

Technical White Paper



Microsoft® IT
Showcase

Deploying Forefront Client Security at Microsoft

Technical White Paper

Published: June 2008. Updated March 2009.

Microsoft

CONTENTS

Executive Summary	3
Introduction	5
Earlier Client Antivirus Solution	7
Opportunities with Forefront Client Security.....	9
Solution Planning and Design.....	11
Topology	11
Infrastructure Integration	13
Server Design	14
Storage Design	15
Pilot Deployment	16
Planning	16
Schedule	18
Process	18
Operations	22
Benefits	24
Next Steps for Microsoft IT.....	25
Lessons Learned.....	26
Best Practices.....	29
Conclusion.....	30
For More Information	31

Situation

Microsoft IT needed a new anti-malware solution that offered top-rated malware detection and removal, unified protection against all types of malware, and centralized management. The solution needed to offer immediate, comprehensive reporting, and support policy development and distribution in the heterogeneous Microsoft corporate network.

Solution

Microsoft Forefront Client Security delivered on these needs on an enterprise scale. Forefront Client Security also used existing IT infrastructure for its management.

Benefits

- Top-tier malware detection and removal scanning engine
- Unified protection against all types of virus and spyware technologies
- Centralized management console for at-a-glance reporting and drill-down problem resolution

Products & Technologies

- Microsoft Forefront Client Security
- Microsoft SQL Server 2005
- Microsoft Operations Manager 2005
- Microsoft Systems Management Server 2003
- Windows Server Update Services

EXECUTIVE SUMMARY

The Microsoft Information Technology (Microsoft IT) group needed an antivirus solution to adequately address the growing threat from the many types of Internet-borne malicious software, also known as malware. When Microsoft IT assessed its requirements for an enterprise anti-malware solution, the group realized the challenge of the ever-changing landscape of client security. Centralized management, rapid reporting, and a positive user experience for clients were some features that Microsoft IT sought in a client security solution.

A product group within Microsoft consulted with the security staff of Microsoft IT for the initial development of a new anti-malware solution, Microsoft® Forefront™ Client Security. As the new product emerged, Microsoft IT volunteered to test it, first in a lab environment, and then in an enterprise production environment.

Microsoft IT developed and tested a server management group for administering the new system. Testing revealed that the server choices more than sufficed, but they required more advanced storage. For this reason, the server management group attached to a storage area network (SAN) for use by data collection and reporting services.

Lab testing was successful, so Microsoft IT rolled out the solution into a production environment in a limited-participant pilot. The initial pilot was successful, and soon 10,000 participants were using the product. The ability to quickly see reports on the security status of all participating clients quickly facilitated executive queries. Moreover, a centralized console simplified client management. If a report on the console alerted Microsoft IT security staff to a misconfiguration that exposed a vulnerability or a possible malware infection, the team could easily resolve the issue. The team could quickly move through console reports and remotely correct the misconfiguration. Or, the team could initiate an anti-malware scan on the client computer without involving the end user.

Microsoft IT worked with the Forefront Client Security product development team to expand the pilot to 50,000 worldwide users. Microsoft IT also integrated the management server group services used by Forefront Client Security into the existing network infrastructure wherever possible.

This white paper shares architecture, design, and deployment considerations. This paper briefly discusses the advantages of advanced Forefront Client Security features. The paper also describes how Microsoft implemented the Forefront Client Security solution in its environment.

This paper assumes that readers are technical decision makers and are already familiar with the following:

- Anti-malware security technologies
- Microsoft server products such as Microsoft SQL Server® 2005 database software, Microsoft Operations Manager 2005, and Microsoft Systems Management Server (SMS) 2003
- Windows Server® technologies such as Windows Server Update Services (WSUS)

IT groups can employ many of the principles and techniques described in this paper to manage risk in their organizations. Similarly, the design considerations for anti-malware security infrastructure can be applied to most enterprise-scale IT environments that use

Microsoft products. However, this paper is based on the experience of Microsoft IT and its recommendations as an early adopter. It is not intended to serve as a procedural guide. Each enterprise environment has unique circumstances. Therefore, each organization should adapt the plans and lessons learned described in this paper to meet its specific needs.

Note: *For security reasons, the sample names of domains, internal resources, organizations, and internally developed security file names that are used in this paper do not represent real resource names that are used within Microsoft and are for illustration only.*

INTRODUCTION

Malware infections, spyware, viruses, Trojan horses, worms, and similar threats remain a costly problem for businesses. Gartner has estimated that 20 to 40 percent of help-desk calls are related to spyware. For the Microsoft IT department, 20 to 40 percent of Helpdesk calls represents an annual ticket volume of approximately 200,000 to 400,000 with an associated cost of \$6 million to \$12 million U.S.

Protection from malware is mandatory for the protection of business networks and their online, connected resources. However, the issue of protecting network resources from malicious programs is not limited to using software to help secure the infrastructure against malware. The protection strategy can include aspects such as client enforcement through centrally distributed software updates and tools, statistics collecting and reporting, and advanced heuristics.

As Microsoft expanded its businesses, the corporate network added many disparate hardware components and software systems that were merged into the environment without standardization. For example, some departments used custom hardware standards, and some client systems became noncompliant with the latest security software tools. This heterogeneity makes it challenging for Microsoft IT to uniformly defend against the latest malware threats.

The Microsoft corporate network is a frequent target of attacks from various sources. Attacks vary from simple to complex and come from many attack points. Attack points include e-mail, Web browsing, file downloads, and more. Pre-attack information is difficult to detect from Internet background noise, such as measurement packets, distributed denial-of-service (DDoS) packets, and port scans. The Microsoft Security Intelligence Report for the period from July 1, 2007, through December 31, 2007, illuminates the scope of the problem:

- Malicious software has become an established tool that skilled criminals use to target millions of computer users worldwide in pursuit of profit.
- The malware detection rate has increased significantly over the past several years (from less than 5 million in the first half of 2005 to more than 40 million in the second half of 2007), both in absolute numbers and in the rate of increase.
- The Windows® Malicious Software Removal Tool ran on more than 450 million unique computers worldwide per month and removed malware from 15.8 million computers during the second half of 2007, an increase of more than 80 percent over the previous half-year reporting cycle. The number of total disinfections performed during this period rose to 42.2 million, an increase of almost 120 percent over the previous reporting period.
- During the second half of 2007, the detection and removal rate of Trojan horse downloaders and droppers, a category of malware that has emerged as a tool of choice for some attackers, increased by 300 percent.
- From July 1, 2007, through December 31, 2007, 129.5 million pieces of potentially unwanted software were detected. This resulted in 71.7 million removals. These figures represent increases of 66.7 percent in total detections and 55.4 percent in removals over the first half of 2007.
- Worldwide disinfections of potentially unwanted software are comparable to those of malware. The top 15 potentially unwanted software families displayed a 114 percent

increase over the first half of 2007, due in part to an increase in the number of users worldwide running one or more of the appropriate detection tools. Nine of the 15 families displayed increases of 100 percent or more, and five families increased by more than 200 percent.

- During the second half of 2007, the Malicious Software Removal Tool removed malware from approximately eight computers for every 1,000 times it ran. The ratio of computers scanned to those infected with malware that the tool detected and cleaned was 1:123.

Note: To review the full details of the latest Microsoft Security Intelligence Report, see <http://www.microsoft.com/security/portal/SIR.aspx>.

Windows Defender detected a great deal of malware in the first half of 2007. The viruses spread through day-to-day operations between unsuspecting users. The statistics show that malware is becoming increasingly complex. Considering that 25 pieces of malware were responsible for only 44 percent of infections, the number of individualized malware threats is growing quickly and becoming more difficult for anti-malware companies to manage.

The malware has touched a large number of computers. The Malicious Software Removal Tool detected and cleaned malware from more than 8 million computers in the first half of 2007. This number represents 38 percent of the total number of computers that the Malicious Software Removal Tool cleaned since the tool's release in 2005. The Malicious Software Removal Tool recorded an average of 2.2 disinfections per infected computer.

EARLIER CLIENT ANTIVIRUS SOLUTION

For years, Microsoft IT used a vendor's product as its client antivirus solution. The architecture of that earlier solution, as shown in Figure 1, consisted of agents on client computers that reported up to a series of data-collection servers. The solution's master servers controlled these data-collection servers.

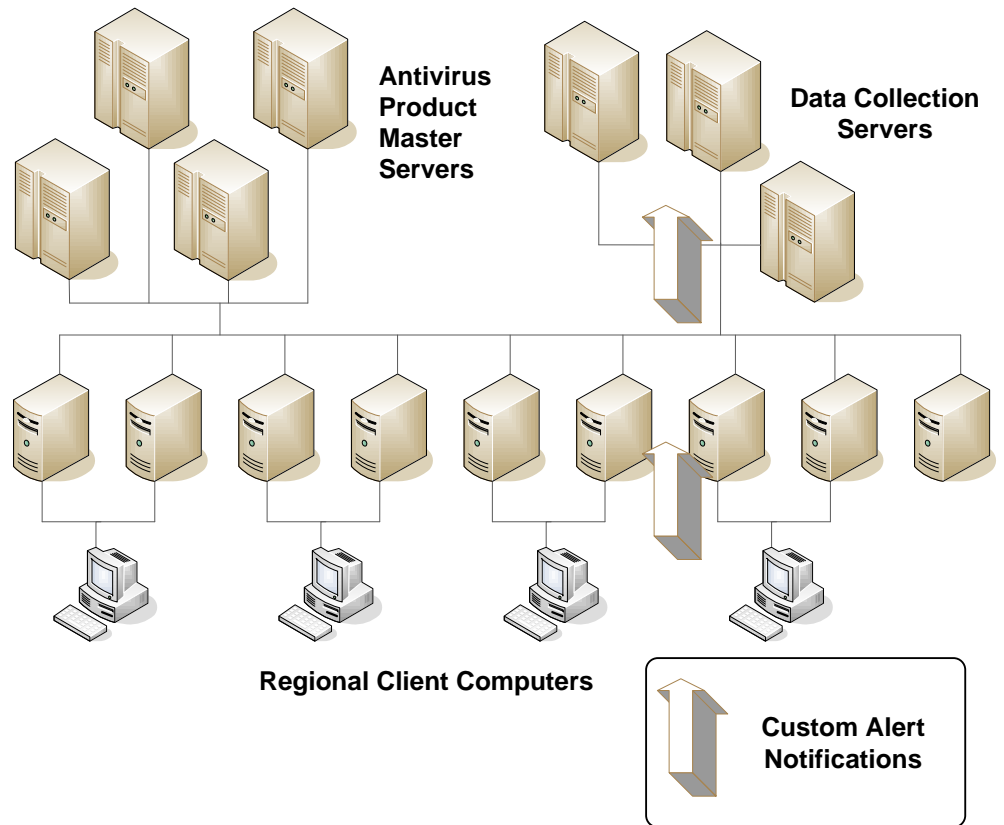


Figure 1. Hierarchy for earlier antivirus solution at Microsoft

Microsoft IT set up each solution server to support up to 25,000 users. For software distribution, Microsoft IT used its existing server architecture. It used 30 general-use distribution servers around the world as a resource for distributing the earlier solution's application and signature updates to clients.

The hierarchy went from 25,000 nodes to a central server and 30 central servers to nine aggregation servers. This all rolled up to three master servers. In the past, because of the complexity of the system and the work that was required to aggregate all the data from the three master servers into one comprehensive report, Microsoft IT employed one or more personnel to create global system security reports. Over time, Microsoft IT automated much of the work in this process. As of this writing, Microsoft IT can create weekly global security status reports in just several hours.

After many years of operating and administering the earlier solution, Microsoft IT developed the following requirements for its next antivirus solution:

-
- A comprehensive tool that would incorporate spyware, adware, and other kinds of related malware detection and removal technology. To achieve this, the earlier solution would have required a second, dedicated tool.
 - A robust virus detection rate, as rated by industry standards. This was necessary to deal with the ever-growing number of malware threats and the increasingly sophisticated stealth technologies that they employed.
 - A centrally managed solution. Microsoft IT could not easily manage the earlier solution centrally because the solution consisted mainly of a client-side software application that had no integrated IT management tools.
 - A solution that would automatically generate enterprise-wide malware detection and removal reports. For a long time, Microsoft IT used at least one dedicated engineer who had the product expertise necessary to generate the reports. Even with a degree of automation, the process of collecting the data and generating the reports was time intensive.
 - Support for the heterogeneous Microsoft IT environment. The policy-authoring tool in the earlier solution did not work in the heterogeneous Microsoft IT environment. This further complicated the management of the earlier solution for Microsoft IT.

Microsoft IT wanted more results from its anti-malware security solution, such as centralized management of the security infrastructure; at-a-glance reporting for trends, vulnerabilities, security state assessments, and remediation status; and unified protection from all kinds of malware threats. Microsoft IT wanted not only the blocking and removal of viruses, worms, and Trojan horses, but also protection from rootkits, spyware, key loggers, and more. Overall, Microsoft IT needed a new security solution that was comprehensive, effective, integrated, and simplified. It chose Forefront Client Security.

OPPORTUNITIES WITH FOREFRONT CLIENT SECURITY

Forefront Client Security is unified malware protection for business desktop computers, portable computers, and server operating systems. It is easy to manage and control, is highly effective in detecting and removing many different malware infections, and offers detailed reporting up through the enterprise. Built on the same highly successful Microsoft protection technology already used by millions of people worldwide in Windows Defender, Microsoft OneCare™ software and services, and the Malicious Software Removal Tool, Forefront Client Security helps guard against emerging threats such as spyware and rootkits, in addition to traditional threats such as viruses, worms, and Trojan horses.

By delivering simplified administration through centralized management and providing critical visibility into threats and vulnerabilities, Forefront Client Security helps protect Microsoft IT's infrastructure by giving the group greater confidence and efficiency. Forefront Client Security integrates with the existing Microsoft IT Windows Server infrastructure, such as Active Directory® Domain Services (AD DS), and complements other Microsoft security technologies for better protection and greater control. Forefront Client Security is scalable, supporting small to midsize organizations all the way up to enterprise organizations of 100,000 users.

The key benefits of the solution include the following:

- **Unified anti-malware solution for viruses and spyware** Through a single client agent, Forefront Client Security detects and removes both spyware and virus-type malware in real time by using a kernel-mode process instead of a user-mode process (meaning that it executes the scan before the suspect file is read into memory). Forefront Client Security also works in user-mode scenarios when an organization is scanning for system configuration errors, corrupted Windows Internet Explorer® add-ins, system services, drivers, and other downloads. By using the Client Security console, Microsoft IT security staff can define the schedule of both full and quick scans that occur on computers in their environment. They can even decide to launch an on-demand scan of targeted systems in the environment. Forefront Client Security offers comprehensive protection mechanisms. The scanning engine also includes additional protection mechanisms to find user mode rootkits, polymorphic viruses, and heuristic detection mechanisms that find new malware and variants.
- **Top-tier malware detection rate, removal, and clean-up** Forefront Client Security delivers top-tier malware detection rate and removal performance, along with special emphasis on the malware removal clean-up processes that leave treated computers in a ready-to-run state. Forefront Client Security helps ensure that a computer is properly functioning after the removal of malware. In comparing malware detection rates, AV-Test.org identified Forefront Client Security as a top-tier performer. For detailed results, see <http://blogs.pcmag.com/securitywatch/Results-2008q1.htm> or go to <http://www.av-test.org>.

Client security includes advanced malware protection capabilities, such as heuristics, tunneling signatures, static analysis, and code emulation. Forefront Client Security is backed by the Microsoft global security research and response system: the Microsoft Malware Protection Center (<http://www.microsoft.com/security/portal>). With facilities in several countries, the Microsoft Malware Protection Center team responds immediately to malware outbreaks around the clock, 365 days a year.

“This kind of on-demand reporting is priceless. When someone needs to know the status, the information is immediately available. Creating such reports used to take a dedicated engineer a couple of hours to a day and a half.”

Daryl Pecelj
Senior Security Strategist-Antivirus
Microsoft Corporation

- **Easy deployment and centralized management** Simplifying IT administrative tasks is a key advantage of Forefront Client Security. Forefront Client Security uses one unified console for managing all security clients on servers and end-user computers, which enables Microsoft IT to view and manage the security of the overall IT landscape at a glance. Forefront Client Security offers Microsoft IT optimized signature distribution through WSUS, by using an Update Assistant.
- **Infrastructure integration** Forefront Client Security helps Microsoft IT gain greater control over client security by integrating with existing IT infrastructure software. For example, Microsoft IT can use a Group Policy setting in AD DS, SMS, or any other software distribution system to deploy Forefront Client Security agent settings. The event logging and alerting system of Forefront Client Security is built on the award-winning technology of Microsoft Operations Manager 2005. Required Microsoft Operations Manager components are embedded into Forefront Client Security to simplify deployment and use. Forefront Client Security uses database and reporting systems from SQL Server 2005 so that it is easier to use and administer.
- **Simplified, enterprise-wide reporting** Forefront Client Security helps Microsoft IT security staff be more proactive about client security by providing critical visibility into threats and vulnerabilities through comprehensive reports and security state assessments that are easy and fast to produce. The Enterprise Management Console of Forefront Client Security helps Microsoft IT security staff prioritize their time and focus on what is most important now through easy-to-use, insightful, real-time reports.

Forefront Client Security helps administrators stay informed through security state assessment scans that run on the clients it manages and that provide “score” and “severity” values. Unique to Forefront Client Security, security state assessment scans evaluate each client according to security best practices, such as having the latest security updates installed for operating systems. This capability helps Microsoft IT security staff determine which computers need updates or configurations that are more secure. The security state assessment feature of Forefront Client Security can help Microsoft IT better protect the infrastructure by identifying the vulnerable computers in its environment.

The Summary Report provides the key information on security state assessment for taking action against threats, together with a snapshot of the top trends and issues in the environment. It also serves as a key launch point for other reports, enabling a quick drilldown into details. Each report is hyperlinked to enable Microsoft IT security staff to connect directly to critical information. Microsoft IT security staff can choose to have reports sent to them in e-mail on a regular basis.
- **Functional policy authoring tool** Forefront Client Security provides a simple policy-authoring tool that enables Microsoft IT security staff to create and set security policy for client computers within their infrastructure. Forefront Client Security enables Microsoft IT to author policies and set alert-level configurations in a detailed fashion, giving it flexibility not often found in similar security products for client computers. A single policy configures the Forefront Client Security antispymware, antivirus, and security state assessment technologies for one or more protected computers. Policies also include alert-level settings that can be easily configured to specify the type and volume of alerts and events that different groups of protected computers generate. Policies can be distributed through any existing software distribution system in the enterprise (Microsoft IT uses a Group Policy setting in AD DS).

SOLUTION PLANNING AND DESIGN

Microsoft IT began the process that led to solution deployment in the last quarter of 2005. From the beginning, Microsoft IT collaborated with the Forefront Client Security product group to provide input on desired features and functionality. Among other things, the Microsoft IT security team gave input for architecture, deployment, and reporting requirements. With the initial development of the product came the opportunity to verify functionality in a real-world environment by running a pilot. During the planning and design phase, Microsoft IT considered the following challenges:

- **Interoperability** Microsoft IT ran early versions of Microsoft System Center Operations Manager 2007 during the Forefront Client Security pilot. However, Forefront Client Security supports only Microsoft Operations Manager 2005. Microsoft considered how to isolate the use of the two products to minimize risks and user impact.
- **Policy settings** Forefront Client Security provides a policy configuration user interface that uses AD DS to deploy policies to Forefront Client Security clients.
- **User impact** Forefront Client Security users had to be able to function normally on the corporate network, and all internal processes and scans had to be updated. For the custom-scripted logon process for remote users, this was especially important. The earlier solution was required for remote access connections. The impact on employee productivity was a significant risk.

“Everything is a moving target for Microsoft IT,” said Paul Terry, Antivirus Security Engineer at Microsoft. “One of our biggest challenges is that during test pilot deployments, there typically is no finished product documentation to read and learn from, because the product teams usually develop their documentation sets at the same time as the software.”

Topology

The Forefront Client Security solution that Microsoft IT deployed consists of server components and an end-user client. The anti-malware service agent on the client runs as a Microsoft Forefront Client Security anti-malware service. The server side of Forefront Client Security provides simplified administration and critical visibility and control to Microsoft IT security staff through multiple server-based components organized into a management group.

Forefront Client Security offers a choice of deployment topologies for the server management groups: one-server, two-server, four-server, or six-server solutions. Microsoft IT determined that the six-server topology was cost-prohibitive for the initial pilot in terms of hardware investment for any relative gain in product performance over the four-server topology. Microsoft IT considered the two-server topology to be inadequate for the anticipated workloads. As a result, Microsoft IT opted to use a four-server topology because it offered the most efficient distribution of the workload among server roles in the new hardware investment. Figure 2 shows the server roles in the four-server management group as used in the Forefront Client Security architecture.

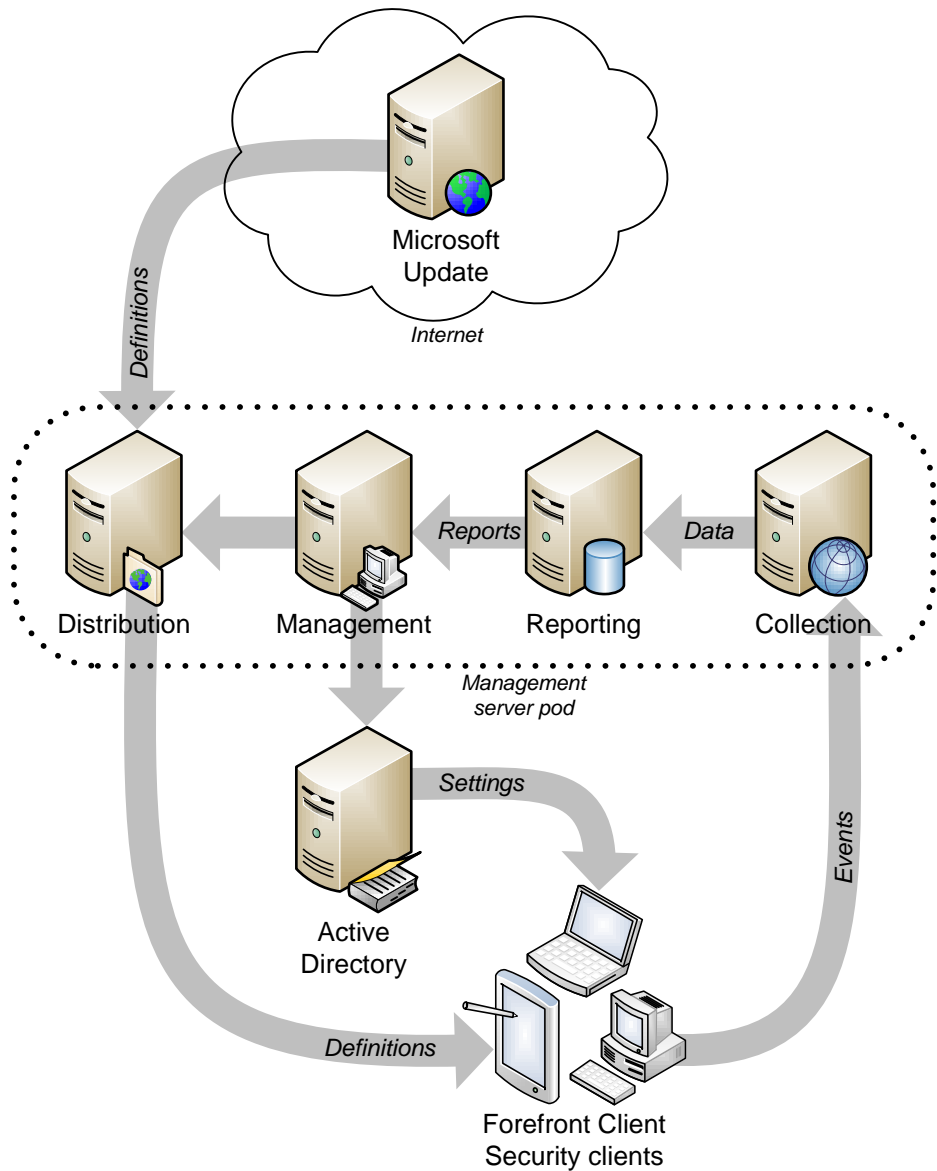


Figure 2. Forefront Client Security architecture

Forefront Client Security depends on the following server infrastructure:

- **Active Directory Domain Services** The various Forefront Client Security settings, policies, and location of signature distribution servers are all stored in AD DS.
- **Microsoft Update** This is the Internet-based service that serves as the original source for the Forefront Client Security updates to signature files.
- **Management server group** The Forefront Client Security management server group is a collection of interconnected servers that collect client security data, store it in a database, and present that aggregated data in a series of readily available reports on the health of the client systems on a management console. Each management server group that Microsoft IT deployed contains the following server roles:

- *Distribution* Manages software update distribution, such as signature files and application updates, through the use of WSUS or any existing software distribution system in the IT environment.
- *Management* Runs a central console for alerting, creating, and displaying reports, setting policies, and pushing them to client nodes. From the management console, Microsoft IT security staff can either select preconfigured settings or change client settings to tailor the solution to their environment's specific needs. Microsoft IT security staff can use the console to schedule local scans, enable or disable real-time protection, set default actions to take against specific threats, and set alerting and reporting levels.
- *Reporting and reporting database* Accesses the database of collected client data to generate reports. Forefront Client Security uses database and reporting systems from SQL Server 2005 to aggregate the data gathered by the collections server into usable reports on the management console.
- *Collection and collection database* Monitors and collects data from client agents on which to assess system security and vulnerability status. The event logging and alerting system is built on the data collected from clients via a tuned version of Microsoft Operations Manager 2005. Required Microsoft Operations Manager components are embedded into Forefront Client Security to simplify deployment and use.

Note: *To maintain compatibility with Forefront Client Security server components, Microsoft IT ran 32-bit versions of the server software.*

For the phase 1 pilot, Microsoft IT housed the management server group in the data center in Redmond, Washington. As the pilot later expanded in phase 2, Microsoft IT housed other groups in data centers around the world.

Infrastructure Integration

As an enterprise-ready product, Forefront Client Security takes advantage of components in an existing Windows Server–based IT infrastructure. When deployed in a small organization that has an unmanaged Windows Server–based IT infrastructure, Forefront Client Security can help to set up an organized, extensible managed infrastructure. Table 1 shows how Forefront Client Security uses various IT infrastructure components.

Table 1. Windows Server Infrastructure Integration

Infrastructure component	Forefront Client Security integration
Windows Server	<ul style="list-style-type: none"> • Use of Filter Manager provides a stable platform for good performance and the ability to scan for viruses and spyware in real time. • Support for Transactional NTFS provides graceful error handling and data protection and a Windows image file for imaging hard disk drives.

WSUS	<ul style="list-style-type: none"> • Use of existing WSUS servers bundled with Microsoft System Center Configuration Manager 2007 reduces overall total cost of ownership (TCO). • Microsoft IT security staff can auto-approve the latest signatures, or alternatively, test and manually approve every new update. • Deployment of signatures is automated through existing WSUS infrastructure.
AD DS	<ul style="list-style-type: none"> • Single policy configures antivirus, antispyware, and security state assessment. • Forefront Client Security console is integrated with AD DS for easy policy deployment.
Microsoft Operations Manager (embedded)	<ul style="list-style-type: none"> • Real-time alerts and reporting. • Event Flood Protection shields reporting infrastructure from infected clients during outbreaks.

Server Design

Microsoft IT knew that the product-recommended limit of 10,000 clients per management group was based on the resource limit for the Microsoft Operations Manager server performing the data collections role in the group. In testing, Microsoft IT pushed the limits of the Microsoft Operations Manager server capacity and determined that it became resource-bound at slightly more than 14,000 client nodes. Microsoft IT learned that the limit of 10,000 nodes per group was not a strict rule, nor was it at the edge of the Forefront Client Security group design capacity, considering the server hardware that the team dedicated to the role. However, to design a series of groups to exceed that limit was an unsupported configuration, and the server that Microsoft IT had available to dedicate to the role of the Microsoft Operations Manager data collector was sized appropriately for a 10,000-node limit with just enough excess capacity to buffer temporary increases in node population.

Microsoft IT designed the initial server specifications with some excess capacity for verification and growth needs. The first management server designs from Microsoft IT employed two HP DL360 servers for the distribution and management server group roles. The two servers used in the collection and reporting roles were HP DL580 servers. Table 2 shows the initial server designs that Microsoft IT selected.

Table 2. Server Specifications

Server roles	Processors	Memory	Raw storage capacity
Distribution (WSUS)	Two dual-core Xeon CPUs	4 GB RAM	Two 149-GB hard disk drives (RAID 1)
Management (console)	Two dual-core Xeon CPUs	4 GB RAM	Two 149-GB hard disk drives (RAID 1)
Collection (Microsoft Operations Manager and database)	Two quad-core Xeon CPUs	4 GB RAM	Two 149-GB hard disk drives (RAID 1), two SAN drives

Report and reporting database (SQL Server and SQL Server Reporting Services)	Two quad-core Xeon CPUs	8 GB RAM	Two hard disk drives (RAID 1), two SAN drives
--	-------------------------	----------	---

Storage Design

A key element for Microsoft IT in identifying how much storage to allocate for Forefront Client Security was to consider the impact of IT industry reporting requirements for current and future regulatory compliance issues. They needed to build an infrastructure that would support these requirements. Microsoft IT consulted with the Microsoft corporate legal department to get some guidance with these requirements, how much data to monitor, and how long the records must be preserved. All of this information played a role in determining the storage specifications that Microsoft IT needed for this solution.

Microsoft IT configured Forefront Client Security to use an alert granularity level of 3 on a scale of 1 through 5, in which 5 represents the highest number of detailed alerts and 1 represents only minimal events. The quantity of the data collected in Forefront Client Security is directly proportional to the depth of the reporting information that can be generated. Microsoft IT testing revealed that the amount of data captured with a setting of 5 results in the highest number of alerts. Microsoft IT determined that the data collection setting of 3 was the optimum balance for its reporting requirements versus data transport infrastructure and storage costs. Of course, future regulatory laws may play a significant role in determining how much data collection and retention IT organizations will require. As these laws change, the antivirus security team in Microsoft IT will monitor these developments to make sure that Microsoft stays compliant.

Microsoft IT determined that it would need to keep 12 months' worth of collected data from pilot participants. Based on that decision, Microsoft IT determined that it required 300 GB for the database on the reporting server and 110 GB for the logging database on the collection server.

Early lab testing revealed that the availability of local disk resources on these server systems started to diminish after 2,000 to 3,000 end-user client nodes were attached to the management group. After the group was populated with 10,000 client nodes, the reporting role within the group was maximized with continuous disk activity. Because of that, Microsoft IT decided to test by using higher-performance, leased SAN drives in the group. That solution worked so well that Microsoft IT maintained this architectural design change when the first pilot went out to production users. Today, both the collection and reporting servers are connected to a leased-space SAN drive in a Microsoft IT-maintained SAN storage enclosure for storing data.

The decision to use a SAN solution rather than another form of mass storage was a solution specific to the data-center standards of Microsoft IT. Configuration requirements, such as available power versus processors, cooling, limited Internet Protocol (IP) v4 addresses and subnets, and more, meant that Microsoft IT did not have the option of adding a rack array of hard disks to attach to the management group. When internal server storage proved to be inadequate to the task in terms of performance, the best remaining solution was to lease space on existing SAN enclosures in the Microsoft IT data centers. Ultimately, the hardware costs associated with setting up each group were approximately \$15,000, including the two leased SAN space drives.

PILOT DEPLOYMENT

Microsoft IT had to plan the pilot deployment of Forefront Client Security carefully to ensure a smooth migration from the previous solution. The process included uninstalling the previous solution and installing Forefront Client Security. The team was concerned about protecting computers during the migration, because the pilot participants' computers were production systems connected to the Microsoft corporate network. Planning included elements such as infrastructure considerations, in addition to managing potential gaps in the process where clients might not be protected.

Moving the pilot out of the free-form testing lab and into a production environment required a proper accounting for Microsoft IT data-center policies and standards, including the existing corporate Microsoft Operations Manager, WSUS, and SMS infrastructures, wide area network (WAN) and local area network (LAN) usage, and more. For example, Forefront Client Security uses its own dedicated Microsoft Operations Manager and WSUS infrastructures, and computers that use dedicated Forefront Client Security versions of these technologies cannot also use the standard corporate versions employed for services like system monitoring and software distribution. As a result, Microsoft IT had to decide how to roll out Forefront Client Security so that the computers receiving the dedicated versions of Microsoft Operations Manager and WSUS would still receive the benefits of the corporate versions even though they were technically disconnected from them.

Microsoft IT managed the client deployment order and locations for the Forefront Client Security pilot. This approach enabled Microsoft IT to determine which computers were disconnected from official corporate network infrastructure and to ensure that the computers enrolled in the pilot were placed on management server groups that were load-balanced with manageable populations of users. Because of the compatibility problems and exclusivity between Microsoft Operations Manager 2005 and its successor, System Center Operations Manager 2007, Microsoft IT limited the pilots to end users—the Forefront Client Security pilot rollout did not cover server computers.

To help ensure a smooth migration, the various Microsoft IT groups affected by the Forefront Client Security pilot deployment, such as administrators of SMS and Microsoft Operations Manager, the Network Security team, and the executive sponsors of each, scheduled weekly meetings to address concerns and share information. These meetings began in September 2006 and continue today.

Planning

Microsoft IT separated the pilot into two phases. Phase 1 was the limited deployment of 10,000 end-user nodes by using one server management group. Phase 2 expanded upon phase 1, increasing the deployment to 50,000 end-user nodes, expanding the number of server management groups to five, and creating a second-level hierarchy that all of the server management groups reported to—the Enterprise Management Console server.

To prepare for the pilot, Microsoft IT created a streamlined deployment team responsible for preplanning, planning, communication, education, and deployment technologies. The team prepared for deployment of Forefront Client Security by setting end-user expectations for those affected, creating a support escalation plan, and training internal support personnel.

Through previous experience, Microsoft IT had learned the importance of comprehensive communication in large deployment projects for properly setting end-user expectations.

Deployment teams need to establish regular communication methods that effectively convey their goals and the project schedule. In addition, development teams must communicate quickly when problems arise. To accomplish this, Microsoft IT used several communication channels:

- **Project Web site** Microsoft IT created a Microsoft Office SharePoint® Server 2007 Web site that contained all of the project details and documentation. The site included deployment schedules, meeting minutes, status updates, problem resolution processes, and other information related to the deployment.
- **Regular status reports** Microsoft IT distributed regular status reports. These e-mail messages discussed project issues, action items, and metrics related to the deployment, and provided a link to project plans.
- **Weekly meetings** Microsoft IT had deployment project meetings each week to monitor the deployment across all teams. A representative from each team that was involved in the deployment attended these meetings.
- **Quarterly reviews with stakeholders and executives** Microsoft IT met with stakeholders and executives about four times a year to communicate deployment progress and to make key decisions.
- **Readiness package for regional IT** The deployment team, centered in Redmond, collaborated with regional IT personnel as part of the pre-deployment planning process. Microsoft IT also created an internal Web site to communicate deployment plans and information to the affected regional IT departments. Regional IT manages Microsoft data centers and branch offices that are not in the Redmond location. The internal Web site contained the information that the regional IT departments needed to deploy Forefront Client Security in their areas. For example, the site included an e-mail template with instructions on how to customize it to the different areas, a partner contact sheet, and copies of a customizable newsletter.
- **Executive sponsorship e-mail messages** When Forefront Client Security was released, a senior executive sent an e-mail message to all full-time employees to request participation in the deployment. Having visible executive support is essential for successful deployments. When employees know that executives support decisions and changes, they are more likely to be positive and flexible.

After end users received the senior executive's e-mail message, they received a newsletter that contained the following information about Forefront Client Security:

- Product information, including what was new and what had changed
- Links to training resources
- Pre-installation information, including hardware compatibility checks and how to migrate files and settings
- Installation instructions based on which operating system the computer was currently running
- Post-installation configuration information to help users minimize downtime
- Customer support resources and instructions for reporting issues about the product

The goal of these two communications was to set users' expectations about installing and using the new security software, and to generate excitement about the upcoming release.

"Running alpha and beta version pre-release software is one of the reasons why it's hard to work in Microsoft IT. But that's why I like working here. It has a certain challenge that you won't find anywhere else."

Daryl Pecelj
Senior Security Strategist-Antivirus
Microsoft Corporation

Schedule

The pilot started with a tiny, 25-node deployment within the Forefront Client Security product development group itself. After a month of successful testing, Microsoft IT expanded the pilot to 100 end-user nodes. The pilot participation continued to quickly expand, all based on volunteer end users excited about testing the new security product. The early pilot was so successful that Microsoft IT expanded it to include 10,000 users on one management server group within only two months of the pilot kickoff.

After Microsoft IT had deployed the 10,000-node pilot and it continued to work well, the Forefront Client Security product development group and Microsoft IT worked together to build additional groups and deploy more user nodes to scale the pilot up to 50,000 nodes. This second phase of the pilot started in May 2007 and finished in February 2008.

Process

At the start of the pilot, Microsoft IT had very specific selection criteria for the potential pilot participants. Each candidate user's computer had to be a member of one of the domains selected to participate in the pilot. This meant that the candidate had to be a member of the same domain as the pilot management group to which he or she would be assigned.

Pilot Phase 1

Because Microsoft IT used SMS to deploy the product in the pilot, each candidate user's computer needed to be healthy and functional in terms of SMS. This meant having an up-to-date, normally functioning SMS client installed, which was able to report back to the SMS server and receive software updates. Microsoft IT chose to use SMS to manage the software pilot deployment so that it could effectively manage end-user node memberships with particular management groups. Microsoft IT was concerned that if it opened a server share with the Forefront Client Security installation package to even a limited number of people, it might have faced a deluge of unmanaged end users self-subscribing, all configured to use one particular management server group. This not only might have adversely affected the stability of the group itself by exceeding the maximum number of users supported, but also would have affected all other users attached to that group, as well as the ability of Microsoft IT to access the vital client reporting data on that group.

At the start of the pilot, each candidate user's computer had to be running Windows XP with Service Pack (SP) 2; early on, full compatibility with the still-in-beta version of the Windows Vista® operating system was not yet resolved. As time proceeded, however, updates from the Forefront Client Security product development team enabled Microsoft IT to apply the last 20 percent of the phase 1 pilot to Windows Vista users. Later in phase 2, as the pilot continued to grow and the Forefront Client Security product development team added more operating system support, Microsoft IT added support for users of Windows Vista with SP1 and Windows XP with SP3 to the pilot, for both 32-bit and 64-bit versions.

As part of the pilot process, Microsoft IT tested Forefront Client Security for product functionality in terms of installation, administration, management, and reporting. It tested for interoperability with existing business applications used internally at Microsoft. It even tested how gracefully the product performed when it was uninstalled. Regular feedback to the product development team was a major part of the testing and trial process, and the team continuously made technical improvements to the product based on that feedback.

Pilot Phase 2

To expand the pilot in phase 2, Microsoft IT had to expand both its Forefront Client Security server architecture and its planned user base. Because the phase 2 goal was to support 50,000 users, Microsoft IT needed to deploy four more management groups. For Microsoft IT to be able to roll up comprehensive management reports, it needed to add another layer to the Forefront Client Security architecture hierarchy. This new top layer, the Enterprise Management Console, was a large, single server that combined the database reporting and management group roles, gathering data from the midlevel management server groups, and presented aggregated reports for all computers that participated in the pilot. As with the midlevel management groups, the Enterprise Management Console connected to two SAN drives for data storage.

Phase 1 of the pilot needed only one management server group, so Microsoft IT hosted that group in its Redmond data center. When Microsoft IT and the Forefront Client Security product team decided to expand the user base for phase 2 of the pilot, Microsoft IT decided to test the new client and management group deployments on a global scale. Microsoft IT placed the four new groups built to accommodate the next 40,000 end-user nodes in Microsoft IT data centers in two locations in North America, Dublin (Ireland), and Singapore. Microsoft IT deployed the Enterprise Management Console—used by the team's security staff through remote access—in Dublin. Figure 3 shows a geographical map of how the phase 2 pilot expanded the hierarchy worldwide.

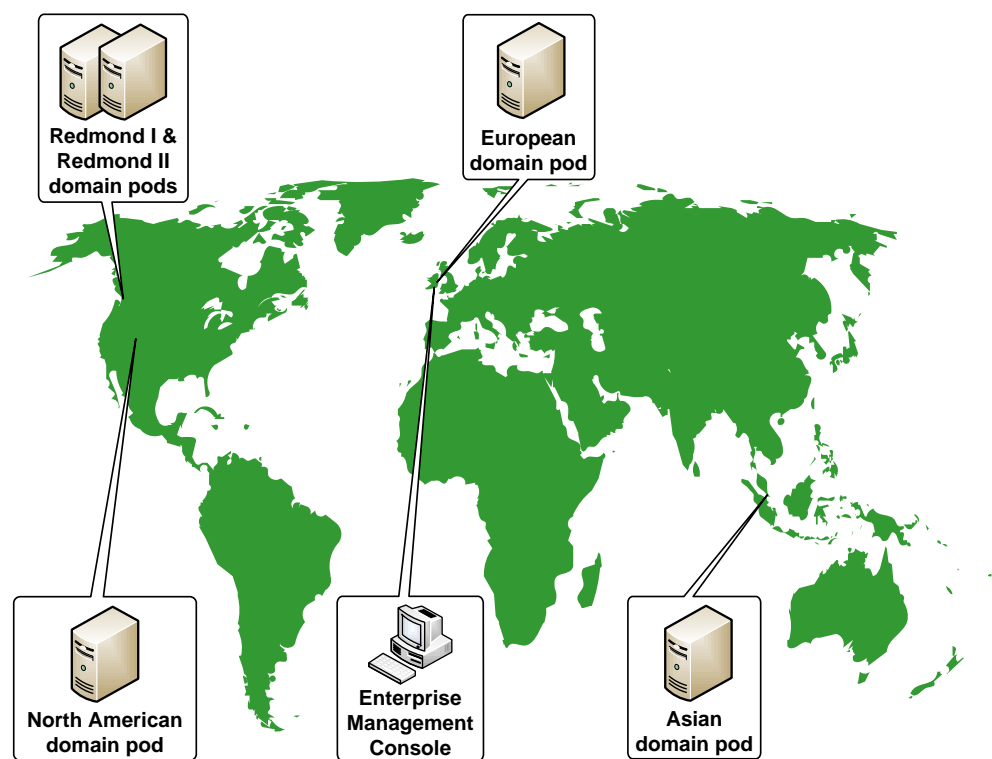


Figure 3. Phase 2 deployment of the Forefront Client Security pilot

To expand the pilot user base, Microsoft IT used SMS to identify targeted groups of technically capable candidate user computers. Microsoft IT sent e-mail to the owners of those

computers to inform them of their selection to participate in the expanded pilot and to give them an opportunity to opt out if necessary.

To help better manage the expanding pilot, Microsoft IT created security groups from the list of candidates that SMS identified as well as for the phase 1 pilot users as part of the phase 2 pilot, and those few people who chose to opt out were manually removed from those security groups. Because security group membership is limited to 2,000 computers, Microsoft IT had to create and maintain many security groups. Microsoft IT decided to create eight security groups per management group, totaling 40 for all five management groups. Because the membership was based on computer name rather than user name—and because users regularly retired old computers, received new ones, or reloaded Windows on existing ones, and then asked to be added back to the pilot—Microsoft IT's antivirus security team had to do a significant amount of manual maintenance to keep the pilot populated at 50,000 users.

As is standard for Microsoft IT, end-user satisfaction was of paramount concern. Maintaining this satisfaction despite the required manual configuration and maintenance of so many members in so many security groups for such a small staff in Microsoft IT (the antivirus security team has only two full-time members) was a challenge. Not only was maintaining security groups a part of the workload of running the Forefront Client Security pilot, but creating and running new SMS packages for installing Forefront Client Security onto those new computers added to the challenges. Considering the various teams that the deployment affected (SMS, IT security, network management, and more) and the steps needed to carefully deploy Forefront Client Security so that the management groups would remain load-balanced, Microsoft IT often took up to two weeks to respond to Forefront Client Security pilot reinstallation requests.

Infrastructure Issues

To conserve resources and avoid creating unnecessary redundancy, as Microsoft IT moved into phase 2 of the pilot, it began using existing corporate infrastructure, such as the WSUS network, for Forefront Client Security. To do this, the Microsoft IT security staff had to work with the existing Microsoft IT teams that managed those servers to begin downloading and maintaining Forefront signatures, application updates, critical updates, and more. After Microsoft IT acquired these update packages, it needed to deploy them to the entire WSUS infrastructure.

Because WSUS has a dependency on the existing AD DS infrastructure, phase 2 involved the team in Microsoft IT that manages WSUS. Windows enables only one WSUS server address to be listed with a client, and Microsoft IT was already using WSUS through its SMS infrastructure. Therefore, instead of creating a secondary, smaller WSUS network dedicated for pilot users that had all of the normal WSUS updates and the new Forefront Client Security updates, Microsoft IT simply added Forefront Client Security updates to the existing WSUS server infrastructure. By using the existing WSUS servers, Microsoft IT could maintain one superset of WSUS servers for all users that it managed.

Regional Issues

The antivirus security team in Microsoft IT, which is responsible for protecting all Microsoft assets worldwide, had to work closely with regional IT managers with phase 2 deployments outside the Redmond domains. This work entailed planning for deployment and obtaining server requirements for overseas data centers. Some regions have specific, local requirements beyond those of centralized Microsoft IT. Work also involved shipping servers

through customs and setting up new server management groups. Microsoft IT selected participants and offered an opt-out option, scheduled user conversions from the earlier solution to Forefront Client Security, built and validated SMS packages, and built and manually maintained security groups. Another added effort for Microsoft IT to manage as part of the Forefront Client Security pilot was training the internal Helpdesk team to support the new product, not only in the United States, but also around the world as the pilot expanded. This effort included training, coordination, and planning.

The delays of setting up management group servers at the regional data centers around the globe extended the overall length of the pilot. Despite being a global company, Microsoft IT does not strictly dictate all details of how its international data centers operate. It must account for regional interests, along with any applicable laws, regulations, tariffs, and customs. Some international data-center operators set their own computer hardware standards, homogenous specifications, and administration processes that differ from those in the Redmond data center.

Furthermore, a project like this spanned multiple groups in Microsoft IT and involved such staff as data-center installers, operations, maintenance, corporate security, support, and more. After Microsoft IT deployed the servers, it had to address additional issues, such as planning for server administration, maintenance, and replacement; planning and budgeting for server obsolescence; setting service level agreements, emergency planning, and alternative sources of updates in case Internet connectivity is severed.

Last, Microsoft IT managers had to stay informed about the plans and agreements set so that when contingencies do occur, the managers understand what will happen, when, and why. Each group in Microsoft IT has limited resources for accepting and managing new projects, so careful planning and coordination between teams were keys to the successful Forefront Client Security deployment at Microsoft.

Table 3 shows the populations of Forefront Client Security users associated with the various management groups, generally organized by domain, at the time of this writing.

Table 3. Forefront Client Security Pilot Population by Management Group

Group (domain)	Client count
Redmond I	13,319
Redmond II	9,885
European	8,452
Asian	9,800
North American	31

Note: Participation numbers are increasing with regular new pilot deployments of approximately 2,000 to 4,000 per week through SMS. However, participation in the North American domain is lower than participation in other domains because another, temporarily incompatible pilot is concurrently taking place there.

OPERATIONS

Each management server group that Microsoft IT deployed typically supports approximately 10,000 users. When deployed in larger environments, such as the phase 2 portion of the pilot, Forefront Client Security enabled Microsoft IT to organize users onto multiple server groups and aggregate all of their reporting data up to a new level in the hierarchy: the Enterprise Management Console, as illustrated in Figure 4.

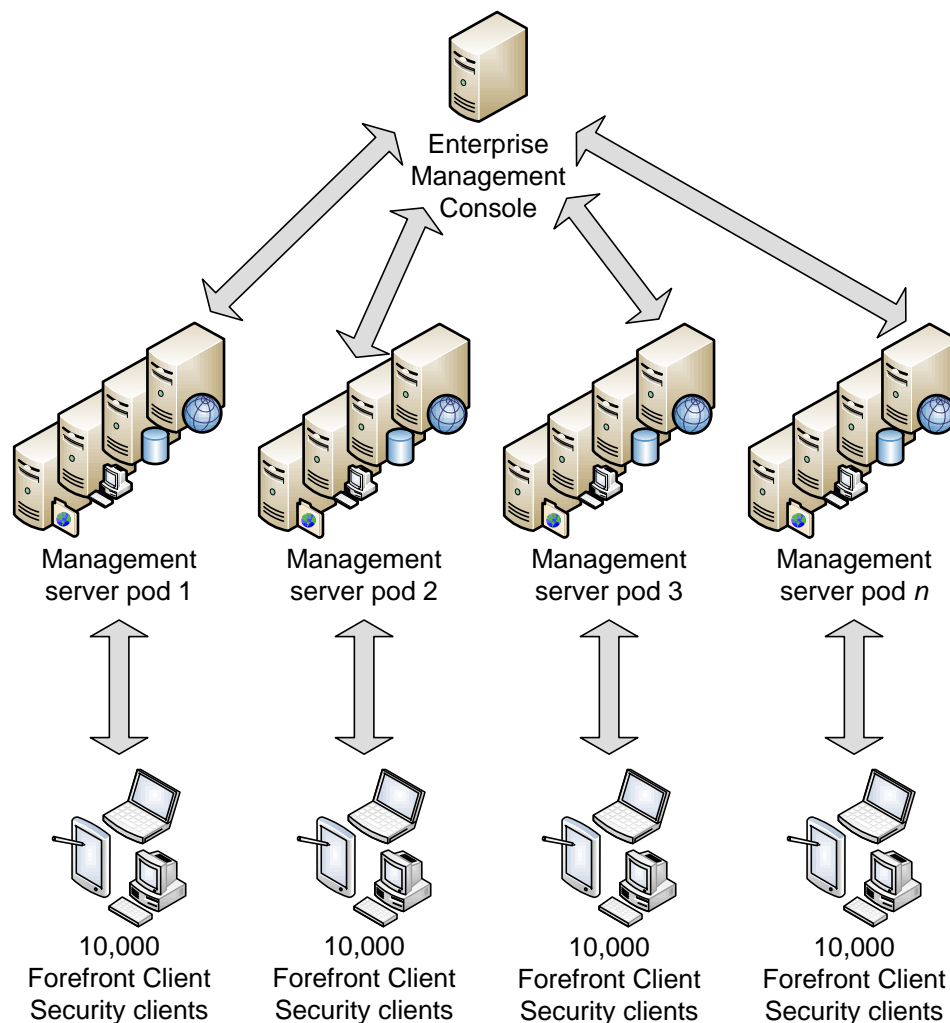


Figure 4. Forefront Client Security hierarchy with the Enterprise Management Console

From the single Enterprise Management Console, Microsoft IT security staff perform the following tasks for all clients:

- Perform centralized management
- Author and distribute policy to clients
- Get a view at a glance of the overall system security state for all connected clients
- Get access to all the views of Forefront Client Security

Figure 5 shows a sample view of the Enterprise Management Console.

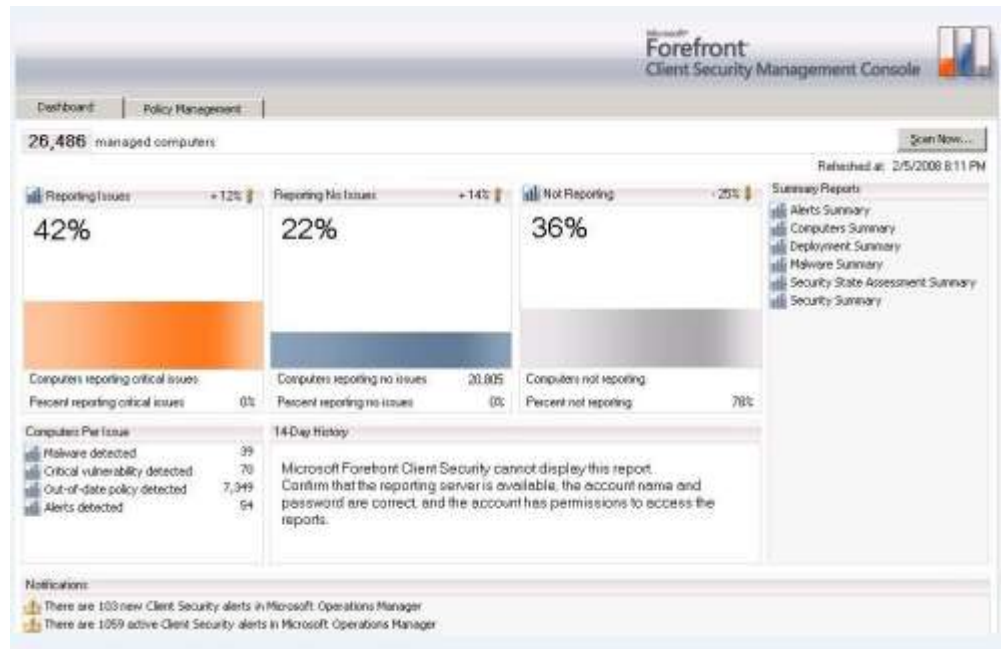


Figure 5. Sample view of the Enterprise Management Console

The dashboard of the Enterprise Management Console displays the following information at a glance about the enterprise:

- The total number of managed client computers that use Forefront Client Security policies.
- The percentage of participating client computers that are reporting an issue.
- The number and percentage of client computers that are reporting no issues.
- The percentage of client computers that are not reporting to the management servers in the groups. Non-reporting could be due to the client computer being offline or a bad connection with the server.
- The on-demand **Scan Now** button, which runs a scan on all participating client computers.
- The number of client computers in each category facing each issue. Clicking the issue begins the drilldown process.
- The number of issues detected in the past 14 days. Many malware attacks evolve rather than simply appearing; a 14-day history can help detect issue trends before they grow.
- A list of the detailed reports available. Forefront Client Security offers several overall reports that give organizations the ability to drill down into details.
- A Security Summary Report that summarizes the enterprise security state and top security concerns. The security summary report becomes almost another dashboard to assess the general health of computers.

Access to additional Forefront Client Security reports is available through the console.

BENEFITS

Even during the pilot phase, Microsoft IT saw some immediate benefits to running Forefront Client Security on part of its infrastructure. For one, Microsoft IT could detect and remove existing instances of malware that the earlier solution did not detect. In addition, the comprehensive reporting mechanism of Forefront Client Security enabled Microsoft IT to immediately see which computers participating in the pilot had security vulnerabilities due to configuration errors or missing software updates.

After Microsoft identified the configuration vulnerabilities, it used the console to apply changes to those participating computers to correct those vulnerabilities without requiring end-user intervention. As a result, the users of Forefront Client Security improved the overall security state of the Microsoft corporate network. Microsoft IT looks forward to continuing to expand the pilot of Forefront Client Security into other domains, thereby improving the security state of the entire enterprise.

As Forefront Client Security continues to develop and mature, deployment will grow beyond the 50,000 pilot end users and step into the data center, helping to protect servers as well. IT departments in other organizations that do not have the compatibility and infrastructure dependencies with Microsoft Operations Manager 2005, as does Microsoft IT, have no reason to exclude testing and piloting Forefront Client Security on their server infrastructure today.

NEXT STEPS FOR MICROSOFT IT

Microsoft IT is planning for the expected beta release of version 2 of Forefront Client Security. Based on feedback from Microsoft IT through the design of version 1 of Forefront Client Security and the beta pilot deployment of the product, there is great anticipation for an even more flexible product that will extend to easily cover the largest enterprise environments and resolve compatibility issues with existing enterprise software infrastructure, all the while maintaining its top-rated malware detection and removal engine and excellent reporting and alerting capabilities.

Version 2 of Forefront Client Security will become phase 3 of the Forefront Client Security pilot. Microsoft IT plans to accomplish the following in phase 3 of the pilot:

- Upgrade the existing 50,000 pilot users
- Retire the earlier antivirus solution from the enterprise
- Deploy Forefront Client Security agents to data-center server computers
- Deploy Forefront Client Security to lab server computers
- Grow the management and reporting infrastructure
- Transition from a pilot to a formal global rollout of the technology

LESSONS LEARNED

Microsoft IT learned many lessons in planning, deploying, and managing Forefront Client Security:

- **Account for new hardware infrastructure requirements** Forefront Client Security deployments need to meet capacity and sizing requirements for building the management server groups, and if necessary, the Enterprise Management Console group. After testing performance with the four-server group design, Microsoft IT discovered potential performance issues with local disk storage, and it augmented initial designs with connections to leased disk storage space on SAN enclosures for the collection and reporting server roles in the group. Because each group in the Microsoft IT deployment supported an average of 10,000 users, Microsoft IT needed six sets of servers (five groups and the Enterprise Management Console group), equating to 24 new servers, to fully deploy the pilot to 50,000 end-user nodes. Microsoft IT could then mitigate the number of required servers somewhat by using existing infrastructure when possible, such as by using existing WSUS servers for the software distribution role in the group.
- **Consider software infrastructure redundancies** Forefront Client Security uses dedicated IT infrastructure services that may be found in existing enterprise installations. Some of the services used in Forefront Client Security may be able to use that existing infrastructure, such as with WSUS for software distribution. In other cases, as with data collection performed by Microsoft Operations Manager 2005, managing those redundancies may be more challenging. Forefront Client Security uses a customized, limited version of Microsoft Operations Manager 2005 that does not perform the same comprehensive monitoring and data collection service for the enterprise as does a typical Microsoft Operations Manager 2005 installation. All Microsoft Operations Manager clients use the same registry key on client computers, creating an unsupported configuration for multiple Microsoft Operations Manager instances on a single computer. Forefront Client Security does not currently support System Center Operations Manager 2007. IT departments with an existing System Center Operations Manager or Microsoft Operations Manager infrastructure must decide whether to run Forefront Client Security without the Microsoft Operations Manager component (eliminates data collection for reporting and security state assessment), or operate segregated Microsoft Operations Manager environments in the enterprise to prevent one infrastructure from interfering with another on computers specifically selected to participate in one. Microsoft IT opted to simply deploy the version of Microsoft Operations Manager used for Forefront Client Security on client computers only. The Microsoft IT Microsoft Operations Manager infrastructure typically does not monitor these computers.

The use of SQL Server within Forefront Client Security requires the use of the Forefront Client Security reporting. Even if a SQL Server environment already exists, most enterprises will likely opt to build a dedicated Forefront Client Security reporting server environment and set it up as part of the group rather than integrate other SQL Server environments into the pod structure.
- **Anticipate the challenges of a global hardware installation** Microsoft, as a global company, specifically included regions outside the United States in its pilot deployment of Forefront Client Security to better understand the implications of such an enterprise-wide effort. It took a full four to five months to get needed Forefront Client Security

servers through the process of being specified to meet regional requirements, ordered from the manufacturers, delivered through international customs, and set up locally in the regional data centers, and then have the software properly installed and configured for centralized management. Enterprises with a global IT presence should plan for the amount of time needed to set up and prepare the entire infrastructure for their deployments.

- **Collaborate with regional IT staff** Microsoft IT not only needed to consult the regional IT staff regarding hardware requirements for their data centers, but also needed to coordinate issues regarding regional IT policies, installation issues, staffing and international holidays, new product training for IT staff and support personnel, documentation, support and escalation procedures, and announcements to end users. After Microsoft IT deployed the product, it provided reports on usage metrics to those regional IT representatives in weekly status meetings.
- **Deploy clients in a phased approach** To adequately design the server groups, Microsoft IT assigned Forefront Client Security end-user nodes to servers slowly at first, checking to ensure that the servers handled the load properly. As the deployments progressed in incremental steps from 100 to 200, 500, 1,000, 5,000, and then 10,000 users, Microsoft IT continued to monitor server performance for problems. If none were reported, Microsoft IT continued to scale up the deployments until it fully populated the server groups. It followed this phased approach of populating server groups with every deployment, rather than simply turning on 10,000 newly configured clients, to help ensure that the infrastructure remained stable throughout the process.
- **Manage post-deployment hardware maintenance** Another aspect of dealing with a global IT deployment is managing the server maintenance tasks that are inevitable with any IT hardware. Like many IT organizations, Microsoft IT employs separate teams for deploying new installations versus maintaining ongoing operations. All such teams must coordinate when deploying new technology. This is even more important with global deployments. Understanding global change management policies, who is responsible for what, and how these tasks are to be performed, is key to maintaining a properly functioning infrastructure.
- **Manage post-deployment service maintenance** Because Forefront Client Security requires client node assignment to specific server groups for service load balancing, the IT department must actively manage all deployments. As a result, a deployment of Forefront Client Security must account for a constant workload level in terms of resources. As users rebuild their computers, get new ones, and retire old ones, and as personnel come and go within the organization, memberships in security groups, which Microsoft IT uses to manage which nodes were associated with which server groups, require regular administrative maintenance. The additional infrastructure associated with the Forefront Client Security management server groups also requires new maintenance work.
- **Limit deployments while the IT infrastructure is in a transition state** Because Microsoft IT is always testing new software products and technologies—often multiple products and technologies simultaneously—testing, evaluating, and troubleshooting a new pilot deployment can be difficult. However, many IT departments have similar circumstances. Although they may not regularly test pre-beta versions of multiple software products and services in the data center like Microsoft IT, they are often in a state of transition between server operating system and application upgrades, hardware

migrations, service changes, and other such conditions that put them in a similar transition state. It is best to conduct the pilot during a period of minimal disruptions in transition state. An organization can best resolve conflicts, measure performance, and validate results when it minimizes external factors that potentially affect the outcome.

BEST PRACTICES

As part of its experience in deploying Forefront Client Security in an enterprise environment, Microsoft IT shares some of its best-practice discoveries:

- **Know infrastructure components for software and services** An organization should know what its current environment is capable of, not only currently, but what is expected in as soon as two years. This knowledge will help with upgrade planning and migration deployments. Microsoft IT knew that its earlier solution infrastructure needed either an upgrade and service enhancement or a total replacement. The advent of Forefront Client Security gave Microsoft IT the opportunity to do that replacement when it was ready to begin the process. That process will continue through 2009 with the beta release of version 2 of Forefront Client Security.
- **Use existing infrastructure where possible** An organization can mitigate the costs of an enterprise-wide technology deployment, such as Forefront Client Security, if it can use existing IT infrastructure with the new deployment. In the case of software distribution, such as WSUS, and software deployment technologies, such as SMS, using those in a Forefront Client Security deployment will conserve costs and reduce the complexity of the installation.
- **Plan for alternative Forefront Client Security functionality options** An organization should always have a backup plan instead of enabling a key service to rely on a single point of failure. It should have a plan for an alternate method of delivering software to clients, updating malware signatures, and managing client alerting.
- **Plan ahead for hardware acquisition** When an organization needs to deploy server groups for Forefront Client Security management, it should plan at least three months ahead for domestic deployments, and at least six months ahead for international deployments. Getting shipments through international customs can take time. If the deployment is on a tight timeline, the organization should allow enough time for placing and setting up the necessary hardware in its plans.
- **Plan for staff resources** If the deployment of Forefront Client Security will affect a large number of users, the maintenance of the server group infrastructure, in addition to membership lists in the security groups that the software deployment mechanism uses, requires appropriate resource levels to perform these ongoing tasks. The organization should account for both the resource time and costs when planning the overall deployment budget for Forefront Client Security.
- **Use a software distribution system, such as SMS, to manage Forefront Client Security deployments** A successful deployment of Forefront Client Security depends on associating each client with a particular management server group to avoid overloading any particular server group. Server groups associated with too many clients may be overwhelmed and unable to adequately serve all of them in a timely fashion, which will adversely affect performance, distribution, data collection, and reporting. Using an enterprise software-distribution system, such as SMS 2003 or System Center Operations Manager 2007, enables IT staff to properly manage the pod populations. An organization should make sure that its software distribution infrastructure can handle mandatory, enterprise-wide installations, including client computers that are exempted from or unable to run its distribution agents. If necessary, the organization should set up a secondary software distribution mechanism for these computers before deploying Forefront Client Security.

CONCLUSION

The emergence of ever more sophisticated and pervasive malware led Microsoft IT to re-evaluate the effectiveness of its earlier antivirus solution. As a result of that review, Microsoft IT decided to migrate to Forefront Client Security. Forefront Client Security offers industry-leading effectiveness rates for malware detection and removal, including unified protection for effective antivirus and antispymware technologies.

Microsoft IT can easily manage the entire installed base of Forefront Client Security from a single management console. From the console, Microsoft IT can access simplified, comprehensive reports and security state assessments anytime. When Forefront Client Security detects issues, Microsoft IT security staff can easily drill down through the reports to the individual computers affected. From there, they can implement the needed corrections either by using Group Policy to change vulnerable security settings or by initiating an immediate malware scan on the client computer. The Forefront Client Security console also offers support that enables Microsoft IT security staff to create and deploy proactive, targeted security policies that help secure their environment.

Forefront Client Security takes advantage of many of the IT infrastructure elements already present in Microsoft IT's network environment, such as AD DS, SMS, and WSUS. Microsoft IT can thus maximize existing investments in both IT infrastructure and technical skills that its engineering staff has acquired.

Though still in pilot mode as of this writing, Microsoft IT intends to expand its deployment of Forefront Client Security company wide. After the deployment is finished, the advantages that Forefront Client Security provides—thorough malware detection and removal, simplified, centralized administration, and quick, comprehensive reporting—will significantly improve the overall security of all resources connected to the Microsoft corporate network.

FOR MORE INFORMATION

For more information about Microsoft products or services, call the Microsoft Sales Information Center at (800) 426-9400. In Canada, call the Microsoft Canada information Centre at (800) 563-9048. Outside the 50 United States and Canada, please contact your local Microsoft subsidiary. To access information through the World Wide Web, go to:

<http://www.microsoft.com>

<http://www.microsoft.com/technet/itshowcase>

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

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.

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

© 2009 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Forefront, Internet Explorer, OneCare, SharePoint, SQL Server, Windows, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.