Hypervisors

Platform	Website
VMware	www.vmware.com
Microsoft Hyper-V	www.microsoft.com/en-us/cloud-platform/server-virtualization
Oracle VM	www.oracle.com/virtualization
Citrix Hypervisor	www.citrix.com/products/citrix-hypervisor
KVM (Open Source)	www.linux-kvm.org
VirtualBox (Open Source/Oracle)	www.virtualbox.org

Tools

Tool	Website
VMware Open Source Tools	www.vmware.com/opensource.html
VMware Security Resources	www.vmware.com/security.html
Microsoft Hyper-V Security	https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/plan/plan-hyper-v-security-in-windows-server
CIS Benchmarks (VMware and Docker)	www.cisecurity.org/cis-benchmarks/

Master Checklists

The following checklist summarizes the steps for auditing virtualization.

Checklist for Auditing Virtualization
❑ 1. Document the overall virtualization management architecture, including the hardware and supporting network infrastructure.
❑ 2. Obtain the software version of the hypervisor and compare with policy requirements.
❑ 3. Determine what services and features are enabled on the system and validate their necessity with the system administrator.
❑ 4. Review and evaluate procedures for creating accounts and ensure that accounts are created only when a legitimate business need has been identified. Also review and evaluate processes for ensuring that accounts are removed or disabled in a timely fashion in the event of termination or job change.
❑ 5. Verify the appropriate management of provisioning and deprovisioning new virtual machines, including appropriate operating system and application licenses.
❑ 6. Evaluate how hardware capacity is managed for the virtualized environment to support existing and future business requirements.
❑ 7. Evaluate how performance is managed and monitored for the virtualization environment to support existing and anticipated business requirements.
❑ 8. Evaluate the policies, processes, and controls for data backup frequency, handling, and offsite management.
❑ 9. Review and evaluate the security of your remote hypervisor management.
❑ 10. Review and evaluate system administrator procedures for monitoring and maintaining the state of security on the system.
❑ 11. Verify that policies and procedures are in place to identify when patches are available and to evaluate and apply applicable patches. Ensure that all approved patches are installed per your policy requirements.
❑ 12. Review and evaluate the security around the storage of virtual machine data.
❑ 13. Verify that network encryption of data-in-motion is implemented where appropriate.
❑ 14. Evaluate the low-level and technical controls in place to segregate or firewall highly sensitive data on critical virtual machines from the rest of the virtualization environment.
❑ 15. Evaluate the use of baseline templates and the security of guest virtual machines as appropriate to the scope of the audit.
❑ 16. Perform the steps from Chapter 5 and Chapter 12 as they pertain to the environment you are auditing.

CHAPTER 14

Auditing End-User Computing Devices

This chapter discusses two separate audits, beginning with Windows and Mac client systems and then covering mobile devices such as Android and iOS phones and tablets. These audits include system management processes, administrative controls, policies, and basic controls that should be present on these systems. The following topics are discussed:

- Background of client and mobile computing technologies
- Essential auditing steps for these technologies
- Key technical resources for additional information

Background

The computing power available to the everyday user has grown exponentially over a generation to the point where today's small desktops and laptops are far more powerful than the room-filling supercomputers of 20 years ago, while mobile phones and tablets are now packing as much power as some modern laptops. The power of these devices means that end users can do more today with a laptop or phone than at any time in history. This also means that these devices need to be managed closely in a business environment, as a powerful, unmanaged system can present a significant risk to business operations.

NOTE For the purposes of this book, even though laptops and similar form factors are "mobile" in the sense that they are portable, we will use the term "mobile device" to refer to smartphones and tablets running smartphone-like operating systems. The terms "client" and "client device" will refer to laptops and desktops running Windows or macOS operating systems.

Until the early 1970s, computing tasks were performed mostly on large, centralized computers, and employees entered instructions by punching individual holes in special paper punch cards and inserting those cards in a precise sequence

into a feeder. During the late 1960s and early 1970s, terminal interfaces were developed, and people could use a keyboard to access the central computer remotely. With the advent of personal computers, including the IBM PC, which arrived in 1981, computing power began moving closer to the user. Over the last 40 years, these systems have evolved, with components miniaturizing, performance improving, and new technologies arriving, all while becoming less expensive. Computers became light enough to carry, battery technology advanced, and soon laptops emerged. As computers improved, employees have become more and more productive, and businesses have continually found new ways to leverage this power.

While computers were shrinking and becoming more powerful, companies began experimenting with pocket-sized computing power, a realm once dominated by calculators. One of the first personal digital assistants (PDAs), the Psion Organizer, was released in 1984. In the mid-1990s, companies like IBM and Nokia began adding telephone features to PDAs, and the smartphone was born. By the turn of the century, companies like Palm and Research in Motion, maker of the BlackBerry, along with Nokia, were considered leaders in the mobile space. Apple, which was an early player in the PDA space with the Newton device, became a major force in mobility in 2007 with the release of the first iPhone. Google wasn't far behind, with the first Android-based devices launching in 2008. Google's Android operating system now dominates the mobile landscape, powering over 85 percent of all smartphones and tablets. Apple's iOS is a distant second but covers nearly all of the remaining market share. Other OS offerings from the likes of Samsung, BlackBerry, and Microsoft now make up just a fraction of a percent.

Much of this would just be interesting trivia and not particularly relevant to managing end-user devices except for a few trends. First, the growing power and lower cost of laptops and phones over time meant that more and more people purchased these for personal use. Second, while laptops and phones became less expensive, they were still a cost for businesses; companies didn't necessarily want to buy them for everyone, and they expected devices to be used for several years before replacing them. This led to a situation in the early 2000s when, for the first time, employees began to have more modern computing technologies at home than at work. Believing they would be more productive and more competitive by leveraging their personal investments in the workplace, employees began to expect that they could bring their phones and laptops to work and use them in place of company-provided systems. This concept, called "consumerization," was a buzzword in enterprise environments in the 2000s and was embraced by many companies, who felt there was an advantage to allowing this kind of flexibility. Companies began to adopt bring your own device (BYOD) programs to allow employees to buy their own laptops or smartphones and use them to do their work. This made employees feel more productive and empowered, while reducing support and device costs for the business. By the 2010s, security, audit, and legal teams began to question the wisdom of this practice, as a personally owned device storing company-owned data can create a difficult legal situation if the employee leaves, and technical controls to address this were only partially effective. As a result, some companies backed away from BYOD programs, while others added policy language or made other changes to protect company resources. The challenge of device ownership remains a key point to consider when auditing end-user systems.

Part 1: Auditing Windows and Mac Client Systems

Microsoft Windows and Apple macOS are the predominant operating systems powering desktops and laptops in most homes and businesses. This section describes audit concepts and steps typical of a client system audit.

Windows and Mac Auditing Essentials

In most home settings, computers are stand-alone devices. You may have a local area network handling computers, printers, smart TVs, thermostats, and more, but the computer itself is usually "unmanaged"—no policy restrictions or management systems are in place to control the options available to you. In most business environments, this is not the case. Businesses spend a great deal of money on computing devices for employees and want to make sure the devices are usable, productive, secure, and supportable. To facilitate this, businesses will deploy management systems along with configuration rules or policies to manage the features, capabilities, and software available to employees. You will have to consider not only the state of the end user's desktop or laptop system but also the management system in place.

Operating a computer in an enterprise also involves processes around installing company software, configuring the system, managing users and passwords, backing up data, and responding to problems. These in turn lead to other systems in the client ecosystem, such as backup systems, trouble or ticketing systems and helpdesks, license management, and more. The steps described here focus on a typical business Windows or Mac client environment. Your business environment may be more or less complex. Work with your client team to understand the full scope of client management before proceeding.

NOTE The term "client" references the client-server computing relationship, where a system providing resources is called a server, and a system consuming resources is called a client. To some extent, referring to laptops and desktops as clients is legacy terminology; in a modern environment, laptops can act as servers, servers can be clients, and so on. In some organizations, the service for provisioning systems like laptops and desktops goes by other names, such as Device Management, but the "client" term is retained here.

Windows and macOS are the prevalent operating systems deployed to end-user desktop or laptop-style devices. Where technical steps are described, tips for both operating systems are included where applicable. These steps deal with high-level principles of managing business systems and are not an attempt to describe the hundreds of possible controls available in Windows and macOS. Resources dealing with detailed configuration options are covered later in the chapter. Work with your company's client system team for more details.

Windows auditors should also review Chapter 7 on the Windows Server platform, as many of the tools and techniques are applicable to the Windows client space.

Test Steps for Auditing Windows and Mac Client Systems

1. Review company policies around client devices and ensure device ownership and user responsibilities are covered.

As noted earlier, the presence of personally owned devices in the business environment creates challenges around device management and data protection. This step ensures your organization has considered these issues and has provided appropriate information to end users.

How

Obtain a copy of the company policy related to the use of personally owned or non–company-owned devices. The policy should clearly define the circumstances under which noncompany assets can be used and how they should be handled. In risk-averse organizations, personally owned computers might not be permitted under any circumstances, or they may be permitted to have only virtualized access to company resources.

Be sure to consider any supplemental labor engagements used by your company. Any policies that apply to employees should apply at least as stringently to third parties.

If personally owned computers are allowed, ensure that language addressing company data is present in the policies. If an employee is allowed to keep sensitive company data on a personal device and that employee later leaves the company or is terminated, it may be difficult or impossible for the organization to regain control of that data.

If personally owned computers are prohibited, determine whether your organization has technical controls to prevent these devices from connecting to company networks. These controls usually are in the form of Network Access Control or Network Admission Control (NAC) technologies that can interrogate a system and take appropriate action to allow or deny access.

NOTE NAC technologies are not covered in this book, but if they are present in your environment, a very simple verification step is to bring a personal laptop into the office and try to connect to either wired or wireless resources. If you are unable to gain access, the NAC system is probably working as expected. Discuss with a network administrator for more information.

Obtain a copy of the client security policy. This should address basic security requirements for client systems. A typical client security policy should include many of the items listed later in this audit, including disk encryption, antivirus software, and basic operating system configuration.

In addition, you should review the company's policies around user expectations. This is often called an acceptable use policy (AUP), which covers what users may and may not do with company-owned equipment or on company time. An AUP should clearly define what is allowed and what is not allowed and should explain the consequences of violating the policy.

Some organizations may allow personal computers to connect to special external networks that cannot access internal company resources. Similar in concept to a coffee shop network, these external networks might be provided as a convenience for both employees and visitors. For AUP purposes, these networks should be thought of as company networks unless separately addressed in the policy.

2. Ensure the organization has a device management infrastructure commensurate with policy goals and company strategy.

Client device management systems allow organizations to track device inventory, manage software, install patches, apply security policies, and more. This step assesses the existence and scope of device management systems. If device management is not in place, the company may not be able to properly secure and protect company assets and data.

How

Discuss the client device management systems with the client administrators. While a number of commercial and open-source products exist in the market, you should expect that any solution should, at a minimum, be able to facilitate the following key functions:

- Provide visibility to the device inventory for the company
- Provide information on the operating system version and patch status for all systems
- Manage the fleet application inventory, providing access to provisioned applications
- Apply security and system configuration policies to managed systems

In larger organizations, Windows systems are often managed as part of an Active Directory (AD) domain. Joining a computer to a domain facilitates the deployment of Group Policy Objects (GPOs) to Windows client systems. Various settings can be enforced via GPO, including account characteristics, Internet restrictions, and software features. While Mac systems don't support GPOs, they are sometimes joined to Windows AD domains. In other cases, Mac machines are managed separately from the Windows fleet.

If your organization uses GPOs, an additional audit check you might perform would be to ensure that a proper change management process is in place to govern GPO changes. Since these can affect the performance and operation of many end-user systems, it's important for businesses to have a sound change process around these configuration systems.

Over time, client device management systems have been merging with enterprise mobility management (EMM) systems. You may find that your organization uses a single platform to manage end-user client devices as well as mobile devices.

3. Ensure that guest accounts are disabled and default administrative accounts are disabled or renamed.

Default accounts on client systems can be exploited by outside threat actors to gain additional access or privilege in the environment. These accounts either should not be present or should be renamed in most business settings.

How

In Windows, you can use a PowerShell command to list local users and verify that the Administrator account and the Guest account are not enabled.

In the search bar, type **powershell** and select the Windows PowerShell app in the pop-up menu. When the shell appears, execute `get-localuser` as shown. You can see in the example output that the default Administrator and Guest accounts are disabled.

```
Windows PowerShell
Copyright © Microsoft Corporation. All rights reserved.
PS C:\Users\Mike> get-localuser
Name         Enabled   Description
----         -------   -----------
Administrator    False       Built-in account for administering the computer/domain
DefaultAccount    False       A user account managed by the system.
Guest        False       Built-in account for guest access to the computer/domain
HostAdmin        True
Mike         True
PS C:\Users\Mike
```

For macOS, you check the status of the Guest account using the Users & Groups icon in System Preferences. The Guest account should be listed along with other accounts on that system. If the account is listed as Off, then the Guest account is disabled. While reviewing this pane, you can also determine the privilege level of the current user, who could be a Standard user or an Admin user.

Checking the status of the "root" account, which has complete power over a Mac system, is more involved. Apple has provided steps to enable or disable the root user at https://support.apple.com/en-us/HT204012/. You can use these steps to verify the current status of the root account. By default, Apple disables the root account in macOS. You should discuss the management of the macOS root account with your client team, particularly if end users are allowed to have administrator rights on a system. Those rights can be used to enable the root user on demand.

4. Ensure that user accounts are provisioned through a centralized process and review policies around existence and use of local accounts.

The use of centralized account provisioning and management simplifies many processes related to the creation, maintenance, and deletion of end-user accounts. Central account management also simplifies application and web logins, as a single sign-on system can be leveraged to allow a user's identity to access many different parts of the environment.

Local accounts are difficult to manage and can create challenges in enterprise environments. A local account exists only on a specific system but could have privileges that increase the risk in the environment. Since local accounts aren't tied to a central identity system, it can be difficult for forensics teams to attribute actions taken using that account to any single individual. This type of attribution can be important in legal situations or when dealing with security incidents.

How

Review the end-user account process with the client administration team. Discuss how accounts are created and assigned to client systems. For many companies, end-user accounts for both Windows and Mac systems are managed via Active Directory and are linked to enterprise identity management systems. This keeps account records in a central location and allows accounts to be created when employees are hired and to be disabled or deleted when employees leave.

Review policies related to local accounts on end-user systems and discuss with the client administration team. If local accounts are permitted, check whether an inventory is kept that also records why each account is needed.

5. Review processes related to administration and remote support of client systems, ensuring that administrators use named accounts.

Client support teams are vital to the operation of the client environment, maintaining systems so that employees can be productive. To perform these tasks, support personnel usually have elevated privileges. This step ensures that client support teams have reasonable processes around their use of these privileges.

How

Interview the client administration team and a helpdesk team member or supervisor. Review the processes used when support teams need to connect to client systems. Determine if the end user must give consent or receives some visual notification when a remote support technician connects to a running session. You can easily verify this by asking a helpdesk team member to walk through the process of connecting to your system and by observing the resulting steps.

Assess processes for handling employee accounts and passwords when a system must be physically taken by the support team for repair. A best practice situation might include the following safeguards:

- The employee does not give any passwords to the technician team.
- The employee's active session is locked or logged out or the system is fully shut down before the support team takes possession of the system.
- The technician uses a unique, identifiable account to perform all maintenance tasks.

While support technicians usually have a high level of privilege on client systems and could use this power to access sensitive data, using a unique account provides additional protection and traceability for forensics teams in the event of a problem.

6. Review the device backup process, ensuring that restoration processes have been tested adequately.

Data from a system backup may be needed for various reasons. This step ensures that the organization has a suitable, proven backup and restore process for client data.

How

Interview the client backup administrator. Discuss practices around backup frequency, missed backups, and methods used to ensure that all in-scope clients are backed up on a regular basis. In most business environments, weekly backups are standard practice, while modern data backup solutions may record file changes in near real time.

Discuss processes for validating backup data and verifying that restore processes are functional. In a larger organization, file restoration may be exercised quite regularly when systems are upgraded or repaired, but in smaller groups, this may be less common.

7. Review the software licensing process and ensure users do not have access to unlicensed software.

Organizations run the risk of incurring large financial penalties for exceeding licensing agreements or using unlicensed software. This step ensures that the busi-

ness has appropriate safeguards to reduce license-related risks.

How

Interview the client administration team to determine how software licensing is managed for client systems. Some software may be licensed broadly for all employees (enterprise license or site license), while some may be limited to a set number of users or even to specific, named users. Many businesses are now provisioning internal "app stores" for client systems, giving users a one-stop shop for most of the software they may need.

Assess the processes for identifying and remediating software found to be out of license. For example, teams may compare a list of installed software to a list of licensed or allowed software and then may uninstall unexpected software remotely. Determine if the organization has processes addressing open-source software as well as freeware, shareware, and trialware, which may have differing license terms for business uses.

Some companies use special software installed on client systems to assist in software inventory or to provide additional controls on software usage. Through configuration, these packages can prevent or allow software installations based on company policy. These capabilities differ in various systems, but can be found in antivirus programs, system management clients, privilege management apps, security suites, and more.

8. Ensure that the organization has a sound process for responding to user problems.

Failure to establish ownership and tracking of end-user issues could result in lost productivity, unresolved security issues, and other risks.

How

End-user issues should be tracked through a trouble ticketing system. An owner for these issues should be assigned, and a group should be held responsible for tracking the progress to closure for any tickets opened because of client issues. Discuss these processes with the administrator or helpdesk supervisor.

9. Review and evaluate the strength of passwords and the use of password controls on client systems, such as password aging, length, complexity, history, and lockout policies.

All accounts should have passwords. The methods used to test these controls depend on the password-provisioning process and controls enabled on the client systems. Some of these controls may be configured centrally, such as in Active Directory. At a minimum, you should review system settings that provide password controls. Password controls are essential to enforcing password complexity, length, age, and other factors that keep unauthorized users out of a system. Many organizations choose to assign more stringent password settings to privileged accounts, such as those with administrator rights.

How

In Windows, you can find the account policies as they affect your system by using the `secpol` command from the search bar. This opens the Local Security Policy panel. From here, choose the Account Policies tree, and examine the listings for Password Policy and Account Lockout policy. You can also see much of the same information at the command line using `net accounts`. For Windows clients joined to an AD domain, these policies are usually set remotely via GPO and should be identical for all client systems. Systems not joined to a domain may not have any password or lockout policies.

For macOS systems linked to AD, password settings will be managed remotely. Systems controlled through a management system like Jamf Pro may have settings applied through that system. Discuss the settings with the client administration team. Unmanaged systems may not have any password or lockout policies.

For either operating system, verify that the policies listed in Table 14-1 are set in accordance with your local policies. Some common settings are listed.

Table 14-1 Account Policies

Policy	Setting
Minimum password age	1 day
Maximum password age	30–90 days
Minimum password length	8–14 characters
Password complexity	Enabled
Password history	10–20 passwords remembered
Store passwords using reversible encryption	Disabled, if possible, but understand and test this before making this decision
Account lockout duration	10–30 minutes
Account lockout threshold	10–20 attempts
Reset account lockout after	10–30 minutes

10. Ensure that end-user administrative privileges are established and maintained according to company policy.

By limiting end-user privileges, companies can reduce their risks and costs associated with rogue software installations, malware outbreaks, and unauthorized system configuration changes.

How

Interview the client administration team and ask whether end users are permitted to have local administrator rights on their systems. The administration team should be able to explain the standard posture and should be able to produce statistics or other reports listing which, if any, end users are permitted to have administrator rights. In many larger organizations, particularly in regulated industries, employees are not permitted any local administrator access. Some companies use commercial software to enable certain administrative features for standard user accounts.

If end users are not permitted administrator rights, you can verify the state of an account using a typical workstation. Select a user who should not have administrative access at random or from your workgroup (in many situations you can test this on your own workstation).

In Windows, open the Control Panel by typing **Control Panel** in the search bar and selecting the Control Panel desktop app in the pop-up. Select User Accounts. The account name of the logged-in user should appear toward the right of the resulting pane. If the user is an administrator, the word "Administrator" will appear

under the account name.

In macOS, open the System Preferences app. Often this is present in the dock, or you can use the Spotlight search bar. After opening System Preferences, select the Users & Groups icon. The resulting pane will show the list of users on the system. Below the usernames will appear the account type, either Admin or Standard.

11. Ensure that a legal warning banner is displayed when connecting to the system.

A legal logon notice is a warning displayed whenever someone attempts to connect to the system. This warning should be displayed prior to actual login and should say something similar to this: "You're not allowed to use this system unless you've been authorized to do so." Verbiage of this sort may be needed to prosecute attackers in court.

How

Log in to your system and determine whether a warning banner is displayed. If your organization permits remote access to client systems using a technology such as Remote Desktop or VNC, log in from another system using those as well and look for a warning banner. Interview the system administrator to determine whether the verbiage for this warning banner has been developed in conjunction with the company's legal department.

12. Verify that systems use a full-disk encryption (FDE) utility to protect company data.

Laptops are lost or stolen every day. If FDE is not in use, anyone in possession of a laptop or desktop can easily extract the data from the drive.

How

In macOS, you can check the status of FileVault, Apple's built-in disk encryption utility, using the System Preferences app and selecting the Security & Privacy icon. The FileVault tab shows the status of the disk. If your organization uses a disk encryption utility for Mac other than FileVault, check with your client administrator on how to verify that encryption is active.

In Windows, you can review BitLocker encryption status using Control Panel. Type **control panel** into the search bar and select the Control Panel desktop app from the pop-up. If your organization uses BitLocker encryption, you should see an option for BitLocker Drive Encryption in the list. Selecting this will provide the status for that system's drive. If your organization is using an alternative disk encryption product, discuss with your system administrator. Most alternative tools have a status icon in the system tray or a resident app to provide information about encryption status.

Your administrators should be able to provide metrics or reports as evidence to demonstrate the compliance of encryption throughout the in-scope fleet. If such metrics or reports are not available, the organization may not know which systems are not encrypted.

While discussing disk encryption with the administration team, you should review processes for storing encryption keys for maintenance or forensic needs. Security teams often require access to disk encryption keys during investigation work.

13. Determine whether the client is running a company-provisioned antivirus program.

Client systems are a primary target for outside hackers. Failure to have basic antivirus protection makes clients an easier target and may allow harmful code to run on the system. Antivirus tools can also identify the presence or actions of hacking tools run by malicious actors. In Windows 10, Windows Defender is installed and enabled by default, but some organizations will use an alternative antivirus program.

How

In Windows 10, you can access the status of security modules, including antivirus, by typing **security** in the search bar and selecting the Security and Maintenance app in the pop-up menu. Select the Security drop-down to see the status of security features. In the example shown in Figure 14-1, Windows Defender is listed under the Virus Protection entry.

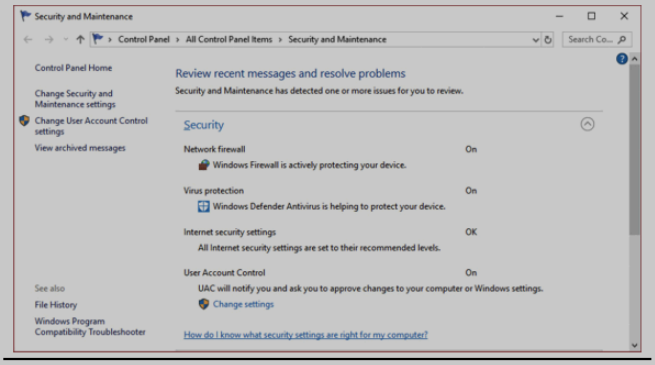

Figure 14-1 Windows Security and Maintenance Panel

Windows also offers the Windows Defender Security Center, which provides a similar view. Either will provide the status of antivirus and other tools. In later versions of Windows, some status information can be hidden from end users through system management configuration. If this is the case, discuss with your client administration team.

Mac clients should also use antivirus software, but macOS does not provide a simple tool to see the status of antivirus tools. Discuss with the client administration team to obtain information about the macOS antivirus software in use in your organization.

Depending on the nature of your audit, you also might want to check the configuration of the antivirus program on the client. For many organizations, the antivirus program is managed centrally, and enterprises will often use the same solution for both Windows and Mac platforms. Ideally, the configuration should not exclude any files or folders from periodic scanning and should be set to protect the system in real time for all file operations. Antivirus tools should also be configured to automatically download and install signature updates. Deviations can put the system at greater risk.

14. Verify that a client firewall is active and review firewall management practices.

Client firewalls protect the system from unexpected network connections. Failure to use a firewall can increase the risk of a malicious threat gaining access to a system.

How

For Windows, use the steps in the previous test to access the Security and Maintenance panel or, alternatively, the Windows Defender Security Center app. The panel indicates the status of the Windows firewall. If your organization uses a third-party firewall, such as those provided with many antivirus programs, the status should appear in the same Windows panels.

For Mac systems, select the System Preferences app, then choose the Security & Privacy icon. Switch to the Firewall panel. This will describe the status of the firewall.

Discuss the firewall configuration with the client administration team or the security team. Firewalls should be configured to block most inbound traffic.

15. Review client logging requirements and settings.

Appropriate client logging can assist operations and security teams in detecting issues with client systems.

How

In Chapter 4, we discussed the cybersecurity program, including policy requirements. Review policies related to logging to determine if requirements exist for client logging. Many companies choose to limit the use of centralized client log collection due to the number of clients, size of log data to be captured, or the potential for network impact from log transfers. If your company's logging policies have requirements for client systems, discuss with the client administration team. Ask to see the log configuration in the system management tool(s) in use. If logs are forwarded to a central system, ask the monitoring team to provide a sample of client logs.

16. Review the patching process for the operating system and key applications.

If applicable operating system and software patches are not installed, widely known security vulnerabilities could exist on the client, allowing harmful exploits from outside threats.

How

Discuss the client patching process with the administration team and the security team. Both Microsoft and Apple release patches for the OS and key applications periodically, as do many third-party software providers. The organization should have a process for assessing the applicability of patches and their resulting criticality. The teams should be able to provide supporting evidence of analysis for the most recent patch releases from either Microsoft or Apple at a minimum.

Discuss the timing of patch installation and the processes for ensuring that all relevant clients receive the expected patches. Companies should have reports or other metrics available describing the patch status of the client fleet.

To verify the metrics, select a client system at random—you can use your own system for this step if desired. In Windows, type **windows update** in the search bar. Open the Windows Update app, which will show the status of the system and provide a link to see recent installation history. The history should show recent installation activity, particularly under Quality updates. In macOS, use the About this Mac app, accessible via the Apple menu in the upper-left area of the screen. Select System report and then scroll down in the left-hand panel to find Installations under Software. You can select the Install Date column to sort the installation info, as depicted in Figure 14-2.

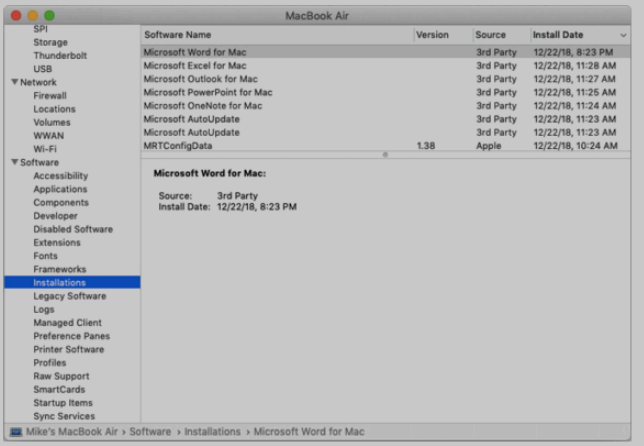

Figure 14-2 Viewing installed updates in macOS

Some organizations may enable automatic Windows and Mac updates for their systems, but others will manage updates carefully to ensure compatibility with company software. Discuss with the client administrators to determine if patches are installed from a central system or if clients update themselves using automatic updates.

You should pay particular attention to Windows 10 OS versions in use in the environment. With Windows 10, Microsoft moved to a semiannual release schedule for Windows, and when a new version is released, support for an older version is immediately discontinued. Depending on your company's licensing arrangement, you may have as little as 18 months of support for each new version of Windows before it is no longer supported or patched by Microsoft. See the Knowledge Base for additional information on Windows life cycles. Apple does not publish end-of-life information for macOS but in general supports security patches for the two prior releases.

17. Verify that the screen will automatically time out after a set interval and require a password to resume.

An unattended work session can be used by anyone walking up to the computer. A screen timeout reduces this risk.

How

In Windows 10, you can find the setting for screen timeout under the Screen Saver Settings application. Enter **screen saver** in the search bar and select the Change screen saver option in the pop-up menu. The panel displays the time duration. The box indicating "On resume, display logon" screen must be checked.

In macOS, several steps are needed to verify this item. First, open the System Preferences app. Next, select the Desktop & Screen Saver icon. Under the Screen Saver tab, you'll see a Start after field at the bottom. This should be set to a time matching your security policy, but preferably a brief duration, such as five or ten minutes. Next, click the back arrow in the same panel to return to System Preferences. Choose the Security & Privacy icon. Under General, the option for "Require password after sleep or screen saver begins" must be checked. Ideally, the drop-down box should be set for immediately or a very short duration. Power options can also affect this setting, but for most Mac deployments, the screen saver timer will be managed by the administration team and will represent the maximum timeout length.

Discuss with your client administration team to ensure that these options are enforced through the client management system.

18. Ensure that AutoPlay and AutoRun are disabled for removable devices.

In Windows, AutoPlay and AutoRun will automatically launch certain types of files upon the insertion of a USB drive, CD/DVD, or other media. If these features are enabled, a malicious file can execute without a user taking any specific action. Mac systems will not automatically execute files on USB drives, but systems with optical drives may play CDs or DVDs automatically.

How

Discuss with the client administration team to determine if AutoPlay and AutoRun are disabled. Both can be adjusted through GPO in Windows. For Mac systems, discuss with the Mac administrator. Most modern Macs are no longer shipping with optical drives, so this may not be an issue in some environments.

Tools and Technology

Most of the steps in this chapter are executed with basic GUI or command-line inputs in a working system. Many other tools are available, particularly for Windows, that will provide additional insight into the status of a client. Some of these are listed here.

Resource	Website
Microsoft Script Center	https://gallery.technet.microsoft.com/scriptcenter
Microsoft Command-Line Reference	https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/windows-commands
Microsoft Sysinternals Tools	https://docs.microsoft.com/en-us/sysinternals/
Microsoft Security Compliance Toolkit	www.microsoft.com/en-us/download/details.aspx?id=55319

Knowledge Base

The following table lists additional resources where you can obtain information about Windows and Mac client environments and controls. Both Microsoft and Apple provide extensive online information regarding their platforms, and the Internet community has supplemented this with additional content. In addition, the Center for Internet Security (CIS) has developed hardening guides for both Windows and Mac client systems that contain hundreds of configuration options. The CIS guide for Windows 10 alone is over 1,000 pages!

Resource	Website
Windows 10 Reference	https://docs.microsoft.com/en-us/windows/windows-10/
Microsoft TechNet	https://technet.microsoft.com/en-us/
Microsoft System Center	www.microsoft.com/systemcenter
Windows Intune	www.microsoft.com/en-us/cloud-platform/microsoft-intune
Windows Lifecycle Fact Sheet	https://support.microsoft.com/en-us/help/13853/windows-lifecycle-fact-sheet
Windows Security Baselines	https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines
macOS Security Overview	www.apple.com/business/resources/docs/macOS_Security_Overview.pdf
macOS Security Checklist	www.jamf.com/resources/white-papers/macos-security-checklist/
The Center for Internet Security	www.cisecurity.org
Computer Security Resource Center	http://csrc.nist.gov

Part 2: Auditing Mobile Devices

While laptops and other portable form factors like Microsoft's Surface line are mobile in the sense that they are easy to move, most organizations consider "mobile devices" to include smartphones, tablets, and other devices running Android, iOS, or another mobile-centric operating system. This section describes concepts and steps to consider when conducting an audit of an organization's mobile device environment.

Mobile Device Auditing Essentials

Conceptually, auditing a mobile device environment that includes smartphones

and tablets is fairly similar to auditing desktops and laptops. There are policies, device management systems, minimum security standards, and so on. As mobile management technologies converge with client management systems, the overlap between these two spaces is likely to increase. However, the complication of personal device ownership is a larger factor in the mobile space; this, along with a few differences in technology, suggests a separate audit is warranted.

There are a few basic questions you should consider as an auditor when assessing a mobile device program. Some of these include

- What company resources can be accessed by mobile devices?
- How is company data protected on mobile devices?
- How does the company handle personally owned devices and apps?
- Is the company considering risk from emerging mobile devices like wearables?

Companies may address mobile devices in a number of different ways. Some companies will purchase devices and carrier plans for employees, while others will pay for carrier plans but not the devices themselves. Some offer a stipend to employees who are free to select their own devices and plans.

Understanding your company's posture and policies around mobile device ownership and authorization for those devices to access company resources is a key element to a mobile device audit. In the simplest case, the company owns all devices and does not permit employees any personal use of the device. While some businesses may manage a subset of devices like this—for example, a shipping company may have special-use devices for delivery personnel—it's rare for all mobile devices to fall into this category.

As in the client audit, you'll need to review several policies in preparation. In addition to policies on noncompany devices and acceptable use, your company's policies should address mobile devices. In some cases, this could be merged with a client security policy or other document, but in many companies this is a separate policy. If a company allows personal mobile devices to access company data via a mobile access gateway, there can be implications for employee privacy and employee personal data; this usually drives a need for a separate policy or even a consent agreement for mobile devices.

Let's briefly establish some common terminology and define some industry terms. The technologies used to configure and secure mobile devices emerged under the term "mobile device management," or MDM. As mobile applications grew, technology providers added many app-related features and developed the mobile application management (MAM) field. After throwing in a few more acronyms, much of the industry settled around the more generic "enterprise mobility management," or EMM. As EMM technologies begin to converge with traditional client system management systems, yet another term, "unified endpoint management" (UEM), is emerging. For the purposes of this chapter, we'll mostly use the EMM terminology.

Test Steps for Auditing Mobile Devices

1. Review company policies around mobile devices and ensure device ownership and user responsibilities are covered.

As we've discussed, establishing policy around device ownership is a key step for companies dealing with client systems. This is also important for mobile devices. This step ensures your organization has considered these issues and has provided appropriate information to end users.

How

Obtain a copy of your company's mobile device policy, if it exists, as well as policies related to the use of personally owned or non–company-owned devices. The policy should clearly define how mobile devices may be used and how personal mobile devices should be handled. You should expect a mobile device policy to address what resources may be accessed by mobile devices, any minimum standards or settings for the device, how the employee and company will respond if the device is lost or stolen, and expectations placed on the employee. If your company permits personally owned devices, the mobile policy should also address privacy-related concerns around device location, personal apps, and personal expenses.

You should verify that policy language or employee agreements around privacy have been developed in conjunction with your company's legal and/or privacy teams. While this audit does not address privacy assessments related to various regulations around personal data protection, you should be aware that mobile device systems are often in scope for this kind of review.

In addition, you should review your company's policies around user expectations. For expectations around mobile devices, this may be covered in a mobile device policy or in an employee agreement, but the AUP may also be relevant, particularly if the mobile devices are company owned.

Some organizations may allow personal mobile devices to connect to special external networks that cannot access internal company resources. Similar in concept to a coffee shop network, these external networks might be provided as a convenience for both employees and visitors. For AUP purposes, these networks should be thought of as company networks unless separately addressed in the policy.

2. Ensure the organization has an EMM infrastructure commensurate with policy goals and company strategy.

Enterprise mobility management systems allow organizations to track device inventory, manage software, apply security policies, and more. This step assesses the existence and scope of EMM systems. If device management is not in place, the company may not be able to properly secure and protect company assets and data.

How

Discuss the EMM systems with the mobile device administrators. Some common commercial products in this area include AirWatch, MobileIron, and Intune. Both Google and Apple closely control how EMM systems interact with devices running Android and iOS, and the basic capabilities for most EMM solutions are very similar. You should expect that any solution should, at a minimum, be able to facilitate the following key functions:

- Provide visibility to the mobile device inventory for the company
- Provide information on the device type and operating system version
- Support application controls, including the ability to block specific applications

- Apply security and system configuration policies to managed devices
- Remotely wipe devices when lost, stolen, or no longer needed

Many EMM systems also facilitate access to company resources through network configuration or through a gateway device. In a typical configuration, mobile devices managed under EMM are permitted to access corporate e-mail, contacts, and calendar information, frequently via Microsoft Exchange protocols. The same systems that allow this kind of access may also allow access to other on-premises or cloud-based applications or services. You should review the architecture and configuration of these systems with your company's mobility team to ensure that the controls around device access are working as intended to protect company data. We'll discuss data protection controls in more detail later in this chapter.

As with other company infrastructure, you should also review access policies for the EMM system itself, ensuring that only designated individuals have access. You should also take this opportunity to review change management and business continuity aspects of the EMM environment. Finally, verify that the EMM system, gateways, and other components of the mobility environment are kept up to date with supported software and patches. The mobile device administration team should be able to assist with these items.

3. Ensure that mobile devices are configured to require a PIN or passcode to gain access to the device and review other PIN/passcode-related settings.

If access to mobile devices is not protected, company data could be exposed if an unauthorized person gains possession of a device.

How

You can discuss this and all of the following steps in this chapter with your mobile device administrators to obtain information about the expected behavior in each step. Discuss the passcode requirements, including minimum passcode length, passcode change requirements, support for alternative unlock methods such as facial recognition, and auto-wipe features. These will differ by company according to risk tolerance, but a standard practice is to require a six-character passcode with annual change, to automatically wipe the phone after ten failed passcode attempts, and to allow facial or fingerprint authentication.

To verify that the policy requirements are implemented, you can use any managed mobile device. First, you can verify that a managed device does, in fact, require a passcode to unlock it. To verify that the passcode cannot be removed, you can check additional settings. For iOS devices, access Settings, then Touch ID & Passcode or Face ID & Passcode, depending on the device model. Scroll down to Turn Passcode Off. This should be grayed out and not selectable for a managed device. For most Android devices, open the Settings app, then select Device, then Lock Screen, then Screen Security. Options to remove the different passcode methods, including pattern or PIN-based unlock, should be grayed out for managed devices.

Different models of Android-based devices may have slightly different menu options; if you are unable to find the settings, discuss with your mobility team.

4. Ensure that device encryption is enforced.

As with client devices, an unencrypted mobile device could reveal sensitive information to someone who gains physical possession of the device.

How

Most EMM solutions can verify device encryption status and permit or deny access for devices based on the result. Discuss this with your mobility administrators.

Since the release of iOS 8, Apple has included device encryption by default for iPhone and iPad. The only prerequisite is to set a passcode for the device. You can also verify the state of the device in the Touch ID & Passcode panel. Scroll to the bottom, where the screen should indicate "Data protection is enabled."

For Android, encryption is also a default setting beginning with the Nougat release. However, this can be disabled for some versions of Android. Open the Settings app and select Security. An Encryption option should indicate whether the device is encrypted. Earlier versions of Android and some lower-performance models did not support data encryption; these versions and devices should not be permitted to store corporate data.

5. Ensure that devices automatically lock after a set period.

An unattended device could be accessed by anyone without the need of a passcode or other authentication. A screen lock timer can reduce the risk of data theft or other malicious activity.

How

Discuss with your mobility team to ensure that this setting is configured in EMM policy for managed mobile devices.

To verify this setting in iOS, you can check the Settings | Display & Brightness panel and review the Auto-Lock setting. EMM administrators can set a maximum allowable time, and the user can select a shorter time if desired. The Never option should not be available.

In Android, the screen timeout is managed under Settings, then Display. The Sleep setting indicates how long the screen will remain on.

6. Review processes for keeping mobile devices up to date.

Obsolete or unpatched operating systems can expose security vulnerabilities that could be leveraged to access sensitive personal or company data or company e-mail accounts. This step verifies that the organization has a plan for maintaining a mobile device security posture.

How

As vulnerabilities are announced regularly in both iOS and Android, Apple and Google frequently release security updates. In addition, both companies typically release a new version of their OS each year. However, upgrade paths for their devices differ. The closed nature of the Apple environment (Apple makes all iPhones, iPads, iPods, and the iOS operating system) means that Apple determines which versions of hardware are compatible with which versions of software, and compatible devices can be updated quickly upon release of a new iOS version. For Android, however, which historically allows device makers and carriers to customize the OS for their needs, upgrades and patches take much longer to deploy, and in many cases, patches and upgrades are not issued even for very recent phone or tablet models. You should discuss the risks of the various operating systems with your security team and determine if the mobility team has implemented restrictions on which versions are allowed to connect to company resources.

Apple does not release patches for previous iOS versions but historically has supported newer iOS versions on devices that are several years old. This allows a fleet with a wide range of Apple devices to run the same, up-to-date software release. Companies therefore have more flexibility with Apple systems to limit the allowed versions without negatively affecting most users. For risk-averse organizations, a best practice is to allow only the currently released version of iOS to connect, with a reasonable grace period for employees to upgrade to the latest release. More risk-tolerant organizations may allow older iOS versions to connect but should have processes to review the specific vulnerabilities and risks present in older iOS releases. Your mobility team should be able to provide an inventory of managed Apple devices by iOS version.

For Android devices, practices vary widely by company. Some organizations attempt to allow only recent Android versions to access company resources; this may require either the company or the end user to upgrade devices frequently. As some Android device makers have a better track record at releasing updates than others, some companies have also taken the approach of restricting which device models are allowed. For example, Google's Pixel models run a "clean" version of Android that can be updated quickly—some organizations may choose to allow only these models. Your mobility team should be able to provide an inventory of managed Android devices by OS version.

7. Review processes for erasing or reclaiming devices in the event one is lost, stolen, or replaced or if the employee is terminated.

When a device is lost, stolen, or replaced, it may still contain sensitive data. Although other safeguards intended to protect this information may be in place, companies should have processes to safely retire devices and remove company data.

How

Discuss the steps involved in the case of a lost or stolen mobile device. People who lose a device may be embarrassed or may fear disciplinary action or financial penalties for losing a device, but it's important that employees can freely report a lost or stolen device to the appropriate personnel. Such reports may come to physical security teams, information security teams, or mobility teams, but the organization should have a process for notifying the mobility team that a device is lost.

EMM solutions support remote wipe features for lost or stolen devices. These can erase the entire device or just remove the company data and configuration. In most situations, it is better to wipe the device entirely if it has been lost or stolen. A remote wipe is not always successful, but it's an essential step. If the device is powered on and within range of a carrier signal or connected to an Internet-capable wireless network, it should receive the wipe signal.

Companies should also have processes for handling employee terminations. For company-owned devices, ensure that employee exit checklists include retrieval of the device. In the case of employee-owned devices, employee termination processes should include a partial or full device wipe. A partial wipe removes only company data and applications, leaving personal data intact. Ideally, these processes are automated and linked to other termination steps.

If you have access to a list of employees who have recently resigned, retired, or have been terminated, you can sample this list and compare against the list of active devices in the EMM system. Consult with your HR contacts and the EMM team.

8. Review additional options for protection of company data on the device.

This step covers additional data protection considerations for mobile devices in typical business deployments.

How

The increasing power of mobile devices and their increased penetration in business environments means that additional configuration areas should be considered to provide adequate controls to protect company information.

Access to company e-mail, calendar, and contacts has been the most popular use case for mobile device access for many years. In the past, this usually involved special network access from devices to on-premise e-mail systems like Microsoft Exchange. However, as cloud-based e-mail systems have expanded, many companies no longer have on-premise e-mail systems. You should review the configuration of e-mail access for mobile users, particularly if your company uses a cloud system like Office 365 or Google's G-Suite. Ensure that any provisions for employee termination also include termination of their mobile access to cloud-based e-mail systems.

Many organizations have deployed one or more mobile apps for business use. In some cases these are commercially purchased apps, like expense managers, HR applications, and the like. In other cases these are internally developed, custom applications supporting a specific business function or process. For any use of mobile applications for work, you should discuss how company data is protected. In best-practice situations, mobile applications used for company business are managed and deployed through the EMM system. This allows the company to revoke access to the application and its data if needed and to establish controls around what can be done with the data on the device.

Mobile devices may have access to or may store sensitive company data. Apple and Google have gradually added more and more business-friendly capabilities to their operating systems, allowing more isolation between company and personal data and inserting more control options. In late 2018, Google released a work profile feature for Android, which creates a separate application landscape for work-related apps and content. Apple offers restrictions to prevent opening company e-mail content in unmanaged applications, as well as settings to add virtual private network (VPN) connections and content protection for company-designated websites. Many options are available; discuss with your security team and mobility team to ensure that proper attention has been given to protecting company data on mobile devices.

Additional Considerations

Licensing

Mobile applications may have differing license terms than traditional desktop applications. While many applications are freely available on app stores, a review of licensing terms may show that they are not authorized for business usage. This can create a challenge for software management teams. Since mobile devices are more likely to be personally owned, a device with mixed use may have business and personal applications present. An employee who uses a personal application for a business function may unknowingly violate the terms of use of the applica-

tion and put the company at risk of financial penalties.

Closely managing mobile applications on employee-owned devices opens a number of privacy and legal issues. Managing applications on company-owned devices is more straightforward. Providing education to end users about the risks of using unauthorized applications for business is a best practice.

Higher-Security Environments

The tests and guidelines in this chapter apply to typical business settings, and you should expect to find most, if not all, of the controls described here to be in place in all environments. However, risk-averse organizations, those with high regulatory burdens, and those with very high security needs should consider deploying additional controls. The Center for Internet Security (CIS) has developed hardening guidelines for both Android and iOS-based devices. If you find that your organization's controls are not sufficient to mitigate company risks, consider reviewing the CIS guidance for mobile devices. See the Knowledge Base for more information.

Wearables and the Internet of Things (IoT)

While this chapter has focused on traditional end-user technology, new uses for computing capability have emerged over the last five years. Wearable technology, including smart watches, includes a class of systems that often pair with a phone to offload data or provide interactive capability. Some of these devices can also connect to wireless networks. Watches in particular are interesting to enterprises because they can be used for authentication; for example, the Apple Watch can be used to unlock a Mac. Companies should be aware of the capabilities employees are bringing to the workplace in these devices.

In addition, hundreds of new devices are being released each month in the IoT space. These include various kinds of sensors and control systems like thermostats, switches, automation systems, and more. Often used in industrial or facilities-related situations, there are also devices like Amazon's Echo series and other Alexa-compatible devices that may appear on your network. Many companies do not address these devices in existing policies, but they should be aware of the potential risks of having these unmanaged systems on corporate networks.

Tools and Technology

Tools	Website
VMware AirWatch	www.air-watch.com
MobileIron	www.mobileiron.com
Microsoft Intune	www.microsoft.com/en-us/cloud-platform/microsoft-intune

Knowledge Base

Resource	Website
Apple iOS Security Overview	www.apple.com/business/resources/docs/iOS_Security_Overview.pdf
Apple iOS Security Guide	www.apple.com/business/site/docs/iOS_Security_Guide.pdf
Android Security	https://source.android.com/security
Center for Internet Security	www.cisecurity.org
Department of Homeland Security study	www.dhs.gov (search for study on mobile device security)

Master Checklists

The following tables summarize the steps listed for auditing Windows and Mac clients and Android and iOS mobile devices.

Auditing Windows and Mac Client Systems

Checklist for Auditing Windows and Mac Client Systems
❑ 1. Review company policies around client devices and ensure device ownership and user responsibilities are covered.
❑ 2. Ensure the organization has a device management infrastructure commensurate with policy goals and company strategy.
❑ 3. Ensure that guest accounts are disabled and default administrative accounts are disabled or renamed.
❑ 4. Ensure that user accounts are provisioned through a centralized process and review policies around existence and use of local accounts.
❑ 5. Review processes related to administration and remote support of client systems, ensuring that administrators use named accounts.
❑ 6. Review the device backup process, ensuring that restoration processes have been tested adequately.
❑ 7. Review the software licensing process and ensure users do not have access to unlicensed software.
❑ 8. Ensure that the organization has a sound process for responding to user problems.
❑ 9. Review and evaluate the strength of passwords and the use of password controls on client systems, such as password aging, length, complexity, history, and lockout policies.
❑ 10. Ensure that end-user administrative privileges are established and maintained according to company policy.
❑ 11. Ensure that a legal warning banner is displayed when connecting to the system.
❑ 12. Verify that systems use a full-disk encryption (FDE) utility to protect company data.
❑ 13. Determine whether the client is running a company-provisioned antivirus program.
❑ 14. Verify that a client firewall is active and review firewall management practices.
❑ 15. Review client logging requirements and settings.
❑ 16. Review the patching process for the operating system and key applications.
❑ 17. Verify that the screen will automatically time out after a set interval and require a password to resume.
❑ 18. Ensure that AutoPlay and AutoRun are disabled for removable devices.

Auditing Mobile Devices