual security and networking components; the degree of functional integration; the degree of management unification; and the suitability and capabilities of the underlying hardware.

In contrast, it is only with a purpose-built network security platform—as defined by this paper—that organizations will be assured of maximum security effectiveness, minimum cost of ownership, and the greatest degree of flexibility and overall performance.

What is Unified Threat Management (UTM)?

Having been bombarded with verbose explanations for the past two to three years, most IT and security professionals are already well aware of the many reasons why security strategies based predominately on point products are increasingly falling out of favor. Accordingly, we will limit ourselves to the following, brief identification and summarization of related factors.

- The primary motivation of hackers has shifted from gaining notoriety to making money, causing a step function change in the diversity, sophistication, and elusiveness of threats.
- The widespread availability of exploit development frameworks means that both new threats and variants of existing ones can be generated very easily and rapidly.
- Despite efforts to improve code quality, the overall quantity of vulnerabilities ripe for exploitation continues to rise as organizations steadily adopt emerging technologies, buy or build new applications, or even just implement upgrades to what they already have—all of which are driven by the business need to remain competitive.
- Opportunities for greater revenue and operational efficiencies are also responsible for virtually all IT organizations consistently enabling much higher degrees of user mobility, interconnectivity, and third-party access to their network systems. The impact is the introduction of more points of entry for threats, as well as increased physical distribution of the data and resources requiring protection.

To adequately respond to these factors, organizations require a multi-threat management solution that provides:

- comprehensive functional coverage—in that it blends a wide range of countermeasures, including ones that are preventive in nature (e.g., intrusion prevention) to complement those that are primarily reactive (e.g., antivirus);
- comprehensive logical coverage—in that it provides protection for threats against all elements of the computing infrastructure (e.g., networks, systems, services, applications, and data); and
- comprehensive physical coverage—in that it is applicable not just at Internet boundaries but at locations throughout an organization’s computing environment (e.g., the data center, in remote offices, and at choke points on internal networks).

Historically, organizations have attempted to address these requirements by continuously implementing additional point products to fill in the associated gaps in their defenses. But they have also come to realize that such a strategy is not sustainable. It invariably results in high capital costs, runaway operating expenses, and, despite their best efforts, is still not very effective due to the holes that inevitably appear at the seams of this type of patchwork solution. Given this situation, it is not surprising that (a) many organizations have begun to turn to UTM technology, and (b) there has been a corresponding proliferation of UTM solutions.

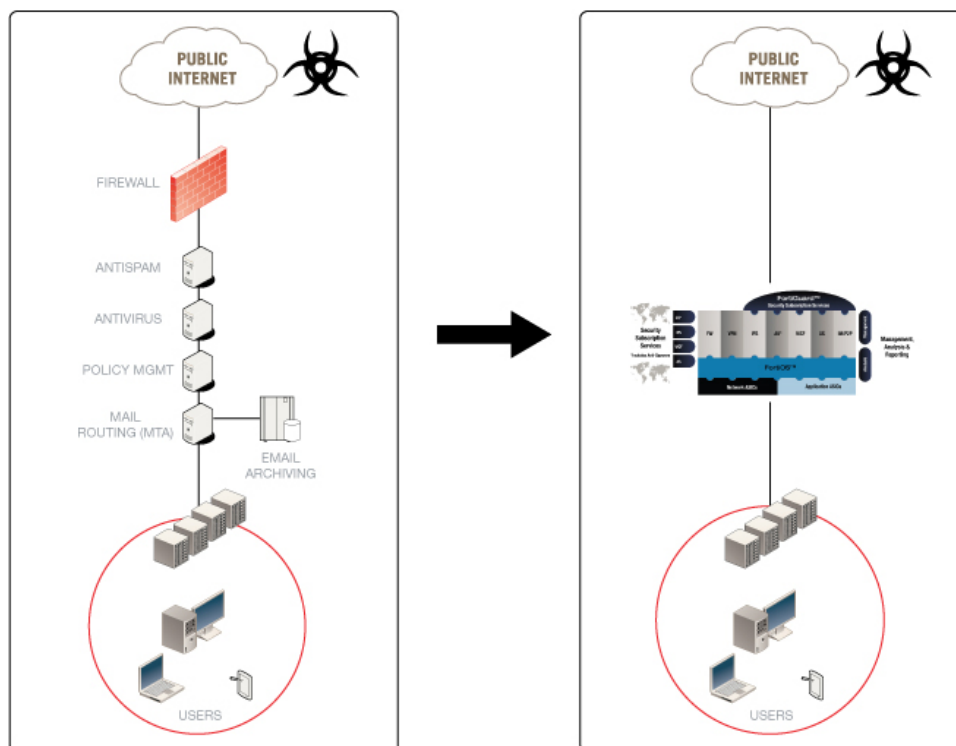
The goal with UTM is to simplify an organization’s overall security solution, despite the factors that are causing the security problem to grow in scope and complexity. Fundamentally, this is accomplished by combining multiple functional and logical security capabilities in a single physical device. On the surface this is all well and good, but it is important to acknowledge two inter-related issues.

First, with so many UTM products now available in the market, it is inevitable that there will be considerable variation when it comes to the degree of value that they deliver. Some products will prove to be marginal. They will only yield an incremental amount of simplification because they do nothing more than reduce the total number of devices an organization must field to achieve a complete security solution. In comparison, better products will also simplify operational management, boost effectiveness, and further reduce the total cost of ownership of the organization’s security infrastructure.

The second, tightly coupled issue is that distinguishing inferior UTM products from ones with significant promise is far from straightforward. It is not simply a matter of evaluating available offerings against a check list of specific security features and capabilities. Instead, it involves a detailed understanding of the how they are built. This includes everything from the quality of the individual components, how they are integrated to form a synergistic and comprehensive set of security capabilities, and the suitability of the underlying hardware, to the ongoing threat research and corresponding subscription and maintenance services that are absolutely essential to having a complete and consistently effective solution.

It is with these issues in mind that the recommendation is made for today’s organizations to look beyond conventional UTM products. To ensure they can optimally address the prevailing security challenges, organizations should instead be seeking solutions that qualify as true, purpose-built network security platforms.

Figure 1: The Consolidating Effect of UTM



What is a Purpose-Built Network Security Platform?

For all intents and purposes, a purpose-built network security platform is effectively an advanced UTM solution—one that employs an optimized design to ensure that organizations can maximize the associated gains. Jumping right in, the three high-level requirements that define a purpose-built network security platform are that it must be a turn-key system, it must have capabilities that are tightly integrated yet remain modular, and, it must be based on engineered hardware.

A Turn-Key System

To qualify as a turn-key system, a given offering must incorporate all of the elements required to have a complete solution. For starters, this entails having a pre-packaged device that combines hardware, network security operating system, and all requisite security software. However, in order to truly be complete, the offering must also include research-fueled, security subscription services, in addition to conventional maintenance and technical support services. To keep matters as simple as possible, all of these components and services should be available from a single source and should be offered with straightforward, per-device licensing (as opposed to cumbersome, per-user licensing). Furthermore, merely incorporating all of these items is not sufficient. In its own right, each element must be functionally complete and must provide capabilities that are on par with those considered to be best-in-class.

The Basic Formula for a Turn-Key System

Turn-Key Security System	=	Hardware + Network Security Operating System + Security Software + Research-fueled Security Subscription Services + Maintenance/Support Services
--------------------------	---	---

Details on what all of the above qualifications actually entail can be gleaned from the following descriptions of each of the high-level components that comprise a turn-key system in this context.

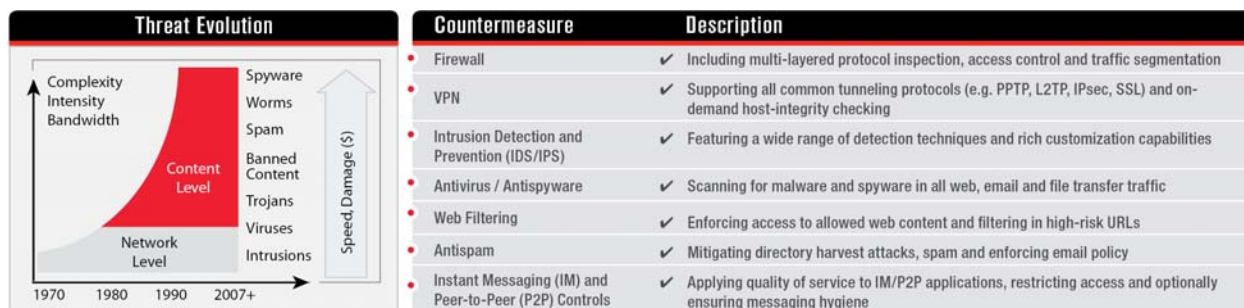
Hardware. This component is covered in detail in its own section later in the paper, but basically entails having hardware that is engineered specifically to ensure maximum performance for the supported security and networking features.

Network Security Operating System. This is an easy component to overlook. In general, beyond merely being present, an ideal operating system should exhibit three key characteristics. First, it should be hardened. To maximize system security and reliability, all unnecessary services should be eliminated, or at least turned off, and all “weak” services should be strengthened or, better yet, replaced with hardened alternatives. Second, the operating system should be pre-tuned. Similar to hardening, this process also involves trimming and modifying services, but in this case the objective is to help maximize performance of the supported applications.

Speaking of applications, the third necessary characteristic is the incorporation of an extensive set of networking capabilities (i.e., service-oriented applications), including support for: multiple routing protocols (e.g., RIP, OSPF, BGP), translation techniques (e.g., NAT, PAT), switching, VLANs, traffic prioritization, virtual systems, and failover and clustering. Overall, the goal with these capabilities is threefold: (1) to provide organizations with the option to forego separate networking devices (e.g., routers, switches, load balancers) in certain implementation scenarios; (2) to enable the resulting security platform to seamlessly fit into virtually any networking environment; and (3), to unlock further security functionality (e.g., by enabling the creation of multiple, separate security domains so that resources with different trust levels can actually be isolated and treated differently).

Security Software. As discussed earlier, adequately accounting for the prevailing conditions that are increasing the scope and complexity of the security problem requires security capabilities that provide both comprehensive functional coverage and comprehensive logical coverage. In general, reactive countermeasures should be complemented with ones that are proactive, and network-layer mechanisms should be complemented with ones that provide visibility and control at higher layers of the computing stack. The goal is to counteract the reality of network and content level threats and a diverse technology environment by establishing what essentially amounts to comprehensive defenses. To satisfactorily meet this objective, a turn-key system should ideally incorporate each of the countermeasures identified in Figure 2.

Figure 2: Network and Content Level Threats and Countermeasures



Security Subscription Services. Similar to the operating system component, there is more to content subscription services than typically meets the eye. Fundamentally, the goal is to obtain virtually continuous updates for all countermeasures that include signature-based mechanisms (i.e., intrusion prevention, antivirus/antispyware, antispam, and Web filtering), as well as issue-specific security guidance, so that top-notch protection can be maintained even as new threats emerge. However, a wide range of behind-the-scenes capabilities are actually necessary to ensure this goal is consistently achieved, including: a global research team that tracks and dissects emerging threats and newly discovered vulnerabilities; multi-disciplinary coverage (to account for all types of technologies, layers of the computing stack, and types of threats); processes for collaboration across geographies, disciplines, and even other security vendors; a mandate for fast response times (enabled by extensive experience); and, of course, the requisite network infrastructure for rapid delivery.

Maintenance Services. This final component is fairly routine, at least on the surface, but can make all the difference between a successful solution and one that comes up short. It includes timely, around-the-clock technical support, in addition to periodic updates to the firmware (i.e., operating system and security software) to ensure that it accounts for the latest advances in both the technology that is being protected as well as the technology that is doing the protecting. However, it is the less tangible characteristics of responsiveness, expertise of the associated personnel, and a pervasive sense of customer-centricity that will ultimately have the greatest impact.

Integrated, Modular Capabilities

The next high-level requirement that defines a purpose-built network security platform is that it must exhibit significant degrees of integration, yet still be modular in nature. Clearly, both parts of this requirement start to get to the heart of the issue of “how a solution is built”. Sensible integration is one of the keys to obtaining optimal performance, and is also the essential element for enabling the combination of individual countermeasures to effectively be greater than the sum of the parts. On the other hand, modularity is instrumental when it comes to having a high degree of flexibility and being able to optimize cost.

The three components that organizations should be evaluating in this case are integrated processing, integrated management, and modularity.

Integrated processing. Actually, this is just another way of saying that, to the extent it makes sense, redundant processing should be eliminated by having different capabilities “share” the execution of common routines. For example, “cracking packets” multiple times, once for each countermeasure, would be highly inefficient. That said, not all processing can/should be consolidated since some countermeasures rely on fundamentally different inspection techniques (e.g., processing for a firewall rule set proceeds progressively until a match is made, whereas processing against a threat database is typically exhaustive).

Integrated management. This is a particularly significant item, especially since it is one of the most common shortcomings of many conventional UTM products. To start with, it includes integrated policy. This way all of the settings pertaining to a given domain can easily be established, as well as subsequently modified, in a single place. It also includes the integration of events between the different security modules. This sharing of knowledge improves detection accuracy and response, regardless of whether human involvement is required. And speaking of response, the associated mechanisms—such as blocking, quarantining, or making a call to an external application (e.g., a patch management system)—should all be shared too.

While on the topic of management, an ideal solution should also incorporate the following features to help minimize operational effort:

- Centralized management—refers to the ability to remotely manage multiple devices at once and also includes other scalability features such as hierarchical policies and flexible grouping capabilities;
- Unified management—refers to the need to have just one set of management applications, even to administer different classes/sizes of devices; and
- Advanced management—involves role-based administration, event analysis and correlation, and detailed logging and reporting capabilities.

Modularity. The concept with modularity is fairly straightforward. Specifically, organizations should be able to mix and match capabilities, especially when it comes to employing different countermeasures. This way they can effectively customize individual instances of their network security platform to best meet the needs of distinct deployment scenarios without having to pay—both financially and performance-wise—for excess functionality. For example, many large enterprises have separate, dedicated security systems for their messaging environment and therefore only require firewall and intrusion prevention capabilities for their security gateways at the Internet perimeter. In contrast, smaller shops with fewer dedicated security products will typically value having a true all-in-one solution. Or, at internal network locations, organizations may only want intrusion prevention and antivirus. This way they can contain the spread of malware but otherwise minimize the potential for impeding communications that are critical to the business.

Engineered Hardware

The third and final high-level requirement that defines a purpose-built network security platform is that it must be based on engineered hardware. In general, what this means is having hardware that guarantees sufficiently high performance based on it being “matched” to the specific security software, networking services, and implementation scenarios that it is intended to support. More specifically what it means is hard-coding all stable, well-known functions into silicon, as opposed to relying solely on traditional PC or server hardware. Indeed, this sort of acceleration should be accomplished not just for network-level processes (e.g., general packet manipulation, firewalling, bandwidth shaping), but for content level processes as well (e.g., Web filtering, antivirus, antispam, antispypware).

To be clear though, specialized processors are really only one piece of the puzzle. Having engineered hardware also entails (a) achieving balance and coordination between these chips and other essential components (e.g., one or more general purpose CPUs, memory sub-systems, physical interfaces), and (b) having multiple, optimized combinations of these components to enable a series of appliances that match the performance and physical needs of a wide range of potential deployment scenarios.

The Benefits of a Purpose-Built Network Security Platform

Having established the key criteria, components, and characteristics that constitute a purpose-built network security platform, it is now appropriate to explore the value proposition of such a solution. In this regard, the overall intent behind the elements described above is to maximize/optimize the four value-centric pillars: security, performance, flexibility, and cost effectiveness (see Figure 3).

Not surprisingly, the net result is an exceedingly pragmatic network security solution—one that thoroughly and uniformly addresses the functional, logical, and physical security requirements of today’s organizations, achieves the highest levels of security effectiveness and operational efficiency, and is not disruptive to business critical communications and application transactions.

Figure 3: Component-Benefit Map for A Purpose-Built Network Security Platform

	Security	Performance	Flexibility	Cost-Effectiveness
Turn-Key System				
Single Source				✓
Per-Device Licensing				✓
Hardened OS	✓			
Pre-Tuned OS		✓		
Extensive Networking Services			✓	
Comprehensive Countermeasures	✓			
Content Subscription Services	✓			✓
Maintenance Services	✓			✓
Integrated-Modular Capabilities				
Integrated Processing		✓		
Integrated Management				
Integrated Policy	✓			✓
Integrated Events / Data	✓			✓
Shared Response Mechanisms				✓
Centralized Management				✓
Unified Management				✓
Advanced Management			✓	✓
Modularity		✓	✓	✓
Engineered Hardware				
Specialized Processors		✓		
Matched / Balanced Design		✓		
Family of Optimized Appliances		✓	✓	

Conclusion

Over the past few years, it has become quite clear that security strategies based predominately on point products are not sustainable. Ongoing changes to the threat and technology landscapes ensure that the resulting, cobbled-together “solutions” inevitably lead to mounting capital and operational costs and, somewhat ironically, to diminishing levels of effectiveness. Faced with this situation, organizations are seeking ways to reduce the complexity, improve the effectiveness, and enhance the operational efficiency of their network-based security defenses.

On the surface, conventional UTM technology seems well suited to these requirements. However, the UTM market is quite crowded and the corresponding products vary considerably in terms of quality and overall effectiveness. Fortunately, organizations can cut through the confusion by embracing purpose-built network security platforms instead. By featuring integrated yet modular capabilities and engineered hardware, these turn-key systems effectively guarantee maximum gains in terms of security effectiveness, operational efficiency, and total cost of ownership.

About the Authors

Mark Bouchard, CISSP, is the founder of Missing Link Security Services, LLC, a consulting firm specializing in information security and risk management strategies. A former META Group analyst, Mark has assessed and projected the business and technology trends pertaining to a wide range of information security topics for nearly 10 years. He is passionate about helping enterprises address their information security challenges. During his career he has assisted hundreds of organizations world-wide with everything from strategic initiatives (e.g., creating 5-year security plans and over-arching security architectures) to tactical decisions involving the justification, selection, acquisition, implementation and operation of their security and privacy solutions.

Freddy Mangum is Vice President of Product Marketing and brings to Fortinet more than 12 years of sales, marketing and business development experience with companies in the networking and security markets. Freddy most recently owned a marketing consulting company that provided product strategy and marketing services to companies such as IronPort Systems, Sarvega (acquired by Intel) and Permeo (acquired by Blue Coat). He was previously employed with prominent security companies, such as Internet Security Systems (ISS), where he directed product marketing activities for product lines generating more than \$250 million in revenue. Freddy has also held numerous senior technical marketing and consulting engineer roles with companies such as Cisco Systems, WheelGroup and UUNET.

About Fortinet

Fortinet is the pioneer and leading provider of ASIC-accelerated multi-threat security systems, which are used by enterprises and service providers to increase their security while reducing total operating costs. Fortinet solutions were built from the ground up to integrate multiple levels of security protection--including firewall, antivirus, intrusion prevention, Web content filtering, VPN, spyware prevention and antispam--providing customers a way to protect multiple threats as well as blended threats. Leveraging a custom ASIC and unified interface, Fortinet solutions offer advanced security functionality that scales from remote office to chassis-based solutions with integrated management and reporting. Fortinet solutions have won multiple awards around the world and are the only security products that are certified eight times over by the ICSA (firewall, antivirus, IPSec, SSL, IPS, client antivirus detection, cleaning and antispayware). Fortinet is privately held and based in Sunnyvale, California.

FORTINET

1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1-408-235-7700
Fax +1-408-235-7737
www.fortinet.com

©2007 Fortinet, Inc. All rights reserved. Fortinet, FortiGate, FortiOS, FortiAnalyzer, FortiASIC, FortiLog, FortiCare, FortiManager, FortiWiFi, FortiGuard, FortiClient, FortiReporter and the "Forti" family of marks are trademarks or registered trademarks of the Fortinet Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners. Licensed under U.S. Patent No. 5,623,600. Although Fortinet has attempted to provide accurate information in these materials, Fortinet assumes no legal responsibility for the accuracy or completeness of the information. Please note that no Fortinet statements herein constitute or contain any guarantee, warranty or legally binding representation. All materials contained in this publication are subject to change without notice, and Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

WPR133-0708-R1