Microsoft® Forefront™ Security for Exchange Server

Microsoft® Forefront™ Security for SharePoint®

Malware Protection: Planning the Right Technology Mix

Paul Robichaux

3Sharp LLC

Published: January 2007

Abstract

Microsoft's security product offerings include a range of anti-virus technologies, including self-hosted products such as Microsoft® Forefront™ Security for Exchange Server and Microsoft® Forefront™ Security for SharePoint®, that administrators install on their servers, and hosted services such as the Exchange Hosted Services Filtering service. The optimal mix of internal self-hosted and external hosted security services will vary from company to company, according to the messaging environment and business requirements. This paper discusses some of the factors involved in balancing these alternatives.

Microsoft®

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2007 Microsoft Corporation. All rights reserved.

Microsoft, Forefront, Active Directory, Antigen, Excel, SharePoint, Windows, Windows Server System, and the Windows Server System logo are either registered trademarks or trademarks of Microsoft Corporation or Sybari Software, Inc. in the United States and/or other countries. Sybari Software, Inc. is a subsidiary of Microsoft Corporation.

All other trademarks are property of their respective owners.

Contents

Contents 3

Forefront Security for Exchange and SharePoint 1

Deploying Defense in Depth 3

Client-Side Security Solutions 3

Server-Based Security Solutions 3

Appliance Security Solutions 4

Hosted Security Solutions 4

Choosing the Optimal Technology Mix 5

Understanding Message Flow 5

Perimeter Security 6

Perimeter Security with Forefront Security for Exchange Server 6

Perimeter Security with Exchange Hosted Services 7

Server Security 8

Server Security with Forefront Security for Exchange Server and Forefront Security for SharePoint 9

Client-Side Protection 10

Conclusion 11

Related Links 12

Forefront Security for Exchange and SharePoint

Microsoft has been progressively building a complete communications and collaboration platform, responding to the market demand for well-integrated communications and collaboration systems that replace individual point solutions. Microsoft's strategy in this space is to build a set of unified communications and collaboration solutions that provide easy access to a wide range of work modes—Instant Messaging (IM), e-mail, calendar, team workspaces, document libraries—all using a familiar set of tools that let people work without disruption from the desktop or on the go. These solutions are based on, and take advantage of, infrastructure services like Microsoft® Active Directory® directory service and the Microsoft® Windows® operating system Rights Management Services.

For these services and capabilities to be truly useful in business, they must be properly secured. Each of these product families includes a wide range of security features, including encryption, authentication, and auditing. However, building an effective communications and collaboration system depends on protection of the system itself *and* the data it contains. Over the last two years, Microsoft has been steadily adding data-centric security functionality, beefing up the message security capabilities of Microsoft® Exchange 2007, adding built-in support for Windows Rights Management Services into Microsoft® SharePoint® Server 2007, and purchasing several security companies whose products fill gaps in Microsoft's own offerings. Microsoft's overall security strategy is to provide end-to-end security for business customers, beginning with the operating system and extending through network access to applications and services hosted on Windows servers. This end-to-end protection strategy is a broad vision that will take some time to execute.

The Microsoft® Forefront™ server security products are a major part of Microsoft's commitment to realizing this vision by providing integrated security and management services for Microsoft's communications and collaboration services. Microsoft acquired the proven and mature Antigen line of anti-virus products, and then updated them to provide better protection for Microsoft's communications and collaboration solutions. Microsoft® Forefront™ Security for Exchange Server and Microsoft® Forefront™ Security for SharePoint® help provide advanced protection for the valuable data transmitted and stored in mailboxes, document libraries, and team sites. These products integrate with existing Microsoft management tools, simplifying deployment and administration.

The Forefront server security products provide several key security capabilities to Exchange and SharePoint customers, including the ability to create file-filtering policies that apply across messaging and collaboration tools and an advanced multiple engine manager that allows you to concurrently run up to 5 of the included Microsoft and third-party anti-malware engines. Using multiple scan engines delivers several critical advantages:

- It increases the chances that emerging threats will be quickly caught.
- It provides redundancy to help protect against scan failures or defects in individual engines; if an engine fails, other engines continue scanning messages.
- It gives administrators an effective way to choose the most appropriate level of protection for their environment given their security needs and server performance capabilities.
- It allows engines to be taken offline for updates or reconfiguration without forcing messages to be queued.

A recent set of tests performed by the independent AV-Test.org group found some surprising differences in signature update times from various vendors. The tests compared AV lab response times for eighty-two “in the wild” viruses and variants that appeared from April to July 2006. Twenty-six of the viruses were quickly detected by all the scan engines, but some engines didn’t detect viruses for more than twenty-four hours. In a few cases (notably 0506 Banwarum.C@mm), some vendors didn’t update their signatures to provide a block until nearly five days had elapsed! Because Forefront Security for Exchange Server and Forefront Security for SharePoint combine multiple engines, the odds that a virus will go unblocked or undetected for long periods are greatly reduced. Organizations benefit from all updates for the set of engines you use, not just from updates to a single engine.

Signature Response Times in Hours								
MM/YY Virus	Forefront Set 1	Forefront Set 2	Forefront Set 3	Forefront Set 4	Forefront Set 5	Vendor 1	Vendor 2	Vendor 3
0406 Mytob.NQ@mm	1.53	1.00	1.00	1.00	3.07	9.93	17.35	2.10
0406 Mytob.NQ@mm	1.00	1.12	1.00	1.00	1.00	28.07	11.57	3.52
0406 Spybot!04C2	23.03	1.00	23.03	25.28	1.00	0.00	29.90	39.02
0406 Nugache.a	1.00	25.45	1.00	1.00	1.00	34.10	12.90	48.05
0506 Numuen.F	0.00	24.43	0.00	0.00	0.00	1.00	10.33	14.95
0506 Numuen.H	1.00	31.72	1.00	1.00	1.00	103.83	251.85	114.78
0506 Numuen.G	3.15	8.20	3.15	3.15	3.15	1.00	151.80	468.97
0506 Banwarum.C@mm	87.47	1.00	87.47	87.47	1.00	116.73	72.95	129.25
0506 Banwarum.B@mm	12.05	1.00	1.82	1.82	1.00	116.73	22.45	32.85
0506 Rbot!E905	0.00	0.00	0.00	0.00	0.00	1,141.78	217.57	1.00
0606 Bagle.EG	0.00	0.00	0.00	0.00	0.00	0.00	7.32	0.00
0606 Bagle.EH@mm	0.00	1.25	0.00	0.00	0.00	0.00	18.43	0.00
0606 Bagle.EG@mm	0.00	3.62	0.00	0.00	1.00	0.00	26.48	0.00
0606 Bagle.LY@mm	0.00	0.00	0.00	0.00	0.00	0.00	6.40	2.47
0706 Feebs.gen@mm	0.00	0.00	0.00	0.00	0.00	0.00	0.00	503.80
0706 Feebs.EU	0.00	1.00	0.00	0.00	0.00	52.30	173.17	38.97
0706 Virut.A	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1,317.02

Less than 5 Hours | 5 to 24 Hours | More than 24 Hours

Figure 1: AV-Test.org signature file response times

Multiple engines also provide a practical way to implement the security principle of defense in depth. The Forefront Multiple Engine Manager helps ensure that each engine is regularly updated, and that when an engine is being updated, other engines continue to process messages and files. This behavior helps maintain consistent performance while still providing excellent security.

The additional protection offered by multiple engines comes at a small performance cost. In benchmark tests performed by 3Sharp, LLC in October 2006 using Forefront Security for Exchange Server, we found that increasing the number of scan engines assigned to a transport scan job added between 1% and 4% to CPU loads per engine—meaning that using a 5-engine scan can add as little as 5% to the transport server’s CPU usage.

Deploying Defense in Depth

Defense in depth is a time-tested security principle. Maintaining multiple layers of security is one of the most effective ways to protect your information assets and systems. Windows Server provides a number of defensive layers on its own: strong authentication and authorization services, a centralized directory, a robust security policy infrastructure, and a mature and certified set of cryptographic services. Exchange Server and SharePoint Server add their own technology-specific defensive layers that focus on specific security requirements and threats in their respective product areas. However, most organizations will want to add extra protection by deploying technologies that focus on blocking malware and enforcing content policies. These products typically fall into four categories:

- Client-based solutions run on desktop, laptop, and mobile clients to protect the information stored on, and the integrity of, those clients.
- Server-based solutions run on messaging, collaboration, or file servers. They may also run on dedicated servers whose function it is to monitor inbound or outbound traffic.
- Appliance-based solutions provide filtering and content control in dedicated devices that sit at the organization's network perimeter.
- Hosted security solutions provide filtering and content control of inbound content before it reaches an organization's server.

Each of these solutions offers distinct advantages, which is why most organizations adopt a combination of these technologies to fortify their defensive capabilities.

Client-Side Security Solutions

Client-side security solutions have a long and illustrious history. Until collaboration and communication systems became interconnected enough to spread malware, the primary vector for malware infection was the individual computer. Client-based antivirus programs quickly became a major industry. However, the client world has changed significantly in the last few years; for example, the once-ubiquitous floppy drive is now rare. The risks related to clients have changed in two ways:

- The biggest potential risk associated with the client is no longer infection of the local client; it's a compromise of the client that leads to infection or compromise of other systems.
- The potential attack vectors have changed from infected floppy disks or executables to Trojans, rootkits, and other malware whose true nature is camouflaged, and which are often spread through peer-to-peer sharing, compromised internet sites, or other indirect methods.

The combination of these changes means that client-based protection is still relevant. Server-based and hosted protection help defend against threats that enter a protected network from the outside. Server-based protection also helps guard against internal threats. However, clients still need protection against threats that are directly accessible to (or even invited onto) the client.

Server-Based Security Solutions

Server-based anti-malware solutions also have a long history, and they too have changed significantly. Before the widespread deployment of collaboration and communications solutions, most organizations

used ordinary file-based antivirus scanners on their file servers. As e-mail systems became more common, so did e-mail-aware scanners that could intelligently examine the contents of messages both as they arrived and after they had been delivered to a user's mailbox. Server-based products typically cover both of these areas. Transport scanning checks for infected messages entering and leaving the system, while mailbox scanning checks messages that have already been delivered against the latest signature definitions to catch infected messages that were previously missed.

Server-based solutions offer a high degree of control. Administrators can choose the schedule used to perform scans and signature updates and the degree of strictness of the scans. They can also choose where to deploy scanners, using whatever combination of perimeter scanning and mailbox or transport server scanning makes the most sense. Server-based solutions offer a degree of protection against internal outbreaks, too, by catching infections that spread from legitimate clients on the network.

However, server-based solutions by their nature interact with messaging and collaboration software, meaning that administrators have one more system component to configure and manage. Poorly written server-based solutions may lower the reliability and availability of the software they are supposed to protect.

Appliance Security Solutions

Security solutions that depend on special-purpose appliances are growing in popularity. These solutions provide security services in a single-function device that typically operates as a perimeter filter. The exact combination of features varies from vendor to vendor, but appliances usually include anti-spam and anti-malware functionality, often using generic or open-source tools driven by a customized Web interface. Appliance solutions are useful in environments that want low-overhead security solutions that don't require adding servers or installing software on additional servers. However, appliance costs can approach the cost of perimeter servers in many cases. Appliances are often less flexible than server-based solutions, and they still require messages to be delivered to the organization perimeter for processing. Some vendors price their appliances on a per-user or per-year subscription model, which may reduce their cost advantages.

Hosted Security Solutions

Hosted content filtering solutions are growing in popularity because they promise to reduce both the management overhead of server-based solutions and the amount of resources consumed by spam filtering and virus scanning.

By filtering and cleaning all inbound mail at the hosting provider before it touches any of a company's servers, these services offer substantial reductions in the number of messages that have be accepted, processed, and delivered by the company, and they can significantly lower the risk of a virus or malware infection caused by incoming infected messages. Web-based user interfaces provide per-user quarantine and release functionality, relieving administrators from having to inspect and clear organization-wide quarantines. In addition, many hosting services offer other features, including spam filtering and content or policy controls, as part of their services.

Hosted solutions require a degree of trust, and this is a compliance/policy consideration in some cases. Many organizations have policies that prohibit routing mail through third parties, and most organizations want a high degree of visibility and control over what happens to inbound mail. Hosted solutions do not protect against infections directly on the client or in internal mail—they only scan mail entering the organization, and thus do not keep attacks from spreading internally.

Choosing the Optimal Technology Mix

Effective defense-in-depth against malware requires a combination of technologies, but choosing the right mix can be tricky. Finding the right balance requires an understanding of the tradeoffs involved in each type of technology and knowing how it applies to individual business requirements. Microsoft offers client, server-based and hosted solutions that allow you to build protection into your infrastructure while taking full advantage of the features of both the Windows Server infrastructure and the communications and collaboration functionality your business needs.

Understanding Message Flow

Figure 2 shows an example organization using Exchange 2007 and SharePoint Server 2007 for messaging and collaboration. The organization sends mail to, and receives mail from, Internet hosts. Examining how messages travel in this environment helps illustrate which protection types are useful in which circumstances.

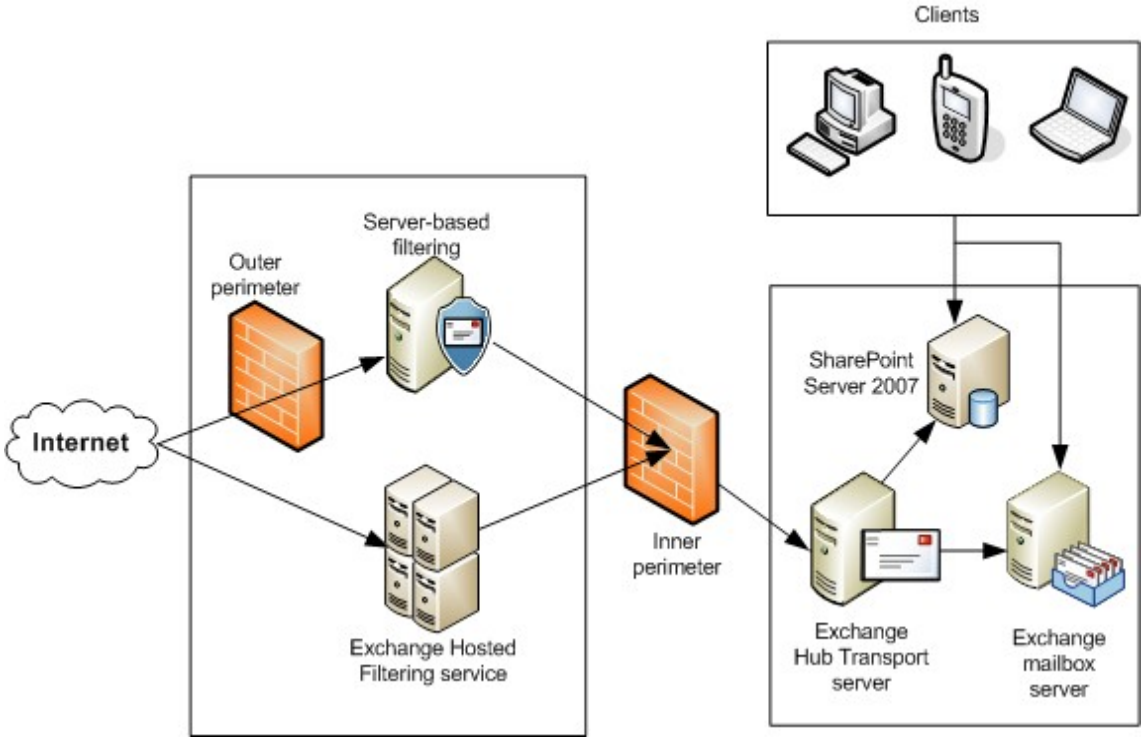

Figure 2: An example Exchange organization

There are several places where a message or file may be inspected and filtered in this environment:

- Inbound messages that arrive from the Internet must transit either the Exchange Edge Server filtering mechanism or the hosted filtering service
- Messages not filtered at the perimeter must transit the Exchange Hub Transport server for delivery; the Hub Transport server will direct the messages to the appropriate Exchange mailbox or external recipient (e.g. a mail-enabled SharePoint document library)

- Messages arriving at the mailbox server or SharePoint server may be inspected on arrival; they may also be scanned at a later time
- Messages sent from one client to another are submitted to the Exchange mailbox server, then sent to the Exchange Hub Transport server for delivery

Let's examine each of these touch points to see what actions are taken.

Perimeter Security

Perimeter security is a crucial first line of defense against malware threats. Every infected object you block at the perimeter is one less object to store and process, and one less object that can pose a potential threat to your information systems. However, perimeter systems do not protect internal servers against threats that originate inside the perimeter, as when a compromised laptop is reconnected to the corporate network or a user submits an infected file to a file share or document library. For that reason, perimeter security must be coupled with server-based protection.

At the network perimeter, both the Forefront Security for Exchange Server scan process and the Exchange Hosted Filtering service accept the inbound message and perform a number of content checks. The first question is simple: *Where did the message come from*, *and what information does the server have about the sender and recipient?* To answer this question, the filtering agent can evaluate the sender's IP address to see whether it's on any real-time block lists; it can also examine the purported sender information using the Sender ID protocol. Safe senders and blocked senders and recipients are used to bias the message rating up or down as part of this process.

These checks actually occur during two separate stages: some filtering can be performed during the SMTP conversation, before the message is accepted for delivery. The remaining checks are performed after sending a "250 OK" to the remote server but before allowing the message to be delivered. These checks include the following:

- *Is there anything unusual about the message*? Is the message's MIME structure correct? Are the message headers (including the sender and recipient fields) correct and complete? A malformed message, or one with incomplete header information, should be treated as suspicious.
- *What's in the message*? After the message is accepted, the content filtering engine will examine the message body and attachment. Malware scanning is a key part of this phase. In addition, the checks in this phase include examining attached files for compliance with any attachment policies (for example, blocking executable files by both file type and extension or disallowing encrypted ZIP files), as well as inspecting nested ZIP files.

Perimeter Security with Forefront Security for Exchange Server

Forefront Security for Exchange Server provides both perimeter-based and server-based filtering. As a perimeter filter, Forefront Security for Exchange Server offers some key advantages:

- Forefront Security for Exchange Server product licenses include support for 64-bit Exchange 2007, as well as providing versions of Antigen that offer protection for previous versions of Exchange.

- You can choose up to five concurrent scanning engines to scan messages in transit; this allows you to fine-tune the level of protection you get by adjusting the mix of engines and their individual settings.
- Forefront Security for Exchange Server provides multi-process scanning, allowing multiple e-mail streams to be scanned simultaneously, providing faster scanning and better protection with fewer delays.
- Forefront Server Security products include configuration and management features that allow you to consistently manage settings across multiple servers in an organization; this helps ensure that all your transport servers are consistently protected.
- Forefront Security for Exchange Server transport scanning works on both Exchange 2007 Hub Transport and Edge Transport servers. Once a message is scanned, it is stamped with a property that exempts it from further scanning. This increases performance while allowing you to decentralize scanning functions where it makes sense to do so—at all times ensuring that *all* messages are checked before delivery to mailboxes.

You should consider using Forefront Security for Exchange as a perimeter protection solution when:

- You need maximum protection against malware threats.
- You want to be able to scan incoming traffic with more than one scan engine to provide redundancy.
- You want complete control over how, when, and where message filtering and scanning take place.
- You want to be able to scan outbound mail to ensure that its content meets your organizational policies and that it's free of malware.

Perimeter Security with Exchange Hosted Services

The Exchange Hosted Filtering service builds on the successful FrontBridge product line (which Microsoft acquired in 2005) to effectively remove unwanted content—including malware, phishing, and spam—before it ever reaches your network. Exchange Hosted Filtering complements Forefront Server Security by providing filtering with a combination of a subset of Forefront's supported anti-virus engines plus engines from Trend and Symantec. Exchange Hosted Filtering also offers powerful spam filtering and an easy-to-use Web-based interface that allows administrators to set up per-user spam quarantines and to manage filtering for their entire organization from almost any Web browser. Because Exchange Hosted Filtering acts as a store-and-forward service, it can also increase the reliability of your mail system by queuing mail during temporary service interruptions at your site.

You should consider using Exchange Hosted Filtering when:

- You want to combine anti-virus, anti-phishing, and anti-spam filtering to screen messages before they reach your network edge.
- You want to deploy hosted encryption or hosted archiving services.
- You want filtering without changing the configuration of, or installing software on, your Exchange servers.

- You want additional redundancy in mail routing; Exchange Hosted Services can store mail for protected domains during outages, then deliver it when the domain's servers become available again.
- You need additional spam and content filtering features not included in Exchange, like per-user quarantines and detailed reporting of filtering actions and results.
- Your organization allows mail routing through third parties.

Microsoft customers who purchase the Exchange Enterprise Client Access License (CAL) get rights to use Forefront Security for Exchange Server *and* Exchange Hosted Filtering, offering a terrific balance of security and administrative flexibility.

Server Security

Server security involves three distinct phases:

- Scanning a message during transport
- Scanning a message on or after arrival in a user's mailbox
- Scanning items submitted to, or retrieved from, a SharePoint document library

Transport scanning requires the server to inspect each message to determine whether it's been scanned before; Forefront Security for Exchange Server and Forefront Security for SharePoint add a message property that indicates if a message was scanned. If the message has been previously scanned by a current version of the signatures and engines in use, it doesn't have to be scanned again on arrival at the mailbox server. If, however, it has not been previously scanned, Forefront will scan it and add the appropriate stamp before the message is delivered to the mailbox store.

Mailbox server scanning allows messages that have already been scanned at the perimeter or during transport to be rescanned because a signature update has occurred. The Exchange anti-virus API (AVAPI) supports two types of mailbox server scans: on-access scans that cause a previously unscanned message to be scanned when it's opened and background scans that allow re-scans of messages with the latest signature definitions.

When a user submits an infected message to the store for delivery, the scan engine will be able to catch it when it's submitted to the sender's Sent Items folder. In addition, because Exchange 2007 uses a Hub Transport server for all message transit operations (including between users on the same server), the transport scanning process can catch messages submitted to mailbox servers that don't have an active scanning process.

Scanning items submitted to a SharePoint document library takes the same general form as scanning items submitted to a mailbox server store: new items are checked for the presence of malware, and to help ensure that they comply with the organization's security policy. For example, your security policy might prohibit the storage of MP3 and WMV files; the SharePoint scanner would prevent documents of these types from being submitted to the SharePoint document library. If the item passes these checks, it continues through the normal SharePoint submission process, and the document is stored in the document library.

Server Security with Forefront Security for Exchange Server and Forefront Security for SharePoint

Forefront Security for Exchange Server and Forefront Security for SharePoint are two of Microsoft's server-based solutions for malware filtering and content control. With the release of the new Forefront server security products Microsoft has updated the mature technology of the Antigen product line to take full advantage of improvements in Exchange 2007 and SharePoint Server 2007, while still providing the innovative features that made Antigen so effective. Chief among these is support in Forefront Security for Exchange Server and Forefront Security for SharePoint for multiple scan engines, which provides broader coverage against emerging threats. Forefront server security products offer a number of advantages:

- Because there are Forefront server security releases for Exchange and SharePoint, you get strong protection across your entire collaboration and communications infrastructure.
- Forefront server security product licenses take advantage of the 64-bit support of Exchange 2007 and SharePoint Server 2007, as well as providing versions of Antigen that offer protection for previous versions of Exchange and SharePoint.
- Forefront server security products use multi-process scanning, allowing multiple e-mail streams or SharePoint documents to be scanned simultaneously, providing faster scanning and better protection with fewer delays.
- Forefront server security products include configuration features that allow you to consistently manage settings across multiple servers in an organization.
- You can vary the mix of scanning engines used for Exchange transport, Exchange mailbox, and SharePoint scanning to give you appropriate coverage across your entire infrastructure.
- Forefront Security for Exchange Server offers both transport scanning (for monitoring messages as they move between servers) and mailbox server scanning (for messages that have already arrived). You can use transport scanning on Exchange 2007 Edge Transport and Hub Transport servers.
- Forefront Security for SharePoint scans Office documents for content to help avoid distribution of confidential or offensive materials.
- Forefront Security for SharePoint can allow or block document library submissions based on file type or extension, adding an extra layer of policy control to keep unwanted content types like MP3 files or video clips out of document repositories.
- Forefront Security for SharePoint takes advantage of the SharePoint Server 2007 support for Windows Rights Management, allowing you to scan and apply policy to messages even when they're protected by Windows Rights Management Services.

Forefront server security products are designed to work well with Exchange and SharePoint, taking full advantage of their features, and are thoroughly tested to ensure compatibility and performance. You should consider using the Forefront server security products when:

- You need maximum protection against malware threats.
- You need effective protection against malware from internal sources to complement your perimeter protection.

- You want complete control over how, when, and where message filtering and scanning take place.
- You need both mailbox and transport scanning.
- You want to control and filter content checked in to SharePoint document libraries.

Customers who license Forefront Security for Exchange Server to protect Microsoft Exchange 2007 will also be licensed to use Antigen for Exchange to protect Exchange 2000 and Exchange 2003. Customers who purchase Forefront Security for SharePoint to protect Microsoft Office SharePoint Server 2007 or Microsoft Windows SharePoint Services version 3.0 will also be licensed to use Antigen for SharePoint to protect Microsoft SharePoint Portal Server 2003 and Microsoft Windows SharePoint Services 2.0 environments.

Client-Side Protection

No matter what kind of upstream anti-malware protection you use, you should strongly consider using client-based software as part of your overall protection strategy. Why?

- You may have machines that touch your network but aren't fully protected by security updates, patches, or good user practices. Examples include unsecure home machines that are used to connect to the corporate network and machines running legacy line-of-business applications on older versions of the Windows operating system.
- Server-based and hosted solutions can't protect against attacks that take place directly on the client (as when a user downloads an infected program from a peer-to-peer service or from a compromised Web site). These attacks can nonetheless affect your network if a compromised machine is able to spread the infection to other machines

Adding client protection helps defend your servers against external and internal threats. Server-based and hosted solutions help protect server data, but you still need protection against worms or other malware that may attack the operating system or applications on your communications and collaboration servers. When deciding which solutions to deploy on your clients, you should consider the following factors:

- *Centralized management capability*. In order to get adequate protection across your organization, every client machine must use consistent security settings to help eliminate islands of vulnerability. If users have the ability to change security settings, some of them will do so, so centralized policy controls and reporting are important to help prevent and identify unauthorized changes to client security software.
- *Flexibility*. Clients face a somewhat different set of threats than servers because users generally have the ability to browse Web sites, download programs, and engage in other potentially threatening activities. It's important to deploy client protection solutions that offer both protection against known malware and against suspicious behavior of programs or Web sites.

Conclusion

Microsoft's security product line includes both self-hosted products that run on your servers as well as hosted services that you can subscribe to. Both of these product types have their place in securing communications and collaboration systems. The Forefront server-based products offer strong protection with multiple anti-virus scanning engines, plus versions for protecting Exchange 2000/2003 and Exchange 2007 and SharePoint. Exchange Hosted Filtering delivers powerful hosted filtering that helps clean your message stream before it ever reaches your servers. The Exchange Enterprise CAL allows you to combine both of these filtering types in a single license if that's appropriate for your organization. Together these products offer industry-leading protection for, and control of, your incoming message stream, enabling you to effectively protect the information resources your company needs.

Related Links

For the latest information about Microsoft Forefront Security products, see the Microsoft Forefront Web site http://www.microsoft.com/forefront/default.mspx