

Comprehensive Protection for Email and Web

The World's Most Critical Business Applications

White
Paper



High Performance Multi-Threat Security Solutions

FORTINET™

Introduction

Email and the web have revolutionized business communications, providing an unmatched blend of reach, scalability, timeliness, efficiency and overall effectiveness. Together they are the most prominent and arguably the most critical business applications in the world. It is imperative, therefore, that they be protected in a comprehensive manner.

However, establishing specifically what “comprehensive protection” entails and effectively and efficiently implementing the associated countermeasures can be far from straightforward. Complicating matters is the fact that high penetration and usage rates have led to email and web technologies being very attractive targets for intrusions and all types of malware. The result is a diverse, overlapping and ever-expanding array of threats. Everything from conventional file-infecting viruses, mass-mailing worms, spam, and denial-of-service attacks to increasingly elaborate and aggressive phishing techniques and blended threats needs to be addressed – and on a continuous basis to boot.

Accordingly, the intent of this paper is to take a closer look at the scope and nature of web and email related threats confronting organizations today. Associated findings will then be used as the basis to define an ideal approach to email and web protection – one that provides comprehensive coverage while simultaneously exhibiting high degrees of efficiency and overall effectiveness

Threats and Challenges Associated with Email and the Web

Ask an executive or line-of-business manager which application, email or the web, their organization is willing to do without. The answer – if one is ever provided – will inevitably be preceded by a prolonged bout of hair pulling, hand wringing, and other acts of anxious indecision. Ask an IT manager the same question, and the response is just as likely to highlight that both applications are a headache to operate and maintain. In light of the challenges that they present, particularly in terms of information security, such a sentiment is certainly understandable.

Of course, gaining further insight into the threats and challenges that are applicable to web and email applications is an essential prerequisite to coming up with a solution that effectively alleviates them. Fortunately this can be accomplished by examining related issues along three distinct dimensions: what is being threatened, how it is being threatened, and where it is being threatened.

A Matter of Perspective

Most discussions of the information security threats that pertain to an organization include a caution to consider “both” directions of flow. This is certainly intuitive for communications that occur within a given computing environment. Though, based on the many-to-many nature of internal connections, it is probably more accurate to refer to “all” directions of flow. The point, however, which is typically made in the context of Internet boundary connections, is that not only are there threats associated with traffic that is headed inbound to an organization, but also ones associated with traffic that is headed outbound. Conventional viruses and worms are examples of the former, while the latter includes items such as communications from keylogger trojans, attempts to access offensive websites, and email messages that contain confidential information.

Considering this directional aspect of the threats to an organization is definitely a valid perspective. However, another useful approach for classifying threats is based on identifying what specifically the threat is targeting. This is particularly relevant for web and email traffic since a substantial percentage of the associated threats are not actually focused on harming these applications or their associated systems. Instead, they are often intended to compromise or disrupt a completely different set of services and systems, or, more likely, to operate in a completely indiscriminate manner. The point is that they are just taking advantage of web and email applications as a means of conveyance.

With this alternative approach then, the fundamental question comes down to whether countermeasures need to be put in place to provide protection from X, or whether they are needed instead to provide protection for X (where X is a given resource – in this case web or email).

As already alluded to, the ‘from X’ scenario involves threats that are merely being conveyed by related traffic. This is typically the case for most viruses, worms, and other forms of malware. Indeed, the popularity of this mode of attack is derived from two, exceedingly threat-friendly characteristics. First, hitching a ride is far from complicated. It can be as simple as creating a new email message, or staging executable code behind an attractive/normal-sounding URL. And the second characteristic is that all such rides essentially include a “free pass”. This is based on the fact that from an access control standpoint, web and email traffic is practically always “allowed.”

In contrast, the ‘for X’ scenario involves providing protection for threats that are intended to compromise or otherwise directly abuse the subject resource and its associated components/systems. First and foremost this means addressing those threats which can jeopardize the integrity or availability of web and email services. After all, the relative criticality of these applications has fostered an expectation that just like with the conventional phone network; web and email “tone” will always be present. Representative threats in this case are typically initiated by unauthorized parties and include generic denial of service attacks, as well as specially crafted targeted attacks (e.g., a threat that is designed to exploit newly discovered buffer overflow vulnerability in a common email application).

However, it is also necessary to account for a slightly more subtle aspect of the ‘for X’ scenario. Specifically, another relevant sub-category of these threats involves both intentional and unintentional misuse of applicable resources by authorized parties. These will be discussed further in the following section but for now are noted to include users accessing or distributing inappropriate content, as well as actions that result in the exposure of sensitive or confidential information.

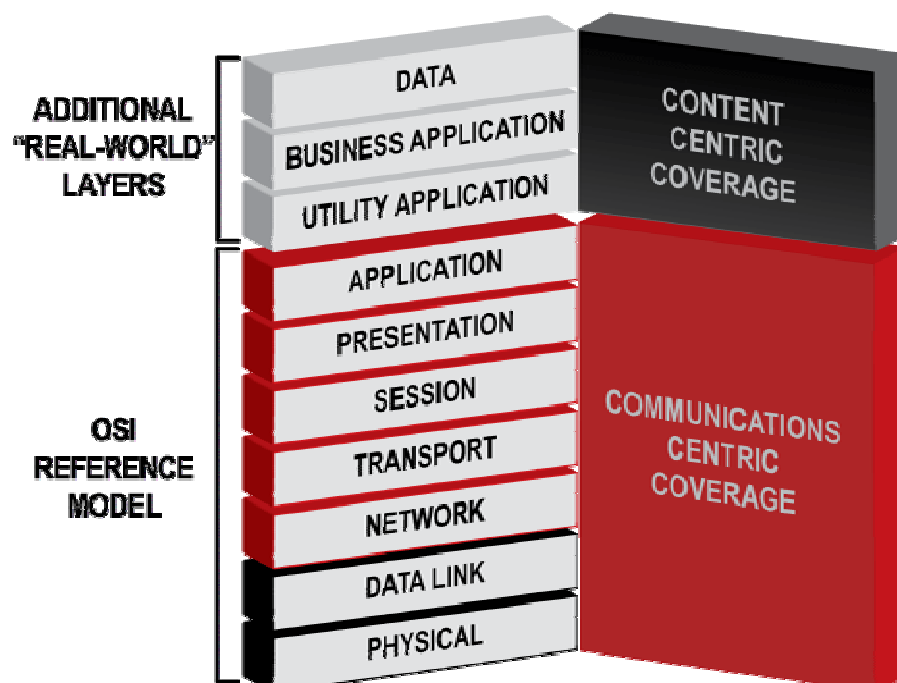
A Matter of Layers

The second dimension that it makes sense to explore to gain a better appreciation for the full scope and nature of web and email related threats pertains to how they operate. The distinguishing characteristic in this case is the layer of the computing stack that is being exploited, or targeted.

Unfortunately, there is considerable confusion and even misrepresentation in the security industry when it comes to the definition of the applicable layers. Particularly bothersome is abuse of the qualifier “application layer” (as in application-layer threat, application-layer attack, or application-layer security solution).

In this regard, it is important to realize that the Open Systems Internetworking (OSI) 7-layer model is actually intended to describe a modular approach for communications between networked end users (*see Figure 1*). It is fundamentally a *network* communications model and therefore has very little to do with actual applications (e.g., a web browser, email, SAP) – other than in terms of conveying their content and commands as payload. Even the unfortunately named “application layer”, where protocols such as SMTP (for email) and HTTP (for web) reside, is really just about providing services to ensure that higher-order applications can communicate across all types of environments.

Figure 1: The OSI Reference Model and Beyond



In other words, while the OSI application layer is indeed distinct from the network and transport layers, they are all focused on *network* communications. Consequently, there are still higher layers that will require protection as well. For instance, threats could be focused on compromising: the code/commands of various utility applications (e.g., browsers, web servers, databases), the code/logic of pre-packaged or custom-built business applications (e.g., Word, SAP), or even individual data elements (e.g., personal health information, SSNs).

Thus, a more accurate and helpful way to divide the problem/solution space is to consider: communications oriented threats/countermeasures (i.e., those pertinent to OSI layers 1-7) and content oriented threats/countermeasures (i.e., those associated with executable programs, documents with executable content or individual data elements).

Perhaps even more helpful in this context however are Figures 2 and 3. These are the product of jointly considering the first two dimensions as they apply to each application, web and email. The result is a framework that provides a comprehensive summary of the threats that are applicable in each case. That said it is important to acknowledge that these frameworks are imperfect tools. The boundaries and placement of threats within them is reflective of the majority of conditions in today's computing environment. But by no means does it account for all of the perturbations and combinations that are ultimately possible.

A Matter of Locations

The final dimension that requires consideration pertains to location. This does not involve any new threats or threat characteristics, per se. Instead it acknowledges the associated challenge of having to provide protection in multiple, physical locations for all those threats that have already been identified. This is due to a number of factors, including: the distributed nature of modern enterprises, the steadily growing implementation of mobility technologies, and the need for organizations to support a wide variety of both remote and local connections by guest, partners, service providers, and other types of users, and even systems. The result is the need to implement multiple lines of defense, not only on Internet connections at headquarters locations, but also within the local/internal network, at branch offices, and on individual hosts.

Figure 2: Threats and Challenges Pertaining to Email Traffic

	Protection From	Protection For
Content-centric	<ul style="list-style-type: none"> • spam • phishing • viruses, etc 	<ul style="list-style-type: none"> • data leakage • inappropriate use • legal issues
Communications-centric	<ul style="list-style-type: none"> • targeted attacks 	<ul style="list-style-type: none"> • targeted attacks • dos/ddos

Descriptions, clarifications, and related discussion:

- Spam, or excessive, unsolicited email is a threat that saps user productivity and wastefully devours bandwidth and email system capacity/resources.
- Phishing, a close relative to spam, is an email-based social engineering attack focused on obtaining sensitive/personal information that can be used to execute fraudulent transactions.

- Viruses, etc. covers the full range of malware (i.e., malicious software) that, at least historically, has been conveyed predominately via email (e.g., viruses, worms, trojans). It also includes so-called blended threats. These blur the lines between traditional threat definitions by combining multiple transmission, penetration, and/or propagation methods – including the use of both web and email communication services – in a single threat package. Indeed, rising prevalence and increased elusiveness of such threats highlights the need for organizations to implement “blended defenses”.
- Targeted attacks most often involve exploitation of communication protocols and services to compromise systems that rely on them (e.g., a client node, or an email server). Though it is not illustrated, such attacks can also be executed at the content level (e.g., by exploiting a vulnerability in the email application itself).
- Denial-of-service attacks primarily involve misuse of communication services to flood a target system with bogus connections. In addition, excessive spam could technically be classified as a content-oriented denial-of-service attack.
- Data leakage involves privacy violations and loss of competitive advantage due to exposure of sensitive or otherwise confidential information via misdirected and/or plain-text email.
- Inappropriate use involves excessive use of email for non-business purposes.
- Legal issues primarily involve instances of inappropriate usage for which an enterprise could be held liable (e.g., distribution of offensive or malicious content). However, being non-compliant with regulatory requirements, such as those which require maintaining records of all communications, could be considered a tangentially related threat as well.

Figure 3: Threats and Challenges Pertaining to Web Traffic

	Threats From	Threats To
Content-centric	<ul style="list-style-type: none"> • spyware • viruses, etc 	<ul style="list-style-type: none"> • data leakage • inappropriate use • legal issues
Communications-centric	<ul style="list-style-type: none"> • targeted attacks 	<ul style="list-style-type: none"> • targeted attacks • dos/ddos

Descriptions, clarifications, and related discussion.

- Spyware could easily be deemed a sub-category of malware, though not all of it is strictly malicious in nature (e.g., adware). It is also kept separate from the more general classification to highlight: (a) that it is focused on obtaining and relaying private information to unauthorized parties (e.g., keylogger trojans), and (b) that it does not self-replicate and, therefore, is primarily spread/contracted by visiting infected web sites.
- Viruses, etc refers to all forms of malware as described in Figure 2, except that in this case web protocols, in particular http, are the vehicle used for transmission. In fact, use of web-based techniques is on the rise (e.g., where spam is used to distribute links to infected web sites), since they improve the likelihood of malware overcoming anti-virus engines, the majority of which are focused on scrubbing email traffic.
- Targeted attacks – the associated description from Figure 2 is applicable here as well. Of particular note in this case, though, are attacks against transactional web applications that exploit vulnerabilities and a lack of thorough input validation predominately at layer 7/8 (SQL injection, cross-site scripting).
- Inappropriate use and legal issues arise primarily from users accessing non-business related sites, especially those which publish offensive or even illegal content. Also problematic are the various collaboration and messaging services, such as instant

messaging and peer-to-peer file sharing. These can be tunneled in standard web protocols, and consequently introduce a significant potential for data leakage.

Comprehensive Protection

It should be clear by now that providing comprehensive protection relative to web and email services requires implementing sufficient countermeasures to address the full range of applicable threats. However, recognizing the need for multi-layer security is only a starting point. Additional items that must still be addressed include:

- Identification of other characteristics that are instrumental to the overall efficiency and effectiveness of a given solution, and
- Identification of which specific countermeasures should be deployed where.

Critical Characteristics of a Pragmatic Security Solution

Beyond multi-layer security, there are three other foundational characteristics that distinguish an ideal security solution. High performance is necessary to ensure that even under conditions of heavy load associated web and email traffic can be fully inspected in a timely manner. Flexibility covers the need for associated countermeasures to remain highly effective over time, as well as the ability to address a wide range of deployment scenarios. And, finally, having low total cost of ownership is primarily about fostering increased levels of operational efficiency, and secondarily about achieving extensive coverage without having to make extensive capital investments.

Concrete examples of features and capabilities that embody these characteristics include: turn-key subscription services, the “power to perform”, and unified management.

Turn-key subscription services are an essential component of a comprehensive web and email security solution. Combining extensive research efforts and a robust distribution network, they are the means by which the various anti-malware and content filtering/control engines are continuously provisioned with the real-time information (e.g., attack definitions, URLs) necessary to counter newly emerging threats.

The power to perform entails the ability to process a suitable volume of communications traffic through the full suite of security services without incurring an unreasonable amount of latency. For network-based components of the defense scheme this depends on having purpose-built appliances that feature pre-hardened, pre-tuned operating systems and superior levels of processing power, memory and I/O capacity. It also requires support for a wide range of reliability features, including redundant components, interfaces for backup connections, high availability (active/passive and active/active), and stateful failover. After all, the amount of available processing power is irrelevant if the system is not kept up and running in the first place.

Unified management is also a multi-faceted concept. In this case, operational efforts and costs are minimized and effectiveness is maximized by (a) being able to remotely manage multiple instances of a given countermeasure at the same time, and (b) being able to do so for all of the applicable countermeasures with a minimum number of separate management applications – which ideally means a single, integrated management system.

The final component necessary to achieve comprehensive protection for web and email applications is an understanding of which specific countermeasures should be deployed where. In this regard, it is recommended that organizations embrace a three-pronged defense scheme – one that is based on locating selected countermeasures at the network perimeter, directly in front of core web and email systems, and, finally, on individual client and server hosts.

A First Line of Defense: The Network Perimeter

As the primary conduit and a natural chokepoint for communications traffic entering and exiting enterprise networks, the Internet gateway is a logical location for organizations to begin establishing their defenses, both for and from web and email applications.

Because this is the first line of defense, the goal should be to provide broad-spectrum coverage for the applicable threats. Ideally, this means implementing, at a minimum:

- Antivirus, anti-spyware, anti-spam, IM/P2P control, and web/URL filtering engines to counteract content-oriented threats, and

- Firewall and intrusion prevention capabilities to counteract communications-oriented threats.

The importance of having the full set of countermeasures cannot be over-stated. Complementary, ideally integrated, capabilities are essential to being able to stop the rising tide of blended and compound threats. For instance, a common practice is for hackers to lure users to sites hosting malware (e.g., keylogger trojans) by getting them to click on corresponding links in deceptively worded email messages. In this case a cocktail of anti-spam, web/URL filtering, and anti-spyware provides the greatest assurance of avoiding an infection. Another relevant example is covered in the sidebar “Preventing Access to MySpace with Web Filtering and IPS”

Of course, implementing all of these point product countermeasures in a single location can lead to considerable cost and complexity. In this regard, suitably provisioned multi-layered security appliances offer an attractive alternative to deploying a corresponding collection of point products – at least to the extent that associated bandwidth and performance requirements can be met.

Conveniently, they are also well suited for use in branch offices. These locations require comprehensive protection as well to help keep threats introduced in them from spreading to other sites. This is particularly relevant given rising levels of user/guest mobility and the growing trend for organizations to provision distributed offices with direct access to the Internet (as opposed to continuing the inefficient and costly practice of backhauling all Internet-borne traffic through a central facility).

A Second Line of Defense: The Client Perimeter

User mobility is also the primary driver for the second component of the recommended three-pronged defense strategy: comprehensive client-based protection. First and foremost this means securing those users and devices that operate remotely and which can, therefore, connect directly to the Internet without the benefit of the organization’s extensive perimeter defenses.

Not surprisingly, mobile users are essentially exposed to the same threats that are encountered at an organization’s Internet gateway. As a result, achieving comprehensive coverage entails provisioning all data-enabled mobile devices (e.g., laptops, PDAs, smartphones) with an equivalent set of protective mechanisms. Specifically, the minimum set of countermeasures required includes antivirus, anti-spyware, a personal firewall, and a VPN client to facilitate encrypted connections to centrally hosted resources/applications. Additional, extended capabilities that should also be considered include the following:

- Antispam;
- Web/URL filtering (ideally in the form of a network-based service);
- Personal (i.e., host) intrusion detection/prevention; and,
- File/disk encryption (assuming it is not available as a native feature of the associated operating system).

Yet another point that deserves attention is the fact that remote devices are not the only ones put at risk as a result of user mobility. Guests and returning mobile users alike have the potential to introduce threats directly on the corporate LAN, thereby circumventing the Internet/network boundary controls that serve as the primary means of defense for all internal, end-user computing stations. Consequently, it makes sense to deploy at least a subset of the aforementioned countermeasures for these devices as well.

A Third Line of Defense: The Application Perimeter

Needless to say, application servers, such as an email server, also require protection from both internally and externally launched threats. Applicable countermeasures include general hardening of the associated operating system, maintaining patch levels for all enabled services and applications, and possibly implementing host-based intrusion prevention software.

Preventing Access to MySpace with Web Filtering and IPS

The challenge that many educational institutions are having controlling access to MySpace further demonstrates the benefit of having a multi-layered security platform. Unfortunately, it appears that many stand-alone web/URL filtering products are unable to effectively counteract certain “features” of MySpace, such as the ability to shuffle its address across two Class C allotments, or the presence of numerous related sites that can act as proxies to it. In contrast, solutions that incorporate complementary firewall, intrusion prevention, and anti-malware capabilities can (a) often overcome these and other similar challenges by enabling creation of custom access rules and detection signatures, and (b) in the event that users still manage to get through to such a site, provide protection from any threats or infections that may be present there.

However, equally important is the need to supplement these and other broad-spectrum safeguards with ones that provide even greater levels of protection, or performance, specifically for the organization's most critical applications. Typically this will involve deploying dedicated, application-specific security appliances that logically "front end" the systems hosting the applications in question.

For email, such a solution should incorporate the following minimum set of capabilities:

- Antivirus and anti-spyware, in particular to address high volume, high performance scenarios as well as other designs where these services are not already accounted for at the network perimeter;
- Antispam that ideally includes additional, advanced techniques beyond those commonly found in most UTM devices;
- Intelligent message routing, to support flexible QoS policies and compliance-related archiving requirements;
- Robust defenses to address denial-of-service attacks, directory harvest attacks, and a wide range of other types of targeted attacks; and
- The ability to implement and enforce custom policies pertaining to message content.

For web, the corresponding solution is a web application firewall. The goal in this case is to further protect transactional web applications, primarily from both general and targeted attacks focused on the upper four layers of the computing stack (see Figure 1).

Summary

The tightly coupled characteristics of widespread adoption and criticality to the business result in email and web applications creating a two-headed security challenge for practically every IT organization in the world. Comprehensive protection must be provided to counter both threats for these applications (e.g., a denial-of-service attack) as well as ones that come from them (e.g., spyware). Furthermore, accounting for factors such as the increasing mobility of users and the distributed nature of organizations, requires that associated countermeasures be implemented at multiple physical locations.

To efficiently and effectively tackle this complex set of requirements a solution must deliver multi-layer security while simultaneously emphasizing features that lead to high levels of performance and flexibility and low total cost ownership. In addition, to provide complete coverage of web and email threats, it should incorporate the following:

- A comprehensive, integrated set of both communications and content oriented countermeasures (e.g., firewall, intrusion prevention, antivirus, anti-spam, anti-spyware, web content filtering, and IM/P2P control) at the network perimeter of both headquarter and branch office locations – ideally in the form of a family of multi-layered security appliances that account for a range of performance and capacity requirements;
- A similarly comprehensive set of countermeasures in the form of software that is suitable for deployment on both fixed and mobile endpoints (e.g., desktops, laptops, and smart phones);
- Application-specific security gateways that provide advanced and customizable protection mechanisms for core systems hosting web and email applications; and
- Turn-key subscription services to efficiently keep up with the rapidly changing threat landscape.

In summary, today's web and email applications require a pragmatic security approach, ideally comprising a turn-key platform with security subscription services, unified management, the power to perform, and the ability to be deployed at various locations in the network to ensure a comprehensively secure and reliable IT infrastructure.

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 antispyware--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 antispymware). Fortinet is privately held and based in Sunnyvale, California.

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.

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 WPR131-1206-R1