

Multi-Layer Security Platforms The New Definition for Best of Breed

White
Paper



High Performance Multi-threat Security Solutions

FORTINET™

Introduction

In the not too distant past, the information security needs for most organizations were fairly straightforward. From a technology perspective, core defenses included a handful of perimeter-based firewalls to policing traffic originating from the Internet, along with software at desktops, and perhaps email gateways, to counter the emerging threat from viruses. A smattering of tools were subsequently added either to “enable the business” or to achieve an incrementally greater degree of defense in depth. Most notable among these were virtual private network (VPN) technology, to support secure remote connections over the Internet, and intrusion detection systems (IDS), essentially to obtain a network-based variation of anti-virus controls – and inevitably yielding a mountain of “event” data requiring a very time-consuming analysis by the security team.

In general, the rule of the day during this period was for organizations to purchase best-of-breed point products to fill their security technology requirements. This approach was practical due to their rather modest needs. Not only that, but it was also appropriate. It was a formative time for the security industry. In other words, “best-of-breed” actually meant something, since even the most fundamental products (e.g., firewalls and AV) were still maturing, leaving considerable room for differentiation. Furthermore, security staff, as well as security programs overall, were also still maturing. Under these conditions purchasing security products one at a time simply made good sense. It allowed organizations sufficient time for digestion before jumping back in the pool.

However, in recent years a number of factors have conspired to change the security landscape – dramatically and forever. Among others, these drivers include the growing ubiquity of communications services, the proliferation of information technology and applications, the emergence of regulatory compliance, and an escalating arms race with hackers. The result is that providing anything but a comprehensive degree of protection is not an option in today’s business and computing environment, where there is an ever increasing quantity of infrastructure and information to secure *and* a greater quantity, diversity, and intensity of threats to ward off.

Given these circumstances, it is not surprising that the conventional approach of utilizing best-of-breed point products is no longer appropriate. The cost and complexity of such a strategy would simply be overwhelming, not to mention counterproductive. Accordingly, it is time for organizations to embrace a new approach – one where best of breed is redefined to also account for the scope of security capabilities that a product provides. In particular, to maximize effectiveness while minimizing costs, organizations should be adopting a strategy that focuses on the broad and flexible implementation of multi-function security *platforms*.

To clarify further, it is also important to realize that:

- It will be unrealistic to rely solely on such security platforms. Indeed, it will typically be necessary to supplement them with selected point products to provide additional, niche or emerging capabilities;
- This strategy is not just about implementing so-called unified threat management (UTM) devices. Instead, it is about extending the UTM concept by enhancing the associated devices so they are applicable to a far greater set of use cases than those they are currently associated with – namely small-to-medium businesses and the branch offices of larger enterprises; and
- The appropriateness of this strategy depends on the availability and selection of a suitable technology solution. It is with this in mind that the second half of this paper is dedicated to enumerating and expanding upon the primary characteristics that define a best-of-breed multi-layer security platform: multi-layer security capabilities, top-notch performance, unbounded flexibility, and a high degree of cost effectiveness.

Today's Security Challenges

A closer examination of the ongoing changes to the security landscape is essential to better understanding both the market need for multi-layer security platforms and the requirements that must be met to achieve a best-of-breed solution.

The Evolution of Threats

Arguably the greatest security challenge facing organizations today is the evolution of threats, those bad elements (e.g., viruses, worms, hackers) which seek to exploit a system's vulnerabilities. To begin with, there are so many different types of threats, taking advantage of so many different techniques, targeting so many different vulnerabilities, and coming from so many different vectors that even having multiple best-of-breed countermeasures is unlikely to provide sufficient coverage to stop them all.

Compounding matters, the past couple of years have seen the steady maturation and growing accessibility of threat development toolkits along with a shift in hacker motivation, from the accumulation of accolades/recognition to the accumulation of cold hard cash. The unfortunate yet predictable result has been a number of significant and undesirable changes to the threat-scape.

Most notable among these is the fact that threats are now being created more quickly than was historically the case. In the past, organizations would learn about a new vulnerability and then have weeks or even months to receive and implement a corresponding patch – or at least to receive and implement updates to their anti-virus software and intrusion detection systems. However, threats/attacks are now being launched only days after the announcement of vulnerability. Furthermore, today's threats are routinely capable of spreading at an alarming pace, often reaching a substantial portion of susceptible targets within a matter of mere minutes.

Equally troubling is the fact that threats are becoming more elusive. On one hand, this stems from a rise in the frequency of blended threats. By creatively employing multiple exploit mechanisms, payloads, and propagation techniques, hackers can enhance the likelihood of their creations being able to elude an organization's defenses. On the other hand, it is also stems from hackers shifting their attention to focus less on exploiting network-layer vulnerabilities and more on those associated with application services, logic, and even data itself. In both cases, the result is the same: an increasing capability and frequency of threats slipping through the predominately network-layer focused defenses that most organizations have deployed to date.

To keep up with these changes to the "threat-scape", security strategies and solutions must evolve as well. In particular:

- They must become more "blended". Not only must reactive countermeasures be supplemented with ones that are more proactive – and therefore capable of addressing even unknown attacks – but network-focused defense mechanisms must also be supplemented with ones that can thwart application-layer threats;
- They must become more efficient. A greater volume of threats inevitably means a greater quantity of security "events" that must be dispositioned by an organization's security staff. In addition, there is also the need to operate and maintain the greater variety and quantity of security mechanisms required per the previous bullet item; and,
- They must become more economical. The security budgets for most organizations are already strained to the point that purchasing a plethora of additional countermeasures is simply not realistic. This leads to multi-function security appliances being an ideal choice. However, it is important to realize that this holds true only to the extent that it is unnecessary to compromise in terms of either the quality of the individual countermeasures or the performance of the overall system.

The Expanding Portfolio of Technology and Applications

Another significant change driving the need for multi-layer security platforms is the growing diversity and quantity of computing resources, both infrastructure and information, that now needs to be secured. Recent years have seen businesses trying to remain competitive, or even get ahead in the game, by implementing a rapidly expanding array of new technologies (e.g., instant messaging, Personal Digital Assistants, smartphones, Wireless Local Area Networks, web services, and IP telephony), by dramatically increasing their online presence, and by deploying a wide variety of revenue generating and/or productivity enhancing applications.

The issue here is twofold. First, as suggested earlier, there is simply more mission critical “stuff” that needs to be secured. This alone reiterates the need for security solutions that are both efficient and which provide greater degree coverage (based on the scope of security services they provide). However, it is also important to acknowledge that much of this “stuff” is relatively new to the market (at least initially), is fairly complex, or may even be highly distributed in nature. Such conditions inevitably yield an indefinite period of time that is characterized by a spike in the population of code-based vulnerabilities, as well as an increased potential for vulnerabilities being introduced through configuration errors (at least until administrators become more familiar with the new technologies).

Overall, what this suggests is that:

- The effectiveness and efficiency gains derived by using multi-layer security platforms are essential to help offset the effort and expense of operating point products to secure emerging (or even legacy) technologies;
- Ideally, a multi-layer security platform should have an architecture that fosters adaptability and flexibility, thereby enabling its scope of coverage to be extended to cover new technologies over time.

The Proliferation of Points of Protection

Closely related to the previous section’s challenge of having to protect a rapidly expanding population of computing resources is the need to provide this protection at a growing number of physical locations within an organization’s environment. Indeed, the implications in both cases are essentially the same. Specifically, the need for substantially more security coverage – be it functional or physical – necessitates the greater overall effectiveness, efficiency, and economy available with multi-layer security platforms, as opposed to an extensive portfolio of point products.

The underlying issue in this case is that organizations no longer have well-defined perimeters characterized by a handful of Internet connections and private Wide Area Network links to their satellite offices and a few key partners. Instead, opportunities for greater revenue and operational efficiencies have driven organizations to enable much higher degrees of interconnectivity and in-depth access to their networked systems. Indeed, over the past few years, virtually all businesses have increased their support for online customer services, business-to-business relationships, local access by guest users, telecommuting and employee mobility, and remote office/branch office computing services. Consequently, they now need comprehensive protection (from a functional perspective) not only at multiple “perimeter” demarcation points, but also on their internal networks, at user endpoints, within their data centers, and at their branch offices.

The Emergence of Regulatory Compliance

Another high profile change has been the emergence of a plethora of privacy and security related legislation and industry specific regulations. However, given that most IT and business personnel are already well versed in or are otherwise numb from hearing about compliance, it is appropriate to spare the details and cut right to the consequences. In particular, these include that:

- Providing comprehensive privacy and security (against all threats, for all resources, and in all locations) is not an option – it is essentially a legal necessity;
- Fulfilling compliance obligations will be a significant drain on already strained IT and security resources, thereby further escalating the need for security solutions that are highly economical and easy to operate; and,
- To help address compliance requirements, security solutions should include capabilities to facilitate the creation, deployment, and confirmation of associated policies (e.g., unified management, detailed logging, and robust reporting).

Point Products Piling Up

Hopefully by this point it is clear that the security landscape has undergone significant changes in recent years. For many organizations, trying to keep up with these changes by sticking with conventional wisdom has led to point products now starting to pile up. And along with them have come rising operational costs, greater complexity, and, somewhat ironically, reduced effectiveness – especially since few if any of the pieces of the puzzle are capable of working together.

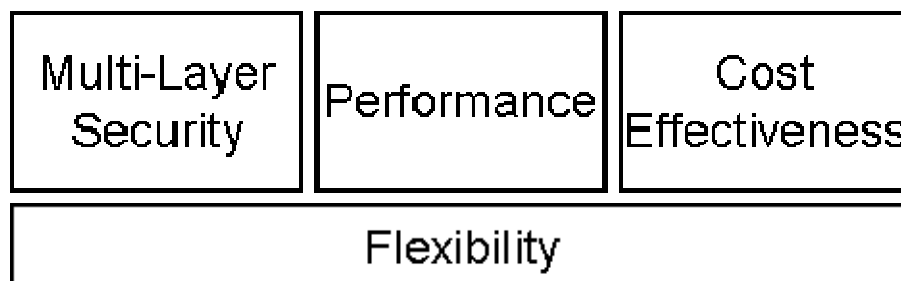
To be clear, best-of-breed point products do in fact provide in-depth security capabilities. However, each product is only narrowly applicable and is therefore unable to provide the breadth of coverage needed in today's IT environments. To put it another way, the (potential) incremental gain in security capabilities that can be attained with best-of-breed products is simply not sufficient to offset the complexity and expense that will result from organizations needing to implement many of them to cover all of their bases.

In contrast, multi-layer security platforms hold the promise of more efficiently and economically providing an effective, modern-day security solution. This is based on integrating a full set of security services into a single, easy-to-manage appliance that is capable of supporting a wide range of deployment scenarios.

The New Definition of Best of Breed

Of course, recognizing the need for multi-layer security platforms is only half the battle. It then becomes a matter of being able to identify a best-of-breed solution that fits the bill. In this regard, organizations are advised to focus on the following four categories of evaluation criteria:

Figure 1: New Definition of Best of Breed



Multi-layer Security

Given that the primary objective of using a multi-layer security platform is to obviate the need for a series of point products, it is clearly a fundamental requirement that such solutions incorporate a wide range of the most commonly needed security services. In part this is necessary to ensure applicability in the

greatest number of use cases, which is a topic that will be covered more thoroughly in the next section. However, from a security perspective it is also about having the ability to protect against all manner of threats with a single device.

In this regard, it is imperative to recall the implications of the previously discussed challenges. Specifically, it should be clear that effectiveness will depend on having a set of security services (a) that provide protection not just at the network layer of the communications stack but at the application layer as well, and (b) that are not just reactive, but which also include proactive mechanisms capable of stopping unknown attacks.

It should also be noted that this blending of techniques and mechanisms can occur not just across different services, but also within the individual countermeasures. For instance, a reactive (i.e., signature-based) anti-virus engine can be made more effective by coupling it with a proactive intrusion prevention engine and/or by enhancing it to include a proactive, heuristics-based virus detection capability. In fact, because it correlates well with security effectiveness, the characteristic of having a high-degree of *both* inter and intra –service blending should be considered an important criterion when selecting a multi-layer security platform.

Of course, just because a given solution incorporates a wide range of security services does not automatically mean it will be effective. This is why it is also necessary to consider the quality of the individual countermeasures that are included. Ideally, there should at least be parity with the main features, functions, and security mechanisms employed in corresponding best-of-breed point products. For example, an intrusion detection and prevention capability included in a multi-layer security platform, in addition to signature-based detection, would ideally incorporate protocol anomaly, behavioral anomaly, and heuristics based mechanisms. Furthermore, there should be sufficient evidence that the associated vendor is serious about continuously improving their solution. Typically this would include (a) having a team dedicated to researching new threats, vulnerabilities, and emerging security techniques, and (b) routinely issuing updates to both content (e.g., signatures) and firmware.

Yet another consideration will be inter-service integration. Products which demonstrate even a basic level of pre-configured capabilities in this area will have both operational and effectiveness advantages over competing solutions, especially most point products.

Finally, accounting for the various requirements cited in this section, figure 1 identifies a minimum set of security services and capabilities that would be appropriate for a multi-layer security platform.

Figure 2: Minimum Security Services and Capabilities

Firewall	Including multi-layer and protocol inspection, access control, and traffic segmentation
VPN	Supporting all common tunneling protocols (e.g., PPTP, L2TP, IPSec, SSL) and on-demand host-integrity checking
Intrusion Detection and Prevention	Featuring a wide range of detection techniques and rich customization capabilities
Antivirus	Scanning for malware and spyware in all web, email, and file transfer traffic
Web Content Filtering	Enforcing access to allowed web content and filtering high risk URLs
Anti-Spam	Mitigating directory harvest attacks, spam and enforcing email policy
Instant Messaging & Peer to Peer Controls	Applying quality of service to IM/P2P applications, restricting access and ensuring messaging hygiene if allowed

Ultimate Flexibility

Whereas multi-layer security capabilities are critical to addressing the evolving threat and vulnerability landscapes, flexibility is another essential ingredient needed to ensure coverage can economically be provided for the widest possible range of IT resources and in the widest possible set of locations. In other words, the key to an ideal multi-layer security platform is having it be appropriate for use in virtually any deployment scenario – not just for small and medium businesses, as is the case with UTM devices.

At a high level, achieving such a degree of flexibility entails:

- Providing multiple hardware choices so that organizations can pay only for what they need by selecting a system that closely matches the performance, capacity, and advanced features (e.g., high availability, virtual domains) they require in a given scenario.
- Providing support for multiple networking interfaces/ports/mediums (e.g., 10/100/1000 Ethernet, ADSL, dial-backup, wireless), features (e.g., QoS/traffic management, VLANs), and deployment options (e.g., transparent, routed, NAT) so that the solution will fit seamlessly into any environment.
- Providing multiple choices in terms of the combinations of security services/modules that can be purchased.
- Providing optional subscription services to keep signatures and other content-oriented portions of the security modules up-to-date with the changing threat, vulnerability, and technology landscapes.

Beyond providing adaptability over time, this will ensure the solution is able to accommodate the needs of multiple constituencies within the IT organization (e.g., network operations, security operations, messaging operations, compliance). Different groups can opt either to embrace the consolidated solution, or associated capabilities can be left out (or just go unused) so that they can retain allegiance to any preferred solution provider they already have. For example, the team responsible for email and other messaging applications may already have associated security capabilities as part of their overall, headquarters-based messaging solution. In this case, anti-virus and IM/P2P modules would not be needed in an upstream multi-layer security platform.

In addition, it is this same selectivity, along with the performance capabilities discussed in the next section, which will enable an ideal multi-layer security platform to be used not just in small and medium business but in larger enterprises as well. For the former customers, all-in-one functionality is a must-have. In contrast, it is expected that entrée into larger outfits will be based, at least initially, on only providing a handful of services to supplement what these organizations already have in place – either at the perimeter or even on internal networks. Subsequently, the multi-layer security platforms can serve as a point of consolidation, either as the organization seeks to simplify matters and/or the other products reach obsolescence/end of life.

Finally, given that it has the greatest potential of meeting whatever needs a customer might have, a highly flexible multi-layer security platform would also be the ideal solution for providers of managed security services, supporting both in-the-cloud and customer premise options.

The Power to Perform

Performance related capabilities comprise the third category of evaluation criteria for multi-layer security platforms. They are essential for the straightforward reason that processing communications traffic through multiple security services is far more taxing than it is with a single-service point product. Furthermore, a considerable degree of a solution's flexibility depends on having sufficient performance and capacity to meet the needs of the wide variety of implementation scenarios that may be encountered.

The key to ensuring an adequate and consistent level of performance is having a purpose-built system. To start with, this entails having an operating system that is pre-hardened and pre-tuned to best meet the needs of the specific applications (in this case security modules) that it will be supporting. However, it also requires having an underlying hardware design that provides sufficient processing power, memory, and I/O capacity not only to achieve rated throughput, but also to do so without incurring an unreasonable amount of latency. After all, without sufficiently high performance a solution will not be able to simultaneously provide multiple security services, including intensive application and content layer countermeasures, while still maintaining proper operation of the business applications passing through it. This is why it makes sense, in general, for organizations to favor solutions which incorporate specialized hardware (e.g., ASICs, network processors) to accelerate as many functions as possible (e.g., general packet processing, content inspection, encryption), as opposed to using solutions which rely solely on PC-based hardware.

Of course no amount of performance will be sufficient if the system is not operating properly, or not at all. Consequently, careful consideration should also be given to reliability features, including: redundant components, support for back-up connections, high availability (active/passive and active/active), and stateful failover.

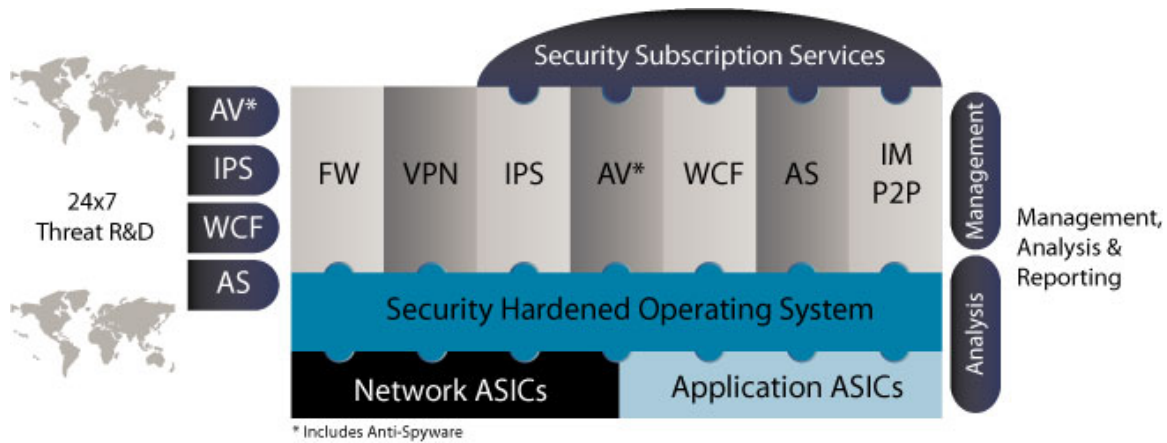
A Pragmatic Solution

The growing need to have more security services in more locations can be an expensive proposition. By their very nature, multi-layer security platforms are intended to help counter this issue by providing a way to obtain, ideally selectively, multiple security functions in a single, easy-to-implement form factor. However, capital expenditures are just one component of a solution's overall cost. A best-of-breed multi-layer security platform should also incorporate features to help minimize operational effort and costs, including:

- Centralized management, which 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, which refers to the need to have just one set of management applications, even to administer different classes/sizes of devices (e.g., branch office versus enterprise perimeter versus data center); and
- Advanced management, which involves role-based administration, event analysis and correlation, and detailed logging and reporting capabilities.

In addition, ease of use should be a pervasive characteristic, exhibited uniformly across hardware, security modules, and management applications alike.

Figure 3: A Multi-Layer Security Platform



Summary

Significant changes in the threat, technology, and regulatory landscapes are forcing organizations to implement an increasing array of security controls in an increasing number of locations throughout their business environments. In response to this situation, organizations should be reassessing their definition for and use of best-of-breed security solutions. Indeed, security strategies based on heavy use of best-of-breed point products are no longer ideal, particularly in terms of cost and security effectiveness. Instead, enterprises and managed security service providers alike should be embracing multi-layer security platforms – particularly those exhibiting high degrees of flexibility, performance, and cost effectiveness – as the new best-of-breed solution when it comes to securing enterprise computing environments.

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, Vice President of Product Marketing, 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, IDS, 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

©2006 Fortinet, Inc. All rights reserved. Fortinet, FortiGate, FortiOS, FortiAnalyzer, FortiASIC, FortiLog, FortiCare, FortiManager, FortiWiFi, FortiGuard, FortiClient, and FortiReporter are 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

WPR125-0606-R1