Microsoft

Security Watch

A QUARTERLY PUBLICATION

CONTENTS

CASE STUDIES
ADVERTISER-SPONSORED

SECURITY WATCH MAY 2003

This special advertising section was produced by the *Windows & .NET Magazine* Custom Media Group in conjunction with Microsoft. This supplement appears as an insert in the May 2003 issue of *Windows & .NET Magazine*. For information about Custom Media opportunities, contact Don Knox (dknox@winnetmag.com).

Develop a Secure Infrastructure with Microsoft's Security Guidance

Various organizations have put forth admirable effort to create security standards for Windows. However, security is not a one-size-fits-all prospect. Different enterprises have different risk levels, usability requirements, and compatibility requirements for previous versions of Windows still in use. Ideal security recommendations don't always work in the real world, where business must continue to flow and where organizations must continue to support a variety of technologies and version levels. Additionally, different server and workstation roles require tailored security configurations. All these issues affect what determines optimum security for each organization. Perspective is important also, because too often security is treated as a machine-by-machine issue when—given the tightly coupled nature of network components—security should be viewed from the top down, starting with the network. And in the current climate of blended threats, where malicious software exploits vulnerabilities from the kernel up through applications, a security strategy must include a coordinated effort that extends beyond the OS and network to other fronts such as desktop applications like Microsoft Office and Internet browsers. Finally, given the heavy demands that stretch IT staff at most organizations, taking advantage of every opportunity to automate security tasks is crucial so that you can achieve consistency and free staff for other pressing needs.

As part of the Trustworthy Computing Initiative, Microsoft is committed to providing customers with a set of security solutions that simplify the security processes associated with the assessment, deployment, and operations of Microsoft products. In this document, we will refer to this set of solutions as the Microsoft Security Solutions or MSS. Taking advantage of MSS doesn't require a huge upfront investment associated with learning a methodology or a commitment to doing things Microsoft's way, nor does it limit your technology options. MSS provides strategic, descriptive guidance (such as analysis methods and requirements planning) as the top layer that drives a lower layer made up of specific security settings and guidance. This approach lets you leverage the most valuable pieces of MSS for your organization but avoid getting bogged down with following a methodology for its own sake. If a specific MSS doesn't fit all your needs or match your environment, MSS enables you to use as much of the solution as makes sense for your organization while providing enough background information to customize the guidance for your own needs. In this way, in addition to using a specific solution, you can use a solution's tools and guidance more as broad solution enablers.

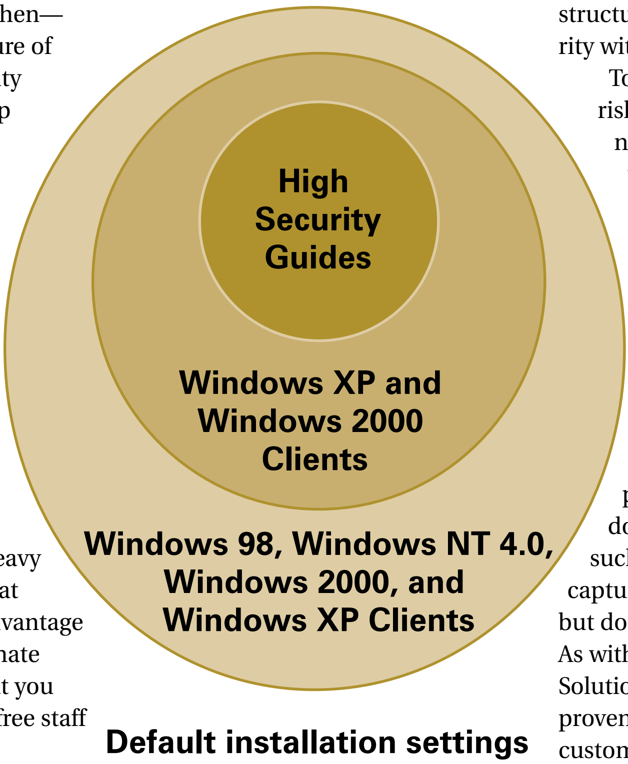

High Security Guides
Windows XP and Windows 2000 Clients
Windows 98, Windows NT 4.0, Windows 2000, and Windows XP Clients
Default installation settings

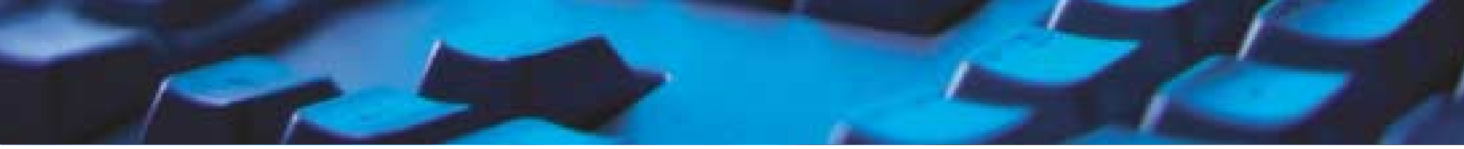
FIGURE 1: The 3 levels of increasing security prescribed by the Windows Server 2003 Security Guide

WINDOWS SERVER 2003 SECURITY GUIDE

One of the latest solutions released is the Windows Server 2003 Security Guide, which you can find at http://go.microsoft.com/fwlink/?LinkId=14845. Because the guide covers the full breadth and depth of security as it relates to Windows Server 2003, the guide has something to offer each role within IT, including architects, business decision makers, information security professionals, and frontline administrators. This guide will help Microsoft partners and customers better understand the different security options that are available to them—and will provide a structured path to help increase security within an organization.

To support the kaleidoscope of risk, usability, and compatibility needs that Microsoft's customers face, the Windows Server 2003 Security Guide defines three different levels of security guidance to provide a baseline for as many different customer environments as possible (Figure 1). The guide covers Windows Server 2003 security from the highest levels of planning and domain structure down to specific security settings such as practical audit policy that captures important security events but doesn't choke system resources. As with all Microsoft Security Solutions,, this guide is based on proven field experience gained from customers and partners, as well as from Microsoft engineering teams, consultants, and support engineers. This guide and its templates, scripts, and instructions have been tested and validated on real networks—and the guide includes the test documentation.

This guide offers not only classic hardening techniques such as locking down services, but also prescribes detailed instructions for using advanced technology such as using IP Security policies to block both internal and external attacks. To mitigate the practical constraints imposed by legacy technologies, the guide prescribes exact security settings for three levels of increasing security: environments required to support down-level clients such as Windows 98 and Windows NT 4.0 Workstation as well as Windows 2000 and Windows XP clients, environments that only have Windows 2000 and Windows XP clients, and environments that require the highest level of security possible. Besides providing detailed checklists to achieve each security level, the guide offers the security templates for each of the



pre-defined levels. To enable secure solutions tailored to fit types of servers, the guide prescribes additional configurations for establishing security baselines for each major class of server, including domain controllers, member servers, and Internet facing hosts. The guide also provides guidance for dealing with the different attack surfaces presented by network services such as DHCP, WINS, DNS, IIS, and important security servers such as Certificate Authorities and RADIUS servers.

TEMPLATES HELP BUILD SECURITY

To deal with the hundreds of security settings prescribed for each system, the guide provides pre-built security template INF files to automatically configure servers. The guide provides one security template for baselining domain controllers and a separate baseline for member servers. To further tailor security controls for different server roles, administrators can apply incremental templates on top of the baseline. For instance, the incremental, role-specific template for IIS servers strengthens file permissions on IIS's metabase and log files. Because the baseline templates enforce strict, "secure by default" settings (see the sidebar "The Microsoft Security Framework"), the incremental templates re-enable functionality where necessary to support the corresponding role. For example, the IIS template re-enables the IIS Admin Service and World Wide Web Publishing services. For servers that are part of an Active Directory (AD), administrators can simply import the templates into group policy objects linked to OUs created for each server role and thereby guarantee consistent, secure configuration for each type of server without leaving their workstations. When new servers are deployed they will automatically pick up their appropriate security settings. For servers that don't belong to an AD domain, administrators can still use the same templates by applying them through the Security Configuration and Analysis tool. Administrators can apply templates remotely to servers using scripts or Terminal Services.

For steps not supported by security templates, the guide supplies scripts that automatically apply many of the necessary changes. For instance, the guide includes scripts to automatically configure IP Security Policy filters to block all IP traffic by default and enable only traffic to the ports necessary to support each server role. For example, the guide includes a script that configures IP Security Policies for a Web server that blocks traffic all traffic except Web-related connections to ports 80 and 443, remote administration ports like 3389 for Terminal Services, and other ports to support authentication to domain controllers such as UDP port 88 for Kerberos. For the few steps that can't be automated, this guide clearly identifies any final steps that administrators must perform manually.

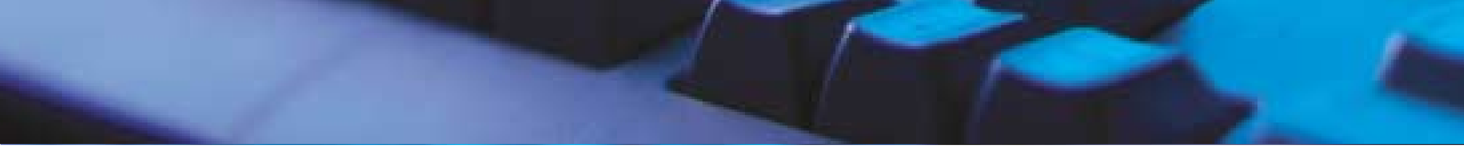
Because security is more than just making the right configuration tweaks, this guide also provides strategic, methodology-based guidance to help customers balance risk and usability needs according to the real business needs of an organization instead of against an arbitrary standard or subjective viewpoint.

This guide helps customers build a strategic security program by starting with an effective risk assessment of an organization. During risk assessment this guide steps a customer through eight areas for consideration: assets and their value, threats, potential losses, vulnerability assessment, countermeasure development, penetration testing, incident response, and cost/benefit analysis to determine the total cost of implementing the right level of overall security. Identifying assets includes not only hardware and software, but also less tangible business assets such as data, processes, transactions, and consumer trust.

Because security is more than just making the right configuration tweaks, this guide also provides strategic, methodology-based guidance.

INCORPORATING BEST PRACTICES FOR AD

This guide also helps you incorporate best practices into your AD design, from forests and domains to organizational units (OUs) and group policy objects (GPOs). For instance, this guide clearly steps you through the process of comparing the trust-related risks of including a domain in your forest or keeping it outside the forest. At the domain level, the guide provides a complete map for server management that ties everything together, from OUs and GPOs to administrative groups and the security templates described above. The sample OU structure, which you can adapt to local circumstances, starts with an OU called Member Servers. The Member Servers OU is an abstract level—meaning that, usually, no server accounts are placed directly in the OU. Instead, you create sub-OUs for each server role in your domain, including File and Print, Web, and Infrastructure servers that provide DHCP, WINS, and DNS services to the rest of the network. Then you simply import the pre-built baseline template file to a GPO linked to the Member Servers' OU and import the template file provided for each GPO linked to corresponding role-level OUs. This guide also shows how you can use the OU structure to



control administrative authority over each set of servers by delegating authority at the root level. This sample structure supports an important security principle, least privilege, by ensuring administrators have no more authority than necessary to perform their jobs. The guide shows how by properly using OU ACLs, GPO ACLs, and customizing permissions inheritance you can delegate authority appropriately without losing control of AD.

Because oversights in any phase of a project, from design through testing and rollout, can derail an otherwise well-planned project, the guide also provides detailed step-by-step planning, testing, and rollout advice—as well as many Excel or Word document job aids so that you can leverage MSS's experience to avoid learning things the hard way. Job aids test worksheets for server and domain functionality in conjunction with rolling out a security solution. Each test case describes the condition to be tested, provides step-by-step instructions for executing the test, suggests the expected results, and provides space to document actual results for each test run.

Because you must address security at multiple tiers within an organization, the Microsoft Solutions for Security will further provide guidance to establish a secure baseline for the client environment. This guidance will be focused on knowledge workers that use either desktops or laptops running Windows XP. The Windows XP Security Guide will contain information relevant to securing the default installation through Group Policy to secure Microsoft Visual Basic for Application settings, Internet Explorer security, Office XP deployments, and the use of the newly introduced software restriction policies.

Late last year, Microsoft released a solution focused on securing Windows 2000 Server. This guidance was created to provide an end-to-end guide to securing a Windows 2000 environment. It covers assessment, mitigation, and operation—several of the key tenets of getting secure and staying secure. The guide is focused on securing a common enterprise configuration, while also providing additional background information to allow an easy customization to fit any specific environment. The Securing Windows 2000 Server solution can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/windows/secwin2k/default.asp.

You can find out more information about future solutions from MSS at http://www.microsoft.com/business/solutions/. In the meantime, the Windows Server 2003 Security Guide is a key delivery on Microsoft's promise to help customers provide guidance to securely deploy Microsoft's products. Whether your organization already has a mature security strategy and just needs field-proven technical details for securing Windows Server 2003 in various roles, or if your organization needs help putting together a scientific methodology for your risk management program, you can pick and choose the portions most valuable to your organization and its current security landscape and thereby re-use the experience and testing captured by the Windows Server 2003 Security Guide.

The Microsoft Security Framework

In January 2002, Bill Gates issued a call to action challenging Microsoft's employees to build a Trustworthy Computing environment for customers that is as reliable as the electricity that powers our homes and businesses. The four goals of Trustworthy Computing are security, privacy, reliability, and business integrity. Microsoft has created a framework to track and measure its progress in meeting the security goals and objectives of Trustworthy Computing: secure by design, secure by default, secure in deployment, and communications (SD^3+C). A detailed white paper is available at http://www.microsoft.com/security/whitepapers/secure_platform.asp. The following outlines this security framework:

Secure by design

- Secure architecture
- Security aware features
- Reduce vulnerabilities in the code

Secure by default

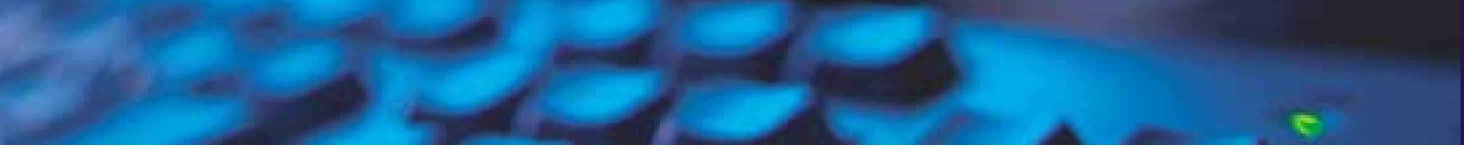
- Reduced attack surface area
- Unused features off by default
- Only require minimum privilege

Secure in deployment

- Protect, detect, defend, recover, manage
- Process: How to's, architecture guides
- People: Training

Communications

- Communicate the Microsoft security commitment and milestones
- Participate in the security community
- Microsoft Security Response Center



Secure Mobile Access is Possible

by Randy Franklin Smith

Without a doubt, to remain a nimble competitor you need to support mobile and wireless access. Businesses need any time, any device access over any connection so that their employees always have access to business-critical applications. Being away from the office is no longer an excuse for not being able to access information. Additionally, companies are cutting costs and recovering office space by sending their workers back out into the field and to their home offices. Wireless access helps companies be more nimble as they grow or relocate or need additional office space on demand. With no wires to pull you can quickly get up and running in a new space and start conducting business.

And without a doubt, you need to provide secure network access. Authentication and encryption become a much larger issue when your transactions and confidential information is traveling over the Internet or the airwaves. Once you implement wireless or remote access, bad guys don't need to breach your firewall or physical security to attack your network. To understand that the bad guys are savvy to the risks, look on the Internet to see the amount of attention being paid to war driving, in which someone drives around office buildings with a laptop and wireless card searching for networks to breach.

OUT-OF-THE BOX SUPPORT FOR SECURE WIRELESS ACCESS

But how do you provide secure mobile access without breaking the bank? If you already have Windows deployed, the answer may be staring you in the face. Microsoft has provided out-of-the-box support for secure remote access by providing built-in functionality that supports all the VPN and wireless IEEE-defined protocols and that works with industry-leading hardware vendors that have standards-based offerings. This article outlines the basic components and steps to set up secure remote and wireless access so that you can see what's possible and what it takes to accomplish it.

With the Windows platform you get remote functionality with the support of IPSec, L2TP, and PPTP for virtual private networking and 802.1x for wireless access. Built on non-proprietary, industry standards Windows gives you flexible hardware options and support for future opportunities. Through out-of-the box availability of Internet Authentication Service (IAS), Active Directory (AD), and Certification Authority (CA), Windows secure wireless and VPN solutions let you leverage investments you might already have made.

802.1X IS KEY TO WIRELESS SECURITY

802.1x is the key to securing a wireless network. The original Wired Equivalency Protocol (WEP) was shown to be vulnerable to a variety of attacks, most having to do with how WEP handled encryption keys and authentication. Microsoft discovered in working with customers, that individuals were exploiting WEP authentication vulnerabilities and attempting to trick wireless users into giving up their credentials by putting wireless access points (WAP) on the corporate network. 802.1x addresses WEP vulnerabilities by augmenting the broader 802.11 wireless protocol (a.k.a., Wi-Fi) to provide authentication and encryption key services. 802.1x has built-in flexibility for different authentication methods such as smart cards or biometric devices, which Microsoft has taken advantage of to give customers flexible options for wireless security.

To implement 802.1x, you aren't required to migrate all your servers to Windows Server 2003. You need only migrate your IAS server, which can communicate with Windows 2000 Server domain controllers. 802.1x not only solves the technical security problems with WEP, but also takes advantage of Windows XP and Windows Server 2003's support for 802.1x to easily integrate authentication and access control of your wireless network into your existing domain, thereby leveraging your investment in AD and Windows technology to reduce rollout costs, ensure privacy, and ease the management of credentials used for wireless access. Please note that a licensing limit of 50

clients exists for IAS standard server. Businesses that have more than 50 clients (e.g., AP, switches, gateways) can move to the Enterprise edition server, which has no such limit.

PEAP SUPPORT OFFERS SEVERAL OPTIONS

PEAP, or protected EAP, is a standard draft presented by Microsoft in conjunction with Cisco and RSA. PEAP offers several options for wireless authentication that cater to varying size and security requirements of different companies. You can use certificate-based authentication or biometrics, but the best value provided by PEAP is that unlike EAP-TLS, PEAP does not require setting up a full-fledged PKI to provide certificates for clients and servers. Some companies need password-based wireless security to maintain a simple infrastructure and keep deployment as simple as possible.

PEAP lets you use password-based authentication without the risks normally associated with sending password-based challenges and responses over the network. PEAP creates a tunnel from the server certificate and uses MS-CHAP v2 within that tunnel. Also, PEAP can use certificates on both ends if you want to limit connectivity to authorized client computers not just authorized users.

To set up a wireless access using PEAP with MS-CHAP-V2, you a need an 802.1x-compliant NIC for your Windows XP workstation, an 802.1x-compliant WAP connected to your LAN, and Windows Server 2003 running IAS and a member of your AD domain. You might also need to purchase a certificate for your IAS server from a third-party PKI—or you can issue your own certificates by installing Certificate Authority (CA) on one of your servers.

With PEAP and the Windows platform, you can start using new Windows XP computers on your wireless network straight out of the box. You simply insert the wireless NIC, boot the workstation, login with a local account, and disable validation of server certificates for wireless connections. After you've entered your user name and password, you're workstation is automatically connected to the wireless network. The best part is that you can do all this for the cost of your wireless NIC cards and wireless access points. Everything else is included with Windows XP and Windows Server 2003. For more information about Windows wireless networking please, visit www.microsoft.com/wifi.

SECURE REMOTE ACCESS

Windows Server 2003 provides exciting opportunities to create highly secure remote access to mobile users whether they are connecting through a dial-up ISP from a hotel, via cable or DSL from home, or from within another company's LAN. With Windows 2000 Server or Windows Server 2003 as your Routing and Remote Access Server (RRAS), you can provide strong two-factor authentication and IPSec-based encryption. The key is Window's support for L2TP with IPSec for encryption. L2TP/IPSec provides certificate-based authentication access to users.

Windows 2000 supports L2TP/IPSec VPN clients but not when a NAT boundary lay between the client and server. This was a problem for clients that needed to VPN into their network when they were connected to some other company's LAN and had to pass through that company's firewall to get to the Internet. Most firewalls use NAT to hide the internal network but because NAT changes IP addresses, IPSec breaks when its integrity-checking logic checks for changes to packets. Therefore, Microsoft enhanced Windows Server 2003 to support NAT-T. NAT-T is an extension to L2TP that, upon detecting an intermediate NAT boundary, switches over to encapsulating IPSec inside UDP packets. In this way, the IPSec packet makes it across the firewall intact. Soon, this functionality will also be available for Windows 2000 Server.

SOLUTION ENABLEMENT (Patterns and Practices)

With the Windows platform you get flexible, standards-based security for remote and mobile access. By leveraging your existing AD infrastructure, you get increased security and decreased costs through unified identify management, monitoring, and automated public key infrastructure.

Microsoft offers out-of-the-box support for secure remote access by providing built-in functionality that supports all the VPN and wireless IEEE-defined protocols and that works with industry-leading hardware vendors that have standards-based offerings. Through out-of-the box availability of IAS, AD, and CA, Windows secure wireless and mobile solutions let you leverage investments you might already have made. And all this functionality comes as part of a company's normal Windows and client access licenses.

Microsoft is building a comprehensive set of planning, deployment, and operation guidance around secure mobile access. This guidance, or Patterns and Practices, is based on extensively tested and successfully implemented lab and customer deployments. These materials are designed to take the guesswork out of deploying and managing an end-to-end mobile access solution based on Windows Server 2003. To download guidance, please go to www.microsoft.com/technet. ◆

Randy Franklin Smith is a contributing editor for *Windows & .NET Magazine* and the primary instructor and course developer for MIS Training Institute's Windows NT/2000 security program.
His firm, Monterey Technology Group, provides security consulting.

Wireless Network Based on Windows Server 2003 Increases Productivity

Fortis Health looked at several possible solutions for a wireless network that would combine high levels of security with outstanding manageability. Microsoft Windows Server 2003 allowed the company to meet its goals and increase employee productivity. Fortis Health was so impressed by the performance of Windows Server 2003 in its wireless solution that it is implementing the operating system company wide. The company also plans to switch to many other Microsoft technologies, such as Microsoft Exchange Server and Microsoft SQL Server.

THE SITUATION

Offering health insurance coverage to more than a million people nationwide, Fortis Health, based in Milwaukee, Wisconsin, is a leading provider of individual, small group, and specialty health insurance products. Things change quickly in the health insurance industry and Sal Valenti, IT Manager at Fortis Health, is tasked with keeping 3,000 employees connected to the company's network, whether they are working at their desks, videoconferencing, or moving to new offices. To keep employee productivity high, the Fortis Information Technology (IT) group needs a network infrastructure that combines maximum mobility with minimal downtime, while it maintains the high levels of security needed to safeguard confidential health information.

The company's first step toward creating a wireless network was to implement Active Directory (AD). "We liked what we saw with Active Directory," Valenti says. "It was a cost-effective solution that gave us the flexibility to easily move people around departments and into different parts of the company. It's easy to use, it's easy to configure, and it makes it easy for us to use other key Microsoft technologies."

Best of all for Valenti, AD worked well with wireless networking. "There wasn't even an overlay," he says. "No wires coming to the desktop for networking." Employees using wireless-enabled portable PCs can be completely connected anywhere in the building and have all of their information instantly available from wherever they are.

"We rolled out Active Directory and we thought it was great," Valenti says, "but we wanted to find a way to achieve even higher levels of security without sacrificing the great features and flexibility we got with Active Directory."

The only other high-security authentication that Fortis Health knew about at the time was EAP Cisco Wireless (LEAP), but Cisco's LEAP protocol created problems for Fortis Health. . "LEAP simulates a broken cable when the user isn't logged on," Valenti explains," which means that we weren't allowed to deliver applications to a workstation after hours." Another stumbling block with Cisco's LEAP protocol was that it delivered security in a way that made it extremely difficult to execute frequent password changes, which are essential at Fortis Health because of the highly confidential information found in the insurance industry. Overall, Valenti says, "LEAP didn't give us the authentication capabilities that we were looking for."

THE SOLUTION

Fortis Health started doing more research about the best way to achieve high security in a wireless network and Valenti asked Microsoft how to solve the problem. When he learned about the Protected Extensible Authentication Protocol (PEAP) and discovered that many companies were implementing PEAP instead of Cisco's LEAP protocol, he knew he had found his answer. "PEAP gave us the capability to change user workstations after hours when people were logged off," he says. "It solved our password issues as well, and it provided a very secure way to authenticate to a wireless network because it is certificate-based."

PEAP is an Internet Engineering Task Force proposed standard that is supported by many wireless hardware vendors, but Microsoft Windows Server 2003 is the only server operating system that works with PEAP and also supports Internet Authentication Service (IAS) with certificate authentication. "Because Windows Server 2003

is optimized for PEAP, which we needed to keep our wireless network secure, we started looking at all of the other functionality and benefits of Windows Server," Valenti says. "We were impressed." So impressed that Fortis Health is making a complete switch from Novell Unix-based operating systems to Microsoft Windows Server 2003. "We want to be ready to use new Microsoft technologies as they become available," Valenti explains.

Fortis Health is also on its way to full wireless networking. "We now have a completely wireless network in one building that houses 700 people, and we are partially wireless in the main building, where another 800 people work. Some areas still need 100-Mbps switches because of the type of work that's done there—people using high-traffic workstations—but it's fair to say that our core network is wireless or soon will be."

Valenti offers a verbal diagram of Fortis Health's wireless network solution: "We start with a workstation, which is part of the Active Directory domain. When a technician boots the workstation, the wireless card communicates with the network and goes directly to that IAS server and says, 'I'm a member of this domain.' The IAS server uses its certificate with its domain controllers to authenticate that workstation. To access network resources, users have to log on with an ID in Active Directory."

One of the biggest advantages of this solution, according to Valenti, is the capability of authenticating and upgrading workstations overnight, as long as the user logs off and the computer is left on. This eliminates costly downtime during the workday.

Fortis also uses wireless networking with Windows CE-based Compaq iPaq and Palm mobile devices. "We link them into our problem-reporting system," Valenti explains. "Technicians receive trouble tickets through our wireless network, over Palms and iPaqs. Technicians can use Terminal Services clients to reboot servers and do remote administration, even if they are away from their desks. It has made us much more responsive."

THE BENEFITS

Enhanced Security

From Sal Valenti's viewpoint, security is the biggest benefit of using Windows Server 2003 as the basis for wireless networking. Health and medical information is highly confidential, so high levels of security are essential. Valenti looked into many other types of wireless communication but found that most were not very secure.

While Cisco's LEAP provided the security that Valenti was looking for, it had manageability issues that were unacceptable. "LEAP was more secure than many other options, but it was harder to manage because it changes algorithms so frequently," Valenti explains. "It gave us the level of security we wanted, but it was almost too secure in a sense. Changing passwords was a difficult process."

According to Valenti, PEAP offers the high level of security that Fortis Health needs without the negative aspects of Cisco's LEAP. Workstations are easier to manage, and changing passwords is a much simpler process.

Wireless networking makes it easier for employees to be productive on the go. "With a laptop and Windows Instant Messenger, we can communicate immediately, without interruptions by phone," Valenti explains. "We also do a lot of video conferencing with people who are out of town. I know I can go to any conference room, turn on my portable PC, and, because we're set up for wireless communication, easily do videoconferencing and share files.

"We move employees around a lot, and we attend a lot of meetings," he continues. "Wireless networking makes it very easy to collaborate in meetings, check e-mail, and review your calendar to know where your next meeting will be. It's such a timesaver to have all of your information at your fingertips."

Increased Productivity

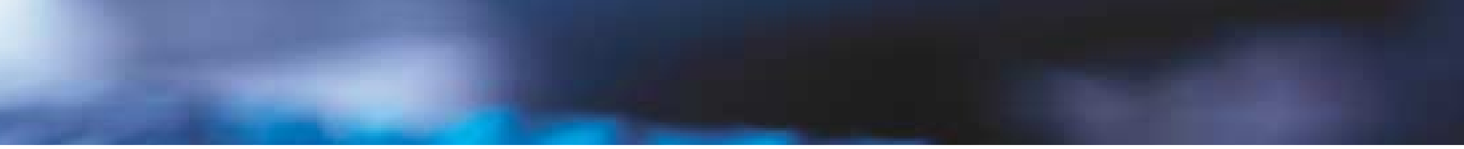
These features have made Fortis Health employees more productive, and the benefits extend to the IT staff. "Because Windows Server 2003 with PEAP is easier for us to manage, it makes our technicians more productive. By eliminating problems with password changes alone, we've significantly reduced the amount of employee downtime and the number of help-desk calls. This results in higher productivity for end users and technicians."

FUTURE PLANS

The year 2003 will be a busy one for the Fortis Health IT staff. Fortis Health currently has two servers running Windows Server 2003 with PEAP, plus one 64-bit ES 7000 running Windows Server 2003, and Valenti expects to expand to at least 20 servers running Windows Server in 2003.

As part of the company's plan to standardize on Microsoft technology, Fortis Health will replace its Novell Unix-based operating system with Windows Server 2003 and will implement Windows Server 2003 domain controllers. Valenti says the company is also starting its migration from Novell GroupWise to Microsoft Exchange Server. Other plans include implementing Microsoft BizTalk Server and Microsoft Content Management Server, as well as Microsoft Host Integration Server to streamline the connection between the company's mainframe and desktop computers.

According to Valenti, Windows Server 2003 is the catalyst for these big changes. "We were so impressed with Windows Server 2003, Active Directory, and IAS with PEAP that we're looking forward to using many new Microsoft technologies as they become available," he says. ◆



Microsoft Delivers Identity Management Solution

If yours is like most companies today, you struggle to manage user accounts, passwords, authorization, roles, and groups across their many platforms and applications. Projects are delayed and opportunities are lost while businesses wait days for user accounts and access to be provisioned for new employees, contractors, and business partners. Security suffers when employees or other relationships are terminated but the business fails to spot and disable all accounts held by the former user, which leads to compromise by individuals now working for a competitor or damage by disgruntled persons. Users, burdened with many accounts and varying password requirements and change intervals, often resort to unsafe practices such as easy-to-guess passwords or writing down passwords. Security suffers further when, because of the complexity and expense involved in handling support calls for forgotten passwords, businesses shy away from strong password requirements and lockout policies. Further breaches occur because of inconsistencies in access control and authorization when administrative groups are not notified of job or responsibility changes. Costs grow because managers, IT professionals, and HR staff must spend increased time entering and updating user data, setting up user accounts, and adjusting user rights on multiple systems. These problems are driving the growing interest in identity management.

Identity management is more than single-signon (SSO) or password synchronization. Identity management is a set of systems and processes for managing the lifecycle of user accounts; credentials; identity information such as department, job title, contact information; and authorization data such as groups, roles, and access control lists. Microsoft offers a solid and powerful identity management infrastructure that uses Active Directory (AD) as the foundation. All of Microsoft's products, such as Exchange Server, Windows file and printer sharing, SQL Server, and IIS, already support integrated identity management and single signon with AD. Many non-Microsoft products already include some level of built-in support for AD or single signon to your Windows infrastructure. To embrace all your applications and systems and connect them to AD, you can use Microsoft Metadirectory Services (MMS). With MMS and AD you can implement an elegant, industrial-strength identity management solution that lets you nimbly respond to new information-sharing and user-provisioning needs, reduce costs associated with identity information maintenance and provisioning, and password management while greatly improving security.

ACTIVE DIRECTORY: YOUR PLATFORM FOR IDENTITY MANAGEMENT

Any application or system that supports LDAP and one of Windows' authentication methods—including Kerberos, NTLM or certificates—can integrate with AD without MMS. AD is an LDAP v3 directory that serves as the organization's core repository for users. Other applications and systems can leverage AD for storing and accessing user account information through Light Weight Directory Access Protocol, the industry standard, non-proprietary protocol for access to LDAP-based directories. Applications and systems can also take advantage of AD for authentication using Kerberos, NTLM, or certificates. Kerberos is especially useful because it is designed specifically to provide password-based mutual authentication between clients and servers and is likewise an industry standard, non-proprietary protocol.

But to support the complex and multi-sourced nature of identity information in many environments, you need to tie everything together to provide true identity management. Consider some of the issues. To tie together every identity component, you must include telephone PBXs, HR systems, and physical security systems such as ID badges and proximity cards. Each of these systems is the authoritative source for certain attributes of a user's identity. The HR system may provide the user's full name, employee ID, job title, department, and manager. The PBX system is the authoritative source for the user's telephone numbers and the facilities security system is the authorita-

tive source for badge numbers and proximity card IDs.

In addition, each system's user directory has fields that store identity information common to all systems, such as username, name, description, ID number, and department. Administrators often make important security decisions based on the copy of that information stored within each system. The labor involved in manually keeping such information synchronized between each system is prohibitive. But even programmatic attempts to synchronize the information are challenging because each system defines the same information in slightly different ways. For instance, some systems use separate fields for first, middle, and last names. Other systems define one field for the user's full name. Still others have a middle initial field instead of full middle name. Similar problems exist with logon name and address formats. MMS, however, can amalgamate identity information from multiple sources into a unified view of a user's identity and then distribute that information to all interested parties—parsed and formatted as needed.

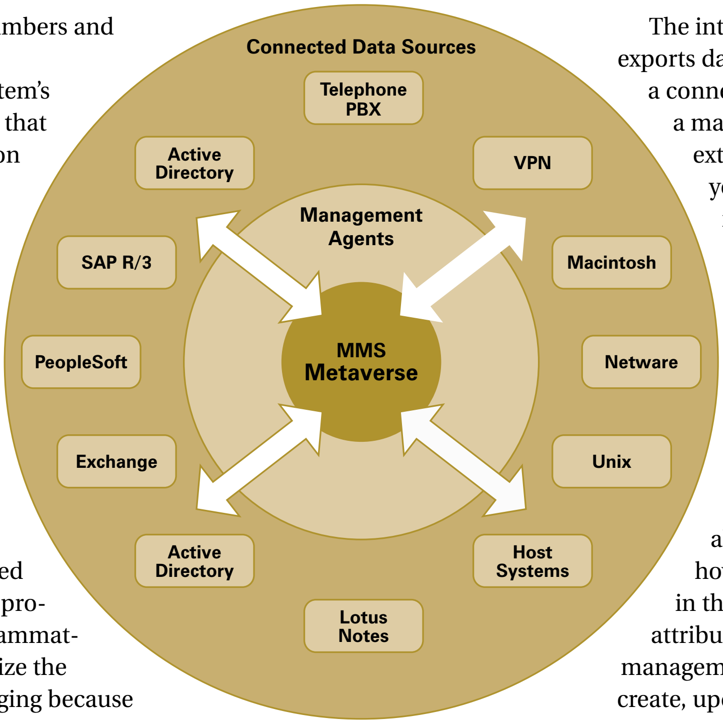


FIGURE 1: MMS can provide enterprise-wide identity management

A TIRELESS MIDDLEMAN

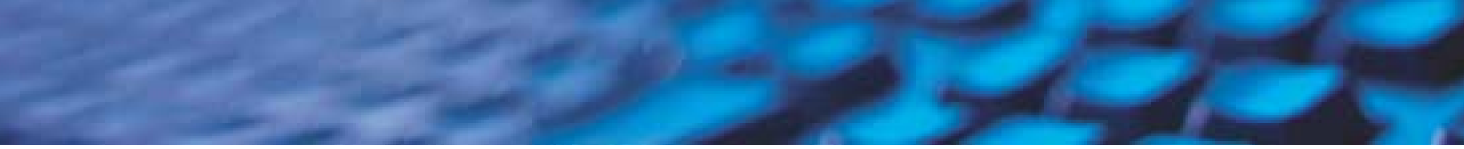
In the past, efforts to implement a single directory or classic single signon solution often ground to a halt in the face of the complexities and political challenges involved in centralizing the identity management process. MMS gives you the capability to manage identities while minimizing the impact on your current processes. HR, telecom, and mainframe staffs don't have to give up control or learn new systems. Instead, MMS brokers identity information in and out of what it calls the "metaverse." The metaverse is a set of tables within MMS that contain the integrated ("joined") identity information from multiple connected sources. All identity information about a specific person, which is stored in multiple connected sources, is synthesized into a single view of a user's identity in the metaverse.

MMS provides a non-intrusive, yet intelligent, identity management infrastructure for your entire enterprise (Figure 1). To integrate an application or system into this infrastructure, you define the system or application as a connected data source to MMS. Out of the box, MMS supports popular LDAP directories such as Sun ONE Directory and Novell eDirectory; HR, ERP, accounting applications such as PeopleSoft and SAP R/3; groupware and workflow applications such as Exchange Server and Lotus Notes; databases such as SQL Server and Oracle; and other repositories in various formats such as flat files, LDIF, XML, and delimited text files.

The intelligence that imports and exports data between the MMS and a connected data source is called a management agent. MMS's extensible architecture lets you plug additional management agents, even customized ones, into the MMS infrastructure. A management agent understands how to find, access, and update identity information in its associated connected data source. A management agent contains customizable rules that determine how the agent maps attributes in the connected data source to attributes in the metaverse. A management agent knows when to create, update, or delete objects in the connected data source based on changes to the associated objects in the metaverse. Also, a management agent can recognize changes to objects in the connected data source and translate them to the appropriate actions in the metaverse, which then triggers updates from the metaverse to other connected data sources. In addition, the management agent can trigger changes to passwords associated with the connected system.

ORCHESTRATING IDENTITIES ACROSS YOUR ENTERPRISE

A multitude of real-world scenarios demonstrate the power of Windows Server 2003, AD, and MMS working in concert with all your other technologies. Consider the sequence of events that can happen automatically when a new employee, Bob, is hired to work in Purchasing. The new hire HR representative, John, creates an employee record for Bob in the PeopleSoft human resources application and fills in Bob's personal information, department, manager, and job title. Next, the management agent for PeopleSoft discovers Bob and exports his information to the metaverse,



where a new user object is created for Bob. Next, the AD management agent sees Bob's new object in the metaverse and creates a new user object in AD, filling in the Address and Organization tabs of Bob's AD user object. Using the department originally assigned to Bob by HR, the AD agent adds Bob as a member of the Purchasing Dept. group in AD. At the same, time a customized management agent automatically generates emails to Workstation Support, Facilities Services, and Telecom, notifying them that Bob has been hired to work in Purchasing and that he reports to Sally.

A technician from Workstation Support receives the email and contacts Sally regarding Bob's workstation or laptop needs. The technician images the proper computer using a basic image that includes Windows 2000 or XP Pro and any company-wide applications such as Microsoft Office and virus-scanning software. The technician joins the computer to the domain, places the computer object in the appropriate OU, and fills in the computer's "managed by" field with Bob's AD user object account, which was created earlier by the AD management agent. The technician assigns the computer's property tag number to Bob's employee ID in the asset management system but does not fill in all of Bob's other information, such as department or phone number.

A technician in Telecom contacts Sally to find out where Bob's extension should ring to and creates an extension in the PBX for Bob. The PBX's management agent exports Bob's office phone number to the metaverse, where it then cascades to all affected systems, including AD, HR, and asset management. Someone from Facilities Services visits Sally to arrange a cubicle for Bob and then updates the facilities management application with Bob's building, floor, and cubicle code and mail stop number. This information flows into the metaverse and updates all connected data sources that accommodate those attributes. While this is happening, John escorts Bob to the facilities security office where he is photographed and given a photo ID badge that also doubles as a proximity card. (You can even implement triple-use tokens that include smart card logon capability—all managed by MMS.) The proximity card admits Bob to areas associated with his department in the physical security system. Next, John takes Bob to the purchasing department and reintroduces him to Sally. Sally shows Bob his cubicle and computer and lets him know he can logon initially with his Social Security number.

MMS provides a non-intrusive, yet intelligent, identity management infrastructure for your entire enterprise.

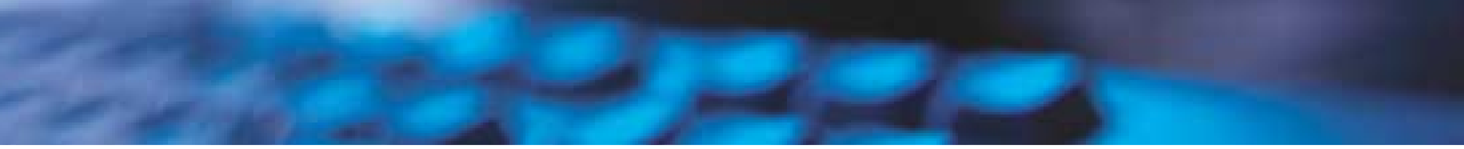
AUTOMATIC DESKTOP CONFIGURATION

When Bob turns on his computer, the computer boots up, contacts AD, and then applies any Group Policy Objects (GPOs) linked to the OU where his computer is located. The GPO configures Bob's computer with standard security settings and enrolls the computer with appropriate certificates. When Bob logs on, he is immediately required to change his password. To determine which group policy objects should be applied to Bob's desktop, his workstation analyzes the OU and groups Bob was placed in by MMS. The GPO automatically installs the SAPGUI so that Bob can connect to SAP and configures desktop restrictions that reflect Purchasing department policy. Finally, the workstation starts a PowerPoint slide show with audio that acquaints Bob with the company's standard applications, such as Outlook, Exchange folders, and intranet portals for benefits and office supplies. Next, Sally acquaints Bob with department-specific Exchange folders, Sharepoint sites, and shared folders and printers on the network. Bob automatically has access to these general department resources by virtue of his membership in AD's Purchasing Dept. group.

As Bob orients himself, Sally logs on to her workstation and opens a Microsoft Management Console (MMC) that displays all the subdepartmental groups for her area of Purchasing, which is Service and Outsourcing Management (SOM). These sub-departmental groups, which reflect different roles and teams, reside in the Groups\Departmental \Purchasing\SOM OU in AD. A group, Purchasing-SOM Manager, of which Sally is the only member, has been delegated authority to manage group membership of that OU. Sally adds Bob to the appropriate groups according to his specific roles and initial responsibilities. These groups automatically give Bob access to additional resources on Windows servers and Exchange folders, as well as transaction codes within SAP. Later that day, management agents export and import attributes from the metaverse so that each connected data source is updated with all of Bob's identity information. Ultimately, you can find Bob's badge number, mail stop, location, phone number, assigned laptop, and so on, in any system or application that maintains such fields for such attributes.

DISABLE USER ACCOUNTS EASILY

The same day, Internal Audit identifies the employee responsible for ongoing theft of company property as Jenkins. The director of Internal Audit contacts HR, which places Jenkins on



suspension in PeopleSoft. Rules in MMS go into action, immediately disabling all accounts for Jenkins, as well as his proximity card and smartcard for VPN access. Because the company's wireless network uses 802.1x, integrated with Internet Access Server (IAS) and AD, Jenkins automatically loses wireless access. Jenkins also loses access to the legacy application on the mainframe, even though accounts on this system are provisioned manually. The management agent for the legacy system sees the change in Jenkins's object in the metaverse, searches the legacy system for an account with the same employee ID, and disables the account.

Also, at 12 a.m. that morning, a contractor's user account in AD expired according to the term of his contract. The expiration cascaded throughout all MMS-managed systems, disabling the contractor's access. If the contractor is still active, his accounts can be re-enabled using a Microsoft Management Console (MMC) designed for the group in Purchasing that handles contractor and consultant relationships. Back in HR, John processes a job change for Rick from Engineering to Technical Sales Support. Wheels in MMS start spinning and the AD management agent removes Rick from all groups associated with Engineering and adds him to the Sales Dept. group. The Sun ONE management agent removes John's access to confidential engineering workstations. Other MMS rules generate emails similar to those generated when Bob was hired, so that Rick's new workspace, phone, and so on, can be provisioned.

SOLUTION ACCELERATOR FOR IDENTITY MANAGEMENT

The Microsoft's identity management solution provides all the functionality described above and more. MMS 2003 requires Windows 2003 Enterprise Edition and SQL Server Enterprise Edition. For deeper integration and single signon capabilities, you can implement specialized technologies from Microsoft such as Services for Unix, Services for Netware, Services for Macintosh, or Host Integration Server. MMS includes password management options such as a single-point, Web-based password administration application (Figure 2) that allows either help desk or user-initiated password reset, or commercial solutions such as M-Tech's P-Synch product. MMS provides clear audit trails so that you can audit sensitive operations such as password resets or track the lineage of data as changes flow back and forth through the metaverse.

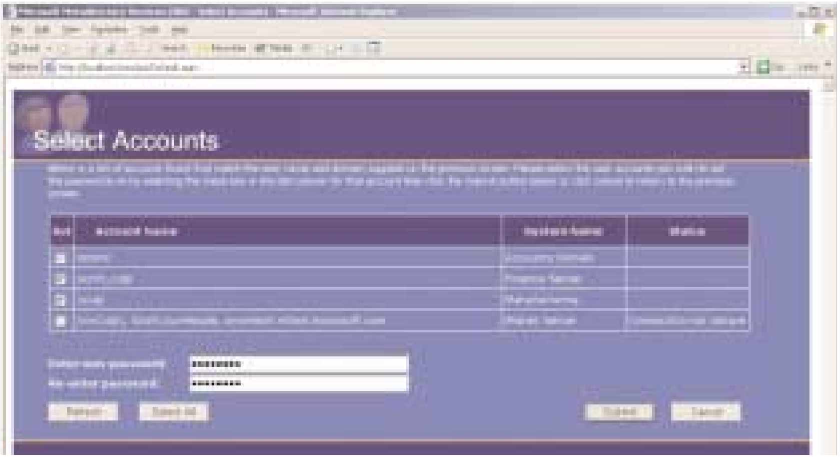


FIGURE 2: MMS password management options

You can use Microsoft identity management tools—including AD and MMS—to build a secure, cost-effective identity management solution

You can manage and extend MMS by using Visual Studio and Windows Management Instrumentation. As your company's computing environment grows increasingly complex with the addition of new systems, new connections to the outside world, and new security risks, managing identity across your entire organization becomes more and more critical. You can use Microsoft identity management tools—including AD and MMS—to build a secure, cost-effective identity management solution that gives your organization more freedom to nimbly exploit new information-based opportunities without sacrificing security.

Microsoft is working with PricewaterhouseCoopers LLP to build a comprehensive set of planning, deployment, and operation guidance for identity management. This solution accelerator is based on extensively tested and successfully implemented lab and customer deployments. These materials are designed to take the guesswork out of deploying and managing an end-to-end identity management solution based on Windows Server 2003 in an heterogeneous enterprise. This solution, focused on Web Single Sign-on, Windows Single Sign-on, and Enterprise Reduced Sign-on, will be available in July at http://go.microsoft.com/fwlink/?LinkId=14843. ◆

Barclays Global Investors Benefits Greatly from AD Implementation

As a leading financial services company, Barclays Global Investors (BGI) grows by using its global reach and applying real-time market knowledge to transform its intellectual property into innovative products and services for its institutional and corporate clients. BGI provides these offerings online as well as at offices in North America, Europe, and Asia.

BGI was challenged by a highly decentralized IT infrastructure that consisted of seven data centers with a mixed infrastructure composed of Microsoft Windows- and Unix-based servers, and that resulted in frequent authentication-related network and application access delays and long lead times to get new solutions deployed with appropriate security mechanisms. This resulted in decreased availability of corporate data and increased the time end-users needed to get information to customers.

THE SOLUTION

Upgrading and maintaining BGI's decentralized IT system in a phased deployment would require replacing redundant hardware and maintaining redundant services. Instead, BGI decided to migrate to a Windows 2000-based solution that improved employee productivity by making security, data management, and network administration more efficient. This would also cut costs by eliminating redundant hardware and IT support, and would improve the agility of BGI's IT department to quickly deliver new solutions integrated with Windows 2000 and Active Directory.

The redesign consisted of consolidating data center-based IT resources into one Active Directory domain and converting the dispersed authentication, security, data management, and administration operations into a single centralized process, all managed from a single Active Directory interface enhanced by NetIQ's Directory and Resource Administrator tool (DRA), resulting in improved management.

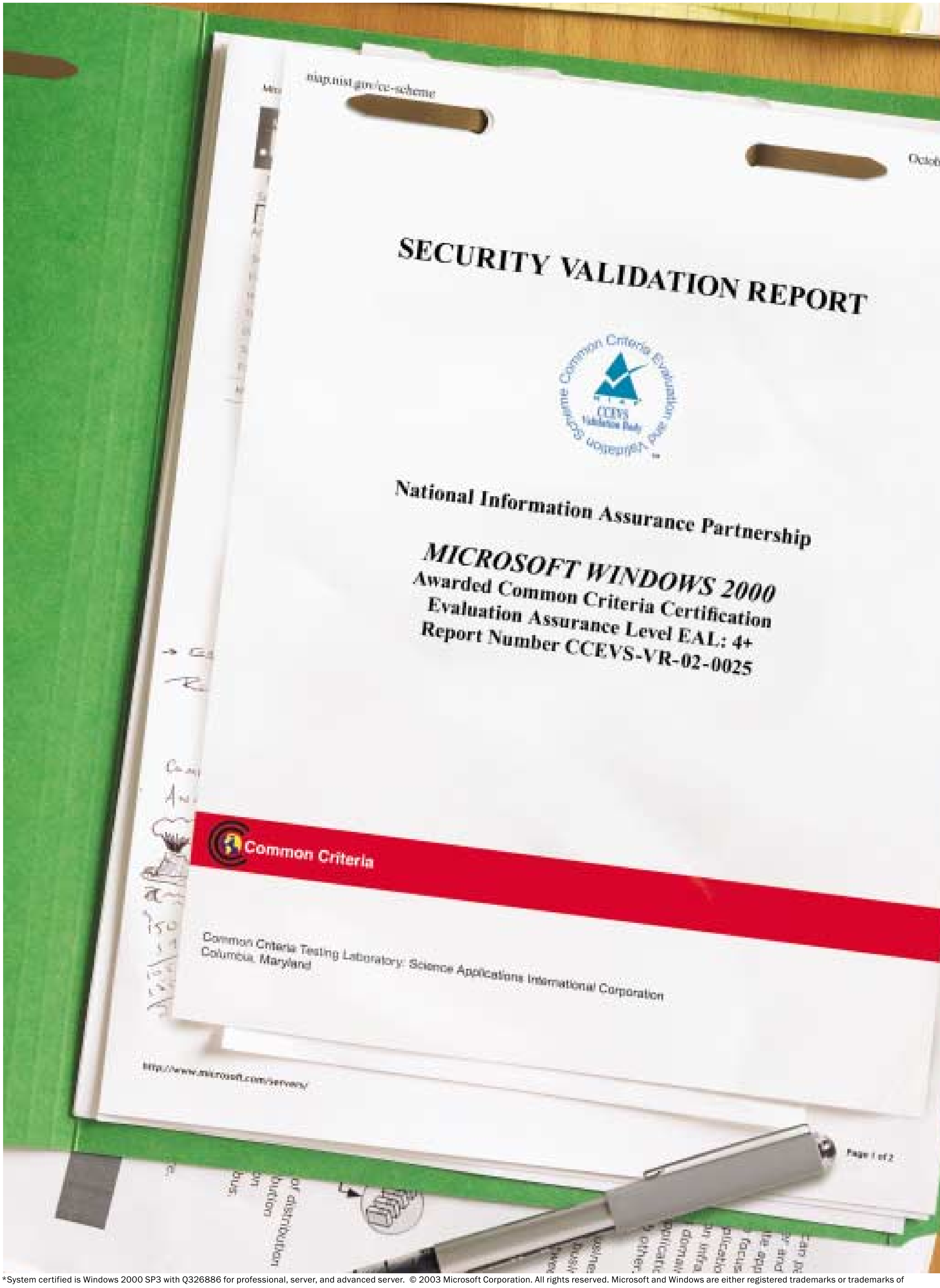
BGI used the Rapid Economic Justification (REJ) framework to assess the business and IT benefits of its new Active Directory infrastructure. The REJ validated that by implementing the new infrastructure, BGI could reduce overall IT security administration costs by 38 percent, reduce end user time spent on new application installs by 60 percent, and decrease authentication time by 30 percent to 48 percent, based on the number of heterogeneous platforms integrated over time. The REJ identified a reduction of up to 23 percent in the user administration time required due to the ActiveViews capability in NetIQ's DRA tool. This allowed administrators to view and manage users in intelligent new ways.

AD PROVES ITS VALUE

Jeff Shore, Manager of Intel Systems at BGI, explained, "The REJ showed us that, while Active Directory supports many of our revenue-generating activities, its greatest value comes from cost avoidance and cost reduction. We determined that every dollar saved or avoided by Active Directory and NetIQ was either adding a dollar of pure profit to the company's bottom line, or adding a dollar of immediately available funding for other IT projects. By reducing redundant services and literally pulling the plug on servers, we were able to both save the company money and fund new, revenue-generating projects."

"To build the global platform, we need the same desktop in every location, a single domain, a single point of management, and single sign on," said Paul Stevens, Global Head of Information Technology at BGI. "We decided that Windows 2000 provided all that we needed to build the global platform. I would not have signed-off if I did not think we would get these outcomes from deploying Windows 2000 Server and Active Directory."

The REJ analysis, assessed by Gartner Measurement, a business unit of Gartner Inc., used post deployment data; as a result, all year one business and IT benefits are realized benefits. The REJ estimated a 105 percent internal rate of return (IRR) and a 248 percent return on investment (ROI) with an eight-month payback.



niap.nist.gov/cc-scheme

Octob

SECURITY VALIDATION REPORT

National Information Assurance Partnership

MICROSOFT WINDOWS 2000
Awarded Common Criteria Certification
Evaluation Assurance Level EAL: 4+
Report Number CCEVS-VR-02-0025

Common Criteria Testing Laboratory: Science Applications International Corporation
Columbia, Maryland

http://www.microsoft.com/servers/

Page 1 of 2

*System certified is Windows 2000 SP3 with Q326886 for professional, server, and advanced server. © 2003 Microsoft Corporation. All rights reserved. Microsoft and Windows are either registered trademarks or trademarks of

Trust the facts first. Microsoft® Windows® 2000* operating system has been awarded the highest level Common Criteria Certification for the broadest set of real world scenarios yet achieved by any operating system, as defined by the Common Criteria for Information Technology Security Evaluation (CCITSE). The Common Criteria (CC) is an internationally endorsed, independently tested, stringent set of standards that evaluate the security of technology products.

Windows 2000 desktop systems and server family were evaluated against CC requirements beyond the Controlled Access Protection Profile to include the following features:

- Sensitive Data Protection Device
- Enterprise Directory Service
- Virtual Private Network (VPN)
- Software Signature Creation Device
- Single Sign On
- Network Management
- Desktop Management

These results arm you with an unmatched level of confidence as you select secure products for your environment and mark an important milestone on the road to providing you the highest level of assurance in Windows and all Microsoft products.

For all the facts on Windows 2000 Common Criteria Certification and managing your security risk with Windows 2000, visit **microsoft.com/CCcertification** **Software for the Agile Business.**

Microsoft®

AD SIMPLIFIES SYSTEM ADMINISTRATION

As BGI extended its services to international markets, its IT assets evolved into a decentralized, geographically dispersed system of seven data centers, each of which managed data independently, using a mixed Windows and Unix environment with various database systems. This environment resulted in a duplication of IT assets and diverted critical IT resources away from the company's planned expansion into more global online investment services.

To better support its current customers and increase its portfolio of global online services, BGI used the Active Directory service in Windows 2000 Advanced Server to consolidate network domains, eliminate redundant servers, reduce IT support, and improve the end user experience. BGI also used NetIQ's DRA tool to improve overall network management.

The single-point management of Active Directory enabled BGI network administrators to spend less time in routine data management and network administration tasks by providing a single interface in the domain. As a result, the management of company-wide users, groups, and network resources was greatly simplified.

In addition, the interoperability capabilities of Active Directory enabled Kerberos and PKI-based security to be used with the company's mixed Windows and Unix environment for secure reduced sign-on across the entire corporate network.

BGI used NetIQ's DRA tool to simplify the management of the accounts in the directory. This resulted in less time finding accounts and an improvement in system administrator management time by providing increased management, auditing and reporting of the Active Directory.

LOGON TIME REDUCED

In the information while-you-wait world of financial services, access to data wherever and whenever a customer needs it will help ensure a satisfied customer. Conversely, downtime that makes corporate end-users wait for network access represents a significant opportunity cost.

"Office-based and mobile end-users at BGI were required to enter security credentials into local systems, as well as through additional location- and platform-specific authentication mechanisms, totaling 150 company wide," noted Carrie Jensen-Badaa, Global Head of Information Security for BGI. "The complexity of authenticated sign-on and inconsistent synchronization contributed to delays in accessing business critical information on the corporate network. This decreased end-user productivity, increased end-user frustration, and prevented timely delivery of information to clients."

Improving end-user and administrative efficiency required a streamlined company-wide authentication process that would eliminate redundant authentication mechanisms and could quickly distribute up-to-date security and employee information throughout the company. Integration with Windows 2000 and Active Directory through the use of Kerberos and LDAP enabled BGI to create a single set of company-wide authentication credentials.

Active Directory's multi-master replication capabilities enabled BGI to easily replicate directory information and security credential changes throughout the company. This reduced the time mobile end-users spent waiting for network access by 30 percent to 48 percent.

In addition to the productivity improvements with reduced sign-on, BGI was able to leverage the Active Directory solution to further enhance the end user experience. Using Active Directory's multi-master replication capability and programming interface, BGI reduced the application installation time for end users by 60 percent.

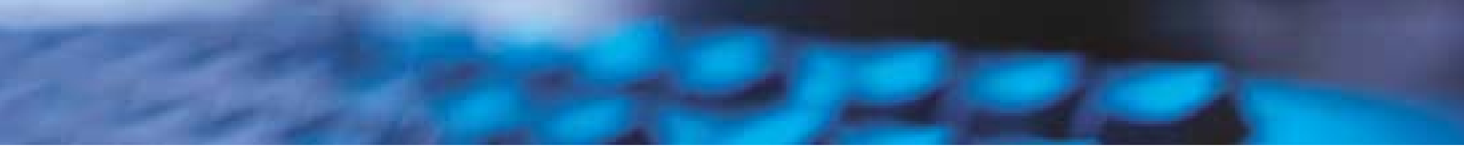
SECURITY-RELATED IT COSTS REDUCED

Corporate financial data is a mission- and business critical company resource. Securing this resource from hackers and other unauthorized network users ensures customer confidence and protects BGI revenue.

In BGI's mixed computing environment, interoperability problems caused IT support staff to spend many hours securing and deploying applications across its various platforms. Password control capabilities are needed on all platforms, which is burdensome to the end-user. Easing this burden can only be accomplished by integrating these heterogeneous platforms with Active Directory through the LDAP security standard.

When BGI changed its focus to offering products and services online and considered expanding those services into global investment markets, difficulties with secure online access threatened current and future revenue. Rather than selecting a costly third-party, public key infrastructure-enabled (PKI) online security solution, BGI chose an Active Directory solution with support for both PKI and Kerberos 5 industry standards, which provides secure sign-on via an industry-standard security system across its various IT platforms and enabled BGI's IT group to consider new solutions requiring these standards.

Shore concluded, "By using an industry-standard security protocol, we expect to spend up to 68 percent less IT engineering time integrating new applications into our security architecture. We have assured customers of the confidentiality of their accounts. This protects revenue, strengthens customer relationships, and paves the way to future growth." ◆



Microsoft Provides Strategic and Detailed Guidance for Secure Infrastructure Implementation

Building an enterprise infrastructure involves integrating hundreds, if not thousands, of components such as routers and switches, servers, operating systems, applications, and management tools. To achieve availability, security, scalability, and manageability, you can't approach each stratum of your data center in isolation. In particular, availability, security, and scalability are only as strong as the weakest link in the chain. And because any implementation usually involves multiple vendors and products, making all these components work together is made more complex.

Wouldn't you like to have a guide to help you design your data center with availability, security, scalability, manageability, and flexibility factored into each stratum of the data center? To take it a step further, what if the guide provided the exact specifications, from hardware requirements to configuration settings, for each component, including router ACLs (access control lists), VLAN definitions, firewall rules, server specifications, storage area networks, firewall rules, and more? Microsoft Systems Architecture (MSA) is just that. Best of all, it's free on Microsoft's TechNet Web site.

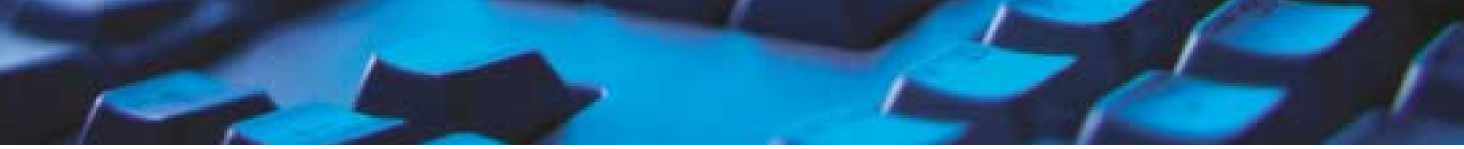
MSA GUIDES INFRASTRUCTURE DEVELOPMENT

Microsoft conceived MSA to help customers build and integrate Microsoft enterprise technologies into their data centers without having to re-invent the wheel each time. MSA provides both architectural and detailed step-by-step guidance on how to use Microsoft products and hardware solutions from various vendors to develop infrastructure that will support a range of enterprise scenarios. The architectural scope of each scenario focuses on the components necessary for supporting such a scenario. For example, MSA Internet Data Center (IDC) v1.5 guidance focuses on the needs of an e-commerce or ASP scenario. MSA Enterprise Data Center (EDC) v1.5 guidance focuses on the needs of a large corporate campus, including the internal network and servers used by employees as well as connectivity to the Internet, remote access via client VPNs, and site-to-site VPNs for connectivity to other campuses of the corporation. This article will provide some additional details about the EDC and the IDC, but it focuses primarily on MSA EDC v1.5.

The MSA EDC guidance covers how to configure backup and restore, secure remote management of all components, provide network infrastructure services such as DHCP, DNS, and WINS, and how to set up user-level services such as directory, file and print, messaging, and data services according to enterprise-level requirements. Figures 1 and 2 illustrate the basic areas covered by both data center models. The MSA EDC model includes components to provide basic Internet services such as DNS and SMTP to clients on the Internet, but they are not designed to fulfill the scale and complexity needs of an IDC architecture. For instance, companies like ServiceMaster and T-Mobile have benefited from both the EDC and IDC guidance, but a large company with only modest Internet presence (e.g., email and a mostly static Web site) would be well served by just the EDC.

AVOID RE-INVENTING THE WHEEL WITHOUT LIMITING YOUR OPTIONS

While MSA focuses on using Microsoft products wherever possible, MSA acknowledges that a Microsoft product may not always be the optimal choice for certain components of a given EDC implementation. MSA guidance is divided into Reference Architecture materials that are used for design and Prescriptive materials that are used during implementation. In the EDC, the Reference Architecture Guide (RAG) spells out the functional requirements for building an infrastructure that is highly available, secure, scalable, manageable, and flexible, but it stops short of defining specific vendors' hardware products. (It does, however, detail the hardware itself.) You can use the MSA EDC as a model for implementing a data center that fulfills the enterprise-level requirements addressed by the RAG, but use your own selection of products. Using



only the RAG helps you implement a data center designed from the ground up to meet enterprise requirements, without limiting your choice of vendors and products.

However, you can leverage even more benefit, cost savings, and risk mitigation by going to the next level and using the MSA EDC's Prescriptive Architecture Kit (PAK). A PAK puts the RAG into practice and demonstrates how to implement an EDC using specific hardware and software products. Participating MSA partners can create PAKs that showcase in minute detail how to use their products in conjunction with the Microsoft platform. Several MSA partners can collaborate on the same PAK to demonstrate how to combine their respective best-of-breed tools with Microsoft products to build a complete EDC. Currently, Microsoft provides two IDC PAKs and one EDC PAK, though other vendors also have PAKs. MSA vendors include Brocade, Cisco, CommVault Systems, Hitachi, HP, Juniper, McData, NetIQ, Nortel Networks, Unisys, and EMC.

PAKS PROVIDE GUIDANCE THAT HAS BEEN TESTED AND VERIFIED

PAKs are more than just shopping lists of products. PAKs also provide tested build guidance for configuring collections of services for different scenarios. In addition, PAKs include the configuration settings for each component, including VLAN definitions on switches, router ACLs, security templates for each server role, firewall rules, IP addresses, guidance for subnetting network zones, and configuration of remote management cards on servers. A PAK is similar to a complete blueprint and bill of materials for building a house.

In the EDC, the PAK includes a prescriptive architecture guide, a build guide, a test guide, and a solution operations guide. The prescriptive architecture guide covers the same ground as the reference architecture guide but at a more detailed, product-specific level. The build guide contains step-by-step instructions for building each component of the EDC. The test guide provides guidance and tools for testing EDC components individually or as a whole. The solution operations guide helps you provide proper care and maintenance for the EDC. This prescriptive guidance is an extremely valuable resource, because it takes much of the difficulty out of selecting and integrating components.

To further reduce the inherent difficulties in trying to make different products work together, MSA partners agree to support and help resolve all issues, regardless of how many partners are involved in a given PAK. Microsoft requires MSA partners to go beyond simply claiming compatibility and puts the burden on suppliers, rather than the customer, to make their products work. The EDC build, test, and operations guides go even further and provide you with the proven project plans for building, testing, and supporting an EDC. None of the MSA prescriptive guidance is theoretical; it is based on actual work performed in MSA labs with rigorous testing. Additionally, case studies of real companies that have implemented MSA are available, demonstrating that MSA works in the real world.

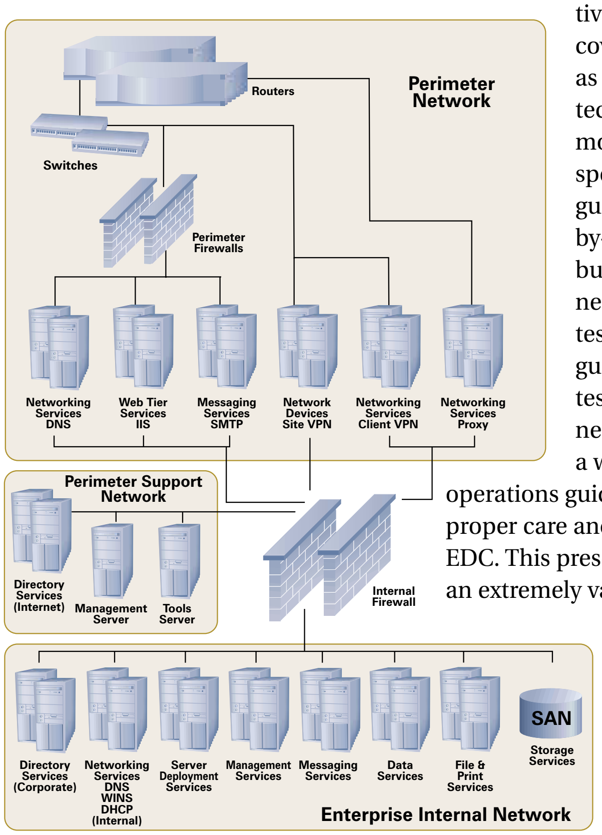


FIGURE 1: Components included in an MSA-defined Enterprise Data Center

IDC SECURITY

When users on the Internet browse Web servers, the perimeter router sends the HTTP or HTTPS request to the external firewall, which is a load-balanced cluster of ISA servers. The external ISA Server firewalls do not belong to the perimeter Active Directory domain and therefore must be configured separately. The MSA IDC uses ISA Server's reverse proxy capabilities to protect the enterprise's cluster of Web servers, as well as to improve performance and offload work from the Web servers by caching content. To the Web browsers on the Internet, the perimeter ISA Server cluster appears to be the enterprise's actual Web server. But after receiving a request, the ISA Server parses the HTML request, inspects it for malicious content, checks its local cache and, if possible, replies to the Internet client from cache. Otherwise, the ISA Server requests the content from the IIS server cluster. For secure areas of the enterprise's Web site, the MSA IDC uses ISA Server's SSL bridging technology to offload SSL processing from the Web server and to make it possible for ISA Server to inspect the request before passing it on to the Web server.

EDC SECURITY

As illustrated in Figure 1, border routers connect the EDC to the Internet and serve as the EDC's first line of defense. The EDC itself comprises three primary networks: perimeter network, perimeter support network, and internal network. The perimeter firewall protects certain servers in the perimeter network and the internal firewall connects and marshals traffic between all three networks. An additional layer of security is provided through the use of 25 VLANs configured on the EDC's two switches. The MSA EDC guides you through configuring switch access control lists (ACLs) to further control the flow of traffic inside the primary network. The use of VLANs also prevents packet sniffing by compromised perimeter systems or by hackers on the internal network.

The perimeter network, which contains all the servers that are accessed by Internet clients, is divided into three logical security zones. The Internet services zone contains the enterprise's SMTP relay servers and public DNS servers. The VPN services zone contains site-to-site VPN devices and client VPN servers for remote access. The proxy services zone contains the proxy servers that provide secure Web access to internal users. The perimeter firewall is a sophisticated application layer proxy firewall that prevents application layer attacks on servers in the Internet services zone. The current EDC PAK uses ISA Server as the perimeter firewall because it provides deep, application-level inspection of DNS, SMTP, POP3, and HTTP traffic. To efficiently manage the perimeter servers, the EDC defines a perimeter support network in which reside the Active Directory domain controllers that host the perimeter Active Directory forest. This perimeter Active Directory forest provides centralized authentication and group policy management for all the servers in the perimeter network. Other servers in the perimeter support zone provide monitoring and management services using MOM. Separating the perimeter support servers from the rest of the perimeter network provides added isolation and protection for servers in the support zone that require access by administrators on the internal network. The internal network contains the enterprise's employee workstations and internal servers.

MSA EDC v1.5 includes guidance for deploying the internal Active Directory forest; internal network services such as DNS, WINS, and DHCP; messaging services with Exchange 2000 Server; data services with SQL Server 2000; and file and print services with Windows 2000 Server. The MSA EDC also shows you how to achieve speedy and secure server deployment by using Microsoft technologies such as Automated Purposing Framework (APF), management services such as MOM, and storage with Storage Area Network (SAN) or Network-attached Storage (NAS) products.

The MSA EDC architecture makes heavy use of the defense-in-depth security strategy. The first level of defense is the border routers in the perimeter network, which connect the EDC to the Internet. The MSA EDC guidance details two routers that provide a fault-tolerant connection to the Internet. (As with all facets of the MSA EDC, you can dial-down the implementation as necessary based on availability requirements or budget.) To survive ISP outages, each router should be connected to a different ISP—or at least different points-of-presence for the same ISP. The border routers use port filtering to expose only the required protocols to the Internet, prevent attackers from introducing spurious traffic with spoofing techniques, and defend against denial-of-service attacks such as half-open connections. The RAG provides the specific TCP and UDP port numbers that need to be opened on whatever product you use as your border router. If you implement a PAK provided by Microsoft or a group of MSA partners, you can use the PAK's build guide to get step-by-step configuration instructions for the specific routers defined by that PAK. For instance, the Microsoft MSA EDC PAK calls for Juniper M5 routers and the build guide includes configuration files for both routers and the commands you use to upload the files to the routers, as well as guidance for connecting the routers to your ISP and testing the setup. For a detailed view of the MSA EDC, go to http://www.microsoft.com/solutions/msa/evaluation/overview/edc/Network.jpg.

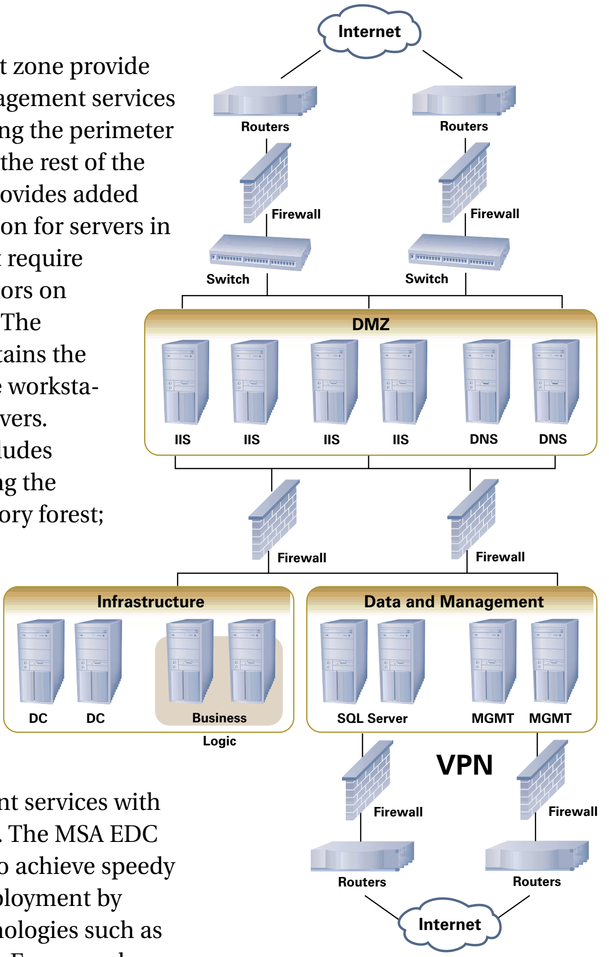
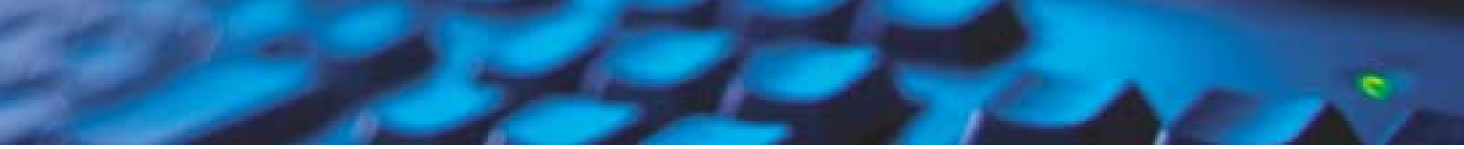


FIGURE 2: Components included in an MSA-defined Internet Data Center



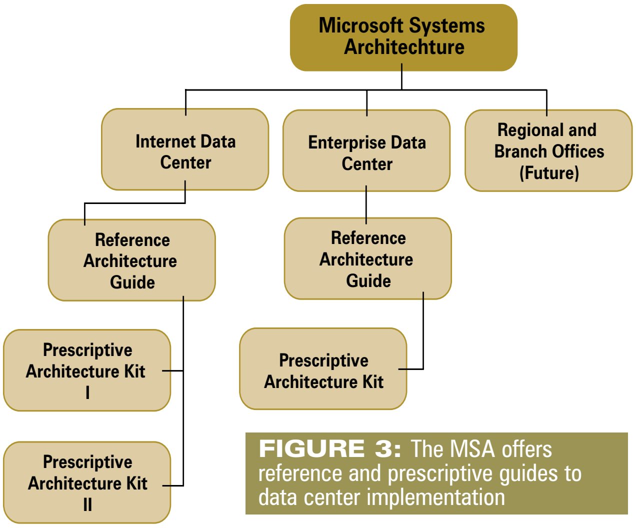

Microsoft Systems Archtechture
Internet Data Center
Enterprise Data Center
Regional and Branch Offices (Future)
Reference Architecture Guide
Reference Architecture Guide
Prescriptive Architecture Kit I
Prescriptive Architecture Kit
Prescriptive Architecture Kit II

FIGURE 3: The MSA offers reference and prescriptive guides to data center implementation

UNDERSTANDING MSA EDC'S SECURITY DESIGN

To help you understand the MSA EDC's security design, let's trace various types of traffic through the components of the EDC. VPN connections from remote users or other sites are dispatched by the border router to the appropriate VPN device or server. The MSA EDC implements the site VPN server with a Windows 2000 server running RRAS, but other Microsoft partners might specify alternative VPN devices. To support 5,000 remote clients, the PAK specifies four Windows 2000 servers running ISA Server. Authentication and authorization for VPN clients is facilitated by IAS in the perimeter Active Directory forest and internal user accounts. From the VPN server, the unencrypted traffic flows through the internal firewall and onto its final destination. The internal firewall performs stateful inspection and selectively passes traffic between the perimeter, perimeter support, and internal networks. Each PAK provides step-by-step instructions, configuration files and scripts to set up the internal firewalls, as well as every other component of the EDC.

The MSA EDC uses ISA Server to provide fault-tolerant Web access to users. When internal users browse the Web, their Web browser sends the request over port 8080 through the internal firewall to the proxy servers in the perimeter network. After retrieving the Web page, the proxy server inspects the page for malicious content and passes it back to the internal user via the internal firewall. ISA Server's extensible architecture lets you choose from a variety of Microsoft partner products to enforce content inspection, Web site restrictions, and virus scanning.

Security and manageability can be competing priorities. The MSA EDC architecture gives priority to security in all design decisions as long as the solution remains manageable, which sometimes calls for some imagination. For instance, administrators must have remote Terminal Services (TS) access to Web and email servers so that they can support those servers without being physically present. However, opening routes directly from administrator workstations to the servers would violate some of the hard and fast network boundaries imposed by the MSA EDC architecture. The MSA team solved the problem by implementing a management server in the Internet services zone with TS access to the Web and email servers, and then allowed TS access from administration workstations to the management server. This approach provides administrators with the ability to TS into the management server and then TS into the Web or email server.

MSA TO THE RESCUE

Beyond network level security control, the MSA EDC provides detailed guidance on securing and hardening each Windows 2000 server role. The build guide provides security templates and scripts that configure features such as password, lockout and audit policies, user rights, and file and registry permissions. The MSA EDC specifies testing and operations activities to validate each component's security using scripts and tools like the Microsoft Baseline Security Analyzer. The MSA EDC also provides guidance for designing a secure Active Directory forest for both perimeter and internal networks, including the design of domains, organizational units, and group policy objects.

An enterprise data center represents a complex integrated system of technologies, devices, and requirements that are configured to maximize availability, security, scalability, manageability, and flexibility. The MSA EDC provides a realistic balance of security and usability to help you define a coordinated security strategy that spans the entire strata—from the physical network boundaries through operating system and application-level security. The MSA EDC Reference Architecture Guide provides best practice, vendor-agnostic security controls for border routers, the perimeter firewall, switches, internal firewall, and within both perimeter and internal forests.

For further value, you can use implementation guidance in the EDC PAKs to benefit from integration and testing already performed by Microsoft and its partners. By doing so you'll reduce implementation costs and risk, and you'll also gain the peace of mind that comes with the knowledge that the vendors whose products you purchase are committed to making them work with other MSA EDC components. The MSA EDC documentation provides guidance for customizing the architecture to your needs and, because the EDC is designed to support the largest of data centers, most enterprises will be able to dial back on the specifications to suit their needs. And because the overall MSA EDC design is modular, you can implement only those pieces that fit your current needs. ◆

TANDBERG Television Deploys *Aspelle Everywhere* to Facilitate Remote Sales Demonstrations

TANDBERG Television (Oslo, Norway) is a market leader in providing open solutions for the digital broadcasting of audio, data, and video across various networks. The company, an innovator in digital broadcasting, has operations in Asia, Australia, Europe, and the United States, TANDBERG Television's customers include major broadcasters, network operators, and convergence players around the world.

THE CHALLENGE

Having a global sales force in place is not enough; a successful company must have tools that enable the sales force to dazzle prospective clients with the breadth of its technology offerings.

Initially, TANDBERG Television gained this competitive advantage for its sales force by deploying a dial-up virtual private network (VPN) to facilitate access to its corporate resources. However, the company soon realized that a traditional VPN solution was too complex, expensive, and troublesome for most of its sales teams. The VPN was resource intensive and was unable to deliver the level of security, functionality, and flexibility the company needed. Employees experienced problems with the delivery of email and other critical business functions while using the VPN. And while it provided secure access to the corporate network, dial-up restrictions such as speed and latency were problematic for a company building its reputation as a pioneer in digital broadcasting.

TANDBERG Television needed a fast, secure, and easy-to-use solution that would let its mobile sales force easily gain access to corporate resources and, more importantly, serve as a mechanism for demonstrating broadcast products in real time at a customer site or in the field. The company also wanted to eliminate some of the multiple points of failure associated with its VPN solution.

Because some of TANDBERG Television's business partners require a VPN to meet their security guidelines, the company could not eliminate it as a resource. Instead, it selected *Aspelle Everywhere* to augment and support its VPN, making it more flexible and better able to meet the needs of its sales force.

THE SOLUTION

The first product on the market to provide secure, managed, clientless access to all corporate applications without the limitations found in a VPN, thin client, or remote access product, *Aspelle Everywhere* requires only a Web browser and an Internet connection. In less than one day, TANDBERG Television installed, tested, and deployed *Aspelle Everywhere*, delivering a more comprehensive remote access solution to its sales employees.

"Once we saw a demonstration of *Aspelle Everywhere* the decision process was simple," said Lindsay Morgan, IS Service Delivery Manager for TANDBERG Television. "Using Aspelle's product to access live demonstration systems has enabled our sales force to show potential customers complex broadcast offerings that were previously unavailable or logistically difficult to display. As a result, we have a competitive edge in the field, which has helped us secure sales—which in turn has already paid for our investment in the system."

Aspelle Everywhere delivers a comprehensive, secure enterprise access solution. Designed to meet the demands of TANDBERG Television's global sales force, *Aspelle Everywhere* maximizes the company's previous technology investments by seamlessly integrating with its existing VPN and network.

"*Aspelle Everywhere* was the most cost-effective and easily deployed remote access product we reviewed," commented Morgan. "Additionally, we were very pleased with Aspelle's customer support during the implementation process. With the support of their dedicated sales and engineering team, we were able to test and implement the product in one working day."

KEY DECISION FACTORS

Aspelle Everywhere's enterprise-class security features were particularly appealing to TANDBERG Television. With *Aspelle Everywhere*, the company can maintain all corporate applications inside the enterprise on existing network ports without exposing additional ports to the Internet-facing firewall. Data is 128-bit encrypted and authentication, authorization, and access are controlled separately. Moreover, Aspelle's innovative single sign on technology lets TANDBERG Television employees connect from public resources (e.g., Internet café, client computer) without risking key data.

TANDBERG Television also benefits from *Aspelle Everywhere*'s easy-to-use management capabilities. It offers a secure, centralized point of management and the uniform delivery of corporate applications, eliminating many time-consuming and costly administrative and maintenance tasks. And *Aspelle Everywhere* was designed to expand to new locations in minutes, merge with new businesses overnight and add new users and applications in seconds.

aspelle®

Aspelle

617-273-8114

www.aspelle.com/info

ADVERTISER-SPONSORED CASE STUDY

Vintela Authentication Service: Active Directory Authentication for the UNIX Community

Companies are deploying their business-critical applications on a variety of platforms, including Windows, UNIX, and Linux. These mixed environments present a variety of problems to Systems Integrators and IT personnel—especially when it comes to security and user authentication.

Companies that are using Active Directory (AD) have a secure solution for integrating their user accounts with their applications running on the Windows platform. However, integrating their UNIX and Linux applications with the user accounts stored in AD has always been a challenge. Many IT staff personnel attempt to solve this problem through account synchronization scripts across multiple UNIX/Linux operating systems. These user account/password synchronization solutions are always costly to implement and maintain.

Center7 Inc. has a better way to integrate these mixed environments with the release of Vintela Authentication Service (VAS). VAS allows system integrators and IT personnel to authenticate their UNIX/Linux applications directly against the user accounts stored in AD. Center7 has a strong background in the UNIX/Linux community and understands how to integrate Windows and UNIX. VAS has been designed to integrate with the Unix operating system using standard UNIX technologies such as PAM and NSS so that it's easy for administrators to deploy and manage their UNIX solutions while still using AD to manage their user accounts.

VAS is not a password syncing or meta-directory solution. Instead, VAS operates in real time with AD by using Kerberos and LDAP to access user account information and authenticate users from the UNIX/Linux hosts. Users have one account and one password to remember for all of their system logins and applications. Users can change their AD password from both UNIX/Linux and Windows machines. AD account restrictions are also supported by the VAS client, allowing administrators to force users to follow good password practices.

These capabilities allow VAS to solve the integration issues that major companies face. One example is Boeing R&D, which has always been a technology leader and which uses a variety of computing environments. The VAS development team was able to work closely with Boeing during the design phase of VAS. Boeing R&D is currently testing the technology and is impressed with it. Boeing researchers believe VAS will reduce the cost of account administration and provide better integration of desktop Linux systems with desktop Windows.

VAS also provides a powerful solution for small- to medium-sized businesses. One example is Dynatronics, a market leader in physical therapy equipment. Dynatronics is using AD to manage its Windows environment, but the company's accounting software, OSAS, runs on Linux. Forty of the 75 employees at Dynatronics need to access this accounting system regularly. "Although the company invested significant resources in training their users to stop the use of sticky notes on their monitors, four or five of them just don't get it," said Blake Brackenbury, Dynatronics' system administrator. "Every few weeks one or more of them will forget their password and I have to go and reset it."

> ***"There is nothing else in the marketplace that can do this type of integration."***
>
> **Stan Skidmore**
> UNIX Administrator
> R&D Group, Boeing

After installing VAS, the Dynatronics employees were able to use their Windows user names and passwords to access the accounting software. VAS also allowed users to print OSAS reports directly to their home directories where they were accessible using the same usernames and passwords. The sticky notes are no longer a problem.

VAS is being deployed by organizations of all sizes, from government departments to small businesses. The time and cost savings provided by the seamless integration that VAS provides with AD is immense. The Vintela team is working with Microsoft to continue to provide the technologies to enable enterprise-class authentication, as well as application security, for both UNIX and Microsoft users.

CENTER7/INC.™

Center7 Inc.
801-805-3000
info@center7.com
www.center7.com

PaeTec Communications Extends Corporate Policies to the Internet with N2H2's Sentian

Based in Fairport, New York, PaeTec Communications, Inc. is an integrated communications provider offering local, domestic, and international long-distance services, high-speed Internet access, advanced data services, and communications management services to medium- and large-sized businesses, colleges, universities, hospitals, hotels, governmental organizations, and affinity groups in more than 27 markets nationwide. Recently ranked the Top Private Company in the greater Rochester, New York area, PaeTec has experienced 134,000 percent growth since its inception in May 1998.

THE CHALLENGE

The PaeTec company Web site features a statement that describes "PaeTec Culture." The statement says, "PaeTec's culture is one in which employees look forward to excelling at their jobs and our customers look forward to interacting with our employees. Every employee of PaeTec is a part owner, thus creating an operating environment where teamwork and consideration for customer concerns naturally occur."

When PaeTec provided Internet access to its employees, company management became concerned about the potential display of offensive and inappropriate material, because this could undermine the environment of mutual respect and teamwork the company had worked to build. Other companies have experienced nightmarish problems related to unfiltered Internet use. In 1999, the Dow Chemical Co. fired 50 employees and disciplined 200 others after an e-mail investigation turned up hard-core pornography and violent subject matter.

THE SOLUTION

PaeTec Director of Enterprise Technology, Jim Raub, began evaluating filtering solutions in December 2001. Raub was seeking a solution that allowed him to further extend company policies to the Internet by setting different levels of Internet access for different departments across PaeTec. In order for such a solution to not become an administrative headache, the solution would need to have a simple interface. Additionally, the solution would require a highly accurate and comprehensive database of blocked sites, so that constantly adding and deleting sites to the database did not waste IT resources. Raub found that N2H2's Sentian for the Microsoft Internet Security and Acceleration (ISA) Server 2000 more than met these requirements. "Sentian has wonderful administrative abilities, with an interface that is great for applying rules and levels of access to different groups of users," said Raub.

Raub was also impressed with N2H2's database, which has been rated superior to N2H2's top competitors at blocking pornography in independent studies by eTesting Labs for the Department of Justice and the Kaiser Family Foundation published in the Journal of the American Medical Association (JAMA)."The quality of the database is very good, and the few times we have needed to customize our block list, it was a fast, easy fix. I would recommend Sentian without hesitation." For PaeTec, managing Internet access makes sense. PaeTec management can feel secure in knowing that their company mission statement is being carried out, in part, by using filtering software, which helps to keep the PaeTec workplace a safe, productive, team environment.

> ***"Sentian has wonderful administrative abilities with an interface that is great...I would recommend Sentian without hesitation."***
>
> **Jim Raub**
> Director of Enterprise Technology
> PaeTec Communications, Inc.

N2H2™
INTERNET CONTENT FILTERING

N2H2
877-336-2999
www.n2h2.com

With Oblix NetPoint, Identity Management Becomes Less Troublesome for National Credit Union

At CUNA Mutual Group, creating financial security is the name of the game. As the leading financial services provider to credit unions and their members, CUNA Mutual partners with nearly 95 percent of the 10,000 credit unions in the United States and offers more than 300 loan, insurance, and brokerage products.

THE CHALLENGE

During the past five years, CUNA Mutual has developed a number of initiatives to deliver a range of financial products over the Web. One key to the success of CUNA Mutual's self-service financial offerings lies in identity management. Not only does the company need to manage the identities of its own employees, but also the many levels of authorization and access needed for credit union employees and members. To do this, CUNA Mutual turned to Oblix NetPoint™. Before implementing Oblix NetPoint in September 2001, CUNA Mutual used a homegrown directory system and access control components to secure Web resources. However, in time, this solution was not enough.

"We weren't doing identity management very well," admits Steve Devoti, CUNA Mutual's IT department manager of directory services. "We didn't have central repositories to store identity information. Our employees were managed in many different systems, with little automated coordination between them. We needed to bring these repositories into a central place where the identities could be stored. We decided to standardize on Microsoft Active Directory."

Adding to the directory services challenge was the question of access control. Because the majority of credit union branch offices are small, credit union employees often take on different roles: an employee may be a claims-payer and also approve loans. Then there are employees who work for multiple credit unions—either part time or as part of a service bureau. For an IT professional, this creates a complicated data model where a person can work for many credit unions performing many roles using many applications.

"Trying to model this information in a directory is very difficult," notes Devoti. "Oblix NetPoint was the only product that could handle role-based authorization as well as the multi-dimensional relationship."

THE SOLUTION

But before CUNA Mutual could implement this complex identity management project, they found other, more pressing uses for Oblix NetPoint. One application allows credit union members to view life insurance policy information; the other provides financial account aggregation—all via their credit union Web site.

"We created the members' directory, put Oblix NetPoint on top of it and used all of NetPoint's self-service features—the ability to self-register, manage your own identity profile, and change passwords. These systems could potentially be used by tens of millions of credit union members. We couldn't afford to have members register on an 800 number or call a help desk to reset their password manually."

In addition to flexible collaboration, Devoti points to Oblix NetPoint's IdentityXML. "This key interface into Oblix is XML-based and tracks with security standards in the industry," he says. "This will have huge benefits when we start to federate security with other credit unions and partners…we'll be able to integrate with whatever comes down the pike."

Another extremely powerful component of CUNA Mutual's system is its ability to delegate identity administration and access approvals to individual credit unions. CUNA Mutual help desks are also delegated granular rights. "With Oblix NetPoint, we can delegate administration to help desks and call centers so that they're able to change certain pieces of people's identity information," says Devoti. "For example, they might be able to reset passwords but not delete someone's Social Security number."

THE RESULTS

For Devoti and his 600 IT coworkers, Oblix NetPoint lives up to its promise of providing security for the way they do business. "By partnering with Oblix, we are providing a high level of security for our Web-based systems. We found out that access control is the easy part. The hard part is identity management. We think Oblix does that better than anyone."

Right on the Money: VirtualBank Delivers Secure Web Services with OpenNetwork and Microsoft

VirtualBank leads the next generation of Internet banking with online financial solutions that offer an unprecedented level of personalization, convenience, and privacy. The company's innovative platform lets customers consolidate and view their financial data in real time and across a full suite of traditional banking and lending products.

VirtualBank's growth rate—a dramatic 2,000 percent increase during the past five years—has necessitated the creation of a world-class IT infrastructure. The company's technological vision has led to numerous awards including "Best Online Bank" from Money Magazine and CIO Magazine's "Top 100 Innovative Companies."

THE VIRTUALBANK CHALLENGE

While other companies talk about the future of Web Services, VirtualBank is realizing their power today. The company launched a .NET-connected IT infrastructure that supports business growth through the delivery of XML Web Services that automate processes and simplify interaction between mission-critical business applications. But with the introduction of new Web applications and services, came the need for a solution that would make it easier for the company to efficiently manage and secure their growing and diversified user base.

THE SOLUTION

VirtualBank selected the OpenNetwork and Microsoft Identity Management Framework to provide end-to-end identity management and access control across intranet, extranet and Internet users. OpenNetwork's unmatched expertise and strategic partnership with Microsoft made it an ideal fit for securing and managing VirtualBank's Microsoft-centric IT environment.

OpenNetwork DirectorySmart facilitates Web single sign-on, secure access, user self-service, password reset and delegated administration by leveraging Active Directory as the central identity repository for both user information and security policies. DirectorySmart is the only identity management software to interact with the directory without extracting data to a policy server for authentication, authorization and management. The result is a streamlined architecture that scales quickly, predictably and with proven performance.

In VirtualBank's current environment, DirectorySmart manages and administers employee access to application resources. One of these resources is an application that automates the loan origination process. Loan officers login to the DirectorySmart-protected application, backed by a Web Service that interacts with third parties for fraud detection and credit checks. The Web Service uses the WS-Security standard to send information about the applicant. Once the credit report is received, the data is converted to XML and is scored using custom Visual Basic .NET business logic to approve, reject, or flag the application for further review. The process significantly reduces the human intervention required to process applications.

In the near future, VirtualBank plans to extend the power of this Web Service to external users. The solution would allow VirtualBank to drive new revenue streams by offering secure, subscription-based Web Services to other financial institutions and business partners.

THE RESULTS

VirtualBank's existing Web Service lets loan officers support a 1,500 percent increase in loan processing—with OpenNetwork DirectorySmart ensuring the integrity of each interaction.

The combined solution of OpenNetwork and Microsoft enables VirtualBank to deliver more services to more users—while reducing management costs and improving security. DirectorySmart's tight integration with Microsoft enabled VirtualBank to quickly implement a scalable and reliable identity management platform. John P. Stoddard, chief technology officer at VirtualBank said, "OpenNetwork DirectorySmart fits perfectly with our strategy... Now we can focus on adding value to our customers by delivering the banking industry's first true .NET Web Services and rely on OpenNetwork to secure those services."

OpenNetwork®

OpenNetwork
727-561-9500
877-561-9500
www.opennetwork.com

PricewaterhouseCoopers Deploys Enterprise Identity Management Solution For Major Financial Client

THE CHALLENGE

A large US-based financial institution was late in addressing a competitive market need—business online banking (BOB). To kick-start the program, the CIO forged a strategic partnership with Microsoft using the Windows 2000 operating system, ASP.NET for building applications and XML Web services, and Microsoft's Internet Security and Acceleration (ISA) Server 2000 firewall.

"Initially, a pilot program would enable 40,000 business customers, geared to roll-out to 100,000 at the end of the engagement. The end-game was that once BOB was successful, we could roll this out to millions of potential customers for consumer online banking," says Dan Trieschmann, Senior Manager, Security & Privacy Practice, Pricewaterhouse Coopers (PwC). The PwC project leader is Gary Loveland, Partner, Security & Privacy Practice.

THE SOLUTION

PricewaterhouseCoopers' team was primarily engaged to help this client design and implement an Identity Management (IdM) infrastructure to be used for their customer-facing Web and eBusiness initiatives. The IdM solution was intended to improve the end-user business customer experience, enhance security and simplify the administrative processes for them, ultimately reducing costs.

"We recognized that a Microsoft-centric site, though late to the market, would enable the client to manage user profile information seamlessly through an integrated Identity Management solution," adds Trieschmann. This solution enables the company to facilitate account set-up for business customers, access clients' profile information, and allow back-end Contact Centers/Help Desk personnel to migrate user data.

By integrating Microsoft Active Directory for the user repository of 40,000 customers, PwC's IdM access and identity management solution allows business banking customers to transfer funds, make payments online with bill paying modules, schedule future payments, delegate administration models, print statements, view account histories, stop payments, and more.

Currently, PwC is addressing the client's needs with its global view of comprehensive enterprise security utilizing the Enterprise Security Business Model (ESBM)™. This four-stage process identifies, creates, captures and sustains the value of security in any organization. Through the framework of the ESBM, PwC is analyzing the company's Public Key Infrastructure (PKI) process, business continuity, disaster recovery, incident response, patch management, and threat and vulnerability management.

PwC also reviewed the company's internal controls policies for managing their PKI environment for digital signatures with Microsoft internal certificate authority, then recommended improvement controls.

> ***"With minimal advertising and promotion, our client expected 1,000 customers a month to sign up for business online banking. They exceeded that in the first week."***
>
> **Gary Loveland, Partner**
> Security & Privacy Practice
> PricewaterhouseCoopers

THE RESULTS

"The initial results have been beyond the client's wildest dreams," says Loveland. "With minimal advertising and promotion, our client expected 1,000 customers a month to sign-up for business online banking. They exceeded that in the first week."

The infrastructure and processes co-developed by the client, PricewaterhouseCoopers, and Microsoft will also be leveraged to enhance the online banking capabilities for individual consumers.

In addition to assisting with the online banking initiative, PwC has designed and implemented an Intranet identity infrastructure for the company's internal employees (50,000), enabling them with business-to-enterprise capabilities.

PRICEWATERHOUSECOOPERS

PricewaterhouseCoopers
Security & Privacy Practice
800-639-7576
www.pwc.com/security

Websense Enterprise Protects Carnival Cruise Line From Rising Tide of Internet Threats in the Workplace

As the Internet has become more prevalent in the workplace, it has also created new distractions for employers that represent new risks for companies. These risks extend beyond non-work-related Web sites and include peer-to-peer (P2P) file sharing and instant messaging (IM) protocols and applications. In addition, the problem of illegal content in corporate networks is quickly becoming a significant legal issue for corporations.

PROACTIVE RISK MANAGEMENT

Carnival Cruise Lines decided it was necessary to proactively manage its employees' computing resources both on land and at sea. After an extensive product search and evaluation, Carnival selected Websense software as its employee Internet management (EIM) solution of choice.

Carnival uses Websense Enterprise, integrated with Microsoft Internet Security and Acceleration (ISA) Server 2000, to manage Web use for more than 3,000 Internet-enabled employees at the company's corporate headquarters in Miami. In the future, the company plans to roll out Websense software in other office locations and on its fleet of ships.

"We chose Websense because it was by far the best Internet filtering product on the market. With its ease of management, comprehensive and flexible features and ability to integrate with a host of products, it was the obvious choice to make the Net more productive for our employees," said Rodney Orange, lead systems engineer, Carnival Cruise Lines. "Websense won easily over the competition with its flexible management tools and ability to integrate with any number of existing Internet infrastructure products, such as Microsoft ISA."

Although a company may initially recognize the bandwidth drain of employees' non-work-related Internet use, it is the security risks associated with the Internet, such as P2P file sharing and IM, which are far more troublesome. These threats can enter a company in three ways: via Web access, by tunneling across various network protocols and by launching on individual employee desktops. As a result, it's important that IT administrators install EIM software that offers all three levels of protection to manage employee-computing security.

MANAGE P2P FILE SHARING

In addition to draining corporate bandwidth, P2P applications carry security risks because they communicate directly with other users' computers, bypassing a company's firewall and often entering the corporate environment without being scanned for viruses.

According to IDC, P2P is primarily used for swapping copyrighted material, so that the problem of illegal content in corporate networks is quickly becoming a significant legal issue for corporations. As a result, the Recording Industry of America (RIAA), which estimates that more than 2.6 million files are copied illegally every month, has warned companies that they could be held liable for violating copyright laws.

With Websense Enterprise, companies can manage P2P file sharing by blocking employee access to P2P Web sites, network-level protocols or desktop applications.

STANDARDIZE IM

Because IM is a form of P2P file sharing, companies face security vulnerabilities. Up to 84 percent of all organizations use some sort of IM application, according to a report issued by Osterman Research. Unfortunately, employees at less than one-third of the companies surveyed use approved IM software.

With Websense Enterprise, companies can standardize IM by blocking employee access to all network-based IM protocols except the one designated by corporate management. In addition, companies can easily enforce a policy in real-time that minimizes bandwidth drain by blocking IM, except by those departments for which it's an essential business function.

As employees' computing environments have evolved, so too have the threats to infiltrate companies. Because the threats can enter a company in three ways, they require a three-tiered EIM solution. Without all three levels of Internet security protection, a company is as vulnerable to threat from employee Internet use as a cruise ship passenger is to seasickness in the midst of a storm.

WEBSENSE®

Websense, Inc.
800-723-1166
sales@websense.com
www.websense.com

Microsoft Partners

ISA SERVER PARTNERS

8e6 Technologies
Orange, CA
www.8e6technologies.com/isaserver

ACP
Birmingham, AL
www.acp-inc.com/isaserver

Aelita Software
Powell, OH
www.aelita.com/isaserver

AEP
Boston, MA
www.aep.ie/isaserver

Akonix
San Deigo, CA
www.akonix.com/isaserver

Aspelle
Boston, MA
www.aspelle.com/isaserver

Authenex
Oakland, CA
www.authenex.com/isaserver

Burst Technology
Bonita Springs, FL
www.burstek.com/isaserver

Castify Networks
Alexandria, VA
www.castify.net/isaserver

Chutney Technologies
Atlanta, GA
www.chutneytech.com/ISAserver/

CornerPost Software
Duffield, VA
www.cornerpostsw.com/isaserver

F5 Networks
Seattle, WA
www.f5.com/isaserver

Finjan Software
Los Gatos, CA
www.finjan.com/isaserver

GFI Software
Cary, NC
www.gfi.com/isaserver

Intellitactics
Bethesda, MD
www.intellitactics.com/isaserver

Internet Security Systems
Atlanta, GA
www.iss.net/isaserver

N2H2
Seattle, WA
www.n2h2.com/isaserver

nCipher
Woburn, MA
www.ncipher.com/isaserver

Nexus Technology
United Kingdom
isaserver@webconsent.net
www.webconsent.net/isaserver

PatchLink Corporation
Scottsdale, AZ
www.patchlink.com/isaserver

Radware
Mahwah, NJ
www.radware.com/ISAServer

Rainfinity
San Jose, CA
www.rainfinity.com/isaserver

RSA Security
Bedford, MA
www.rsasecurity.com/isaserver

Sane Solutions
North Kingstown, RI
www.sane.com/isaserver

Secure Computing Corporation
San Jose, CA
www.securecomputing.com/isaserver

Stonesoft
Atlanta, GA
www.stonesoft.com/isaserver

SurfControl
Scotts Valley, CA
www.surfcontrol.com/isaserver

Symantec
Cupertino, CA
www.symantec.com/isaserver

Venation
United Kingdom
sales@venation.com
www.venation.com/isaserver

Wavecrest Computing
Melbourne, FL
sales@wavecrest.net
www.wavecrest.net/isaserver

Websense
San Diego, CA
www.websense.com/isaserver

WebSpy
Kirkland, WA
sales@webspy.com
www.webspy.com/isaserver

GLOBAL SERVICES PARTNER

Accenture
Chicago, IL
www.accenture.com

Avanade
Seattle, WA
www.avanade.com

Cap Gemini Ernst and Young
Paris, France
www.cgey.com

Ernst and Young
Boston, MA
www.ey.com/global/content .nsf/
International/Services_-_Assurance_&
Advisory-_Technology_and_Security_Risk

HP
Boston, MA
www.hp.com/hps/tech/security/

PricewaterhouseCoopers LLP
New York, NY
www.pwcglobal.com/security

Schlumberger SEMA
Houston, TX
www.slb.com

Unisys
Boston, MA
www.unisys.com/security

ISV PARTNERS

Aladdin Knowledge Systems
Arlington Heights, IL
www.ealaddin.com/isaserver

Bindview
Houston, TX
www.bindview.com

Cereton
Waltham, MA
www.cereton.com/isaserver

NetIQ
San Jose, CA
www.netiq.com

Network Associates
Santa Clara, CA
www.nai.com

Oblix
Cupertino, CA
www.oblix.com

OpenNetwork
Clearwater, FL
www.opennetwork.com

Rainbow
Irvine, WA
www.rainbow.com/isaserver

Trendmicro
Cupertino, CA
www.trendmicro.com