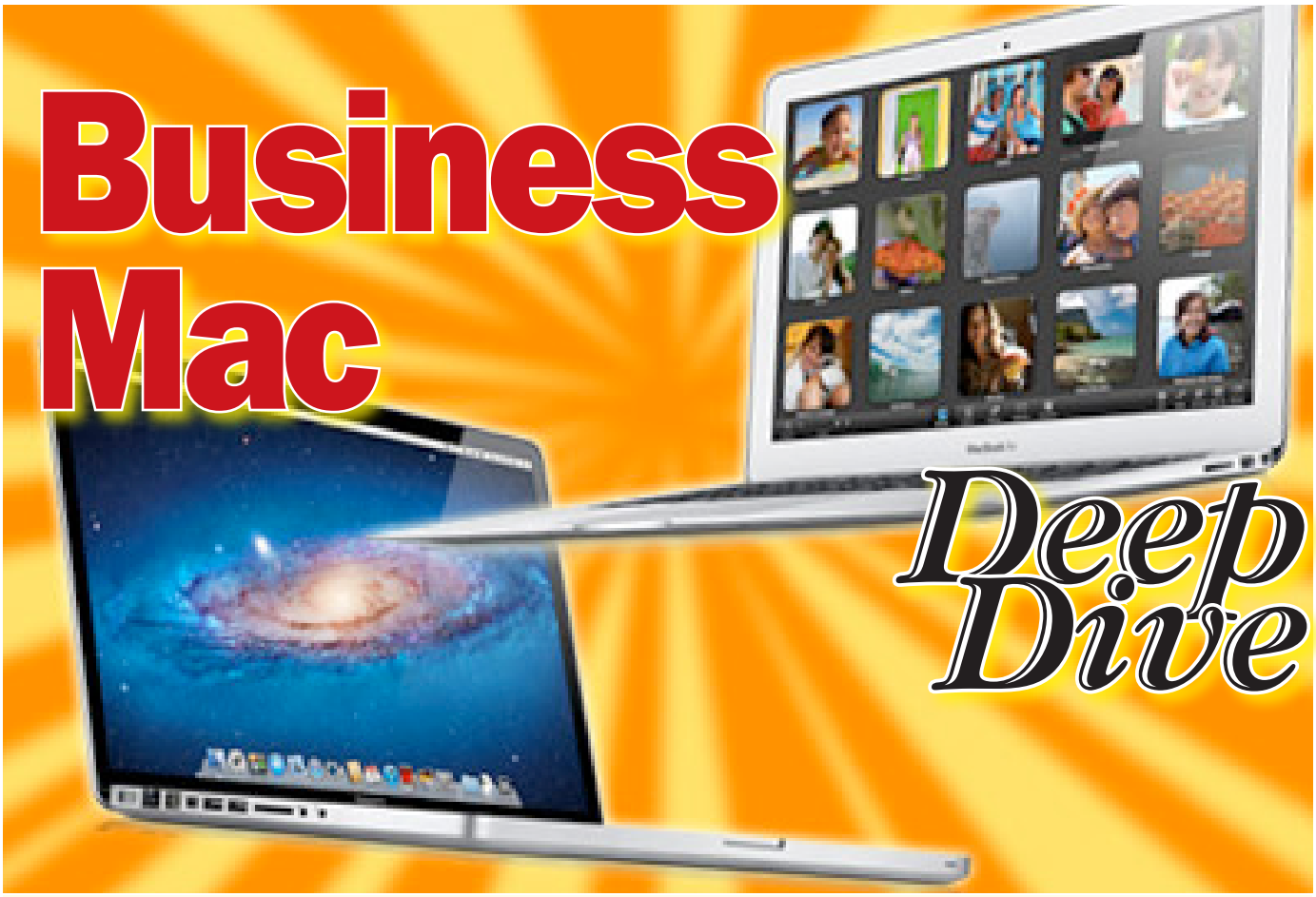
InfoWorld

SPECIAL REPORT

NOVEMBER 2011

Business Mac Deep Dive



Deep Dive Articles

HANDS-ON

IT's Guide to Managing Macs 2
22 Essential Mac IT Tools 6
- Tools for Enterprise Mac Support 9

Why IT Won't Like Lion Server 10
- Apple's Radical New Mac Server Strategy . 12

Dealing with Mac (In)security 13
- No Contest: Mac vs. Windows Security . . 16

STRATEGY

Macs in Business: IT Stories 17

HANDS ON

IT's guide to managing Macs

What you need to know to manage Macs in the OS X Lion era

By Ryan Faas

NO LONGER RELEGATED TO THE FRINGE, MACS ARE FAST BECOMing integral to today's business organization. As a result, IT can no longer rely on one or two dedicated "Mac guys" to maintain its Mac fleet. Instead, Mac management has become an issue that any CIO or systems administrator may be faced with on any given day.

Along the way, the tools and techniques of managing Macs have changed as well. Pushed beyond their traditional business niches, Macs can no longer be managed independent of other processes and infrastructure. They must be integrated with your existing directory service. They require an efficient, scalable deployment model that hooks into asset management. They require secure, auditable patch management and a device and user management solution that secures each Mac's core OS components and apps.

In other words, Macs take the same requirements that apply to every Windows PC in your organization, as well as to a growing number of mobile devices. This Mac management guide will help you extend your existing support strategies to Mac workstations, and provide tips and techniques for embracing Macs as they become more prevalent in your business environment.

If you're new to Mac OS X, let InfoWorld take you through what's new in OS X Lion:

- "Mac OS X Lion's top 20 features"
- "Lion letdowns: Where it disappoints"
- "Mac OS X Lion: The InfoWorld review"

ACTIVE DIRECTORY: THE HUB OF MODERN MAC MANAGEMENT

Integration with Active Directory is the foundation for Mac management in the modern enterprise, as the OUs (organization units) in Active Directory can be used as the backbone for nearly any enterprise task, from enabling access to resources to setting group policies to pushing out updates and monitoring workstations. Through Active Directory, Macs gain access to the wide range of Windows Server tools and third-party solutions that key off Active Directory to determine which objects to affect with a given task.

In Mac-only environments, Apple's own directory service, Open Directory, plays this role. But with Active Directory entrenched in today's enterprise, extending Active Directory to be the central directory service for your Mac fleet is your best bet. Fortunately, Apple and third-party developers have enabled Active Directory to perform many of the same functions for Macs that it does for Windows clients, whether directly or indirectly.

Apple's OS X directory service support is built around LDAP and includes a plug-in architecture. The company provides a small set of plug-ins that enable support for Open Directory, Active Directory, and generic LDAP services. The big advantage for enterprises, however, is that this approach allows third parties to create additional plug-ins that offer greater capabilities than what Apple includes with each OS X release.

Apple's Active Directory plug-in has steadily updated since it was introduced five OS X generations ago, with the most notable improvement in OS X Lion being support for DFS browsing. That said, Apple's Active Directory support has its limitations, as it is primarily aimed at providing authentication and, on its own, offers almost no client management capabilities.

A Mac joined to Active Directory will have a computer account and you can restrict access to that Mac as you would any PC. You can also grant members of certain AD groups, such as the various admin groups, local admin privileges. Beyond this, the only management capability relates to whether user credentials and home directory items are cached on Mac notebooks so that users can log in when they leave your network and sync automatically when they return.

Some versions of Apple's Active Directory plug-in have proved problematic in certain Active Directory environ-

ments. Because of the scalability and flexibility of Active Directory, troubleshooting these problems can be burdensome. Early versions of Lion displayed issues with Active Directory, though the 10.7.2 update appears to have resolved most of them.

LEVERAGING ACTIVE DIRECTORY FOR MAC CLIENT MANAGEMENT

Apple has traditionally relied on Managed Preferences for client management. Often abbreviated as MCX, Managed Preferences act like Active Directory Group Policies, providing a powerful, granular system for configuring a complete user environment, including system settings and application preferences. Like Group Policies, Managed Preferences can also be used to restrict access to applications and system components.

Managed Preferences are stored as LDAP objects and attributes in a directory system. Any LDAP schema, including Active Directory, can be extended to support Managed Preferences without having to rely on Apple's OS X Server and Open Directory to provide client management via Managed Preferences.

There are three primary ways to implement Managed Preferences in an Active Directory environment:

1. Extend the Active Directory schema: Using Microsoft's Active Directory Schema Analyzer, you can scan Apple's Open Directory schema and create LDIF files that can extend the Active Directory schema with all the object data needed to support Managed Preferences data.

You can then use Apple's Workgroup Manager (freely available as part of the OS X Server Admin Tools package) to populate and manipulate that data — pointing to an Active Directory domain controller instead of an Open Directory server running on OS X Server.

Workgroup Manager can also perform a handful of user management tasks for Active Directory, though the preferred (and safer) option is to use it only for client management.

2. OS X Server and augmented records: With Leopard and Leopard Server, Apple introduced what are known as augmented records. In this approach, OS X Server is installed and configured to connect to an existing directory, typically Active Directory.

Once joined to Active Directory, the Mac server imports user data and groups from the primary directory into a secondary directory that it maintains. Mac clients connected to this secondary directory rely on the primary directory for authentication, single sign-on, and access to network resources, and the Mac server appends attributes to the primary directory's records to provide client management and Mac-specific services.

Although effective, this approach is better suited for Mac-based departments that are isolated within a larger organization, as it doesn't scale well and limits administration to OS X Server's simplified admin tool set.

3. The magic triangle: This option also requires OS X Server. In this case, however, the server hosts a full secondary directory system that scales through use of Open Directory replication. That server is joined to Active Directory, and clients are joined to both Open Directory and Active Directory.

Groups specific to Mac systems and users are created in the secondary directory, then are populated with Active Directory users. Managed Preferences are set using these groups.

This solution, which is usually implemented using OS X Server's advanced administration tools, is more scalable than using augmented records. This scalability, however, is limited to Open Directory's replication parameters, which are adequate for most environments, but not on par with that of Active Directory.

DEVICE-BASED MANAGEMENT USING LION SERVER'S PROFILE MANAGER

With Lion Server, Apple has introduced Profile Manager, a directory-independent alternative to Managed Preferences. Less of a client management solution than a mobile device management tool, Profile Manager offers the ability to manage both Mac workstations and iOS devices. However, as opposed to Managed Preferences, Profile Manager is device-focused. This enables IT to enroll devices (iPhones, iPads, Macs) and apply policies to them, but these policies are not applied based on user accounts or group membership — just devices.

Being device-focused, Profile Manager doesn't allow anywhere near the granularity of Managed Preferences or third-party solutions. It simply covers the core needs of client management and allows for self-enrollment by users through a Web-based interface that supports SCEP. When policies are updated, Apple's push notification system alerts

enrolled devices to download the update. This combination makes Profile Manager worth considering as part of a BYOD program, particularly if you will also be supporting employees' iOS devices.

Profile Manager is easy to implement. There's no need to worry about schema extensions or multiple directories. If your organization requires minimal Mac management beyond the integration offered by Apple's Active Directory plug-in, Profile Manager may be worth a look.

Keep in mind that Profile Manager requires Lion Server, and it supports only Macs running Lion. Scalability is a factor of Web server implementation, and multiple Profile Manager servers can be used to distribute load. With Apple's cancellation of the 1U rack-mounted Xserve hardware last fall, ensuring a scalable solution may be difficult, limiting the capability of Profile Manager in many, but not all, environments.

MONOLITHIC IMAGING VS. PACKAGE-BASED MAC DEPLOYMENT

There are two core ways to roll out and update Mac workstations, as there are with Windows PCs. The first is to capture a snapshot of a system to a disk image file, then push that image out to each workstation, either over a network or locally by a connected drive.

he advantage of this monolithic-imaging approach is that, once a machine has had an image deployed to it, all software is installed and all configurations are preset.

The other option is package based. You start with a base system (either a stock system from Apple or a minimally configured system image), then deploy additional software or configuration files after the fact.

This approach is advantageous when deploying Macs with a variety of application and configuration needs, as it eliminates the need to maintain a large number of images. It also allows you to simply add packages to an install workflow without having to edit or re-create your original system image.

Macs offer one distinct advantage over Windows-based PCs when it comes to monolithic imaging: Because Apple produces both the operating system and hardware, OS X is highly portable. A single image can be rolled out to a variety of Macs and be perfectly functional without further adjustment, providing that the hardware is not significantly newer than the OS X release in the image.

PACKAGE INSTALLATION AND PATCH MANAGEMENT

OS X relies on specific file types to install software and updates, much like Microsoft's .msi format. These package (.pkg) or metapackage (.mpkg) files are read by the OS X Installer service, which installs the bundled executables and support files in the requiste file system directory, usually /Library or /System/Library. This can occur manually, when package files are opened on a Mac, or it can occur unattended or in the background using a variety of tools.

Of course, some applications are installed without the use of package files. These apps often do not require support files, or they create them at first launch. As such, they can be installed simply by copying them to a Mac's Applications folder or the Applications folder inside a user's home directory to limit access to just that user.

Other applications, most notably software from Adobe, may use a proprietary installer. For these cases, you can use package file tools to take snapshots before and after installation to create an appropriate package file for the application, if needed. You can also include such files in a monolithic image or use a deployment tool that supports the proprietary format. Note that package files can simply include files and no actual applications. This makes them an ideal way to mass deploy updated configuration files or documents to specific file system locations.

APPLE'S DEPLOYMENT AND PATCH MANAGEMENT TOOLS

Apple provides a number of deployment and installation tools. These include Disk Utility for creating system images and Apple Software Restore for deploying images locally or using a unicast or multicast network connection. Package Maker, available as part of Apple's developer tools, can be used to build package files and code the installer command to install package files in the background, even via SSH. All of these features are available free of charge. (For an overview of these and other mostly free Mac management tools, see "22 essential Mac IT tools" on page 6)

As far as commercial tools available from Apple, OS X Server's NetBoot, NetInstall, and NetRestore can be used to streamline monolithic image deployment, enabling you to set up a network-based deployment operation for installing a variety of specific package files. This option allows you to combine a small number of base images with specific

packages to automatically customize your Mac fleet during deployment. NetInstall can even be configured to roll out nonsystem package collections.

OS X Server also includes a Software Update Server feature that mirrors the contents of Apple's update servers. This offers two advantages. First, by mirroring updates locally, it improves update performance while reducing the load on your organization's Internet connectivity. Second, it allows administrators to vet updates for problems before making them available. It does not, however, provide a mechanism for ensuring updates are distributed, and it cannot be used to provide non-Apple updates.

As mentioned above, the scalability of OS X Server functions has become limited due to Apple's decision to stop producing enterprise-grade server hardware. For mass deployments using only Apple technology, the ideal solution is Apple Software Restore running in a multicast configuration — with Apple's NetRestore to automate deployment completely or a series of bootable drives (even small flash drives) with a technician touching each machine to initiate the deployment process.

Finally, there's Apple Remote Desktop, which can be used to remotely deploy package files, run scripts, and perform other user support and administrative functions, including hardware and software inventory, to ease license management. Apple Remote Desktop is the Swiss Army knife of Mac management, an invaluable tool that every organization should consider purchasing even when supporting just a handful of Macs.

WHAT MAKES THE OS X LION ERA DIFFERENT

Although most of the concepts and tools discussed in this article aren't new or specific to Lion, the latest version of Mac OS X represents a new chapter in Mac management and Apple's enterprise strategy.

Until last year, when Apple announced it was discontinuing the Xserve, the company continued to position its server and related technologies as a core option for Mac management and support in business environments of all sizes. There was native support for enterprise standards like Active Directory, and OS X Server had begun to offer simplified setup for small businesses, but Apple continued to push its enterprise-specific products.

That approach seems to have drastically changed. Apple no longer produces data center-ready hardware. The company has gutted many of the advanced admin tools in Lion Server, leading to a product that seems to be a transitional release. Most enterprise features are still present, but in a manner that strongly suggests they're included for legacy support and likely to disappear in a future revision that will focus solely on small business.

At the same time, Apple seems to be building better enterprise support directly into the consumer platforms. This enables enterprises to implement them with no Apple-provided intermediary in many cases. Given Apple has never acted like a true enterprise vendor, this seems a more logical approach and will likely support and accelerate the influx of iOS devices and Macs into the workplace.

Where these products don't offer enough enterprise abilities on their own, Apple seems content to let third-party vendors fill the void. While a better approach on some levels, it remains clear that understanding the basic concepts and Apple's original approaches to integrating its products in the enterprise is still useful when it comes to evaluating the available solutions.

Ryan Faas is a freelance writer and technology consultant specializing in Mac and multiplatform network issues.

HANDS ON

22 essential Mac IT tools

The notions of risk and control differ with mobile devices and other BYOD

By Ryan Faas

DEPLOYING AND SUPPORTING MACS PRESENTS DISTINCT CHALLENGES, particularly in organizations where Macs are in the minority or are being introduced for the first time. As with many aspects of IT, having the right tool for the job is the key to managing a new or existing population of Apple desktops and notebooks.

The good news is that there are many tried and true solutions for handling common Mac deployment and management tasks. The better news is that many of the best are available for free, whether from Apple, as open source projects, or as free/donationware creations of other Mac administrators and IT professionals.

Here you will find the top 22 tools — most of them free — for managing the Macs in your IT environment. As you'd expect, the list focuses on the core areas of systems administration: deployment, client management, and directory integration.

ESSENTIAL MAC TOOLS NOS. 1 AND 2: DISK UTILITY AND APPLE SOFTWARE RESTORE

If you have more than a couple of Macs to deal with, you'll need an easy way to configure them. For monolithic imaging, the process by which you create a snapshot of one workstation and copy it to others, nothing beats Apple's Disk Utility and Apple Software Restore, both of which are included free with every Mac OS X install.

Disk Utility comes as both a GUI tool and the `diskutil` command-line option. It is equipped with plenty of local disk management functions, including partitioning, formatting, integrity checking, and repair. It also offers the ability to clone volumes and create disk images using the .dmg format, which makes it perfect for capturing a configured volume for monolithic imaging.

Apple Software Restore, which is available only from the command line as `asr`, allows you to locally or remotely deploy disk images to one or more clients. It can be used to image a Mac from a disk image on a local drive, a network share, or a multicast stream (the best option for mass deployments). When used for multicast streaming, one Mac hosts the stream via `asr` commands for others to join. As you might expect, any client imaged using `asr` must be booted from a source other than the destination volume, such as an external hard drive, a flash drive, or a bootable network volume.

While Disk Utility and ASR provide the backbone for Mac deployment, either individually using an external drive/unicast network connection or a multicast stream, there are several tools to speed up, automate, and improve your workflow for capturing a source image, preparing it for use with ASR, and initiating deployment. Be sure to check out SuperDuper and Carbon Copy Cloner for image capture and basic single-Mac deployment, and Blast Image Config for setting up ASR sessions.

ESSENTIAL MAC TOOLS NOS. 3 AND 4: NETINSTALL AND NETRESTORE

Building off of Apple's free image-based offerings are two features of the company's Mac OS X Server: NetInstall and NetRestore.

Network booting has been a staple since OS X Server debuted, and Apple has built off the NetBoot concept with NetInstall and NetRestore, both of which allow servers to host boot volumes, thereby enabling clients to boot directly from the network based on your deployment options.

NetInstall is designed for booting into the OS X installer utility and allows admins to configure options for a traditional OS X install. (It is not monolithic imaging per se, though that is possible.) It also performs pre- and post-install tasks such as disk partitioning, directory binding, and application installation.

NetRestore is designed around ASR and provides a broader range of options for monolithic imaging. It can be configured to automatically deploy specific images or to allow clients to select from available images. As with NetInstall, many deployment-related tasks can be included in the NetRestore process.

Both NetInstall and NetRestore come with the current release of Lion Server and require no client or usage license

beyond the $49 cost of the Lion Server to the $29 Lion.

ESSENTIAL MAC TOOL NO. 5: DEPLOYSTUDIO

Heterogeneous organizations looking to standardize on a single deployment tool should check out DeployStudio, a freeware monolithic imaging solution for Mac and Windows clients. DeployStudio offers local disk deployment, network deployment, and multicasting. It comes equipped with solid image management and client selection tools, integrates with Apple's NetBoot, and provides excellent deployment monitoring, all of which make it a great deployment workflow management solution. The biggest drawback — if you can consider it a drawback — is that it relies on OS X Server to create a complete network-based solution, including both boot and deployment.

ESSENTIAL MAC TOOLS NOS. 6 AND 7: STARDEPLOY AND MUNKI

Apple's package (.pkg) and metapackage (.mpkg) files are the primary software installation mechanisms in OS X. While these are typically installed by a user, OS X supports package deployment without user intervention — for example, by adding packages to a NetInstall workflow.

Organizations looking to deploy packages over a network should check out donationware StarDeploy and open source Munki. These network-based solutions, along with the commercial Apple Remote Desktop, allow admins to deploy packages in the background; they're excellent updating tools as well.

Because packages are simply a series of files along with instructions for their ultimate location in a Mac's file system, you can easily configure non-application packages for deploying configuration files and documents. Coupled with StarDeploy or Munki, this method makes it easy to add, remove, or update almost any item over the network, including browser bookmarks, security certificates, and default system or application settings.

(Note: Adobe doesn't use Apple's package format, but Munki does support remote install of Adobe applications.)

ESSENTIAL MAC TOOLS NOS. 8, 9, AND 10: PACKAGEMAKER, INSTALLEASE, AND ICEBERG

If you're going to deploy non-application packages, you'll need a tool to create them. Apple's PackageMaker is a great tool for this, and it is included with the company's Xcode developer suite, which is free and available via the Mac App Store.

Intended for use by developers to create install packages, PackageMaker provides admins with an easy way to build packages to push out to clients on their network. As noted above, these packages can be almost anything you want to deploy to a range of client devices, including documents.

Two free alternatives are openly available, but not quite as developer-friendly: the open source Iceberg and the free InstallEase, which was developed as a companion to the Absolute Manage client management suite.

ESSENTIAL MAC TOOL NO. 11: PROPERTY LIST EDITOR

Admins looking to edit system and applications preferences will want to turn to Property List Editor, a GUI tool for editing the XML .plist preference files. A similar free tool, Plist Editor, is available for modifying these files from Windows machines. You may, however, find modifying preferences from within an app and copying the resulting .plist files an easier process than using these tools.

ESSENTIAL MAC TOOL NO. 12: FILE DISTRIBUTOR

File Distributor is a slightly different form of deployment tool. It allows admins to replace files at various locations within a file system. You can even make use of wild cards to specify multiple locations. This is particularly helpful if you are using network home directories and need to deploy documents or configuration files across multiple user accounts.

ESSENTIAL MAC TOOL NO. 13: FILEWAVE

Another deployment tool worth investigating is the commercial FileWave. This Mac/Windows tool can be used to dynamically manage application installations across your network. FileWave's approach has advantages for license compliance and reclamation, as well as flexibly deploying and redeploying applications as needed.

ESSENTIAL MAC TOOLS NOS. 14 AND 15: APPLE'S ACTIVE DIRECTORY CLIENT AND DIRECTORY UTILITY

Creating a functional, secure environment requires

more than just rolling out computers and software. Global accounts stored in a secure directory service, single sign-on, the ability to secure network and local resources, and the ability to preconfigure and manage the user experience on any workstation is critical. The undisputed leader in directory services, even in Mac environments, is Microsoft's Active Directory. Thankfully, many worthwhile tools for integrating with Active Directory are available, beginning with Apple's Active Directory client and Directory Utility.

OS X's built-in Active Directory client allows you to join an Active Directory domain, and it supports secure access to resources and single sign-on via Kerberos. Moreover, it doesn't require downgrading security levels, and it allows account synchronization for off-network access.

The client can be accessed using the Users and Groups pane of OS X Lion's System Preferences app (called the Accounts pane in older OS X releases). Detailed configuration, including account and home directory sync, preferred domain controllers, and so forth, can be performed using the included Directory Utility.

It's worth noting, however, that Apple's AD client has limitations. For example, it doesn't support client management of any kind beyond basic password policies. It also doesn't support DFS browsing. There are some issues specific to various releases, including Lion.

ESSENTIAL MAC TOOLS NOS. 16, 17, AND 18: OS X SERVER, APPLE'S OPEN DIRECTORY, AND PROFILE MANAGER

OS X may support Active Directory, but Apple's native directory is an LDAP-based solution called Open Directory.

Open Directory domains, hosted by OS X Server, afford centralized accounts all the advantages that Active Directory delivers for Windows, including secure Kerberos single sign-on and client management. This system, referred to as Managed Preferences (or abbreviated MCX), is entirely LDAP-based and allows for user/group/computer-based client management that rivals the capabilities of Group Policies in Active Directory for Mac clients.

In a dual-directory setup, Mac clients can be joined to both Open Directory and Active Directory, allowing for secure access to AD accounts and resources but with complete Open Directory client management applied.

In Lion Server, Apple introduced a new Profile Manager feature that supports iOS device management and Mac client management without the need for a directory service. This alternative offers the core security client management features with a simplified setup, though it is device/client-specific rather than more granular at the user or group level.

ESSENTIAL MAC TOOLS NOS. 19 AND 20: MICROSOFT ACTIVE DIRECTORY SCHEMA ANALYZER AND APPLE WORKGROUP MANAGER

If adding a second directory isn't an option (it can often be a challenge), the fact that Apple's MCX architecture is completely LDAP-based offers an alternative: extend the Active Directory schema to support the Apple-specific attributes.

Microsoft's Active Directory Schema Analyzer is a great tool for generating the needed LDIF files. Once the schema is extended, Apple's free Workgroup Manager tool (part of OS X Server's administration utilities) can be installed on a Mac and pointed to an Active Directory domain, where it can manage some basic user account details and configure the full range of Apple's Managed Preferences.

ESSENTIAL MAC TOOLS NO. 21: THIRD-PARTY ACTIVE DIRECTORY SUITES (FREE AND COMMERCIAL)

Apple's solutions are good for Active Directory integration, but they aren't perfect. In some cases, Apple's AD client may have issues with a specific Active Directory environment, while in others, some features just don't have full parity or may not even be available (DFS is a great example). For these situations, there are worthwhile third-party options, some of which are available for free.

For more basic needs, you may want to consider Centrify Express and PowerBroker Identity Services Open Edition for broader authentication and basic access capabilities.

If you want to integrate client management capabilities without the complexity of using either a dual-directory setup or schema extensions, Centrify's Direct Control and PowerBroker Identity Services Enterprise Edition are worth considering, along with Thursby's ADMit Mac. ADMit may be particularly appealing for small Mac populations because it is a solely client-side solution that includes DFS support.

ESSENTIAL MAC TOOL NO. 22: APPLE REMOTE DESKTOP

Apple Remote Desktop is the Swiss Army knife of Mac

IT tools. Its robust feature list includes the ability to monitor the use of remote Mac computers (overall status, current application and user, full- or thumbnail-screen viewing), share screens for troubleshooting and user assistance, control a Mac without allowing users to see your actions, send global message alerts, message with users, deploy packages and individual files in the background, send Unix commands in the background, and remote startup/shutdown.

Individual actions can be grouped together as workflows. Additionally, Apple Remote Desktop offers immense reporting capabilities that can be used to identify and track virtually every minute detail of a Mac's operation, including basic hardware inventory, application usage (great for license compliance/reclamation), breakdown of which users access which Macs, and much more.

Although Apple Remote Desktop is pricey at $299 for a single license (there is no per-client license fee), the value it offers is well worth the investment for administrators, help desk agents, and even teacher/trainer workstations in Mac-based classrooms or training facilities. Quite frankly, Apple Remote Desktop is easily the must-have tool of this list.

Ryan Faas is a freelance writer and technology consultant specializing in Mac and multiplatform network issues.

TOOLS FOR ENTERPRISE MAC SUPPORT

The knock on managing Macs in business environments has long been Apple's ambivalent attitude toward providing significant enterprise support. Apple does, of course, offer tools for deploying, configuring, and managing Macs. But to move Macs beyond a departmental setting, IT will often find it necessary to look to third parties for help.

One of the biggest issues with Apple tools in enterprise environments is scalability. This has become a larger concern now that Apple has moved out of the enterprise hardware market, and has refocused its Mac OS X Server on the small-business community.

The good news is that there are some very good and significantly more scalable solutions to fill the void. Here, I've gathered the nine support tools you should consider in addition to the management tools identified in the main feature.

JAMF Casper Suite Casper Suite is an Apple-specific solution that integrates with Apple's global enterprise support services. It offers complete life-cycle management, including inventory/asset management, system deployments, software rollouts and patch management, software license auditing and control, and remote control for user support needs.

JAMF also offers iOS device management features that use the same inventory and user management capabilities as its desktop suite.

LANDesk LANDesk is multiplatform systems and life-cycle management suite. It supports Windows, Linux, and OS X and offers inventory/asset management, software distribution and discovery, centralized security and antivirus services, patch management, and help desk functionality. It also supports cloud solutions and some mobile device management capabilities.

Flexera Flexera offers software and license management solutions. For Mac systems, it supports software distribution, auditing, and license management. It also offers support for these and additional features in Windows and Unix environments, including Windows 7 migration and virtualization tools.

Puppet Puppet is a multiplatform IT automation suite. For Mac management, Puppet offers remote discovery of Mac systems and configurations, as well as centralized system administration and software update distribution. It also offers public/private cloud management and policy compliance solutions.

Faronics Deep Freeze for Mac Deep Freeze is a well-known product for ensuring consistent configuration of systems by reverting PCs to a specified state at each reboot. The Mac version doesn't include a centralized administration solution, but can be managed remotely via SSH or remote management tools such as Apple Remote Desktop or the remote management features of other suites in this list.

Dell's Kace Kace offers a range of network appliances that support Windows, Linux, and OS X. These appliances can be used for network-based system discovery and inventory/asset management, software distribution and patch management, and some limited policy management. Kace appliances also include a help desk module.

Quest Quest provides a number of enterprise management solutions for technologies such as Active Directory, Exchange, server and cloud virtualization, and network security. Quest offers a Group Policy for Mac feature that, like Centrify's Direct Control, extends Active Directory and the standard group policy tools to include Mac-specific policies based on Apple's Managed Preferences architecture.

Symantec's Altiris Client Management Part of Symantec's broad range of enterprise IT management suite, Altiris Client Management supports Windows, Linux, and Mac end-user systems. For Mac systems, it supports system discovery and inventory/asset management, monolithic system imaging, software distribution and patch management, and remote control of systems for end-user support.

Absolute Manage Absolute Manage is a suite that focuses on complete life-cycle management for PCs, Macs, and iOS devices. For Macs it offers inventory/asset management, monolithic system imaging, software deployment and patch management, license management, and security/system change management.

HANDS ON

Why IT won't like Lion Server

The new version of OS X Server just doesn't work like a server is expected to

By John Rizzo

MAC OS X 10.7 LION SERVER ADDS INNOVATIVE FEATURES AND a new low price tag, but cuts in services and the elimination of advanced GUI administration tools may force some enterprise departments to think twice about the role of Mac servers on their networks.

Some of the new features will please managers in business and education: The Profile Manager, a slick new Web-front-end tool for providing automatic push configuration and group policy management for Mac Lion and iOS clients, is miles ahead of Mac OS X Snow Leopard Server's old Managed Preferences features. Then there's built-in support for Microsoft's distributed file system (DFS) and Apple's Xsan file system, the latter for accessing storage-area networks (SAN) over Fibre Channel.

But once the initial excitement subsides and you start looking more deeply inside Lion Server, it's impossible to avoid the conclusion that Lion Server is not built for those of us in IT.

The $50 price tag — down from $500 — is the first clue that Lion Server trying to be a server for the consumer. Apple's slogan is "servers made easy." To that end, a new administration tool, called Server, is more logical and easier to use than the old Server Preferences that it replaced. And Server can do more than Server Preferences could.

But the ironic part for IT administrators is that Lion Server actually requires a greater degree of technical knowledge than its predecessors. Many routine tasks that were formerly a mouse click away now can be accomplished only via the Unix shell command line. Worse yet, some routine tasks are no long possible at all.

LION SERVER: A GREAT BIG APP THAT'S TRICKY TO INSTALL

For the enterprise, the first clue that something is amiss in Lion Server comes right at installation. Lion Server installs like a great big iPhone app. It's available only as a download from the Mac App Store and self-installs as soon as it's downloaded; all you can configure is the admin email address. Finally, it deletes the installer, though you can stop the install to make a copy before it's deleted. This app philosophy filters down through the software as well.

But Lion Server isn't Angry Birds. The installation process includes downloading the 4GB Lion OS client installer, plus hundreds of megabytes more of server components. Depending on the type of installation (such as upgrade or new), you may have to make a second trip to the App Store to get the server components. A problem for administrators is that there is no supported way to make your own bootable installation DVD. There is an unsupported hack to create one, but it can bring up other complications.

Worse, there's no clean install option from within the installer itself. To do any install, you need to boot the Mac with Mac OS X 10.6.8 Snow Leopard or Mac OS X 10.7 Lion from a volume (hard disk, partition, or USB flash drive) and run the installer from that boot drive. To do a clean install, you need two volumes: one to boot from, one to install onto.

Apple has streamlined the server configuration process from previous versions, with fewer screens asking questions and more done automatically. The installer is smarter as well. If you tell the setup assistant to create an Open Directory master, it will do that as well and DNS for the server's IP address if it doesn't find it on the network or the Internet.

That's pretty nice, particularly if you don't know what DNS is. Unfortunately, if you do know what DNS is, the Server application — now the only management tool installed with Lion Server — won't show you the DNS configuration is. It provides no way to edit settings for DNS, DHCP, Open Directory, and other network services.

The old administration tools that can access to these services — Server Admin and Workgroup Manager — are no longer part of Lion Server. Instead, they are available are a separate download — but not from the Mac App Store, where you get Lion Server app. You have to go to Apple's support site. Nothing I could find in the installation screens, the help files, or Apple's main Server website even mentions them. To quote Douglas Adams, the tools were "on display in the bottom of a locked filing cabinet stuck in a disused lavatory with a sign on the door saying 'Beware of

the leopard.'"

LION SERVER'S MANY MISSING SERVICES

Once you locate and download the Server Admin tool, experienced Mac OS X Server administrators will notice it's a much thinner tool than it used to be. Roughly half the services that used to be there are missing. Most user-based services, such as file sharing, calendaring, and Web services, have been moved to the simple Server application. Others, such as QuickTime Streaming Server, have been completely removed.

One of the more significant feature rollbacks comes in reduced support for Windows clients. For years, Mac OS X Server's LDAP-based Open Directory had the ability to function as a primary domain controller (PDC) to support Windows clients. The PDC provided Windows clients with single sign-on authentication, and for those who work on both platforms, it gave users access to the same accounts and server-based home folders from their Windows PCs as well as their Macs. In Lion Server, Windows clients still have access to file sharing, but are now second-class clients.

On the flip side, Lion Server retains Open Directory integration with Active Directory. Mac clients can still bind to Active Directory using the "golden triangle" configuration, where Mac OS X Server and Open Directory bind to Active Directory.

Another service that Apple deleted is the print server of previous Mac OS X Server builds. Lion Server contains only the same ability to share printers found in every copy of Mac OS X client for the past five years: the open source Common Unix Printing System (CUPS), which gives Macs the ability to host shared print queues and simple pools of printers but lacks the enterprise features that previous print servers had. For example, Lion Server's CUPS cannot prioritize printers in the pool or set quotas for individual users or printers. And you can't publish printers to Open Directory.

LION SERVER: GUI, GUI, GONE

Other services that appear to be missing in Lion Server are actually still there. NFS (the Unix-based file sharing protocol) is gone from Server Admin, but it is accessible via the command line. Podcast Producer, Mac OS X Server's podcast workflow system, still uses NFS, and you can create NFS-based home folders for users. But where before you could click check boxes to configure it, you now need to type Unix commands. Similarly, the FTP server isn't available in Server or Server Admin but is available through the command line.

If you're looking for the configuration for MySQL, you won't find it, either in the GUI or in the command line. That's because Apple has replaced it with PostgreSQL, another open source database. On one hand, this is an improvement, because PostgreSQL is considered to be more powerful than MySQL. But whereas Snow Leopard's Server Admin tool had GUI settings for MySQL, PostgreSQL is command line only in Lion Server.

With others services, GUI administration tools survived — barely. Lion Server still has industrial-strength Apache Web services, but it has replaced several windows' worth of settings with little more than an on/off switch and a button to add another host website path and domain name. This makes it more difficult to host multiple websites as virtual hosts or at least more difficult to figure out why it isn't working.

The admin tools no longer provide a way to set URL aliases and redirects, which point to files or folders while keeping the location hidden from uses. Also eliminated is the ability to set domain-name-level Web alias. And the GUI tools provide no way to configure the execution of CGI scripts on a website. You can no longer set maximum simultaneous connections, connection timeouts, or persistent connections. These and other configurations were available in the Server Admin tool in previous incarnations of Mac OS X Server. Rather than simplify Web configuration, this puts much of Apache's features out of reach to those less adept in editing config files.

The same is true for VPN configuration, iChat (Jabber) service, and to a lesser degree the iCal calendaring service.

The exception to all this is email service, which still has the same level of configuration detail as in previous versions of Mac OS X Server, and with a better Web mail implementation.

LION SERVER'S PROFILE MANAGER: THE SOLE BRIGHT SPOT

For business and education, Profile Manager is the shining spot in Lion Server. Once you turn on services and switch on Profile Manager, it automatically creates configuration profiles, which are XML files that can be pushed to Mac and iOS clients that automatically configure them to

receive the service. You can send out an enrollment profile, which enables changes to be pushed out (when the user accepts it). You can have different sets of profiles that apply to groups of users, as well as to individual devices and groups of devices.

Profile Manager goes well beyond simply configuring clients for networking, VPN, and mail. You can set hundreds of group policies. For example, you can prevent iOS and Mac users from accessing the App Store, prevent Mac and iOS applications from launching, block users from making changes to system preferences, block Macs from accessing external storage devices or optical discs, prevent iOS users from watching YouTube, set parental controls, and much more. (Users can see the settings applied to their Mac in the new Profiles system preference, or in the familiar Settings app in iOS.)

The drawback to Profile Manager is that the Mac clients it supports must run Lion. Fortunately, the old Managed Preferences for older versions of Mac OS X clients is still available through Workgroup Manager.

Still, Profile Manager does more than Managed Preferences, and it does more automatically, and in way that is easier and faster to set up, no command line necessary.

But even here, one item may rub IT managers the wrong way: The data stores for Profile Manager, Address Book Server, iCal Server, Webmail, and the built-in wiki are bundled in one database in a location that cannot be moved: on the server's boot disk. I suppose the thought is that consumers usually have only one hard disk.

SO WHAT DOES IT DO NOW WITH MAC OS X SERVER?

Lion Server's debut poses a dilemma to many IT shops using Mac OS X Server. Of course, IT departments can keep running Snow Leopard Server to serve clients that include Mac OS X Lion, older Mac OS X versions, Windows, and Linux. Or you can use both the Lion and Snow Leopard Mac OS X Server versions. For example, if you wanted to keep the Windows PDC functionality but also want Profile Manager, you could run Snow Leopard Server as an Open Directory master (and PDC) and bind Lion Server to it. You could even run both servers in virtual machines on a single Mac.

But in the longer term, I won't be surprised to see some enterprise sites phase out Mac OS X Server and move to Windows Server – even as they embrace more Mac clients. When you consider Lion Server's truncated capabilities along with the discontinuation of the Apple Xserve rackmount hardware, the signal from Apple seems to be it's not that interested in keeping businesses on Mac OS X Server.

John Rizzo runs MacWindows, a website devoted to helping Mac OS X and Windows get along. He is the author of "Mac OS X Lion Server for Dummies" and "Mac OS X Snow Leopard Server for Dummies."

APPLE'S RADICAL NEW MAC SERVER STRATEGY

By Tom Yager

The first app made for Lion to hit the App Store is a real eye-opener: Mac OS X Lion Server, costing $49, a tiny fraction of Snow Leopard Server's $499 price tag. With that, Mac OS X Server as we knew it is no more. To sweeten the deal, Apple is throwing in Xsan, the SAN software Apple used to sell for $999. With Mac OS X Lion Server, a Mac Pro with a Fibre Channel card becomes a scary-fast, bulletproof distributed storage server for Mac networks.

Sounds like a steal, but it's also a move that raises prickly questions. Critics point to Lion Server's drop in price, the abolishment of node-locked licensing, and simplification of the administrative GUI as foreshadowing Apple's departure from the server market. The $49 price tag doesn't mitigate the risk of implementing a server platform that's in decline.

However, I seriously doubt that's an issue. Lion Server looks nothing like a last gasp. It appears instead to signal a shift in mission: Instead of trying to displace enterprise Windows, Linux, and Unix servers, Lion Server focuses on providing easily managed native network services to workgroups of iOS and Mac users.

Lion Server's Profile Manager is key to enterprise deployments of iOS devices. For user-owned devices that connect to company infrastructure, Profile Manager can configure the device for company services, including services not hosted by Mac OS X or iCloud. Company-owned iPads and iPhones can be locked down with profiles that apply to arbitrarily defined groups of users or devices. In both cases, all the user has to do is visit a Web portal that Lion sets up and hosts automatically; no tethering to an IT configuration terminal is required. After the profile is loaded, updates can be pushed to a device over the air, along with emergency commands like remote wipe and password change.

That's just one of Lion Server's rich array of services. For $49, it equips your network with any combination of file, email, calendar, Web, chat, podcast, VPN, directory, and backup (Mac only) services. Apple's commitment to standards means that Lion Server remains a good candidate for general-purpose use. As I've alluded to here and will elaborate on in a forthcoming review, Lion Server takes a hard turn toward usability and places an emphasis on service to users with Apple hardware.

Tom Yager is a Web developer and a Mac expert.

HANDS ON

Dealing with Mac (in)security

The Mac is a minor malware target, but IT has other issues to watch for

By Glenn Fleishmann

MACS ARE IMMUNE FROM SECURITY THREATS, RIGHT? IT'S WINdows we have to worry about. That water-cooler wisdom needs to be flipped on its head, security experts and IT managers warn. Microsoft has gotten its security act together with Vista and its current security-response program; meanwhile, Apple is fast becoming the company most in need of getting its security mojo going.

Many IT and security managers who have focused on securing Windows need to turn their attention to the Mac OS, as these six Mac security flaws attest. And with Macs increasingly making their way into the enterprise, they shouldn't wait: According to a recent Yankee Group study, 80 percent of senior managers at 700 companies had Macs in house, with 21 percent boasting 50 or more Macs in use.

A few security holes in Mac OS X are already known, such as the ARDAgent vulnerability. But that's not where the principal Mac security threat lies. From interviews with security experts and corporate IT managers, it's clear that security concerns and potential risks are much more quotidian — exactly the kind of bread-and-butter stuff that is easy to ignore, especially for Macs, where IT's familiarity with the Mac is slight because users have typically managed the computers themselves.

It's time for IT to figure out where the Mac's security holes are so that you can plug them before your corporate knowledge starts bubbling out. Here are the six main flaws.

SECURITY FLAW NO. 1: UPDATE MANAGEMENT

Across the board, IT and security folks peg patch and update management as Apple's biggest lacuna. The problem is not that the Apple doesn't release security patches, bug fixes, and functionality upgrades on a continuous basis. Instead, the issue is with four flaws in Apple's update process:

1. Unlike Microsoft's Patch Tuesday, Apple offers no predictable schedule on which critical updates are released.

2. There's no simple rollback or uninstall provision.

3. Many updates don't fully document their changes.

4. Apple doesn't provide hooks for third-party software to assist in managing patch installation or rollbacks, although such software does exist. (Apple does allow configuration so that software updates are downloaded from an intranet server, however.)

"Apple just goes ahead and issues an update without anyone knowing it's coming, and no one knows what's inside it," says Rich Mogull, an independent security consultant, formerly of Gartner.

This demonstrates Apple's newness to the enterprise environment with Mac OS X, despite the operating system's many years on the market and its growing adoption rate. For single users and midsize offices, these patch policies raise few eyebrows. But for large corporations, they're insufficient.

Third-party patch management software for Mac OS X is available (such as LANrev, Bigfix, and PatchLink), but only a few suites are designed for anything but Mac OS X — which makes it hard to have a unified suite for Windows and Mac patch management.

The danger here is in allowing individual users to manage their patches, which could lead to systems — especially laptops carried by mobile users — being far out of patch compliance and, thus, vulnerable to long-fixed security holes.

Solution: Install an intranet proxy for Apple's updates.

Solution: Review Mac-oriented patch management; these suites also include options for distributing other software updates and corporate documents, as well as auditing settings and installed software. Check with your patch management vendors about plans to add Mac support if yours do not. Send reminders to Mac-using employees whenever critical patches appear to install the updates as soon as possible.

Solution: Schedule patch sessions for laptops that are primarily out of the office, as they are most vulnerable to proximity attacks via Wi-Fi or Bluetooth, as well as attacks from untrusted networks on which they are located.

SECURITY FLAW NO. 2: SERIOUS THIRD-PARTY SECURITY FLAWS ARE SLOW TO BE FIXED

Most of Apple's most serious security updates, ones in

which remote code execution or arbitrary code execution are possible, typically involve third-party software — often open source or free software components. (Notable exceptions are Safari and QuickTime, Apple-developed products that have had dozens of serious flaws, none of which have so far turned into attacks prior to being patched.)

While the project running the software often patches such vulnerabilities in hours or days, Apple often lags in releasing such updates. For example, Apple included version 2.2.6 of the Apache Web server in Mac OS X 10.5 (Leopard) in October 2007. Apache was updated to 2.2.8 to fix several security flaws in January 2008, but Apple didn't ship an update until March 2008.

But other times, Apple is speedy. For example, an Apple researcher discovered a set of flaws in the Ruby language and environment, which were documented and patched June 20, 2008. In this case, Apple took only 10 days to release its security patch.

In both cases, it's critical to note that neither Apache nor Ruby is used by default in Mac OS X. Apache must be enabled either through the Sharing preference pane's Web Sharing service check box or at the command line. Ruby isn't used for any native Apple products, and it must be wired in at the command line or through third-party packages.

Locking down this sort of access would prevent the most likely security flaws from being exposed, but that's problematic with the current OS. Configuration management software does exist to help such a lockdown, but again, Mac support may not exist in the software you're running companywide.

That should change. "We are starting to see early signs that some vendors are supporting Mac as a platform for those configuration management systems," Mogull says.

Solution: Consider limited deployment of third-party software to restrict configuration by administrative users if your current solution doesn't include Mac support.

SECURITY FLAW NO. 3: EVERYBODY'S AN ADMINISTRATOR (OR NOT)

Apple has a binary attitude when it comes to modifying system settings, gaining access at the command line to its Unix underpinnings, and installing software: You're either an administrator — or you're not.

For home users and small businesses, the distinction is probably enough. An unprivileged or normal user can be restricted via parental controls and typically can't create user accounts, enable file-sharing services, or install certain kinds of software. For that, an administrative-flagged account is needed.

But with administrator privilege set, a user can turn on features through switches in System Preferences, such as enabling Samba (Windows SMB networking) — "the Mac version is typically three to six months out of date," Mogull says — or using the Terminal application to activate any of the thousands of Unix daemons and servers that ship as part of a stock Mac OS X system.

"It's hard to enable those things on Windows," says Thomas Ptacek, a principal consultant at security firm Matasano Chargen, noting that even when such settings are available in Windows, the settings are typically obscure or complicated enough to deter average users. By contrast, a single click might be enough in Mac OS X.

Solution: Limit administrative accounts to users that require them.

SECURITY FLAW NO. 4: NAÏVE USE OF BACK TO MY MAC

Mac OS X includes one special service that sounds alarming at first glance — and can be a real security hole in unmanaged environments. Back to My Mac, a remote access system built into Mac OS X 10.5, requires both a MobileMe account (formerly .Mac) or iCloud account from Apple and administrator privileges. Back to My Mac operates like the GoToMyPC familiar to Windows administrators, although it's less insistent about working around intentional blockades.

While Apple uses IPv6 tunnels, IPsec encryption, and Kerberos tickets to secure connections, starting up such a connection from anywhere on the Internet requires just the password to someone's MobileMe account. With that password, all computers with Back to My Mac enabled can have their files examined or screens remotely controlled.

In a managed enterprise, security experts don't believe that Back to My Mac creates any real risk, despite its feature set. "No enterprise is going to allow something like Back to My Mac unless it's running through a VPN tunnel," Mogull says, at which point it would conform to the enterprise's policy. If users are running Back to My Mac on their own, "it would mean that [IT] royally screwed up" the firewall, he adds.

Matasano Chargen's Ptacek says that Back to My Mac

will eventually fall under the category of services that businesses ban their employees from using in the office. "Enterprise users are not allowed to use Gmail or Yahoo Mail," he notes, and Back to My Mac should be treated the same.

Solution: Confirm that Back to My Mac won't work in your environment. Establish a policy that bans its use.

SECURITY FLAW NO. 5: COMPLACENCY OVER MALWARE

The recent appearance of a kit that lets malicious parties install Trojan horses in legitimate software to, in turn, obtain root access to a Mac seems to run counter to the widely held view that Macs are immune from many of the exploits that once plagued Windows (and that Vista ameliorated).

But that Trojan horse doesn't meet the smell test: Like a few other "concept attacks," the exploit requires that someone download and install software, although no password is required for the malware to run. (The exploit relies on the escalated privileges available for the Apple Remote Desktop agent, or ARDAgent, even when it's turned off. An AppleScript command can be sent to the agent, which is handed off as a root-level shell command.) A survey of security experts and the buzz among the Mac enterprise management community shows that this threat is a nonstarter.

The fact is that the Mac has not been a malware target, and it is safer than Windows from such threats. And that's where the risk lies: The Mac is safer from malware today, and there's very little concern about the Mac being a gateway to infecting Windows users.

But that may not be true in the future, and there is some concern that IT won't be ready to protect Macs from malware when that day comes.

Today most of those who follow Mac security closely seem to abjure antivirus software. "It's not unreasonable to use antivirus in an enterprise, especially if compliance is an issue," says Mogull — but "I wouldn't necessarily recommend that for a consumer," he adds, because today's antivirus apps don't address Mac OS X's actual risk profile today. "Antivirus is an industry failure," Ptacek says. Because of this, he can't recommend that companies install antivirus software at all.

Dino Dai Zovi, an independent security researcher, is concerned about acceleration in this area. "Because there is still very little malware in the wild targeting Apple, it is still a safe platform, and it is in a lot of ways safer than the Windows equivalent. But I think that that time is rapidly changing," he says.

Mogull cautions that the worst could be yet to come. "It isn't that the Mac is immune or even more resistant to these attacks, there just hasn't been very much interest in them," he says, a sentiment echoed by security experts and IT managers. With more Macs in the enterprise, it's likely that attacks designed to extract information or take over Macs to use them as zombies will hit the wild.

Apple got a taste of what it's like to be a target in spring 2011, when a fake antivirus app widely infected Macs. Apple quickly released an update to Mac OS X Snow Leopard (and included it in Lion) that detects such malware and updates its threat profile every day.

While the Mac OS itself is fairly safe, at least for now, from malware, the Mac OS X's default Safari browser is not. "We've long since moved into this place where it's about the browser and about JavaScript," Ptacek says.

Even security experts unconcerned over OS-level malware threats are worried about browser-based threats. The fears center on as-yet-undiscovered flaws in the Safari browser and on Apple's use of the WebKit, a browser engine that's both employed throughout OS X and available to third-party developers. The concerns are not theoretical: A flaw in Safari on the iPhone found in a TIFF library module lets an iPhone forfeit root control just by visiting a Web page. (This was briefly a popular way of jailbreaking iPhones to install third-party software.)

Solutions: Keep abreast of security updates and security news related to Macs. Make sure the same outgoing firewall monitoring tools cover Macs as other platforms to identify hallmarks of hijacked systems.

SECURITY FLAW NO. 6: APPLE'S SECURITY IS HALF-BAKED

The strongest concerns over Mac OS X security have to do with improvements introduced in various versions of Mac OS X that fall short of what's fully needed.

That doesn't mean Apple is not trying. Mac OS X 10.5 Leopard, for example, put in place a strong foundation on which more enterprise-oriented features should be built, as well as a greater extension of integrity and attack resistance for individual users on their own or in companies. For example, Apple added library randomization to Mac OS X 10.5, which prevents virus writers from finding code at specific places in memory each time. However, unlike

with Vista, only a subset of what can be protected is actually protected.

Mac OS X 10.6 Snow Leopard added stack protection and sandboxed more elements within the core OS and apps such as the H.264 video engine and Safari plug-in mechanism. Mac OS X 10.7 Lion added application sandboxing and full-disk encryption, and it improved the address space layout randomization (ASLR) technology introduced in Leopard.

Solution: Monitor carefully what Apple updates, and consider joining the Mac OS X developer program (it costs $99 per year) to get better insights as to what future versions are adding and what issues other businesses are experiencing.

DON'T BE COMPLACENT ABOUT MAC SECURITY

It's vital that security planning takes place before holes appear, and that the IT staff is ready to handle the differences between the Windows, Unix, and Linux systems they may be accustomed to and what Mac OS X brings with it. Dai Zovi said, "The biggest danger is a sense of complacency: 'Oh, it's a Mac, we don't need to worry about this.'"

Glenn Fleishman writes the Practical Mac column for the Seattle Times and writes about Wi-Fi and mobile broadband on his blog Wi-Fi Networking News.

NO CONTEST: MAC VS. WINDOWS SECURITY

By Roger A. Grimes

For nearly two decades now, security experts have debated whether Microsoft or Apple offers superior security. The battle heated up again in the wake of news out of Black Hat about a newfound weakness in the Mac platform. However, the question of whether Microsoft or Apple is more secure is no longer even relevant: Security threats of today and tomorrow aren't as tied to specific desktop platforms as they once were.

Macs have far more theoretical vulnerabilities than Windows machines. (I am a full-time principal security analyst at Microsoft.) It's been that way for a long time. However, Macs are attacked far less because they are used less than machines running Windows. Call it security through obscurity. Now that Macs are increasing in popularity in the enterprise and beyond, though, they're no doubt on the cusp of being targeted by hackers. However, I predict that Apple will rise to the occasion and fill the vulnerability gaps. It has to, or growth will slow.

Still, the question of whether Mac or Windows is more secure is no longer relevant. The computer security paradigm is shifting at this very moment. Cloud computing, Web 2.0, and mobile technologies are exploding, and with those changes, traditional attacks are making way for a new crop that ignore platforms. Think ANSI bombs, boot sector infectors, macro viruses — seen any of those lately?

I worry about the risks associated with cloud compromises more and more. For example, if someone compromises a public cloud product and takes over one customer's instance, how easy would it be for that person to get to all the cloud's data? I know hackers have a far easier time taking over multiple websites hosted on a single Web server than they would taking over sites hosted in separate machines. Whether you're a Mac or a Windows shop doesn't factor into the equation.

Default data syncing, too, is becoming a fact of life, and it opens new potential security holes, regardless of platform. The mere act of opening a document on any computer or device could automatically send a copy of that document into the cloud, regardless of your intention. Is it well protected in the cloud? If you then open a document on your least secure device, can that machine access all your synced cloud documents? Who else in the cloud can see my documents?

How does IT manage security when it can manage only a few of the devices connecting to the most valuable data? How long until we have our first XML-written virus or worm? If someone compromises my worldwide, biometric ID, how do I repudiate everywhere it might be used and how can I use something else? For example, if my logon is my fingerprint or face, and the attackers steal my authentication token and fake being me, how can I get it back? What will I use instead?

Users, too, remain a huge security threat, regardless of what OS they're running. People remain susceptible to sophisticated phishing and social engineering attacks that dupe them into giving up their credentials, for example. They continue to install programs they shouldn't on their machines, allowing hackers an opportunity to pounce.

Heck, my own kids have a verifiable computer security expert in their house, yet they couldn't care less about computer security in their daily lives. They haven't changed their Facebook or online banking passwords since they set them — again, they're leaving themselves susceptible to attacks regardless of what platform they might be using.

So when I'm asked if Microsoft or Apple's security is better than the other, it's not a question even worth answering. Overall, computer security is pretty bad. Nearly any company can be hacked, with just a little research and know-how. Fake malicious programs still abound. Antivirus software is struggling like never before. Most people have had their identity and credit card information compromised several times over the last few years. Most people have had their computers infected over the same period.

Our security paradigm is shifting in a huge way before our eyes, and we're not using our best defenses while we argue over the relative minutiae of the competing platforms' relative security. Meanwhile, we're taking casualties with more to come — all the while wondering why our current strategy doesn't work.

Roger A. Grimes writes InfoWorld's Security Adviser blog.

STRATEGY

Macs in business: IT stories

Learn the hows and whys of organizations that have taken the Mac plunge

By Leon Erlamger

IT'S NOT YOUR IMAGINATION. APPLE MACINTOSHES ARE TURNing up in businesses beyond the creative departments, increasingly becoming a normal part of the IT fabric. One recent IT survey by researcher Information Technology Intelligence shows that 23 percent of respondents had at least 30 Macs in their businesses, 12 percent had at least 4,000 Macs -- and 68 percent said they would let users choose Macs as their work PCs in the next year. (Both IDC and Gartner report that Macs now make up more than 13 percent of all PCs sold to individuals.)

IT's acceptance of the Mac appears to be genuine, not a grudging response to unwanted user demand: "Desktop managers are painting a rosy future for Apple on the corporate desktop," the recent Forrester report states. One reason is the quality of the Mac hardware and operating system; Information Technology Intelligence's survey shows that 82 percent of IT respondents rated the Mac platform as very good or excellent, compared with 60 percent for Windows Vista.

"About a year ago, I started noticing that every time I brought my MacBook Pro to a conference, just about everyone else had one too," says Carl Howe, a research director at the Yankee Group. Howe is not alone: "We're definitely hearing more stories of Mac consumers pushing IT to let them use Macs at Windows-based work environments," says Tim Bajarin, president of the consultancy Creative Strategies.

The growth in Mac adoption has been driven by several factors, everything from Apple's conversion to an Intel-based platform with several virtualization options to run Windows to the Webification of corporate applications, the rise of software as a service, and Apple's dramatic ascendance in consumer mindshare.

"IT shouldn't be afraid of Macs," says Kunal Malik, IT director at Citrix Systems, a virtualization provider. "They're very manageable. You just have to prepare the environment, understand how to manage the Mac's limitations, and then help your users adopt the platform they want."

Several companies share the lessons -- good and bad -- that they have learned. Among the main consideration: desktop management, security, and Apple's non-enterprise focus. But with some creativity and an increasing reliance on users to be more responsible for the systems they choose, the majority experience is positive.

CITRIX SUCCEEDS BY PUTTING USERS IN CHARGE

A perfect example is virtualization provider Citrix Systems, which has instituted Bring Your Own Computer (BYOC), a program that lets employees choose their own laptop computer, which they can use for both work and play. "We wanted to give employees the opportunity to use the device they're most comfortable with," says CIO Paul Martine. More than a third have chosen Macs. (IBM has a similar initiative.)

Martine estimates that the traditional IT procurement, imaging, and tracking process costs Citrix about $2,500 to $2,600 every three years, so under the BYOC program, Citrix IT gives each participant a $2,100 stipend to get whatever system he or she wants. And IT has no problem if users spend more than the stipend -- from the users' budget, of course -- to get their preferred systems.

But participating in BYOC does come with two requirements: The user must purchase a three-year warranty and maintenance program and must have client security software installed. Citrix's IT group provides the security software at no charge. Users so far have been responsible in managing their security: All four virus incidents that occurred this past year all started on IT-managed systems, not those under BYOC.

Given Citrix's business, it's not surprising that it handles application incompatibilities and security issues thin-client-style using Citrix's own XenApp application (provided free to employees), which serves up corporate and most client applications, including Microsoft Office, from servers in the data center. However, if employees want to run Mac versions of Office or other applications, such as Apple's Keynote presentation tool, they are free to do so.

Users are responsible for their own hardware mainte-

nance and repairs. "That's what the three-year warranty is for," says Martine. "Even my kid knows how to keep his system up to date," he adds, "and we've found that the users take care of their own equipment much better than they take care of IT's."

For other issues, the help desk — which has both Mac and PC expertise — is available. User files are kept on the servers and backed up internally, but users are allowed to copy files to local drives, as long as they understand securing such files are their responsibility.

A survey taken both before and after the pilot of the program found that 56 percent of participants felt that using their preferred device made them more productive. Their managers weren't so sure, but they did notice a definite increase in staff job satisfaction. Meanwhile, IT is saving on acquisition costs and has fewer client PCs to manage.

FACEBOOK FACES FEW LIMITATIONS TO MAC INTEGRATION

Facebook is even more of a mixed Mac and Windows corporate environment than Citrix. IT director Kunal Malik estimates the company is 60 percent Mac and 40 percent Windows. "We found early on that Macs were better at multitasking and a much better environment for coding than Windows," he says.

As the company grew, Macs spread to sales, marketing, and business development, whose users much prefer Apple's Keynote to Microsoft PowerPoint. "Our CRM, ERP, and financial applications are all Web-based and Firefox-compliant, so we have no issues running them on a Mac." But most of their financial users are primarily Windows-based because the latest Mac version of Excel doesn't allow the use of Visual Basic macros.

Like its more Windows-based brethren, the company runs Active Directory, which integrates well with Apple's Open Directory. But integration with Microsoft Exchange is not so smooth. The Mac Exchange client, called Entourage, doesn't support all Exchange functions, but Mac users have managed to get around most of them by relying more heavily on their BlackBerrys and iPhones and using discussion forums to substitute for long e-mail threads.

Despite the Mac's dearth of malware, Facebook requires Mac users to run client security software, since the Mac has recently become a network entry point for Windows malware.

ORANGE COUNTY SHERIFF MISSES DELL'S LEVEL OF SERVICE

Although many companies have successfully brought Macs into their Windows-oriented infrastructure, not all mixed Mac/PC shops' experiences are rosy.

After using Macs to create training podcasts, the Orange County (Calif.) Sheriff's Department expanded Mac use to its investigative staff and environments with little desk space, such as in a helicopter. "Dell didn't have the form factor we were looking for," says Chris Cao, a technical system specialist. So the agency deployed Mac notebooks running Windows via Apple's Boot Camp technology, which creates a separate partition to boot into Windows.

What IT hadn't planned for, however, was the hard time it would have getting Dell's enterprise level of support from Apple. "Apple won't let us crack open the cases unless we're Apple certified, and replacement parts take a while to get here," says Cao. For confidentiality reasons, investigator laptops simply cannot leave the grounds, but it took a full nine months to convince Apple that on-site service was needed. "Dell would just come out the next day, part in hand," says Cao. (Facebook's Malik points out that it's easy to protect confidential data with encryption and that, unlike Orange County, he hasn't had any problems getting next-day on-site service.)

Updates and reimaging are also more involved, since there are two OSes to deal with. "With Dell, you just yank out the drive, put it in the drive image machine, and you're done in 10 minutes." However, as with Citrix, many organizations address Apple's enterprise support shortcomings by shifting more of the management and repair burden to their Mac users.

There are also the usual complaints from IT departments about Apple's lack of product road maps, which makes planning just about impossible. To address that issue, Facebook simply keeps extra inventory around. "We accumulate lots of inventory right before Apple events because we know that's when they'll probably announce changes. This allows us to react and manage those changes until we're ready to move to a new platform."

And the road map issue may not be that critical in reality: "Beyond three months, most technology road maps are lies anyway," says John Welch, senior systems engineer for the Zimmerman and Partners ad agency.

Leon Erlanger is a freelance author and consultant specializing in security.