Unifying Your Threat Management Practice:
A Pragmatic Approach to IT Security

White Paper

FORTINET®

Abstract

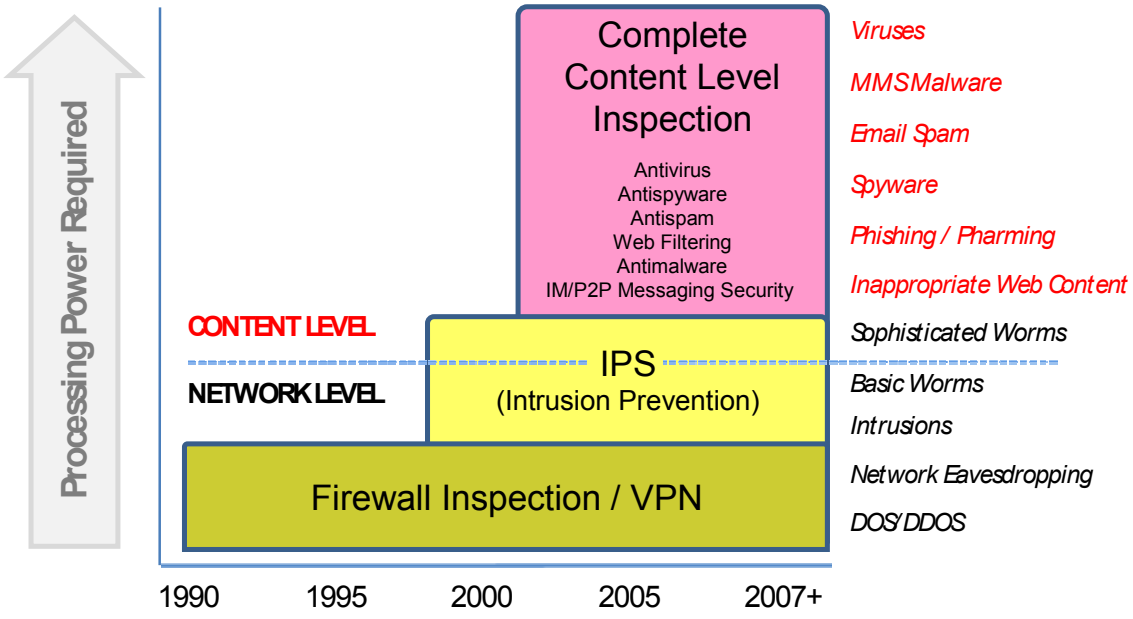
Ever more sophisticated threats, increasing compliance requirements, and evolving applications continually expose new gaps in your network security. You know that more point solutions aren't the answer—it's hard enough for your team to manage what you already have. But trying to unify your threat management infrastructure by choosing a vendor that provides a single security function won't necessarily solve your problems. In fact, unless your vendor offers unified management, reporting, and global threat research, you'll end up with just as many management headaches as a multi-vendor solution. This white paper will help you perform a pragmatic security gap analysis with an eye to selecting the right vendor to help you improve network security without multiplying management complexity.

The Network Security Dilemma

As an IT executive trying to keep on top of network security, you face a difficult task, due to the growing sophistication of the threats you face, an ever-increasing compliance burden, and the vulnerabilities exposed by new applications and technologies.

Hackers are no longer focused so much on notoriety as on financial gain—in fact, organized crime is becoming an ever-larger part of the network security struggle. Combined with the widespread availability of exploit development frameworks, the addition of the profit motive means that threats arise and evolve faster than ever before, and threats are no longer dependent on a single exploit mechanism. Furthermore, it's not just network-level security you must be concerned with, for which firewalls and intrusion prevention systems (IPS) were developed, but content (data) level security as well. Messaging security, antivirus, antispam, Web filtering, antispyware…the list of required technologies just keeps getting longer.

Figure 1: Threat Complexity Has Increased Over Time



Given this pressure, it seems like salt in the wound that you also face the possibility of criminal and civil sanctions for failure to keep up with these threats. Regulatory and best practice guidelines like Sarbanes-

Oxley, Basel II Accord, and PCI/DSS place an enormous due-diligence burden on IT executives. Not only must you keep up with the latest technologies for dealing with potential attacks, to prove that you did all you could to protect sensitive data and your networks, but you must be able to log traffic and events, as well. This is not only necessary for the legally-required audits that prove your compliance, but also for forensic operations, which are critical to discerning and quickly remediating weaknesses in your security regime.

Finally, to top it all off, the ultimate dilemma facing IT executives: In your efforts to improve operational efficiencies and support the drive to competitive advantage and business success, you have worked assiduously to provide greater user mobility, interconnectivity, and third-party access to your network. As well, you've carefully adopted new technologies where they promised bottom-line improvements, implemented new applications, and kept existing applications up to date. And what's the payoff? In all cases, in addition to improving business performance, you've inevitably added new openings for attack—or rather, your vendors have. And this doesn't even take into account the Internet applications like Skype, that your users may add to the mix, with all their vulnerabilities!

Pragmatic Network Security

Unfortunately, you're doing all this on a budget that may seem miniscule compared to the urgency of these threats. The reality is that IT security is only a one part of your overall IT budget, which in turn is only a small part of the overall business budget. You not only have to be careful to rank threats in accordance with their potential impact on the business, but also balance the appropriate remedial technologies and products against everything else in your IT budget. And, to top it all off, you must do so under the imperative to reduce operational expenses relative to capital expenditures. The best threat management strategy in the world won't do you much good if you can't afford the people and time to operate it!

All this explains why IT executives are so interested in unifying threat management, since it promises to reduce the complexity, and thus the cost, of implementing and managing the security infrastructure. But it also imposes an extremely pragmatic approach on IT executives concerned with that unification, which can be summed up under three heads:

1) Security cannot be viewed as an end in itself. It is more usefully seen as a critical part of network and application availability—of enabling users to get their jobs done. Your choices of security technologies and products will be determined by how, in practice, they serve this goal. One advantage of this perspective is the resulting ease with which security decisions can be related to your overall IT goals, and to the bottom line of the business they serve.
2) Vendor consolidation becomes key. The OpEx imperative demands simplicity, not multiplicity. Continuing to buy disparate "best of breed" single function products—a term that's meaningless if you end up with an unmanageable mess—to respond to the evolving security "threat-scape" is a recipe for management disasters. As we'll see below, this also demands unified management, reporting, and research from the vendor you choose.
3) No forklifts! Whatever you implement must complement existing security investments. This is almost too obvious to be worth mentioning, except that so many vendors seem to assume that their solution trumps years of careful investment, implementation, training, and experience on your part. But, again, this makes unified management, reporting, and research even more important, to avoid multiplying management touchpoints beyond your team's ability to deal with them. Management complexity is never entirely avoidable, but it can be minimized with the right choice of vendor.

Finding and Filling the Network Security Gaps

The essence of pragmatism is the refusal to consider theory and practice as opposing concepts. Instead, a pragmatist uses theory as a kind of map for finding a way to a practical solution. One way to construct a useful map for finding your way to unifying your threat management infrastructure is to divide up your IT infrastructure into functional network segments, which may be either physical (e.g., data center or core) or logical (e.g., guest access or email messaging). Then you can try to discern what security gaps may exist in each of them. This will enable you to come up with the right questions to ask as you further research technologies and vendors, develop a short list, and make your final decision.

Following this pragmatic strategy starts with a simple question: do I have the right products and technologies in place in each of these functional network segments?

- Perimeter
- Data Center
- Core
- ROBO/SOHO
- Secure Email Messaging
- End Point

The table summarizes these segments and the technologies needed to protect them. To help you begin to construct your map of potential vulnerabilities, we will review each very briefly in terms of the challenges that can create particularly harmful gaps.

IT Infrastructure Deployment	Perimeter	Data Center	Core	ROBO/SOHO	Secure Email	End Point
Network Level Protection Needs						
Firewall	X	X	X	X		X
IPSEC VPN	X			X		X
SSL VPN	X			X		
Intrusion Detection System (IDS)	X	X	X	X		
Intrusion Prevention System (IPS)	X	X	X	X		
Network Adminssion Control (NAC)				X		X
Content Level Protection Needs						
Web Filtering	X			X		X
Antivirus, Antispyware & Antimalware	X	X		X	X	X
Antispam	X	X		X	X	X
Instant Messaging Firewall	X			X		X
P2P Firewall	X			X		

Perimeter

The network perimeter used to be the central point of contention of network security. No more, but even so, the perimeter is your first line of defense, and it's where many external threats are focused, particularly those with criminal intent. Here you face multiple threats on both the network and the content level. The potential gaps with which you should be most concerned will be found in your VPN (IPSEC or SSL), firewall, intrusion prevention system (IPS), and antivirus solutions—throughput, availability, up-to-date threat programming, and so forth. Consider how closer integration of these may create a protective synergy that increases network and content level security.

Data Center

The data center is the heart of your business. Here reside the servers and applications that enable your users to do their jobs. Overall, though, your greatest challenge here is throughput and real-time operation, especially with regard to antivirus and content scanning for mission critical applicaitons—if your solution can't keep up, something will eventually slip through, affecting many, if not all, your users. Here is where Unified Threat Management solutions come into their own, but only if they offer scalable capacity and performance, as well as high availability. For the highest reliability and flexibility, look for ATCA (Advanced Telecom Computing Architecture) compliant hardware.

Core

At the core the challenges are massive bandwidth, and an enormous number of simultaneous sessions, as well as the presence of real-time applications such as VOIP (Voice Over IP) that are characterized by small packet size. Be aware that many solutions—especially software running on commodity hardware (e.g., PCs)—can claim high throughput for 512-byte packets, but the fine print reveals a dramatic degradation in performance when processing the smaller packets characteristic of applications like VoIP. Although in the core you're primarily concerned with firewall, VPN, and IPS operations, the solutions you choose must offer scalable capacity, performance, high availability and redundancy. This is the domain of ATCA hardware and dedicated ASIC processors that accelerate both network and content level protection capabilities!

ROBO/SOHO

Remote Office/Branch Office (ROBO) and Small Office/Home Office (SOHO) operations pose many of the same problems as traditional perimeter defense. What they add is the fact of roaming users and devices and the vulnerabilities of wireless networking and various access devices (e.g. DSL modems), as well as the presence of voice and other real-time applications. Again, check the small-packet performance of any solution to make sure its throughput claims are valid for these applications. Perhaps most critical here is good centralized management. You can't afford IT staff at every branch, and certainly not at your employees' homes! You'll be relying on the strengths of your UTM vendor's offering to help: e.g., antivirus, antispyware, web content filtering, and so forth that can easily be managed in a centralized fashion.

Secure Email Messaging

Users take email for granted, but no IT executive concerned with security can afford to do so. In many ways, this is the ultimate gap: email is the number-one vector for virus infections, a major source of data insecurity (from either clueless or malicious users), and often the medium for legal hassles (e.g., various forms of inappropriate and/or tortious behavior). The challenges here are manifold. Top of mind, of course, is inbound security: spam, spyware, viruses, and other forms of malware. But don't overlook outbound security: advanced archiving capabilities can be a critical feature when it comes to regulatory compliance, and outbound content filtering can protect important confidential information.

End Point

Defense in depth requires close attention to the end points on your network: the desktops, laptops, and increasingly and PDAs. A gap here can compromise both network and application integrity, and being able to enforce compliance with corporate security standards is key. If they're dirty, they don't get in! Of particular importance is the quality of protection against spyware and viruses. A personal firewall and a solid VPN client can add another layer of protection.

Putting It All Together

It's important, as you consider Unified Threat Management solutions, to look for a vendor that not only offers a wide range of security technologies, but, even more important, gives you unified management, reporting, and threat research. Otherwise, you'll end up with the same management burdens that a collection of disparate point products would deliver, with disastrous effects on your operational expenses.

Unified Management

Managing your security infrastructure is primarily about developing, distributing, and enforcing security policies, as well as managing the configuration of multiple security devices in the various segments of your network, as discussed above. Your UTM solution should offer a single management console for policy provisioning and configuration revision control. Furthermore, given the dynamic nature of the threatscape, you need real-time, site-wide visibility into security events and system events through the central console, integrated with the reporting feature. Finally, to avoid piling up the management burden on a few key staff, insist on role-based administration to give you granular control over administration.

Unified Logging, Reporting & Analysis

Policy management requires powerful reporting capabilities that can integrate events from multiple devices and technologies, as well as deliver network capacity and utilization data to help your team plan and manage your network efficiently. You'll need both scheduled and on-demand reports, and to help you avoid re-inventing the wheel, your vendor should supply a large number of standard reports based on their customers' experience, while permitting you to customize them to your particular needs. To get the most out of the integration offered by a UTM solutions, look for capabilities such as event correlation, forensic analysis, and vulnerability scanning. And, of course, close integration with the management console!

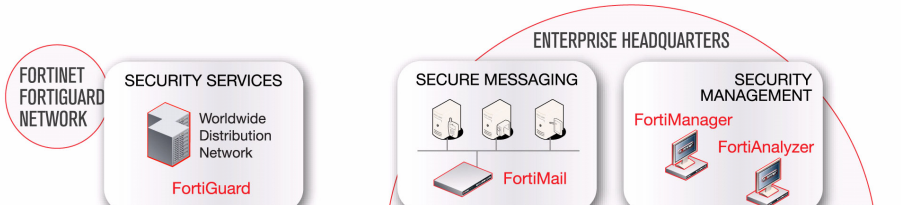
Unified Threat Research

Finally, keep in mind that many of the technologies in a UTM solution rely on timely updates of profiles, signatures, URLs, and other threat information to enable you to keep up with rapidly-evolving threats. But automated update alone isn't enough. Your UTM vendor should be willing to give you an update SLA, hopefully one measured in hours, not days. Threat response time is critical! These updates should be backed by an extensive library, global threat research teams (the wider the net, the sooner new threats are likely to be discovered), and 24/7 operation. Finally, look also for threat feedback mechanisms so that your experience rapidly becomes part of the solution.

Summary

Unified security solutions offer IT executives concerned with network security a way to integrate multiple new security technologies into their network infrastructure without multiplying management touchpoints. These solutions include not only Unified Threat Management network appliances, but in some cases dedicated email security appliances and end-point protection, along with timely and complete global threat research to keep the protection up to date. Above all, such a solution must offer unified management and reporting consoles to pull it all together—as without these, the solution cannot deliver the promised reduction in operating expenses demanded of every part of the IT department. A security gap analysis is the first step in choosing the right UTM solution and integrating it with your existing security investments.

In short your network should be comprehensively and uniformly protected with an end to end UTM solution, as depicted in the figure below, that empowers you with the flexibility to protect various parts of your networks and with the corresponding secuirty features that make sense for your environment.



About the Author

Freddy Mangum is Vice President of Product Marketing and brings to Fortinet more than 13 years of product 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 unified threat management, or UTM, 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, VPN, spyware prevention and antispam—designed to help customers protect against network and content level 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 in six programs by ICSA Labs: (Firewall, Antivirus, IPSec, SSL, Network IPS, and Antispyware). 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

WPR135-1007-R1