

Microsoft® Forefront™

Security Products for Business

Microsoft Corporation

Published: September 2006

Updated: October 2006

Abstract

The Microsoft® Forefront™ family of business security products helps provide greater protection and control over the security of an organization's network infrastructure. Forefront's products easily integrate with each other, with the organization's IT infrastructure, and can be supplemented through interoperable third-party solutions, enabling end-to-end, defense-in-depth security solutions. Simplified management, reporting, analysis, and deployment allow administrators to more efficiently protect their organization's information resources and provide secure access to applications and servers. With Microsoft Forefront, businesses can confidently meet ever-changing threats and increased business demands.

Microsoft®

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

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

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

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

© 2006 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Forefront, Visual Studio, Windows, Vista, Longhorn, the Windows logo, and Windows Server 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.

Contents

Introduction	1
Security Challenges and Trends	2
Increasing Connectivity.....	2
Evolving threats.....	2
Fragmented solutions	2
Operational difficulties.....	2
The Microsoft Forefront Product Line	4
Design Tenets	4
Comprehensive	4
Integrated	4
Simplified.....	5
The Forefront Product Line	6
Protecting and Controlling Access to the Network Edge	7
Microsoft Internet Security and Acceleration Server 2006.....	7
Intelligent Application Gateway	7
Protecting Server Applications.....	8
Microsoft Forefront Security for Exchange Server	8
Microsoft Forefront Security for SharePoint	8
Microsoft Forefront Security for Office Communication Server.....	8
Protecting Client and Server Operating Systems	9
Microsoft Forefront Client Security.....	9
A Comprehensive Approach to Security	10
Microsoft and Well-Managed Security	13
Related Links	15

Introduction

Over the past decade, the Internet has become a critical resource for organizations of all sizes. Employees, partners, suppliers, and customers can communicate with each other more effectively, obtain information wherever and whenever they require, and can save time and money through self-service and streamlined processes.

Along with its many advantages, however, Internet access has opened the door to a host of challenges. The dynamic information services that enable customized information have also spawned privacy concerns and associated regulations. The very connectivity that improves business productivity has made it easier for malicious users to launch widespread attacks and for unauthorized users to access valuable data on corporate networks. And the threats themselves have become more advanced and dangerous over the years.

Managing network security in the face of ever-evolving threats is a complex task that often requires integrating and securing multiple technologies in order to strike a balance between easy access and rigorous security. Burdensome security solutions can lower productivity if they unduly delay authorized access to IT resources, while an inability to communicate easily and securely with customers or partners can result in lost business opportunities. However, being too open can result in the exposure of confidential information, financial loss, and jeopardize the well-being of the organization.

As a leader in the computing industry, Microsoft has committed itself to deliver more secure products and to help its customers efficiently deploy and maintain them. Among the results of this commitment is Microsoft Forefront, a family of comprehensive security products for enterprises of all sizes. Microsoft Forefront helps organizations to provide secure access anytime, anywhere, while protecting information assets against unauthorized users and attacks.

Security Challenges and Trends

Despite the enormous investment in computer and network security over the last ten to fifteen years, security challenges have increased rather than diminished. Today, businesses are vulnerable to an ever-increasing array of threats, from viruses to spam to attacks designed to steal valuable company information.

Increasing Connectivity

The Internet has become a critical resource for organizations large and small, enabling organizations to provide real-time information to employees, increase the reach of their marketing efforts, save money through customer self-service, and streamline business processes with suppliers and other partners.

While the benefits of a highly connected organization are many, so too are the challenges. Widespread connectivity has opened the door to a host of ever-evolving threats, making it easier for malicious users to launch widespread attacks and for unauthorized users to access corporate networks. And the more constituents an organization communicates with, the more potential avenues of attack.

Evolving threats

The computer and network security space has seen a troubling evolution in the types of security threats as well as the motivation behind them. Because traditional network firewalls are not designed to detect and prevent intrusions at the application layer, the vast majority of Internet-based attacks have now moved “up the stack”, targeting applications such as e-mail, Web servers, and on-line collaboration software.

The impetus for these attacks has also evolved; hackers have become motivated by criminal profit, targeting specific organizations for confidential—and highly valuable—information such as names, addresses, Social Security numbers, and financial data. To compound the challenge, broad-based, indiscriminate attacks have not disappeared, but have instead risen exponentially with the advent of “script kiddies” who use automated hacking tools to attack organization of all sizes. The increasing volume of attacks has become more and more costly, increasing the downtime necessary for recovery and negatively impacting productivity and the usability of the IT infrastructure.

Fragmented solutions

Historically, IT security solutions have required disparate products from several vendors, requiring multiple tools and infrastructure for management, reporting and analysis. Properly deploying and configuring these complex security solutions can be challenging and time-consuming. Additionally, far too many security products have poor interoperability and integration with the existing security and IT infrastructure. The resulting solutions are difficult to manage, have increased total cost of ownership, and potentially leaving gaps in the security of the network.

Operational difficulties

The business-critical nature of security amplifies the need for effective management and centralized policy control, yet the fragmented nature of most security solutions often prevents this. Without centralized management and reporting tools, and the critical visibility they provide into the network’s

overall security state, deploying and managing security can be difficult, inefficient, error prone, and time consuming.

Despite the challenges, the need for centralized reporting and policy control has never been more acute. This is especially true due to the complex security demands driven by Sarbanes Oxley, the Health Insurance Portability and Accountability (HIPAA) Act of 1996, and other domestic and international regulations. Organizations must now weigh the regulatory implications of network intrusions and failure to implement adequate security infrastructure. Liability and the threat of lawsuits must also be a consideration for any company doing business over the Internet, particularly in the areas of privacy, file sharing, human resources, health, and investor relations. In this environment, malicious users pose a risk not only to data but also to a company's ability to comply with these requirements.

The Microsoft Forefront Product Line

The Microsoft Forefront family of business security products helps provide greater protection and control over the security of an organization's network infrastructure. Microsoft Forefront's products easily integrate with each other, with the organization's IT infrastructure, and can be supplemented through interoperable third-party solutions, enabling end-to-end, defense-in-depth security solutions. Simplified management, reporting, analysis, and deployment enable more efficient protection of information resources, as well as more secure access to applications and servers.

Design Tenets

Microsoft developed the Forefront family of business security products to address the challenges of widespread connectivity, evolving threats, fragmented solutions, and operational difficulties. Microsoft believes that in order to address these challenges, any properly constituted security solutions must be comprehensive, integrated, and simplified. These three characteristics are the tenets around which all Forefront security products are designed.

Comprehensive

Forefront products offer a comprehensive solution with end-to-end protection of the IT infrastructure.

- **Protect operating systems:** Forefront helps protect Microsoft client and server operating systems. The highly responsive anti-malware capabilities of Microsoft Forefront Client Security provide real-time, scheduled, or on-demand detection and removal of viruses, spyware, rootkits, and other emerging threats.
- **Protect critical server applications:** Forefront helps protect Microsoft-based application servers through a defense-in-depth strategy. ISA 2006 provides robust access control as well as application- and protocol-specific data inspection. Forefront's server security products protect specific server applications from malware by utilizing a unique multi-engine architecture that provides high levels of protection and reliability.
- **Enable secure, controlled access:** Forefront offers a broad array of firewall, VPN, and encryption technologies, as well as identity management capabilities that help ensure only authorized users can gain access to appropriate IT resources and data.
- **Safeguard sensitive data:** Forefront products safeguard sensitive data and protect intellectual property. ISA 2006 provides a combination of application-specific filters throughout the network, as well as technologies that ensure the confidentiality and authenticity of valuable data.

Integrated

Forefront products offer multiple levels of integration so that administrators can achieve greater efficiency and control over the security of the network.

- **Integrate with applications:** Microsoft Forefront anti-malware and secure access products are specially designed to integrate with and protect business critical server application such as

Exchange, Outlook® Web Access and SharePoint. This integration provides critical protection against the newest generation of application-specific attacks.

- **Integrate with IT infrastructure:** Security products work with the existing IT infrastructure, including directory services, systems management tools, and software distribution and update services. There must be a unifying infrastructure enabling the seamless management of security service deployment, distribution, configuration, and enforcement. Moreover, this must all be managed with a fine level of granular control.
- **Integrate across Forefront:** Forefront products are designed to work together so they can leverage their capabilities for greater security coverage.
- **Integrate with other products:** Forefront products are designed to protect and secure Windows-based infrastructure. However, because many organizations deploy security products from other companies, Forefront products are designed to better integrate with multi-vendor solutions.

Simplified

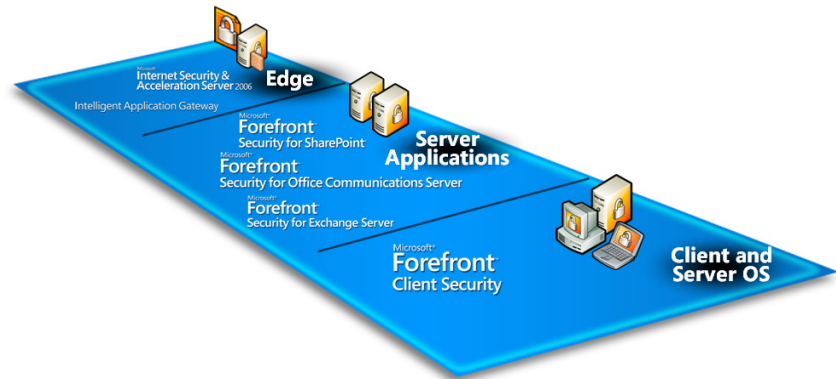
Forefront products are designed to simplify deployment, configuration, management, reporting, and analysis so that users and administrators can have greater confidence that the organization is well-protected.

- **Simplify deployment:** Utilities such as ISA Server Best Practices Analyzer Tool and configuration wizards help set a solid basis for robust security installation. Forefront's integration with Active Directory and update systems such as Systems Management Server provide a common foundation for change and configuration management. Users and administrators both benefit from the centralized distribution of up-to-date configurations, policies, and operating system or anti-virus updates for server and client hosts.
- **Unify reporting and analysis:** Forefront centralizes the collection and analysis of security management information by storing all security information in a single SQL Server™ repository and utilizing SQL Server Reporting and Analysis Services to identify and interpret security events.
- **Simplify management:** Security management and reporting is centralized in Forefront; its components integrate fully with existing management systems including Microsoft Operations Manager, Microsoft Systems Management Server, and Windows Server™ Update Services. Forefront's integrated management consoles offer Microsoft's familiar interfaces and ease-of-use, reducing training time and helping to control business costs.

The Forefront Product Line

Microsoft Forefront¹ consists of several products, some of which provide edge protection and access control, while others protect Windows operating systems and application servers from malware such as viruses, spam, and rootkits.

- Microsoft Internet Security and Acceleration Server (ISA) 2006
- Intelligent Application Gateway (IAG)
- Forefront Security for Exchange Server
- Forefront Security for SharePoint
- Forefront Security for Office Communications Server
- Forefront Client Security



¹ Microsoft introduced the Forefront brand on June 11, 2006. Over the next several months, the current product names will change to reflect their inclusion under the Forefront brand. The new names for ISA 2006 and the Intelligent Application Gateway have yet to be determined.

	Current	H2 2006	2007+
Client			Microsoft® Forefront Client Security
Server	Microsoft® Antigen for Exchange Microsoft® Antigen for SMTP Gateways Microsoft® Antigen Spam Manager Antigen for SharePoint Antigen for Instant Messaging	Microsoft® Forefront Security for Exchange Server Microsoft® Forefront Security for SharePoint	Microsoft® Forefront Security for Office Communications Server
Edge	Microsoft® Internet Security & Acceleration Server 2006 Intelligent Application Gateway		TBD TBD

This comprehensive product line protects information and controls access across operating systems, applications, and servers, helping protect businesses from ever-changing threats.

Protecting and Controlling Access to the Network Edge

Microsoft Internet Security and Acceleration Server 2006

Intelligent Application Gateway

Enterprises are facing an onslaught of increasingly targeted and sophisticated attacks on their networks. Protecting corporate resources at corporate headquarters and branch offices, while at the same time providing seamless access for legitimate business functions, requires a sophisticated and multi-functional edge gateway that is able to combat the more sophisticated, application-oriented attacks prevalent today.

Microsoft
**Internet Security &
Acceleration Server 2006**

Intelligent Application Gateway

ISA Server 2006 is an integrated edge security gateway that helps protect IT environments from Internet-based threats while providing users fast and secure remote access to applications and data.

ISA Server 2006 addresses three core deployment scenarios:

- Secure application publishing with ISA Server 2006 enables organizations to make their Exchange, SharePoint, and other Web application servers accessible in a secure manner to remote users outside the corporate network.
- Organizations can use ISA Server 2006 as a Branch Office Gateway to connect to and secure their branch offices, while efficiently utilizing network bandwidth.
- Web access protection with ISA Server 2006 can help organizations protect their environments from internally- and Internet-based threats.

ISA Server 2006 examines network traffic at the application layer; instead of just looking at network packet headers, it examines the packet contents to ensure that they are properly formed and conform to what the applications are expecting. ISA then forwards only the conformant packets to the servers, thereby preventing malicious attacks enabled by malformed packets. ISA Server also has the ability to inspect encrypted content by terminating inbound SSL connections, examining the contents, and re-encrypting valid packets before sending them onward.

In addition to ISA 2006, organizations can take advantage of the Intelligent Application Gateway (IAG). Recently acquired from Whale Communications, the Intelligent Application Gateway provides SSL VPN and Web application protection, enabling broad access to a full-range of network applications from both managed and unmanaged devices. The IAG provides sophisticated access capabilities based on its SSL VPN features:

- **SSL VPN:** SSL VPN for broad connectivity, access, policy-driven user authentication, and authorization from a wide variety of devices and locations
- **Endpoint security:** Enforces granular policies at the browser and helps ensure endpoint compliance and session security through integrated endpoint security and access control features, such as the Attachment Wiper cache cleaner

- **Application optimization:** Software modules that add the benefits of customized policy and content inspection for Microsoft applications and third-party CRM, ERP and collaboration platforms. Customers with custom business applications can use the Optimizer Toolkit to instrument IAG for specific security and policy needs. Microsoft is committed to the continued investment and support of this technology and its focus on optimizing both Microsoft and third-party applications.

Protecting Server Applications

Microsoft Forefront Security for Exchange Server

Microsoft Forefront Security for SharePoint

Microsoft Forefront Security for Office Communication Server

Microsoft Forefront helps protect business-critical Microsoft messaging and collaboration servers from viruses, worms, spam, and inappropriate content before they can impact businesses and users. These application servers include Exchange Server, Windows-based Simple Mail Transfer Protocol (SMTP) gateways, Microsoft Office Communications Server, and Microsoft Windows SharePoint Services. The benefits of Forefront server application security include:

- **Advanced Protection:** Multiple scan engines at multiple layers throughout the messaging infrastructure provide improved protection against threats.
- **Availability and Control:** Tight integration with Microsoft servers maximizes availability and management control.
- **Secure Content:** Helps organizations eliminate inappropriate language and dangerous attachments from internal and external communications.

The Forefront server security products provide truly best-of-class malware protection based on a unique, multiple scan engine approach. The concept of layered defense has long been a staple of enterprise security, employing the logic that any attack that slips past one layer of protection will be caught by subsequent layers. Forefront has applied this concept to the realm of malware protection--while any single scan engine might fail to identify a particular virus, it is improbable that a virus can circumvent multiple antivirus engines, each developed by different companies using different technologies and virus researchers. Forefront employs this type of layered defense by intelligently managing up to nine² industry-leading antivirus engines within a single solution. Each of these engines have unique strengths; some, for example, excel at detecting worms while other engines are better at detecting Trojan horses. Forefront makes the most of those strengths by combining multiple, industry-leading antivirus engines into a single product for improved overall

Microsoft®
Forefront
Security for Exchange Server

Microsoft®
Forefront
Security for SharePoint

Microsoft®
Forefront
Security for Office Communications Server

² Available engines are from Microsoft, CA InoculateIT, CA Vet, Norman, Sophos, Authentium, Kaspersky, VirusBuster, and AhnLab.

reliability and protection³. Without the expense of procuring and deploying numerous antivirus products, a business can reap the benefits of multiple engines in a single solution.

With Forefront server security, business can reap the benefits of multiple engines in a single solution without the expense of procuring and deploying numerous antivirus products

Protecting Client and Server Operating Systems

Microsoft Forefront Client Security

Forefront Client Security provides unified malware protection for Windows-based business desktops, laptops, and server operating systems that is easily and centrally managed. Built on the same highly successful Microsoft protection technology already used by millions of people worldwide, Forefront Client Security helps guard against emerging threats such as spyware and rootkits, as well as traditional threats such as viruses, worms, and Trojan horses.



By delivering simplified administration through central management and providing critical visibility into threats and vulnerabilities, Forefront Client Security helps protect businesses with greater confidence and efficiency. Forefront Client Security integrates with existing infrastructure systems such as Active Directory, and complements other Microsoft security technologies for better protection and greater control.

The benefits of Microsoft Forefront Client Security include:

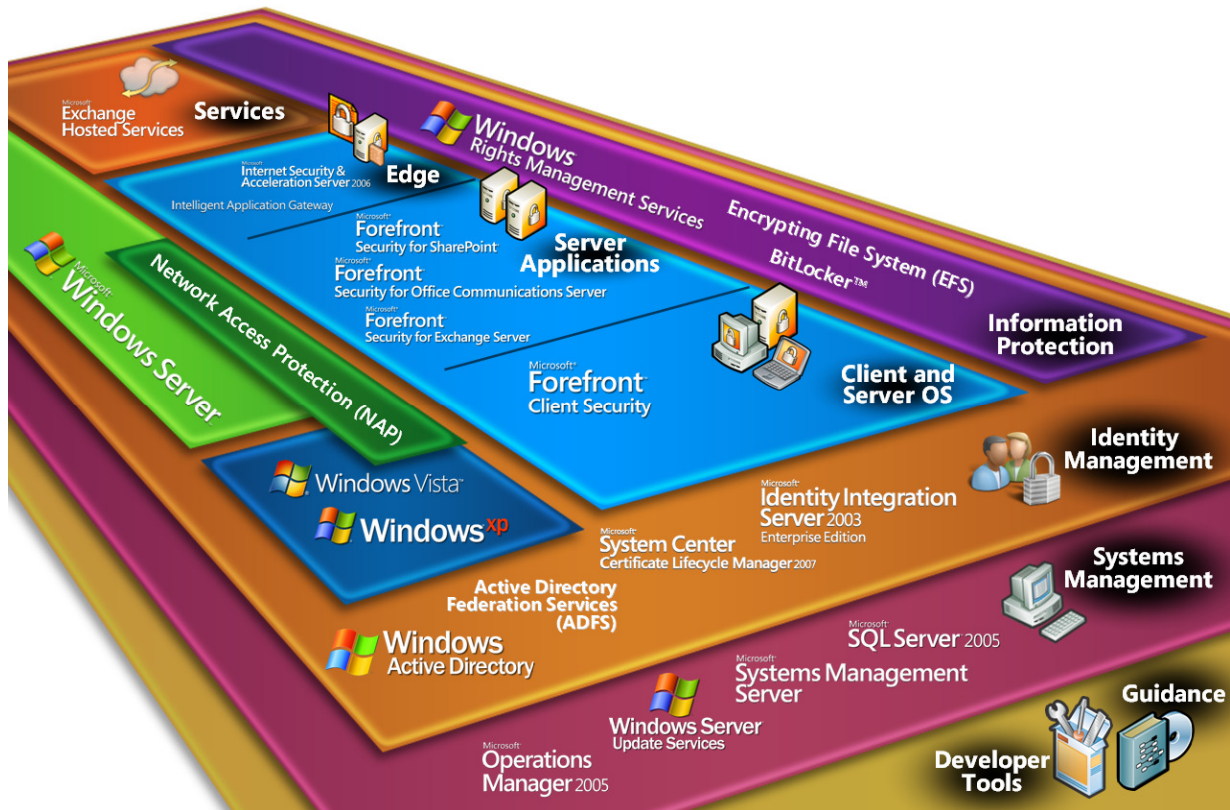
- **Unified Protection:** Forefront Client Security delivers unified protection from current and emerging malware, providing users and administrators the confidence that their information systems are better protected against a broad range of threats.
- **Simplified Administration:** Forefront Client Security provides simplified administration through central management, thereby protecting the organization with greater efficiency.
- **Critical Visibility and Control:** Forefront Client Security produces insightful, prioritized security reports and a summary dashboard view, providing visibility and control over malware threats.

Forefront Client Security is currently in development. Microsoft plans to make a public beta of the product available to customers in the fourth quarter of 2006.

³ As a best practice, Microsoft recommends that customers do not activate more than five engines in any given product installation. This provides the best balance between protection and performance.

A Comprehensive Approach to Security

As a leader in the computing industry, Microsoft has committed itself to deliver more secure products and to help its customers efficiently deploy and maintain them. While Forefront is a key component of Microsoft's strategy for providing end-to-end security for business customers, numerous other products and initiatives play significant roles in Microsoft's vision of a well-managed and secure network infrastructure.



Operating Systems

Over the past several years, Microsoft has expended enormous resources redesigning its operating systems to be the most secure versions of Windows ever. With the release of Windows XP Service Pack 2 (SP2) and Windows Server 2003 Service Pack 1 (SP1), important & critical vulnerabilities were significantly reduced, making both operating systems significantly less susceptible to malware. However, those improvements pale in comparison to those designed into the upcoming releases of Windows Vista and Windows Server code name "Longhorn." Vista and Longhorn were designed with security as a major goal, and provide a hardened OS environment upon which even the most critical and confidential tasks may be performed with confidence.

Network Access Protection (NAP)

Network Access Protection (NAP) is a policy enforcement platform built into the Microsoft Windows Vista and Windows Server "Longhorn" operating systems that enables better network protection by

defining and enforcing compliance with “system health” requirements for laptops, desktop computers, and servers. Health requirement policies can include, but are not limited to, software update levels, antivirus signatures, specific configuration settings, open and closed ports, and firewall settings.

When a client machine attempts to access the network, NAP determines whether the client complies with the organization’s IT policies. If it does, the client is granted appropriate access to the network. If not, the non-compliant machine can be granted limited access, or, more typically, is automatically quarantined while it is automatically updated to bring it back into compliance. Once remediation is complete, the machine is granted network access.

Information protection

A defense-in-depth approach to security must consider not only how to secure data within an organization’s network, but also how to protect information outside that secure perimeter. Microsoft Windows Rights Management Services (RMS) augments an organization’s security infrastructure through persistent usage policies which remain with the information whether online and offline, both inside and outside of the firewall.

RMS-enabled applications help safeguard sensitive digital information—such as financial reports, product specifications, customer data, and confidential e-mail messages— from unauthorized distribution or use. For example, a company could mandate that the recipient of a particular email not be able to forward the email, print the email, copy and paste from the email, or use print screen to capture the content in an email. Likewise, policies can be applied to prevent certain users from accessing content in a Word document or seeing specific cells in an Excel spreadsheet. As a result, data can be carefully controlled and organizations can minimize their data exposure risks.

Services

Many organizations rely on managed services instead of deploying and managing the solutions themselves. This is often true of companies with limited budgets or internal expertise, but can also include very large organization looking for extra layers of capabilities.

Microsoft Exchange Hosted Services offers a set of fully managed and hosted messaging security services that help organizations protect themselves from e-mail-borne malware, satisfy retention requirements for compliance, encrypt data to preserve confidentiality, and preserve access to e-mail during and after emergency situations. The services help minimize additional capital investment, free up IT resources to focus on other value-producing initiatives, and mitigate messaging risks before they reach the corporate firewall.

Identity management

Network security and access control is as much about *who* wants access as it is about *what* information they want. As a result, identity and access management processes, technologies, and policies play a central role in any security solution. Microsoft’s security products are tied together through a powerful identity management infrastructure based on Active Directory and an array of related products. These products enable organizations to manage digital identities and specify how they are used to access resources. The integration of these capabilities with Forefront products helps enable “single sign-on” solutions than can even span multiple organizations.

Systems Management

Microsoft offers a broad set of management and reporting capabilities that offer robust event collection, analysis, and reporting, as well as the tools to create and enforce security best practices. Microsoft's primary systems management tool is Microsoft Operations Manager (MOM), a comprehensive network monitoring solution that radically improves the availability, performance and security of Windows networks and applications. MOM provides central monitoring and automatic problem resolution for networks of tens to thousands of computers, continuously monitoring user actions, application software, servers and desktop computers.

A common security management task is to ensure proper patch management. Microsoft's Systems Management Services (SMS) and Windows Server Update Services (WSUS) enable the automatic distribution of software, updates, and patches for Microsoft operating systems and applications. In addition, SMS has improved patch management tools for mobile devices and non-Microsoft products installed in the enterprise. Through their integration with Active Directory, Microsoft's software distribution and patch management can be carefully managed on a large scale through policy-based mechanisms.

Developer Tools

Many organizations develop and utilize custom applications. Because so many of these applications provide business-critical capabilities, it is vital that they are as secure as the products obtained from Microsoft and other companies. If not, these custom applications can become the avenue through which security breaches can occur, particularly those initiated inside the organization.

Microsoft has learned a great deal over the past several years on the best ways to design and develop secure software, resulting in the Security Development Lifecycle (SDL). The SDL is a collection of best practices covering every stage of software creation. The SDL is used throughout Microsoft, and has now been made publicly available⁴.

The SDL is supported by development tools such as Visual Studio 2005, which enables individual developers and software development teams to build dynamic Windows, Web, mobile, and Office-based solutions while being more productive. Visual Studio helps developers generate secure code through the use of managed code and other techniques. Visual Studio also incorporates many tools to help generate secure applications, including the Threat Analysis and Modeling Tool (TAMT). The TAMT allows a developer to input data sources, users, roles, systems, and other information and build a threat analysis for their application. Additionally, the tool will create use cases and other testing points to help developers minimize the total risk from their code.

⁴ <http://msdn.microsoft.com/security/sdl>

Microsoft and Well-Managed Security

Microsoft offers a uniquely comprehensive, end-to-end portfolio of security products, from the client PCs to network access to the servers and even the data stored on them. Even so, this is only the beginning of a truly secure solution. If access to a wide variety of security technologies were the answer, security problems would have decreased over the years, not increased. In fact, most of the security challenges customers face today have less to do with the technologies themselves than with their proper deployment and management. The Gartner Group has found, for example, that as many as 65% of all security breaches were due to mismanagement and misconfiguration. Security is a complicated endeavor, and the interrelationships between a wide variety of products from multiple vendors can be subtle at times. It is not surprising that even the best-managed networks experience unexpected gaps.

Recognizing that the operational side of security is at least as important as the technologies—an improperly configured firewall does no one any good—Microsoft is concentrating much of its development efforts on addressing the operational aspects of security. Through integration and simplified management aspects of security—the “securability” of the infrastructure—Forefront helps organizations:

- Centralize security management
- Tighter integration with existing infrastructure
- Prevent misconfiguration
- Deploy security pervasively
- Gain a unified view into network security

Addressing these issues makes the network more secure—the configurations are correct, security is deployed where it needs to be, instead of where it is easiest to do so, and the security administration console helps clarify what is happening across the network.

Unified data collection, reporting, and analytics across the product line helps administrators ensure that data protection is compliant with the organization’s security policies and consistent with strict regulatory requirements. This also minimizes the need for expensive training and retraining of administrative staff in a variety of unrelated management and reporting consoles.

Microsoft’s emphasis on the operational aspects of security—in particular how the technologies must integrate with and embody the security policies of an organization—improves the security of the organization’s IT infrastructure. In addition, this emphasis helps accelerate the evolution of security from a reactive technology used to put out fires, into an infrastructure that enables business agility and the ability to pursue strategic business goals. To describe this evolution, Microsoft developed the Infrastructure Optimization Model⁵, a framework with which enterprise can quickly understand the strategic value and business benefits to the organization in moving from a “basic” level of maturity (where the IT infrastructure is generally considered a cost center) towards a more “dynamic” use, where

⁵ <http://www.microsoft.com/windowsserversystem/solutions/io/default.aspx>

the business value of the IT infrastructure is clearly understood and the IT infrastructure is viewed as a strategic business asset and business enabler. Microsoft's approach to security aligns with this model. From an organization starting with a single firewall, Microsoft can help evolve that into a pervasive, policy-based solution that enables the organization to proactively protect information and provide appropriate access to employees, partners, and customers.

By offering multi-level integration with existing IT infrastructure and simplified, centralized management, Microsoft Forefront business security products provide greater protection and control so that administrator can deliver a more secure environment for their organizations.

Related Links

For the latest information about the Microsoft Forefront family of security products for business, visit:

Microsoft Forefront: <http://www.microsoft.com/forefront>

Internet Security and Acceleration (ISA) Server 2006: <http://www.microsoft.com/isaserver/default.mspix>

Intelligent Application Gateway (IAG): <http://www.microsoft.com/isaserver/whale/default.mspix>

Forefront Server Security: <http://www.microsoft.com/antigen/default.mspix>

Forefront Client Security: <http://www.microsoft.com/forefront/clientsecurity/default.mspix>

To learn about other Microsoft security and security-related products, visit:

Operating Systems

Windows Vista: <http://www.microsoft.com/technet/windowsvista/security/default.mspix>

Windows XP: <http://www.microsoft.com/windowsxp/default.mspix>

Windows Server 2003: <http://www.microsoft.com/windowsserver2003/default.mspix>

Windows Server "Longhorn": <http://www.microsoft.com/windowsserver/longhorn/default.mspix>

Network Access Protection (NAP)

Network Access Protection (NAP): <http://www.microsoft.com/technet/itsolutions/network/nap/default.mspix>

Services

Exchange Hosted Services: <http://www.microsoft.com/exchange/services/default.mspix>

Information Protection

Rights Management Services: <http://www.microsoft.com/windowsserver2003/technologies/rightsmgmt>

BitLocker: <http://www.microsoft.com/technet/windowsvista/security/bitlocker.mspix>

Encrypting File System (EFS): <http://www.microsoft.com/technet/security/topics/cryptographyetc/efs.mspix>

Identity Management

Active Directory: <http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspix>

Certificate Lifecycle Manager (CLM): <http://www.microsoft.com/windowsserversystem/clm/default.mspix>

MIIS: <http://www.microsoft.com/windowsserversystem/miis2003/default.mspix>

Active Directory Federation Services (ADFS):

http://www.microsoft.com/WindowsServer2003/R2/Identity_Management/ADFSwhitepaper.mspix

Systems Management

Microsoft Operations Manager (MOM): <http://www.microsoft.com/mom/default.mspix>

SQL Server 2005: <http://www.microsoft.com/sql/default.mspix>

Systems Management Server (SMS): <http://www.microsoft.com/smserver/default.mspix>

Windows Server Update Services (WSUS): <http://www.microsoft.com/windowsserversystem/updateservices/default.mspix>

Developer Tools and Guidance

Security Development Lifecycle (SDL): <http://msdn.microsoft.com/security/sdl>

Visual Studio 2005: <http://msdn.microsoft.com/vstudio>