PIQUE SOLUTIONS

Security: Windows 10 versus Apple macOS and iOS

Security Feature and Functionality Comparison

PIQUE SOLUTIONS

April 2019

MICROSOFT SPONSORED THE DEVELOPMENT OF THIS WHITE PAPER.

THE UNDERLYING RESEARCH AND ANALYSIS WERE EXECUTED INDEPENDENTLY BY PIQUE SOLUTIONS.

Contents

Executive Summary

Where the goal of cyber prevention has been to reduce the probability of an attack against the organization, cyber resilience looks to reduce the impact of these attacks through risk management. A cyber-resilience program still considers detection and prevention techniques, but it also assumes that a breach is likely. This stance emphasizes anticipation, agility, and adaptation.

The first objective of cyber resilience is to align security with assets. The security stack should protect the business against the threats specifically relevant to those business assets. Often, security is misaligned with no awareness by the business due to a lack of data from which to decide. A growing number of technologies and architectural practices exist to improve resilience in the face of cyber threats. These improvements, however, come with costs as well as benefits.

Pique Solutions was requested to conduct a comparative analysis of the resilience of capabilities of Microsoft's Windows 10 against Apple's operating systems. The resulting analysis assesses the level of assurance those capabilities provide an organization and their utility.

For this white paper, the specific operating system reviewed is Microsoft's Windows 10 version 1809, referred to hereafter as Windows 10. For Apple, the operating systems reviewed are macOS 10.14 and iOS 12, referred to hereafter as macOS and iOS, respectively.

Within the current landscape, where organizations must acknowledge targeted, persistent attacks by well-funded adversaries, the requirements for devices with high security assurance levels go beyond the need to meet basic capabilities for enterprise security. To compare security capabilities objectively, Pique has defined the core requirements of what an ideal resilient and secure operating system would need to attain. Scoring is based on how well the operating system satisfies those requirements and whether functionality is native or requires third-party implementation.

The key findings from our research are summarized here.

Identity and Authorization

- Windows 10 supports native two-factor authentication and universal biometrics using the Windows Hello framework. Windows Hello for Business lets user authenticate to an Active Directory or Azure Active Directory account.
- macOS and iOS use local account authentication with biometric support for either fingerprint or face recognition, depending on the device and OS.

Information Protection

- Windows 10, macOS, and iOS all support default drive encryption with trusted key storage.
- Windows 10, macOS, and iOS all have equal support for virtual private networks (VPNs) to ensure encrypted communication.
- Windows 10 has native support for restricting and sharing data based on user role and profiles even in a single app. macOS and iOS support managed apps, which means any data inside the app is approved or unapproved.

Threat Resistance

- Windows 10, macOS, and iOS all support a form of secure boot to ensure a device's hardware and software have not been tampered with.
- Sandboxing has become the standard method of running applications across all the operating systems evaluated, including memory isolation techniques.

Methodology

The methodology developed and followed by Pique Solutions is as follows:

1. Determine the security characteristics and capabilities required to mitigate the risks of device access to enterprise resources, including storage, sharing, and use of information.
2. Evaluate through research how selected devices meet the defined security characteristics and capabilities.
3. Publish a detailed assessment of findings.

To assess Windows 10, macOS, and iOS using industry-accepted standards and definitions, Pique Solutions referenced the security characteristics and required capabilities founded in the principles identified in Special Publication (SP) 1800-4b of the National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide. The NIST analyzed the content and concepts from multiple standards to generate the necessary security characteristics, including findings documented in NIST SP 800-124, NIST SP 800-164, the National Security Agency mobile capabilities package, and the appropriate National Information Assurance Partnership protection profiles. Pique Solutions revised and updated the NIST characteristics where it deemed appropriate to address missing functionality, to correlate security characteristics with vendor-described capabilities, and to improve the overall presentation and flow of the white paper.

To organize the presentation, we grouped the capabilities into the following three areas.

Identity and Authorization

- Authentication: Local authentication of user to device and apps, remote authentication of user, remote authentication of device.
- Trust Model: Implementation of user and device roles for authentication, credential and token storage and use.
- Biometric Support: Methods, store, use.

Information Protection

- Protected Storage—Data at Rest (DAR): Device encryption, trusted key storage, hardware security modules.
- Protected Communication—Data in Transit (DIT): VPN, per-app VPN.
- Data Protection in Progress—Data in Use (DIU): Protected execution environments, data management, data sharing.

Threat Resistance

- Device Integrity: Boot/app/OS/policy verification, trusted integrity reports.
- Application Protection: Sandboxing, memory isolation, trusted execution.
- Browser Protection: Sandboxing, plug-ins/extensions, URL blacklisting.

The criteria are defined based on Pique's subject matter expertise and, where appropriate, based on the above-described guidance of the NIST for Security.

In our analysis, we used the following scoring system (maximum score = 15).

Scoring Category	Score	Scoring Methodology
Feature	0 or 4	0 = Feature Not Present 4 = Feature Present
Native Functionality	0 to 3	0 = 3rd-party Tool Required to Achieve Full Functionality 3 = Full Functionality Native in OS
Granularity of Controls	1 to 3	1 = Low Granularity of Controls 3 = High Granularity of Controls
Functionality Compared to "Ideal Scenario"	1 to 5	1 = Low 5 = High

Identity and Authorization

Identity and access management (IAM) provides the right people access to the right resources at the right times for the right reasons. The enterprise needs IAM capabilities that address agility in managing distributed systems where users maintain access across multiple device types. IAM should ensure integrity and authenticity of each user's identity while considering costs of the IAM infrastructure. More importantly, IAM must maintain user simplicity balanced with strong authentication controls.

Authentication

The most common form of identity is user name and password. Most users need to remember on average at least three passwords, limiting the desire or ability of most people to remember highly complex passwords, thus rendering them susceptible to being cracked on modern computers in a matter of minutes, if not seconds. Simply knowing a user's credentials allows another individual to impersonate that identity. Mobile devices, once considered simple low-risk personal devices, standardized on a less complex 4-digit PIN for convenience reasons, significantly reducing the complexity factor. Yet, while not strong, password and PIN persist, as they are relatively convenient, easy to implement, and personal to a user. As part of a multifactor authentication strategy, the password and PIN have the potential to be effective and convenient.

Windows 10 natively provides local user-to-device authentication with a choice of password or PIN and goes further by providing two-factor authentication for remote enterprise domain authentication of domain user to device and apps, including support for multiple user accounts. Windows Hello technology replaces passwords with the combination of a specific device and a biometric gesture or PIN. Windows Hello supports Microsoft accounts, Active Directory (AD), Azure AD, or a non-Microsoft service that supports FIDO 2.0 authentication. Windows 10 is the first OS to utilize FIDO 2.0 in an enterprise environment, and it is a major step forward. FIDO 2.0 supports multifactor authentication with asymmetrical keys in conjunction with hardware-based attestation to confirm the legitimacy of the keys. Critically, Windows 10 was built for both local and remote multiuser authentication, allowing for multilevel permission assignment and shared access.

Windows 10 Enterprise protects the authentication system even further by running it in a limited-access virtual container called Credential Guard. Access tokens and tickets are all stored there, fully randomized and managed, with full-length hashes to avoid brute-force attacks.

While all macOS devices support local multiuser authentication with different levels of permissions, iOS was built to be a single-user OS with authentication mapped to the hardware and not the user account. No Apple device supports domain user-to-device authentication. On all Apple devices, domain account authentication occurs to apps after the local user-to-device authentication. Even more confusingly, Apple offers native two-factor authentication for Apple ID, which is for users leveraging an iCloud or iTunes account for device authentication. The use of this Apple-native two-factor authentication requires an Apple-specific device as the secondary form of authentication. This is a workaround based on a cloud authentication system and not a native two-factor system built into the OS. An authenticated user does not authenticate on that device again except at a specified time-out period or if he or she erases the device or needs to change the password. There are third-party tools that try to address this gap, but most of these tools target application authentication instead of the device.

Biometric Support

By leveraging biometrics, user identity becomes unique, more personal, and more convenient to the user and the enterprise; however, one of the challenges in implementing biometric authentication systems is deploying safeguards to mitigate against presentation attacks, commonly known as biometric spoofing. This is especially true in uncontrolled environments where there is not an operator monitoring the placement or capture of a biometric. There are multiple ways to mitigate the risk of a successful presentation attack, known as presentation attack detection, which includes the categories Artefact Detection and Liveness Detection.

Leveraging Windows Hello, Windows 10 integrates biometrics with the other security components of the device. The user's biometric data used with Windows Hello does not travel across the user's devices, and it is not centrally stored in the cloud. Windows 10 converts the biometric image taken by the sensor into an algorithmic form and destroys the original image, rendering it irretrievable. The algorithmic form of the image is then stored on the Trusted Platform Module that is required on every Windows 10 device. The implementation of native biometric authentication is fully dependent on vendor implementation and changes from device to device. Because Windows Hello supports third-party devices, it is possible to add fingerprint or facial recognition authentication using third-party hardware.

Touch ID and Face ID are Apple's biometric authentication technology. With Touch ID, touching the Home button unlocks an Apple device and authorizes purchases in App Store and iTunes Store. With Face ID, facial recognition software using the front-facing device camera unlocks the Apple device. App Store–distributed apps also can integrate Touch ID or Face ID for authentication. Apple devices convert the fingerprint or facial picture into a mathematical formula, encrypt it, and carry it over a hardware channel to the secure enclave on the Apple hardware chipset.

Critically, the presence of Touch ID or Face ID depends on the Apple device, whereas Windows Hello is present on every Windows 10 device with support for all biometric authentication methods. Even in the case of a Windows 10 vendor not natively integrating the hardware for biometric authentication, third-party devices can be leveraged for biometric authentication. Apple devices are limited to the method Apple supplies. For example, newer iPhones and iPads only support Face ID, whereas only the top-end MacBook and older iPhones and iPads support Touch ID. **Table 1** provides a summary of scoring for Identity and Authorization features and functionality.

Table 1. Summary of Scoring Results for Identity and Authorization

OS	Feature	Native Functionality	Granularity of Controls	Functionality vs. "Ideal"
Windows 10	●	●	●	●
macOS	◕	◕	●	◕
iOS	◕	◕	◕	◕

Poor ○ ◔ ◑ ◕ ● *Excellent*

For enterprise security, Windows 10 scores higher than both macOS and iOS in authentication by having full native multiuser domain-to-device authentication. Windows 10 provides two-factor domain authentication without a password or a secondary device, at least one of which is required by macOS and iOS. Furthermore, Windows 10 supports domain accounts for local authentication. Apple only supports local accounts with domain authentication occurring in supported applications. The macOS identity management system lacks any level of assurance beyond protection against malicious intent using simple methods. It is not a suitable authentication system for enterprise use without the support of third-party tools.

Information Protection

As defined with data loss prevention, data controls relate to three functional groupings that correspond to the data life cycle: DAR, for data stored on a device and other forms of media; DIT, for data shared between users and the associated methods of information sharing; and DIU, for the creation and manipulation of data on the device residing in apps, documents, and system memory. In any data protection strategy, controls would be located as close as possible to the data. The most effective method for data protection is to implement controls on the data, followed by apps serving as data custodians, and lastly on the device and network. Controls may exist at all the preceding locations for complete management of the data life cycle.

Protected Storage (DAR)

Encryption is the primary means used to ensure that a lost, stolen, or misused device does not lead to the loss or compromise of sensitive information. The cryptographic keys used for encryption should be stored in protected locations in either the software, firmware, or hardware, with hardware providing the highest level of protection. Tamper-resistant hardware is also preferred for performing cryptographic operations.

Windows 10 implements BitLocker for whole-disk encryption, including OS and data storage partitions. It applies encryption automatically when policy requires it, or the user enables it in the Windows settings. Windows 10 accelerates encryption through processor extensions to avoid compromising device performance. Windows 10 Enterprise supports 128- and 256-bit XTS-AES to provide additional protection from a class of attacks on encryption that rely on manipulating cipher text to cause predictable changes in plain text.

To encrypt the startup disk and the user’s home drive, macOS FileVault full-disk encryption uses 128-bit XTS-AES encryption. FileVault will not work if all FileVault-authorized users have their home directories residing on volumes other than the startup disk, which is the default configuration for macOS. Any user with authorized access to the disk has access to the entire drive when authenticated. Additionally, a FileVault-authorized user only needs to log in the first time for decryption.

iOS uses a 256-bit device-unique secret key stored in the phone’s hardware and does not store these values elsewhere. No software or hardware can read this key. The device-unique key combines with the passcode to generate a passcode key to secure data on the device. The intent is that an attacker cannot remotely extract the device-unique key from the device.

Protected Communication (DIT)

The objective of controls for DIT is the ability for the user to establish a protected connection between the device and trusted enterprise resources or with enterprise apps, usually through VPNs. The value of a VPN is that it encrypts a device’s internet connection to provide secure remote enterprise access. The use of VPNs, however, does have a negative impact on network performance, although it is largely imperceptible on modern networks. VPN access also unnecessarily exposes an organization to other apps on a device. VPN access should be granular with the ability to limit access to specific apps.

Windows 10 supports several OnDemand and Enforcement methods to simplify and secure the VPN connection. Always on enables the VPN to connect automatically when the user turns on his or her phone or if there is a network change. LockDown VPN further enforces policy by only allowing network traffic over the VPN tunnel. An app-triggered VPN allows for automatically triggered connections when an app launches. Traffic Filters offer enterprises the ability to manage per-app behavior so that only traffic originating from an approved list of apps flows across the VPN. As another layer, Traffic Filters also provide filtering based on host destination attributes. Both app- and traffic-based rules can be applied.

macOS includes a universal VPN client with support for L2TP over IPSec and PPTP, allowing for the use of both digital certificates and one-time password tokens from RSA or CRYPTOcard for authentication. In addition, the L2TP VPN client supports Kerberos authentication and VPN On-Demand. The VPN client includes support for Cisco Group Filtering and DHCP over PPP. For applications, macOS does support per-app VPN connectivity.

iOS supports VPN On-Demand for networks that use certificate-based authentication defined through profile configuration. iOS 10 also supports per-app VPN, facilitating VPN connections on a much more granular basis. Mobile device management (MDM) can specify a connection for each managed app and/or specific domains in Safari. iOS supports always-on VPN, which can be configured for devices managed via MDM and supervised using Apple Configurator or the Device Enrollment Program. Always-on VPN tunnels all IP traffic back to the organization. The default tunneling protocol, IKEv2, secures traffic transmission with data encryption.

Data Protection in Progress (DIU)

The goal of data protection in progress is to limit the sharing of enterprise data with personal apps and services to prevent data loss. This can be accomplished in several ways, including data encryption, app management, and secure containers. Of the three methods, data encryption incurs the lowest impact on system resources and usability. Secure containers and segregated apps incur a higher impact on system resources and usability. In addition to methods for managing enterprise data within the app, data residing in memory needs to execute in a protected memory space.

Windows Information Protection (WIP) in Windows 10 integrates with the OS and does not require secure containers or duplicate apps. WIP encrypts data dynamically based on defined organization policies. By focusing on managing enterprise data regardless of app, WIP provides the enterprise visibility and control of enterprise data without altering the personal user experience. WIP classifies data and apps as personal or work to determine which apps have access to business data. This classification also determines what data to encrypt and how users can share that data. AppLocker, a part of the configuration service used by MDM to specify which apps are allowed and/or disallowed, manages app classification sans app wrapping or app modification with an SDK. This means admins do not need to add or remove any classified app from a device, including when wiping enterprise information. WIP does not tamper with existing personal apps and data.

macOS does not provide native data protection for data management beyond file system access controls. Investment in third-party data management technology is required to address data management. Microsoft does provide RMS document management for Office 365 on macOS and iOS that meets the requirements of data protection across any device type. In most organizations, this is enough to meet corporate data policy needs and compliance requirements.

iOS limits the sharing of enterprise data using managed apps. If a preferred app for personal use is considered managed, the user is required to find an alternate means of managing personal documents. If the user has a current app that is unmanaged, such as Adobe Acrobat Reader DC, the enterprise will reclassify the app as a managed one and will no longer support unapproved data. This requirement creates redundancy in the associated apps for opening attachments, a common operation on mobile devices. iOS also provides a restriction that prevents managed apps from backing up data to iCloud or iTunes, preventing recovery of managed app data if the user reinstalls the apps. **Table 2** provides a summary of scoring for Information Protection features and functionality.

Table 2. Summary of Scoring Results for Information Protection

OS	Feature	Native Functionality	Granularity of Controls	Functionality vs. "Ideal"
Windows 10	●	●	●	●
macOS	◕	◕	◑	◕
iOS	◕	◕	◑	◕

Poor ○ ◔ ◑ ◕ ● *Excellent*

Encryption of DAR is seamless and transparent across Windows 10, macOS, and iOS with hardware-based key management. Support for encryption of network communication is equally supported across all operating systems.

Where Windows 10 shows an advantage is with native information protection, as it provides WIP to manage business data without the need for secure containers or app wrapping. Neither macOS nor iOS provide native data management at the OS level, instead relying on the implementation of managed apps. Secure management of business information with macOS and iOS require an additional investment of enterprise-level data protection. Parity can be achieved across all operating systems by leveraging application controls in Office 365, which offers the same level of support for data management.

Threat Resistance

It is unrealistic to consider any system free from all defects and secure from all external threats. Attackers exploit vulnerabilities to infect devices with malware through two methods: program errors and intended features. Program errors introduce methods by which an attacker can exploit the system by circumventing access controls to allow for remote access. These exploits subsequently use this error to download and execute other malware, propagating on the system and across the network. Intended features allow for unintended use, such as browsers that allow execution of code on the local operating system, introducing a method by which viruses, worms, and other threats can obtain remote access to a system.

Device Integrity

No operating system is perfect and prevention controls should be viewed as a method of slowing down attackers. In this manner, the more granular a control is for identifying system tampering, the more likely an intrusion will be detected. Integrity refers to methods of ensuring that a device is safeguarded from unauthorized user modification. A device should remain unchanged from unapproved external sources. To reduce the impact of data loss and malware propagation on a compromised system, operating systems need to be resilient and designed in a manner that prevents new or unknown apps from gaining unreasonably broad or complete access to files stored on the disk or apps running on the device.

Windows 10 devices utilize the Unified Extensible Firmware Interface with Secure Boot to validate the integrity of the device, firmware, and bootloader. All boot components have digital signatures that are cryptographically validated, which helps ensure that only authorized code can execute to initialize the device and load the Windows operating system. This process establishes an essential root in a chain of trust that extends from the device hardware and firmware to the OS.

On iOS, a secure boot chain also validates the integrity of the device, firmware, and bootloader. At the initial power on, the device application processor executes code from read-only memory known as the Boot ROM. This is the hardware root of trust, laid down during chip fabrication, and is implicitly trusted. The Boot ROM code contains the Apple Root CA public key used to verify that Apple has signed the Low-Level Bootloader (LLB) before allowing it to load. Each subsequent step ensures that Apple also signs the next layer of the boot process. When the LLB finishes its tasks, it verifies and runs the next-stage bootloader, iBoot, which in turn verifies and runs the iOS kernel.

macOS does not have hardware root of trust for any form of integrity validation. For the boot process, a firmware password can make it more difficult for an attacker to modify the boot process, but it is easy to compromise with physical device access.

Application Protection

On Windows 10, every app and even portions of the operating system itself run inside their own isolated sandbox called an AppContainer. The security policy of a specific AppContainer defines the operating system capabilities that apps have access to from within the AppContainer. A capability is a Windows 10 device resource such as geographical location information, a camera, a microphone, networking, and sensors. Apps are isolated from one another and can communicate only by using predefined communications channels and data types. Windows 10 applies address space layout randomization (ASLR) holistically across the OS to help mitigate the risks of sandbox escapes.

macOS sandboxing uses the mandatory access controls implemented at the kernel level. Sandboxing profiles exist for each application that runs in a sandbox, describing precisely which resources are accessible to the application. Many of the system's helper applications that normally communicate with the network are sandboxed to guard them from abuse by attackers trying to access the system. In addition, other programs that routinely take untrusted input (for instance, arbitrary files or network connections) are sandboxed.

In iOS, all third-party apps run in an app sandbox, so they are restricted from accessing files stored by other apps or from making changes to the device. This prevents apps from gathering or modifying information stored by other apps. If a third-party app needs to access information other than its own, it does so only by using services explicitly provided by iOS 10. Users' apps are segregated from system files and resources. The majority of iOS runs as the nonprivileged user "mobile," as do all third-party apps. The entire OS partition mounts as read-only. APIs do not allow apps to escalate their own privileges or to modify other apps or iOS itself. Built-in apps use ASLR to ensure that all memory regions are randomized upon launch. Xcode, the iOS development environment, automatically compiles third-party programs with ASLR support turned on. **Table 3** provides a summary of scoring for Threat Resistance features and functionality.

Table 3. Summary of Scoring Results for Threat Resistance

OS	Feature	Native Functionality	Granularity of Controls	Functionality vs. "Ideal"
Windows 10	●	●	◕	◕
macOS	◕	●	◕	◕
iOS	●	●	◕	◕

Poor ○ ◔ ◑ ◕ ● *Excellent*

Every operating system does a good job of validating the integrity of the device at boot time. Windows 10 and iOS do a better job of validation, as they rely on hardware root of trust. iOS has hardware root of trust, laid down during chip fabrication, that is implicitly trusted and provides very strong integrity validation from the hardware to apps. Windows 10 provides similar hardware validation and improves on that capability by allowing for remote attestation of conditions to define criteria such as not allowing unencrypting of the drive on a jailbroken device. Application protection using sandboxing has become a standard feature across most operating systems including Windows 10 and macOS and iOS. This is a key change in operating system architecture from just a few years ago, when an attacker could easily use an application to gain permissions to unintended components of the operating system.

Conclusion

Measured against the key criteria for this analysis, Pique Solutions found that Microsoft Windows 10 provides a higher level of capabilities compared to Apple iOS and macOS in all three categories of assessment, as shown by the cumulative scoring results in **Table 4**.

Table 4. Summary of Cumulative Scoring Results for All Categories

OS	Identity and Authorization	Information Protection	Threat Resistance
Windows 10	●	●	◕
macOS	◕	◕	◕
iOS	◕	◕	◕

Poor ○ ◔ ◑ ◕ ● *Excellent*

Windows 10 provides native two-factor authentication for mobile devices, tablets, and PCs, whereas Apple only supports two-factor for applications and not the device. Windows 10 protects enterprise data in a way that is transparent to the user, including allowing a user to share a single app for both personal and work tasks, whereas Apple does not provide similar functionality.

Windows 10 provides biometric support with Windows Hello that can be implemented for any kind of biometric authentication based on OEM implementation. Apple has strong biometric support in Touch ID and Face ID, but the implementation depends on newer iOS devices with Face ID and the latest MacBook with Touch ID. While valuable, especially for online commerce and user convenience, this is not a two-factor authentication system for enterprise authentication.

Windows 10 excels at information protection, predominantly due to the availability of WIP to manage business data without the need for secure containers or app wrapping. Neither macOS nor iOS provide native data management. Secure management of business information with either Apple OS requires an additional investment of enterprise-level data protection.

Windows 10 provides one distinct threat resistance feature over both macOS and iOS. Its Measured Boot uses hardware to measure the system boot process for integrity. iOS has hardware root of trust, laid down during chip fabrication, that is implicitly trusted and provides very strong integrity validation from the hardware to apps, but it does not allow for remote attestation of conditions to define criteria such as not allowing unencrypting of the drive on a jailbroken device. Application protection using sandboxing has become a standard feature across most operating systems, including Windows 10 and macOS and iOS.

Overall, although Apple iOS and macOS have strong security features, Microsoft Windows 10 scored higher for security due to native functionality of those security features.