Shields Up! Getting Better Protection with Microsoft Forefront Security for Exchange Server and Microsoft Forefront Security for SharePoint

Paul Robichaux
3Sharp LLC
Published: October 2006

Abstract

Microsoft has expanded its security strategy by adding products and technologies that address the most pressing needs of IT management and administration. The Microsoft Forefront line of security products includes anti-virus and content filtering tools for Microsoft Exchange Server and SharePoint products and technologies. Through tight integration with Exchange and SharePoint, Microsoft® Forefront™ Security for Exchange Server and Microsoft® Forefront™ Security for SharePoint® offer a number of valuable benefits, including improved manageability, performance, and security. This paper describes these benefits at a high level.

Microsoft

Contents

Communications, Collaboration, and Security

Companies of all sizes are moving away from a focus on individual products or point solutions that deliver specific services like e-mail, instant messaging, or document management. Instead, driven by competitive pressures that place a high premium on effective, timely communication and collaboration, they're choosing solutions based on how well different collaboration and communications products and protocols work together. Microsoft has been investing heavily in its collaboration and communications solution line, which contains three major components that are interesting from a security standpoint.

Exchange Server is Microsoft's messaging and calendaring platform. Exchange is both the most mature and the most widely deployed of Microsoft's collaboration and communication products. It acts as the key repository for voice mail, e-mail, and fax messages, calendar and free/busy data, and contact information, and it makes that data accessible through desktop, Web-based, and mobile clients.

SharePoint products and technologies include Microsoft Office SharePoint Server 2007, Windows® SharePoint Services, and SharePoint Portal Server 2003. Microsoft intends SharePoint to be a central document and information repository, combining rich metadata, searching of both SharePoint repositories and other data sources (including Lotus Domino databases, Web content, and file shares), workflow, and electronic content management.

Live Communications Server complements SharePoint and Exchange by offering real-time communications, including text, voice, and video instant messaging, application and desktop sharing, web conferencing, and extended presence information. These capabilities are available from the desktop via the Windows Messenger and Office Communicator clients, the Communicator Web Access Web-based client, Communicator Mobile for Windows Mobile, and APIs that allow presence and IM capability to be built into SharePoint team sites and document libraries, as well as applications in the Office family.

Microsoft's strategy in this space is to build a complete set of unified collaboration and communications solutions that provide easy access to a wide range of work modes—instant messaging, e-mail, calendaring, 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 Active Directory and Windows 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 steadily been adding data-centric security functionality, beefing up the message security capabilities of Exchange 2007, adding built-in support for Windows Rights Management Services into Microsoft Office 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 metaphor is a broad vision that will take some time to execute; the recently launched Forefront product line is a major part of Microsoft's commitment to realizing this vision by providing solid security and management services for its collaboration and

communications services. Forefront Security for Exchange Server, Forefront Security for SharePoint, and Microsoft® Forefront™ Security for Office Communications Server[1] 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, so they're easy to learn, use, and deploy. These Forefront products are new iterations of the proven and mature Sybari Antigen products that Microsoft acquired in 2005.

[1] Microsoft plans to have this product available in the second half of calendar year 2007.

Defending Your Communications and Collaboration Infrastructure

The first step in mounting an effective defense of your collaboration and communications infrastructure is to use the security tools that the platform provides. For example, Windows Server supports authentication, authorization, confidentiality protection, and security update management mechanisms that allow you to effectively secure the underlying network, workstations, and servers. Active Directory adds a robust authentication mechanism that allows you to effectively segregate critical systems and apply different levels of security policy to them; Exchange and SharePoint both include additional security mechanisms that, when properly used, help maintain security at the server level. These measures are necessary prerequisites that help protect the organization's data, but many organizations want a higher degree of protection that safeguards their critical resource by protecting against a wider variety of threats.

The Threat Landscape

The security landscape is continually changing; attackers are always seeking new vulnerabilities in software systems and networks. Many common threats of the past, like denial-of-service attacks based on fragmented TCP packets, have largely been mitigated. The emergence and deployment of security capabilities like network access protection and smartcard authentication have helped to deliver more secure network access, and Microsoft's sustained efforts to deliver "trustworthy computing" are bearing fruit by reducing the number and severity of vulnerabilities in their products.

However, attackers haven't been sitting still. Attacks based on malware—loosely defined as viruses, worms, Trojans, and spyware—are continuing to grow in both frequency and severity. Malware has become easier to catch but harder to get rid of; a growing number of rootkits, once installed, can effectively disguise themselves from most major anti-malware tools The attackers themselves have changed; in the past, it was common to see viruses or worms developed by interested amateurs, but today's attacks are often conducted by professionals who either target individual organizations or compromise groups of computers and sell access to them. There are other motivations, too; an increasing number of attacks are being undertaken for information gathering, industrial or political espionage, or ideological motivations.

Specific Threats against Exchange and Outlook

Microsoft has steadily improved the security of Exchange Server and its premier client, Outlook. The current versions, Outlook 2007 and Exchange 2007, incorporate both design decisions and features that reflect Microsoft's increased focus on security and the actual security problems faced by users and administrators of previous versions. However, Exchange has to accept mail from the outside world, and Outlook is used to store and process it. Because many attacks are spread via e-mail messages, it's important to protect Exchange and Outlook with appropriate security services. These services include:

- Scanning messages for unwanted or malicious content before the messages enter the organization's messaging system. This keeps unwanted content out of the organization's network altogether. This scanning can be performed by bastion scanning servers like the Edge Transport role of Exchange 2007 or hosted services like Microsoft Exchange Hosted Filtering.
- Scanning messages in transit from the entry gateway to the mailbox server. Edge scanning protects against malicious content that originates outside the organization, but it may not

adequately filter content generated inside the organization (as when an employee uses a compromised home computer to connect via VPN to a corporate network), and it may not filter content coming from ostensibly trusted sources like business partners or trusted suppliers.

- Scanning messages that are already in, or are submitted to, user mailboxes. At first look, this may seem redundant if transit and edge scanning are both in place. However, an infected client may send infected messages to a previously clean store, and one infected client within an organization can quickly spread the infection across the organization. Scanning existing mailbox content helps proactively protect servers and services by catching these infections before they get out of hand. As detection tools and signatures get better, it's possible to find and clean infected messages that may have been missed during previous scans.

According to the 2006 computer security study jointly conducted by the US Federal Bureau of Investigation and the Computer Security Institute, nearly 97% of the organizations surveyed had anti-virus and firewall protection in place, yet 65% experienced virus infections. This is a disturbing statistic, since it indicates clearly that conventional anti-virus solutions aren't adequately protecting messaging systems.

Threats Specific to SharePoint

SharePoint provides a rich set of tools for storing, managing, indexing, and finding documents, task and calendar data, and social networking information. The chief threats to SharePoint-based environments all revolve around attacks against, or infection of, the documents and data stored in SharePoint repositories; an infected document that's stored in a library may be kept for years, exposing any user who downloads it to re-infection. Microsoft Office SharePoint Server 2007 adds the ability to e-mail-enable SharePoint repositories so that users can submit items to a document library or list by sending e-mail to a specified e-mail address.

These threats may seem to pose a minor risk by comparison to the risks inherent in accepting e-mail from the Internet. However, the growing use of SharePoint as a key component in extranets that extend business functionality to users outside the corporate network raises the risk that an untrusted machine, or an actively malicious user, can pollute a SharePoint collection with infected documents. As SharePoint servers increasingly replace conventional file servers, protecting them against malware becomes more and more important, especially since the conventional file-based solutions used to protect file servers can't scan SharePoint document collections.

An additional SharePoint concern revolves around compliance. Because Microsoft Office SharePoint Server 2007 includes electronic content management (ECM) and retention tools, as organizations adopt these tools they must be especially careful of what content they allow into their libraries because that library content may live on for a long time. To maintain appropriate regulatory compliance, it's important to make sure that security and content management policies are consistently applied across the organization; for example, if a particular content type is blocked from e-mail systems, it should probably also be blocked from SharePoint and instant messaging, and vice versa..

Meeting the Threat: How Forefront Server Security Helps

Microsoft has designed the Forefront Security product line to deliver some specific benefits: better protection against current and future threats: improved availability and performance; and simplified management.

Comprehensive Protection

Sybari's Antigen antivirus technology for Exchange was widely regarded as technically innovative because it linked advanced protective features like multiple engine support to unique methods of accessing messages in transit and in the mailbox store. Forefront Security continues to deliver Antigen's support for multiple engines, which provides better coverage against emerging threats and more flexibility for administrators; the Forefront line also takes full advantage of the interfaces that Microsoft built into Exchange and SharePoint for antivirus scanning. For example, Forefront Security for Exchange can take advantage of the new transport scanning interfaces included in Exchange 2007 to efficiently scan messages on Edge and Hub Transport server roles. Messages scanned by Forefront for Exchange in transport mode are stamped with a flag that indicates to other Forefront scan services in the organization that the message has already been scanned; this helps optimize performance by eliminating duplicate scans. For example, a message that's scanned on an Edge Transport server need not be rescanned when it's delivered to a user's mailbox server, and a message that transits several Hub Transport servers will only be scanned on the first hop.

Forefront Security for SharePoint fully supports Microsoft's virus scanning API (VSAPI) for SharePoint 2007. This helps protect both the contents on the SharePoint server and the integrity of the document library; conventional file-based scanners that depend on scanning files on disk may cause problems with SharePoint logs and queues. Forefront Security for SharePoint can also block file types according to their contents, type, size, or extension, providing an effective way to enforce organizational policies about what kinds of content can be stored in SharePoint. These policies can be applied even if the file extension is incorrect.

Forefront Security for Exchange runs on Exchange 2007 servers; it includes Microsoft Antigen for Exchange, which you can run on your Exchange 2000 and Exchange 2003 servers. This approach gives you maximum protection on all of your Exchange servers, taking advantage of the new security features built into Exchange 2007 while still delivering Antigen's advanced protection for older versions of Exchange.

Optimized Performance

Forefront Security includes an engine manager that monitors each engine's processes and automatically restarts them when necessary; in addition, scanning behavior can be monitored with Microsoft Operations Manager or other Windows-aware monitoring tools. This reduces the risk that an engine failure will leave the organization unprotected. Because messages are flagged as they're scanned, if one server fails to perform a scan, the message will still be scanned at the next hop when that server detects that the message hasn't been scanned yet.

The full line of Forefront Server Security products provide performance bias controls that give administrators control over which scan engines run and how they use system resources. This provides an effective way for administrators to tailor the speed and frequency of scanning to their security needs and the performance of their underlying servers.

Forefront Security for Exchange is cluster-aware, so it can be used on clustered Exchange mailbox servers[2]. This extends the security protection that Forefront Security for Exchange offers by ensuring that it will remain available during failover and failback operations.

[2] Forefront Security for Exchange Server runs on Exchange 2007 mailbox clusters; Microsoft Antigen for Exchange runs on Exchange 2003 and Exchange 2000 clusters.

Forefront Security for SharePoint supports both 32- and 64-bit versions of Windows Server; this provides flexibility in scaling your SharePoint deployment without giving up protection. Forefront Security for SharePoint is designed to take advantage of Microsoft Office SharePoint Server 2007; it includes Antigen for SharePoint to help protect older versions of SharePoint and the data they contain.

Layered Defenses

Providing defense in depth is a time-honored principle of both military strategy and computer security. Having multiple defensive layers reduces the risk of a successful attack by forcing an attacker to breach more than one, and it helps eliminate single points of failure. Sybari introduced the concept of running multiple scan engines in parallel in its Antigen product over five years ago, and Microsoft has extended it by providing a set of up to eight engines (from Authentium, CA, Kaspersky Labs, Norman Data Defense, Microsoft, Sophos, and VirusBuster) to choose from, with up to five engines in concurrent use.

Using multiple engines has some important benefits: it significantly helps reduces the risk that an infected message or file will slip through because to do so, it must defeat more than one scanning technology and signature update. It also helps reduce the risk that a software defect or failure in a single engine will allow an infection to occur. Multiple engine support is a key part of the Forefront Security for Exchange Server and Forefront Security for SharePoint advantage, because it supports the use of multiple scan engines without adding management overhead or administrative hassle.

Because you can choose to run any combination of engines on any or all protected servers, you can choose the appropriate balance between the additional protection that comes from using more than one engine against the performance requirements of each server role. In addition, most major antivirus firms are generating signature file updates more often and distributing them more frequently. Because most scanners have to stop scanning to load new signature updates, using a single engine may introduce a window of time during which messages are delayed because the engine is updating itself. Paradoxically, the more often the vendor ships signature updates the bigger this window may get! Forefront's engine manager addresses this problem by allowing engine updates to proceed while the remaining engines continue scanning.

Forefront Server Security also provides defense in depth by allowing you to run it against messages in transport and messages stored in SharePoint libraries or Exchange mailboxes. The combination of in-memory scanning, transport scanning, and scanning of stored items provides a flexible approach to content protection, giving you the freedom to tailor scan behavior to your requirements.

Consistent Application of Security Policies

One major challenge of security management is ensuring that security policies are consistently applied across the organization. Forefront Security for SharePoint and Forefront Security for Exchange Server address this problem by providing a flexible configuration mechanism that allows you to define a protection configuration and automatically apply it to multiple servers. This helps ensure that policy settings for filtering, engine management, and scan behavior are consistently applied, helping reduce management cost and increasing security.

Forefront Security for SharePoint includes filtering controls that allow keyword and file type-based exclusion of files. These controls supplement SharePoint's existing policy controls because they protect files in a variety of formats, including Office XML documents and documents protected by Windows Rights Management Services. Additionally, both Forefront Security for SharePoint and Forefront Security for Exchange Server include tools for rejecting messages that contain certain types of files; this

helps reduce the risk of unwanted content (like MP3 files) entering and being stored in corporate systems.

Conclusion

Protecting your communications and collaboration infrastructure requires a layered approach. It's necessary to supplement the infrastructure protection features built into Windows Server, Exchange Server, and SharePoint with additional security to help protect the data they contain and the servers themselves. Forefront Security for Exchange Server and Forefront Security for SharePoint provide an excellent combination of features that deliver extremely powerful security protection, improved performance and availability, and reduced management costs.

Related Links

- For more information on Forefront Security for Exchange Server and Forefront Security for SharePoint, visit www.microsoft.com/forefront
- For in-depth information on computer security, including the latest updates, best practices, and tips for IT professionals and businesses, visit www.microsoft.com/security.
- For more information on Microsoft Exchange products and technologies, visit www.microsoft.com/exchange
- For more information on Microsoft SharePoint products and technologies, visit www.microsoft.com/sharepoint

For the latest information about Microsoft Windows Server System™, see the Windows Server System Web site at http://www.microsoft.com/windowsserversystem.