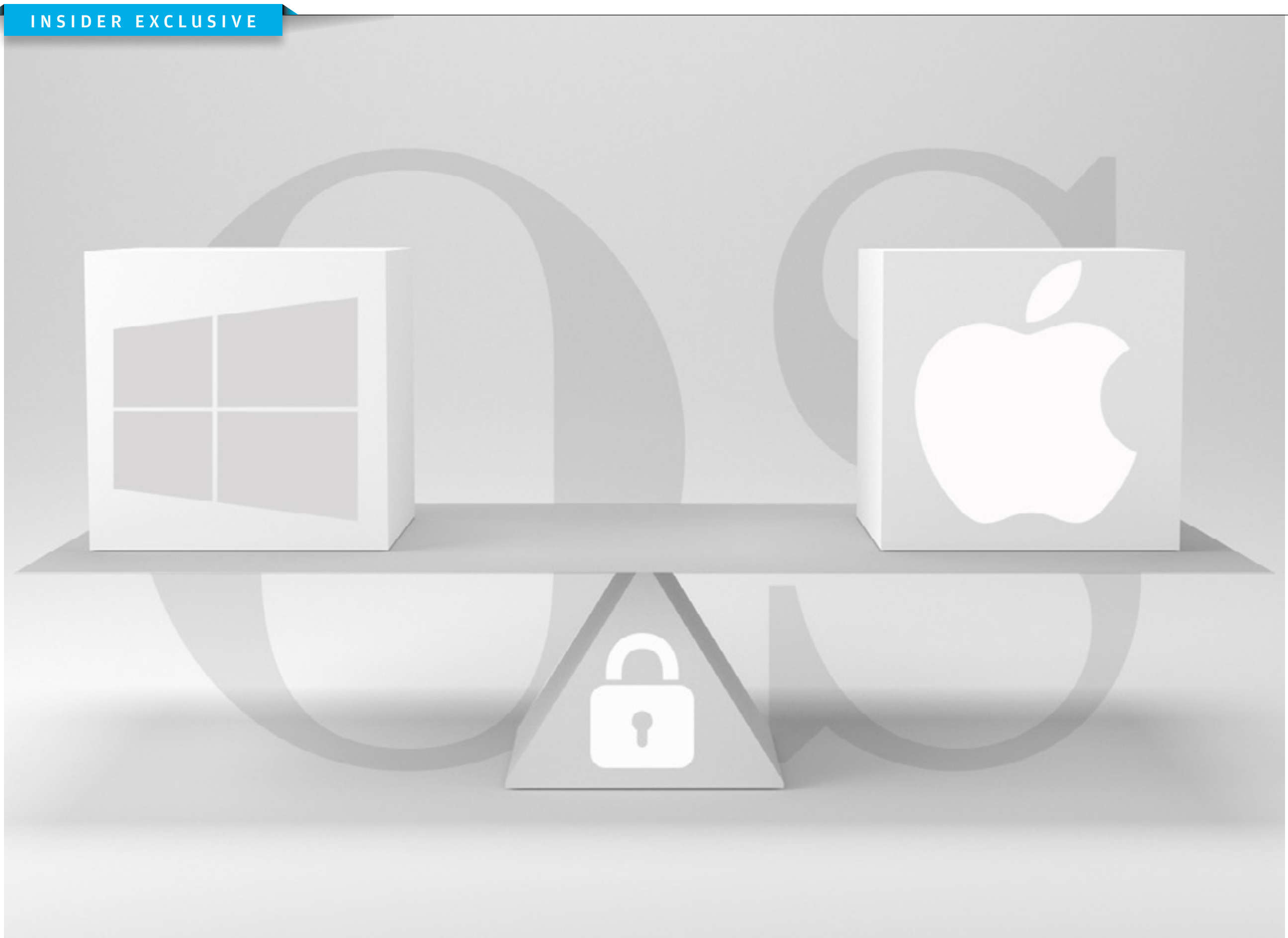
CSO
FROM IDG

BUSINESS RISK LEADERSHIP

INSIDER EXCLUSIVE



Microsoft Windows 10 vs. Apple macOS security features

*A side-by-side comparison of how the **world's two most popular desktop OSes** keep systems and data safe from malware, unauthorized access, and more.*

BY ROGER A. GRIMES AND MIKE DEAGONIA

ONE OF THE QUICKEST ways to troll IT security professionals is to proclaim that either Microsoft Windows computers or Apple Macs have better security. In reality, both OSes are adequately secure when operated with their default security settings along with their vendor's best practice recommendations, but after decades of intense competition for passionate consumers, the subject borders on a technical religious war. You won't

GETTY/MICROSOFT/APPLE, MODIFIED BY IDG COMM gain many friends by claiming both are secure.

With that said, not everyone knows what makes the two most popular OSes secure out of the box. Below is an overview of each OS followed by a comparison of the base security features found in each. We didn't include other solid enterprise features that aren't built into the OS and enabled by default.

Microsoft Windows 10 security

IN THE FIRST DECADE of its existence, Microsoft's flagship Windows program was easily the most successfully attacked OS in the history of computers. The number of attacks led to public distrust of Windows as a secure operating system. In response, Microsoft co-founder Bill Gates wrote an infamous memo on January 15, 2002, known as the Bill Gates Trustworthy Computing memo, which directed Microsoft to dedicate more resources to making Windows more secure.

Microsoft not only made Windows more secure by default, but actually co-opted or created dozens of new computer security technologies. One of the most important outcomes of Gates' 2002 was the wholesale adoption of the secure development lifecycle (SDL) across Microsoft. SDL puts secure coding and practices at the forefront and beginning of every software development project. It's a combination of education, requirements, and tools, and Microsoft shares every bit of its experience.

The outcome of SDL is significantly fewer security bugs per thousand lines of code, more security features and choices, less surface attack area, and more secure defaults. The security of Windows 10 is the continuation of Microsoft's efforts to offer an appropriately secure, general purpose, operating system that would work for the masses across multiple devices.

Apple MacOS security

FOR A LONG TIME, Mac users didn't have to worry about viruses and malware. Vulnerabilities in the Mac operating system were rarely exploited in the real world. Mac users have always been aware of potential security threats, but much of that was because Windows-using coworkers have been the target of malicious software for ages. The numerous vulnerabilities in every version of Windows in concert with a very large user base made PC users a perfect target.

These days, the potential Mac threat landscape still isn't as worrisome as on other platforms, but Mac users can no longer afford to ignore the possibility of being compromised by malicious software. These threats will only grow more numerous and more sophisticated as time goes on and more Apple devices are purchased.

It's happening now: 2017 was a big year for security breaches. In February, a fake Adobe Flash installer carried MacDownloader malware that attempted to transit Keychain data (which includes user names and passwords, among other personal data). Last autumn, several vulnerabilities were detected in shipping versions of the latest Mac operating system, High Sierra, one granting root access to certain areas without a password prompt. Shortly thereafter, we learned that the processor vulnerabilities called Spectre and Meltdown affect the majority of computers in the world.

Boot-up protections

Microsoft Windows 10: Microsoft has long led the way with pre-boot, boot, and post-boot protections. Some of the defenses were borrowed from other open-source operating system initiatives, some from industry-wide initiatives, and many others self-invented. Today, Microsoft places many of them under the larger branding umbrella of Windows Defender System Guard. Boot protections, in particular, are known as Secure Boot.

> * In the first decade of its existence, **Microsoft's flagship Windows program was easily the most successfully attacked OS** in the history of computers.

With Secure Boot, everything starts pre-boot by requiring computers to have the updated, more secure, Unified Extensible Firmware Interface (UEFI) and Trusted Platform Module (TPM) chips installed on the motherboard and used. Both chips require cryptographic approval before they will accept new code or configuration settings, and both allow the boot process to be cryptographically measured and verified. Earlier verified components often securely store the previously verified hash of later components, which must match, before the booting process can continue normally. Microsoft also refers to these processes as Measured Boot or Trusted Boot.

If anything, like a rootkit, tries to modify the pre-boot or OS booting process, one of these two chips will be alerted and either stop the attempted modification or give the user a critical warning upon next use. If you remember all the press about rootkits and boot malware and wonder why we don't hear about them as much anymore, it's because of pre-boot and boot protection processes like these. Mark it as one of the few significant successes against hackers and malware.

> **Microsoft went future** and allows any device driver, which essentially becomes a part of the OS, from being installed, on a per-device driver basis.

Both UEFI and TPM are open standards that any vendor or OS may use. UEFI replaced the more vulnerable BIOS chips, and the TPM chip hosts a core set of cryptographic features, including the secure storage of critical system cryptographic keys. Both chips allow any OS vendor to better maintain the integrity of their OS, and other applications, such as data storage encryption, during and after boot.

Windows also includes a feature known as Configurable Code Integrity (CI). CI allows only previously defined and trusted code to run after the trusted boot process is complete. CI is a major step forward in a general purpose OS in only allowing trusted code to run, but it takes significant planning, testing, and resources to get it right for normal operations beyond what Microsoft has already tested and approved. Still, if you want to have the most secure Windows OS you can have, CI allows you to do it.

Microsoft has also improved with every OS version its ability to prevent industry standard pre-boot I/O interfaces, such as direct memory access (DMA) or IEEE 1394, from being used to control a disk or device pre-boot. Preventing these interfaces from being used maliciously while not significantly slowing down or impairing the OS has been a huge challenge for all OS vendors. Microsoft went future and allows any device driver, which essentially becomes a part of the OS, from being installed, on a per-device driver basis.

Microsoft Windows 10 also introduced an improved version of device health attestation. DHA allows OSes to be verified to have clean boot and other processes before continuing. What is included in the health check depends on the OS, the OS admin, and the service they use for DHA. Customers can do their own DHA checks or outsource the it to Microsoft or a third-party vendor.

Apple macOS: Apple adopted an early version of UEFI with far less protection known as EFI 1.0, but hasn't adopted the more secure, later, versions of UEFI. Instead, Apple has created many proprietary features with some of the same, but not identical, protections. Because Apple has not released detailed information on its proprietary protections, it is difficult to get more specifics on Apple's pre-boot and boot protections to see how well they compare.

However, several boot-up protections can be enabled on the Mac, specifically to prevent access to the data on a Mac's hard drive if it falls into the wrong hands. The standard user account password provides rudimentary protection against access on a properly booted Mac, but does nothing against someone with access to the equipment and with knowledge of Target Disk Mode.

To prevent unauthorized access, startup disks can be encrypted using FileVault 2, and the Mac can be set to prevent booting to external devices via firmware passwords. FileVault 2 encrypts the entire drive using the AES-XTS mode of AES with 128-bit blocks and a 256-bit key, and it prevents anyone who does not have an unlock-enabled account from seeing disk contents whatsoever.

The new iMac Pro released in late 2017 features an Apple-designed T2 chipset. This chipset consolidates a bunch of hardware subsystems into one chipset, but also introduces some interesting security features that will be adopted on other Macs, eventually.

• • • • •

Memory protections

Microsoft Windows 10: Microsoft has done much security work in memory protections, usually to prevent initial exploits, zero days, and privilege escalations. Most are gathered under the Windows Defender Exploit Guard, and many came from a previous exploit protection add-on called Enhanced Mitigation Experience Toolkit (EMET).

Data Execution Protection (DEP) has been around since Windows XP. DEP attempts to prevent malicious buffer overflows, where a malware program attempts to place executable code in a data area, and then trick the OS into executing it. DEP prevents the OS from executing anything in areas marked as data.

Microsoft Windows Vista introduced many new security features, including Address Space Layout Randomization (ASLR), Structured Exception Handling Overwrite Protection (SEHOP), and Protected Processes. ASLR places common, critical, system executables in different places in memory between each boot. This makes it significantly harder for malicious programs that attempt to manipulate and modify these components to find them.

SEHOP attempts to stop malicious, rogue, error handling from being installed and executed when an execution error is found. These security features and other preventative technologies morphed into what Microsoft now calls Control Flow Guard. It is enabled on every Microsoft program and is available in programming tools such as Microsoft Visual Studio 15.

EMET also arrived in Vista, as an add-in to help prevent 0day attacks. It contained memory protections, digital certificate handling improvements (like certificate pinning), early warnings, and improved reporting to both the OS admin and Microsoft so they could identify the technical specifics of different new attacks. EMET expanded to over 15 separate mitigations, and its proven protection became so recommended that Microsoft built it into Windows 10 with the Creators Update release (as Windows Defender Exploit Guard).

Apple macOS: Macs have an XD (execute disable) feature built into Intel's processors that prevents memory used for data and memory used for executable instructions from accessing each other. This is a common attack used by malware to compromise a system, but the XD creates a barrier of sorts.

> * Basically, with ASLR enabled, **a hacker is more likely to crash the app they're trying to exploit** than gain access to do anything malicious.

Also built into every Mac is the macOS kernel's use of ASLR, which makes it more difficult for attackers to pinpoint application vulnerabilities by randomly arranging the values of target addresses. Basically, with ASLR enabled, a hacker is more likely to crash the app they're trying to exploit than gain access to do anything malicious.

• • • • •

Logon/authentication options/IdM/protection

Microsoft Windows 10: Once an OS boots up, the most important security feature it can have is in limiting who has allowed, authorized access to it. This is controlled by a logon authentication security feature and might include passwords, biometrics, digital certificates, and other multi-factor devices, such as smartcards and USB authentication tokens. It has also become especially important to protect logon credentials after the authorized party has logged on, temporarily or permanently, whether stored in memory or on disk, to stop various credential theft and re-use attacks.

Windows 10 has strong support for broad password policies, and for biometric, multi-factor, and digital certificate authentication. Microsoft's newest and most secure logon feature is known as Windows Hello. It supports face and fingerprint recognition, which allows for quick and easy sign-ons, but behind the scenes uses secure digital certificate technology. Users can still use a password or a shorter PIN, although each of these can only be enabled as an option after setting up more traditional authentication methods (such as password). Windows Hello also works with enabled applications, such as Dropbox and multiple password managers.

Microsoft, worried about the theft of credentials in memory, created Virtualization Based Security (VBS), where logon credentials are secured in a hardware-based, virtualized subset of the operating system that is nearly impervious to malicious attacks. You may hear VBS also referred to as Virtual Secure Mode (VSM).

Using the VBS core, they created Windows Defender Credential Guard and Device Guard. Credential Guard protects multiple types of logon credentials including NTLM, Kerberos, and other non-web, domain-based credentials stored in Microsoft Windows' Credential Manager.

> Once hackers or malware have established a foothold on a system, **they usually try an additional privilege escalation attack** to obtain top administrative access.

Credential Guard defeats many of the most critical and popular password attacks. Credential Guard requires 64-bit version of Windows, UEFI, TPM (recommended, not required), Secure Boot, and an Intel or AMD processors with the appropriate virtualization extensions.

Hackers have long been using stored service credentials to take over computers and networks. Windows Vista introduced the concept of Virtual Service Accounts and (Group) Managed Service Accounts (the latter of which requires Active Directory). Both are new types of service-only identities that, once initiated, take over the complex task of randomizing and periodically changing service account passwords so that if stolen, are of less value across an enterprise.

Apple macOS: Firmware passwords can be set to prevent choosing anything but the designated startup disk, and a firmware password also ignores the standard startup key combinations. Be aware that both FileVault and firmware password protection requires the use of a strong password; if a weak password is used and then guessed, the entire contents of the drive will be exposed to anyone with the proper credentials.

The 2017 iMac Pro is the first to ship with the T2 chipset, and specific features can be modified using the new Startup Security Utility. This utility was designed to make it easier to secure the Mac against unauthorized access by combining firmware password protection, Secure Boot, and External Boot options in a single interface. From here, you can set how strict the Mac is about using the operating system and installing updates and third-party software.

Privilege escalation prevention

Microsoft Windows 10: Once hackers or malware have established a foothold on a system, they usually try an additional privilege escalation attack to obtain top administrative access. The mitigations contained in Windows Defender Exploit Guard are Microsoft's first line of privilege escalation attack prevention, but it has many others.

User Account Control (UAC), introduced in Vista, attempts to "de-elevate" a privileged user (e.g., an administrator) if they are only performing standard user tasks, such as reading email or browsing the Internet. If a user logs on with privileged credentials, UAC, splits their access into two tokens: one privileged and one non-privileged. The non-privileged token is used by default with all applications and tasks unless the user is prompted for elevation or if they run one of the many predefined tasks requiring elevation. Early on, many users and administrators cursed UAC's intrusiveness. Today, most users run in UAC-enabled mode without noticing an overly burdensome number of interruptions.

Apple macOS: Most users on Apple's operating systems are created as administrators. With their username and password, they can install apps or make changes to settings that affect the entire system. Thankfully, there are protections built-in to the macOS that make it difficult for rookie users with admin privileges to make obvious mistakes, like attempting to delete the /System folder or its contents. Even if malicious software is inadvertently installed with admin privs, the built-in System Integrity Protection acts as a failsafe so that malware can't wreck the operating system. (More on this later.)

The macOS isn't always flawless: It was revealed a few months ago – and the bug since patched – that Apple's latest version would allow root access without a password. While the flaw was quickly addressed, it's a not-so-subtle reminder that your hack-proof computer is only for the moment, and an exploit could be discovered at any time.

Data protection

Microsoft Windows 10: OS security doesn't matter if you can't protect the data. Microsoft has long had file and folder encryption (Encrypting File System), but added volume encryption with Vista using BitLocker. The ultimate encryption keys can be stored on the TPM hardware chip, on the network, on a removable media device, and other options. Later Windows versions added options and encryption features, including the ability to encrypt and require encryption on removable media using BitLocker To Go. With or without requiring encryption, administrators can configure what removable media devices are allowed to be installed and used.

Apple macOS: As mentioned earlier, FileVault 2 can be used to encrypt startup disks to prevent unauthorized access. The Mac can be set to prevent booting to external devices via firmware passwords. FileVault 2 uses the AES-XTS mode of AES with 128-bit blocks and a 256-bit key. In concert with a firmware password – which prevents booting with modifier keys, potentially bypassing the startup disk – FileVault 2-encrypted disks locked with a strong password are virtually impossible to crack.

Recovery keys can be used if the storage device is moved to another Mac, or if users with unlock privileges available. The recovery keys can be kept in management systems, like JAMF, or they can be stored on Apple's iCloud servers, behind your Apple ID.

The native Disk Utility app can be used to encrypt external drives, or create encrypted disk images.

File integrity protections

Microsoft Windows 10: Windows has many features that provide integrity to the OS and user data files. Microsoft Windows Millennial Edition (Windows ME) introduced an OS file protection process called System File Protection (SFP). If anything deleted a system critical file, SFP ensured that Windows would immediately replace it with a known good copy. Windows Vista introduced a version of SFP known as Windows Resource Protection, which also protected critical Windows registry settings, although what was protected and automatically replaced diminished overall.

Vista also introduced Mandatory Integrity Controls (MIC) and file and registry virtualization. With MIC, every user, file, and process in Windows is explicitly assigned a MIC level (high, medium, low). Users, files, and processes of lower MICs cannot modify objects of higher MICs. With file and registry virtualization, most of the OS critical files and registry settings are protected by virtualization so that if an unelevated user or process tries to modify them, the modification will instead happen to an additional, virtual, copy of the file or registry. This prevents unelevated users and malware from modifying system-critical files and registry settings as easily as they did before.

Introduced in Windows 8, the PC Reset and PC Refresh features allowed users to reset a device back to its new state (PC Reset) or back to a near-new state, but save your user files, customizations, and some applications (PC Refresh). If you're worried about malware, it's best to reset it to start with a known clean state.

Apple macOS: Introduced in El Capitan in 2015, the security feature called System Integrity Protection (SIP) addresses the problem with unrestricted root access if malware or hackers gain access to the account credentials. SIP protects the contents and permissions of certain important files and directories, even from actions performed as root. SIP protects against running unsigned kernel extensions, and it protects processes against code injections and real-time modifications to code without specific entitlements. Only properly signed apps can modify the protected system directories, and those apps must be tied to a developer ID and with entitlements signed by Apple.

> * **OS security doesn't matter** if you can't protect the data.

Cryptography support

Microsoft Windows 10: Starting with Windows Vista, Microsoft no longer tried to invent its own encryption ciphers and algorithms. Instead, it deployed respected cryptography (e.g., ECC and SHA-2), and frequently updated it to get rid of proven weak ciphers and to support new, emerging crypto.

Apple macOS: The T2 chip features a hardware-encrypted Secure Enclave to store the Mac's encryption keys, which pass to the hardware encryption engine on the same chip. The T2 chipset also controls the two striped NAND memory chips that are used for storage, including dedicated AES encryption hardware that encrypts/decrypts storage data on-the-fly with no performance hit.

The T2 chipset manages the Mac during boot to ensure the operating system software hasn't been compromised. Upon startup, the T2 chip takes over, and using its hardware-encrypted Secure Enclave to compare keys, loads the bootloader, ensures its validity, validates the firmware, and then validates the kernel and drivers that allow the Mac to run.

> *****Since 2007, Macs have shipped with Time Machine.** This service aims to make the backing up process easy, in a set-it-and-forget-it kind of way.

Disk/data backup/restore

Microsoft Windows 10: Every version of Windows has had multiple ways to backup and restore files. Since Windows XP, users could use the System Restore feature to restore the OS and settings to a previously saved version of the OS. The Previous Versions Windows XP option was built-in by Windows 8. It allows individual files to be restored from previously saved versions, if covered by the Previous Versions saving process.

Starting in Windows 8, a backup-and-restore feature called File History is available. While not a complete system backup, File History is often just what users need, especially when the Windows OS can be restored separately already. File History, by default, attempts to back up the most popular areas for people storing files and configuration settings, such as My Documents, Music, Documents, Videos, Desktop, Downloads, and AppData, but you can also include and exclude any files and folders you wish and then make a backup schedule.

Apple macOS: Since 2007, Macs have shipped with Time Machine. This service aims to make the backing up process easy, in a set-it-and-forget-it kind of way. If Time Machine hasn't been configured, plugging in a hard drive prompts a dialog box offering to set that drive as the backup destination. Once confirmed, the backup process begins.

Time Machine keeps hourly backups for the past 24 hours, consolidates that data into daily backups for the last month, and then consolidates everything older than that into a weekly backup set. When storage space runs low, Time Machine compensates with the deletion of the oldest weekly backup. Time Machine settings can be modified under the System Preferences.

Application protection

Microsoft Windows 10: Microsoft started to get very strict on what an application could do to another application or what an application could do to the operating system with Windows Vista. It put a hard separation between the OS, services, and end-user applications. With Windows 8, Microsoft created a more protected class of applications called Metro apps. They were eventually named Modern Applications.

Modern Applications, following the lead of Apple and others, could only be installed from the official Microsoft Store and only after review and approval. All Modern Applications run in a dedicated "sandbox container" (known as an app container) with limited access to each other and the OS. Modern Apps could only run if UAC was enabled.

In Windows 10, Microsoft debuted Windows Defender Application Guard. Application Guard works on Windows 10 and in conjunction with Microsoft Edge. Microsoft Edge and the sites and applications it hosts now run in an isolated VBS-based, virtualized environment that is separate from the OS. Sessions opened in Application Guard cannot start browser extensions, save files to the local file system, or do other higher risk actions. Rumor has it that future versions of Application Guard will be expanded to support more applications.

Controlling which applications are and aren't allowed to run (known as application control, blacklisting, or whitelisting) has long been a way to achieve very high levels of security. Microsoft included application control in Windows XP using a feature known as Software Restriction Policies (SRP). SRP was superseded by AppLocker in Vista and later. Both features allowed admins to configure which programs, scripts, or installers did or didn't run based on name, location, or digital certificate.

In Windows 10, CI and Device Guard have become Windows Defender Application Control. With WDAC, very specific allows and denies are managed by a hardware-based enforcement. Admins are allowed to decide what level of application control is right for their environment and can choose among AppLocker, CI, Device Guard, and WDAC. One of these features will have the right level of control versus operational trade-off for your sphere of influence.

Apple macOS: The best and simplest way to stay a step ahead of potential hackers is by keeping the operating system software and apps as current as possible. Apps should be downloaded from a trusted source, such as the vendor's main site or, even better, the Mac App Store.

The Mac App Store resides in /Applications, and each app within it has been vetted by Apple employees and assigned a digital certificate. If the app is caught misbehaving, Apple can pull the plug on the offending app. Considering the alternatives, the Mac App Store is as safe as it can be for app downloads.

The problem: Not every app is available at the Mac App Store and sometimes a download from a third-party site is unavoidable. That's where Gatekeeper comes into play. Gatekeeper is a security feature that checks the digital signature of software and blocks the software's installation if any of the checks fail. Apps need to be signed with a code received from Apple to run, and those apps that pass the code check run without issue.

Gatekeeper can be configured in the Security & Privacy System Preference pane, and from there one of two options can be chosen: Allow apps downloaded from 1. the App Store or 2. the App Store and identified developers. When trying to install software that fails this check, the Security & Privacy preferences has manual over-ride, but this should only be used if certain the software is from a trusted source.

> * The best and simplest way to **stay a step ahead of potential hackers** is by keeping the operating system software and **apps as current as possible.**

Another feature is app sandboxing. Sandboxing limits an app's access to system resources, data, and other apps, which in turn limits the potential damage malicious software can do. The strengths to sandboxing also happen to be its drawbacks, so not every app supports this capability. Many built-in apps (including the built-in web browser, Safari) offer sandboxing protection.

Another feature worth noting in macOS High Sierra: any kernel extension installed by an application needs explicit approval to run. This should cut down the probability of malware sneaking in unauthorized software without user knowledge and consent.

• • • • •

Browser protections

Microsoft Windows 10: Microsoft replaced Internet Explorer (IE) with Microsoft Edge with Windows 10. As a significantly cut-down browser, Microsoft Edge doesn't share much code with IE. It doesn't run traditional high-risk browser add-ins; it only accepts reviewed and approved extensions from the Microsoft Store. It has one-button configuration resets (to get rid of any possible malicious modifications) and can be put in the Windows Defender Application Guard mode.

Every website and download is evaluated by the Windows Defender Smartscreen feature, which in Windows 10 extends across the whole Windows OS and not just the browser. With significantly less code and surface area, Edge is stricter about what applications and websites can and can't do. It's thought to be a vast improvement over IE.

Apple macOS: Every Mac ships with Safari, Apple's web browser, and Safari is equipped with anti-phishing technology, settings to prevent cross-site tracking, and a strong-

> **A long-time network defense** built into Windows is the ability to **put any network or wireless connection on a separately managed profile.**

password generator with links to iCloud Keychain.

Network/wireless protections

Microsoft Windows 10: Microsoft is often on the cutting edge of network and wireless security technologies. Besides long supporting wireless and network standards, it often adopts them early and pushes them to customers before most customers are ready (e.g., IPv6 and DNSSEC). A long-time network defense built into Windows is the ability to put any network or wireless connection on a separately managed profile. This allows different firewall, router, and other security settings to be enforced on a per-connection basis.

Anti-malware

Microsoft Windows 10: Windows Defender Antivirus has proven to be a top notch and un-intrusive anti-malware program, especially when deployed its default state along with Windows other anti-malware features like Smartscreen and Windows Defender Exploit Guard. Windows allows any anti-malware program to load itself just after the critical OS boot processes and before any other, non-essential applications load with a featured called Early Loading Antimalware (ELAM).

Apple macOS: In April 2017, Check-Point security researchers found malware capable of bypassing Gatekeeper. Then in May, the popular video transcoder Handbrake was hacked, and an infected version was distributed with the OSX.PROTON remote access Trojan. Attacks are becoming more sophisticated, and so are the mechanisms in place to help deal with potential breaches.

On the Mac, routable network services are disabled by default, and many modern applications and services are sandboxed. That means that apps (and system services) have limited access to available system resources; malicious code is prevented from interacting with other apps or the system.

Apple also has a more extreme way to fight malware. Using a silent automatic update, Apple maintains a blacklist of known malware threats on every Mac. Every file that is downloaded by Safari, Messages, and Mail is flagged with metadata that marks whether the file is safe, the source of the file's download, and the time and date of the download. Any file marked unsafe opens a warning notification, with the option to move said file to the trash.

Certain programs and any associated are automatically deleted, and any modifications the app made are tracked and reverted. If this ever occurs, the next time someone with administrator rights logs onto the Mac, a notification announces that changes had occurred.

Firewalls

Microsoft Windows 10: Windows has had an always-on, installed by default firewall since the days of Windows XP Service Pack 2 in the form of Windows Firewall. It comes with dozens of built-in rules, denying inbound connections unless by exception, and allow additional rules to be created by user, group, admins, networks, services, or applications. Windows Firewall is versatile and non-intrusive. It is also easily configurable along with IPSEC. The only flaws are the poor logging (sometimes too much) and lack of notification to the end-user about any significant, ongoing recognized security event, like a denial-of-service attempt or port scan, which other third-party firewalls often give.

Apple macOS: All Macs ship with a built-in firewall service, but it is off by default. Firewall can be configured under the Security & Privacy System Preference, including enabling a Stealth Mode that allows the computer to ignore ICMP requests and connection attempts.

Remote access

Microsoft Windows 10: Although Microsoft recommends that all remote administration be performed using

MORE ON WINDOWS SECURITY

- The 10 Windows group policy settings you need to get right
- 6 new and noteworthy security features in Windows 10 Fall Creators Update
- The paranoid user's guide to Windows 10 privacy
- How Windows 10 data collection trades privacy for security
- Microsoft adds another layer to the Windows 10 patching onion

PowerShell or Microsoft Management Consoles (MMC), the Remote Desktop console and protocol (RDP) remains one of the most popular was for an admin to remotely access a Windows computer. RDP has been upgraded many times over the years. Now users can connect using digital certificate authentication and protection, and use Windows Defender Credential Guard to protect their admin credentials.

Apple macOS: The Mac supports many protocols for remote access, including native support for SSH and sftp. The Macs can also be remotely managed using Apple Remote Desktop, remote screen sharing can be accomplished with the native support for VNC, and iCloud subscribers can enable Back to my Mac to remotely access their Macs from any Mac logged in with the same Apple ID.

• • • • •

Security configuration

Microsoft Windows 10: Local security policies were introduced in Windows NT Service Pack 4 and significantly expanded with Windows 2000 and XP using Active Directory Group Policies. Today, no other operating system allows as much built-in point-and-click security configuration options as Windows. There are thousands of options across the OS and other popular applications, such as Microsoft Office. Admins can use PowerShell scripts to accomplish the same things they could manually or using group policy.

• • • • •

Patching

Microsoft Windows 10: Patching for the Windows OS and Microsoft applications is built in and turned on by default. Windows checks for new patches at least daily and automatically apply them without interaction with admins or end-users. New installs benefit with a set of built-in, hard-coded, can't easily turn off firewall rules that protect PCs from most network attacks while being patched for the first time. Thank the MS-Blaster worm of 2003, where admins had difficulty patching new computers before they were infected by malware.

Apple macOS: Apple has historically responded quickly to patch high-profile exploits.

• • • • •

Privacy

Microsoft Windows 10: After decades of being accused of invading end-user privacy, Microsoft is among the strong advocates for privacy, and provides myriad customizable settings within Windows, where any admin or user can determine, at a detailed level, what information is or isn't collected, and why.

Apple macOS: Apple executives have been leaders at the forefront of user privacy issues, in some cases publicly sparring with the federal government on behalf of protecting user data. Apple doesn't harvest user data to sell at the highest bidder, security information like fingerprint- and face data never leave the device, and Apple's privacy policy is refreshingly direct and well worth the read.

• • • • •

Logging

Microsoft Windows 10: Microsoft products contain dozens of log files that can be used for security analysis, depending on which features and services are installed. Central is Windows Event Log service. Traditionally, it contained three main logs (Security, System, and Application). Today it contains over a hundred far more specific logs, all XML-enabled and configurable. You can forward logs or specific events to other collector machines and trigger console messages or other applications. If there is a complaint about Windows logging, it's that it does too much logging about too many minor events. In the world of computer security, we'd rather start working with that problem than not enoughgood information.

Apple macOS: Last year's macOS Sierra introduced a unified logging system, in an effort to provide a single and efficient API to capture and store all system and app activity. Logs can be configured to record varying levels of detail, and this data can be viewed using the built-in Console app. ♦