jamf

WHITE PAPER

Security Differences of macOS and Windows

As Mac becomes a familiar face in enterprises and small businesses around the world, the days of relying on legacy management tools to secure modern devices has come to an end.

When you take in to account Microsoft's decision to end extended support for Windows 7 on January 14, 2020, more (primary) Windows admins and users will be entering a world that may be unfamiliar — Mac.

With security being arguably the most important component of technology, this white paper provides an overview of macOS and explains where it differs from Windows.

To see how you can maximize your Mac investment, visit **jamf.com**

MACOS STRUCTURE OVERVIEW

Apple designed macOS with an integrated approach to hardware, software and services that provide security by design and make it easy for IT teams to configure, deploy and manage. Just as employees expect a consistent experience when using a computer at work, IT should expect a similar experience when managing the platform for employees.

Apple has specific enterprise programs to help streamline deployment and security to create an out-of-box experience for users. Apple Business Manager combined with mobile device management (MDM), result in consistent and protected management across the entire Apple ecosystem.

Some organizations look to one tool to address the needs of all macOS computers and Windows PCs. This leaves organizations with gaps in management, user experience and security. When a single management tool is used to manage multiple platforms, security features are not properly utilized — as this is not how Apple or Microsoft intended devices to be secured.

What is Apple Business Manager?

Apple Business Manager provides IT admins with one consolidated portal to automatically deploy Mac, iPad, iPhone and Apple TV devices directly to users — configured with settings, security controls, apps and books.

The macOS framework

To articulate Apple's approach to security, one must first understand the basics of the Apple framework.

HOW MACOS MANAGEMENT DIFFERS FROM WINDOWS

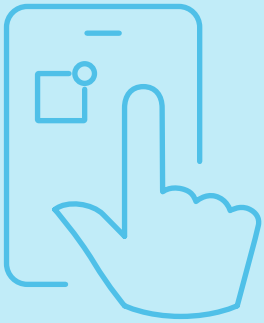
How does Apple differ from traditional Microsoft endpoint management for Windows PCs? The key to macOS ease of use is its built-in management framework known as mobile device management (MDM). MDM allows IT to build configuration profiles that manage various settings inside of the OS. These profiles are delivered over the air via Apple Push Notification Service (APNs). APNs keeps a constant connection to Mac computers (as well as other Apple devices) so IT doesn't have to. MDM enables management capabilities that traditional Windows admins may only believe they can get through binding or Group Policy Object (GPO).

APNS STRENGTHENS AN ORGANIZATION'S SECURITY POSTURE

APNs is a secure and highly efficient service for propagating information to macOS, iOS, tvOS and watchOS devices. APNs is a critical layer for Apple deployment programs and other security features, such as Remote Lock and Remote Wipe. In fact, Apple Business Manager or MDM will not work without APNs in place, because these programs cannot be leveraged through a proxy connection. They must be accessed through a direct channel with Apple, i.e., APNs.

Additional benefits of APNs include:

- Enhanced security posture for managing corporate-owned Mac computers. APNs allows you to remotely lock/wipe a lost/stolen/compromised device over the air.
- MDM is dependent on APNs for sending critical commands such as software installations or inventory updates.
- While MDM configuration profile payloads can be delivered to macOS "offline," this method requires significantly more overhead than managing over the air.
- APNs triggers each device to automatically check-in with the MDM server.



Unique security features for Mac

The foundation of macOS is formed by integrated and secure software. Built-in macOS system security features include:

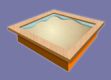
FileVault is a layer of encryption built into macOS to protect user data if a device is lost or stolen.

Malware Removal Tool allows Apple to remove malware that manages to get on the system.

Software updates come directly from and are digitally signed by Apple so organizations and IT know they can be trusted.

App Store apps available in the App Store are always vetted by Apple and only Apple-approved resources are available. Apple has the ability to remove app availability and revoke developer certificates instantly.

System Integrity Protection (SIP) protects core operating system files that could otherwise be targets for exploits from user and application access.



App Sandboxing ensures that apps do not share (or steal) data from the system or one another.

XProtect is an automated anti-malware utility, kept up to date by Apple. This prevents malicious software and/or often outdated, vulnerable plug-ins like Java and Flash from running on a Mac.

Privacy controls are available for users and IT to define – a transparent process, which lets users know when location services are used, which apps have access to contacts or calendars, and what information is being shared with Apple and/or app developers.

Gatekeeper lets IT define where users can download their applications from. It works to prevent unsigned apps (or malware) from running and therefore works together with XProtect to swiftly halt the spread of malware.

For a complete list of Mac security features, please visit: **https://www.apple.com/macos/security/**

BENEFITS OF FILEVAULT FOR DISK ENCRYPTION

FileVault is built-in disk encryption for macOS, meaning IT does not have to add any additional software in order to encrypt a drive. This can be enabled manually, or IT can remotely enable it across all Mac computers. Encryption keys can be centrally managed so IT can access necessary data after an employee leaves the organization or if they simply forgot their password and need assistance logging in. Encryption keys can also be rotated easily for increased security.

APPLE T2 CHIP FOR EVEN GREATER SECURITY

New Mac computers like MacBook Air and certain models of MacBook Pro include a custom Apple T2 Security Chip, featuring a Secure Enclave which provides the foundation for new security features and also protects Touch ID fingerprint information.

The Apple T2 Security Chip also features a solid-state drive (SSD) controller with automatic, on-the-fly data encryption — offering the most secure storage of any computer. It also ensures software loaded during the boot process has not been tampered with. This provides the most secure boot process of any computer.

DIMINISH THE NEED FOR THIRD-PARTY SECURITY SOFTWARE

Unlike Windows, an additional layer of security or bolt-on third-party tools is less commonly used for Mac.

Traditional Windows-focused security companies tend to lag behind Mac development cycles, potentially slowing the adoption of new operating systems and security features. In fact, treating Mac as you would Windows often prohibits employees from being their most productive and disrupts the user-friendly experience Apple is known for. Plus, adopting a Windows software version on a Mac is a recipe for poor code execution, memory hogs and kernel extension (KEXT)-based panics — all equating to endless IT and security headaches.

Mac's built-in encryption and anti-virus enable many organizations to operate without third parties, but some still look for solutions for managing corporate data leakage. However, corporate data leakage can be monitored through MDM, with additional protections on the network side leveraging tools such as Cisco Security Connector.

Organizations who attempt to treat Mac computers like Windows PCs may be spending unnecessary funds on additional malware protection software. And aside from the extra cost, the add-ons could also impact Mac performance and stability.

Malware Protection

Mac
(built-in security features)

Network Firewall
Gatekeeper
XProtect
System Integrity Protection

PC
(third-party add-ons)

McAfee
Kaspersky
Symantec
BitDefender

CLOUD SERVICES AND MAC

The shift to the cloud is growing. With cloud-hosting, access to the database is limited rather than sitting on a server in your network. For decades, organizations built "walls" around their company and leveraged network perimeters as the first line of defense.

As workspaces become increasingly mobile and data no longer simply lives behind the firewall, organizations must move to a more modern, identity-based model of security. As such, Microsoft is moving enterprise data to the cloud with Microsoft Azure Active Directory.

To ensure that only trusted users on trusted devices using trusted apps are accessing this corporate data in the cloud, Microsoft and Jamf offer an exclusive integration to achieve proxy-free conditional access.

Read more here: **https://www.jamf.com/resources/white-papers/conditional-access-going-beyond-perimeter-based-security/**

ELIMINATE ACTIVE DIRECTORY BINDING

A common practice is to bind Windows PCs to Active Directory (AD) for deployment workflows. But when organizations attempt to bind Mac to the network, it creates a password-syncing problem and Apple Business Manager workflows are impacted if Doman Controllers are not exposed externally. Binding also hinders organizations from drop-shipping new Mac computers to remote employees.

While binding is an option (although not recommended), organizations using dedicated Apple management solutions like Jamf Pro and Jamf Connect can manage local accounts to apply the same password complexity and expiration requirements without worrying about connections or getting out of sync with AD. This means less password prompts for end users and less calls to the IT help desk.

To accomplish maximum security without binding, Jamf Connect offers identity management. Through integrations with common cloud identity providers — Okta, Microsoft Azure Active Directory, Google Cloud Identity, IBM, OneLogin and Ping Identity — Jamf Connect allows for a simple provisioning of users from a cloud identity service during an Apple provisioning workflow, complete with multi-factor authentication.

Jamf Connect offers the flexibility to leverage local users controlled by the same policies and controls from a directory service or identity provider. Plus, a user can unbox their Mac, turn it on and securely access every system-approved application after signing on with a single set of cloud identity credentials.

ENFORCE INDUSTRY SECURITY STANDARDS

As most InfoSec teams know, enforcement depends on what the security standards are, and which compliance standards must be met. SOC 2 is different from HIPAA and PCI is different than CIS. Knowing what to adhere to is an important first step.

Jamf Pro provides a flexible framework to help comply with many common regulatory standards. IT can simply define the applicable standards, build the corresponding profiles and policies, and apply. These could include restricting consumer features such as iCloud Drive, enforcing Gatekeeper to ensure only secure apps are being downloaded, enforcing FileVault to encrypt Mac, or restricting apps by searching for a restricted app (or even macOS) across all managed Apple devices and once located, delete the app.

IT simply needs to define what the settings are and use that information to build out configuration profiles and policies and apply them to devices.

Check out this white paper to learn how to adhere to the Center for Internet Security (CIS) guidelines: **https://www.jamf.com/resources/white-papers/macos-security-checklist/**

UNMATCHED HARDWARE, SOFTWARE, USER AND NETWORK SECURITY

The most secure platform requires the most robust management solution to ensure all possible security features are enforced and installed. No other mobile device management company integrates with Apple and its services better than Jamf, and no provider is more suited to ensure Mac success.

If you're considering offering employees a Mac choice program or want to implement Mac across the board, we can help.

Contact us today to get started or take Jamf for a free trial and put our Mac security capabilities to the test first.

Contact Now **Request Trial**

Or contact your preferred authorized reseller of Apple devices to take Jamf for a test drive.

jamf

www.jamf.com

To learn more about best-of-breed Mac security and Jamf, **visit jamf.com**.

06/12/14 June 24, 2019 8:29 AM