PIQUE SOLUTIONS

Security: Windows 10 versus macOS and iOS

Security Feature and Functionality Comparison

PIQUE SOLUTIONS

April 2018

THE DEVELOPMENT OF THIS WHITE PAPER WAS SPONSORED BY MICROSOFT. THE UNDERLYING RESEARCH AND ANALYSIS WERE EXECUTED INDEPENDENTLY BY PIQUE SOLUTIONS.

Contents

Pique Solutions is a competitive research and market analysis firm supporting Fortune-500 companies in the information technology sector. Pique is based in San Francisco, California.

Executive Summary

Based on in-depth review of product documentation supplemented by hands-on lab testing, Pique Solutions conducted a comparative analysis of the protection and resilience capabilities of Microsoft Windows 10 and Apple macOS High Sierra and iOS. The analysis assessed the level of functionality those capabilities provide, the utility of those capabilities, and their impact on user experience.

Pique Solutions research found that Windows 10 natively provides superior functionality and more integrated security controls as compared to those provided natively by macOS and iOS. Not surprisingly, Microsoft's lead over Apple is more apparent in the enterprise segment, as Apple is geared toward the consumer market first, with a growing presence in the education market (e.g., Apple Keynote, Numbers, Pages, the App Store Ecosystem of education applications). Most enterprise organizations are devoted to the Microsoft ecosystem, and bring your own device (BYOD) is a standard among their employees; however, most enterprise organizations also need to support a subset of Apple users. These multi-OS environments make it extremely difficult for organizations to ensure the same level of security across all platforms. Unlike Apple, Microsoft addresses the security needs of both the consumer and the enterprise segments. Microsoft does this natively—that is, without the need to deploy third-party tools. To achieve equal levels of protection, resilience, and the security functionality of Windows 10, macOS and iOS users need to purchase and integrate multiple third-party security tools. Our analysis showed that this multilayering of different tools creates complexity and fragmentation and increases the risk of leaving security vulnerabilities exposed. The comparatively greater cohesiveness and completeness of the Windows 10 security offering is a compelling differentiator against Apple, as Apple's reliance on third-party tools negatively affects not only data security but also user productivity and total cost of ownership.

When evaluating identity management, Pique Solutions learned that macOS and iOS provide device-level Identity Access and Management (IAM) but limit the enterprise to an application-based approach for enterprise domain authentication. In comparison, Windows 10 supports domain user accounts, enabling device-level domain authentication.

For threat resistance, Pique Solutions concluded that Windows 10, macOS, and iOS all provide strong security controls for applications, including app scanning for malware when using the respective app stores, and the ability to remove malicious code after it has been installed on a device. While Windows 10, macOS, and iOS all provide application sandboxing to limit malicious code from accessing critical information on the OS, and to prevent it from accessing other applications, Windows 10 extends its protection against malicious apps with additional security countermeasures that look for potential unknown exploits and malware using machine learning techniques. In an environment where new security threats emerge at a rapid pace, this capability is extremely valuable and further differentiates Windows 10 from the Apple operating systems.

Pique Solutions' analysis found that Windows 10, macOS, and iOS all offer equivalent levels of device encryption. Windows 10, however, provides an additional layer of file-based encryption, encryption-in-transit, and data controls for managing how information is shared. While Windows 10 provides these capabilities natively, macOS and iOS require the implementation of third-party data management tools to achieve the same level of functionality.

Introduction to Security

One of the most critical imperatives for enterprises is to protect data from being exploited or inadvertently compromised by a user sending sensitive information to his or her personal email account or from an enterprise-controlled application to his or her personal app. Protecting sensitive intellectual property requires a robust data leakage prevention solution that not only protects information on the endpoint but also includes application visibility and application control that spans from the endpoint to the cloud. Ascertaining data security is not a trivial task, as enterprises are dealing with data sprawl that has been exacerbated with the rapid adoption of cloud and hybrid cloud environments and the resulting flow of data between on-premises and cloud.

An effective data-centric security program requires the following nine components:

1. **Data Discovery:** Where and what type of data is stored; continuous process to provide visibility, outline risk, validate employee role assignments, and confirm awareness level and policy compliance. Policy compliance can be tied to an enterprise corporate security policy and regulatory compliance.
2. **Classification:** Policy, data-handling procedures, report/detect/protect, IR/forensics, risk-based approach, identify business owners.
3. **Data Tagging/Watermarking:** Non-intrusive, tied to classification, low-hanging fruit (e.g., PCI, HIPAA, PII).
4. **Data Loss Prevention:** At rest, discovery; in transit, including mobile in the cloud, policy integrated with continuous monitoring.
5. **Data Visibility:** Database activity monitoring, monitoring who and when data is accessed, validate sensitive data is stored securely, alert on policy violations.
6. **Encryption Strategies:** Consider SSL decryption at gateway points of access, data-in-motion, data-at-rest, data-in-use.
7. **Enhanced Gateway Security Controls:** FTP/email file transfer, Next generation firewall, third-party service providers, secure web browsing.
8. **Identity Management:** Directory unification, access management, federation privileged access, access management and authentication.
9. **Cloud Access:** Access and authentication, data analysis, discovery, data loss prevention, encryption.

Protecting data within the enterprise goes beyond just data loss prevention, as this provides an enterprise visibility of their data in use, in transit, and at rest. It also allows the enterprise to control macro information flow within the organization and micro information flow from the user that also includes identity and authorization. Enterprises need to be able to defend against cyberattacks by quickly detecting, preventing, and responding to them. This also requires enterprises to maintain operational resiliency in the wake of an attack. Time to detection and prevention are extremely important and require a layered defense model and a comprehensive approach to security from the endpoint to the cloud. Existing third-party security controls are limited in their ability to protect against certain categories of threats. Without being built into the operating system and applications, they are limited to publicly disclosed vulnerabilities, uncovered zero-day vulnerability through independent research, or

purchasing a zero-day vulnerability on the dark web. Like Microsoft, many leading third-party security vendors are moving away from signature-based detection to machine learning and artificial intelligence to keep up with the adversary.

The adoption of cloud, software as a service (SaaS), mobile devices, laptops, and tablets has collectively changed the traditional security paradigm. Traditional security best practices no longer provide the coverage and visibility of enterprise due to device sprawl and disparate cloud-driven services. The attack surface has grown exponentially, which increases the attack vectors tenfold. The largest threat vector is email. Threats are constantly shifting vectors, and the controls required to protect and maintain an on-premises Microsoft Exchange server could cost between $250,000 and $1,000,000. At a minimum, third-party tools need to address SPAM, phishing, and malware, as well as the ability to perform link analysis of URLs that might be malicious. This does not consider the time spent learning new systems, configuring policies, and maintaining multiple management systems. This creates an operational nightmare for most enterprise organizations when having to maintain several disparate security products.

The operational cost and complexity in maintaining an on-premises mail server has driven many enterprises to migrate their email to the cloud. The main drivers for cloud-based email are decreased infrastructure cost and reduced labor costs associated with managing an email system. The flip side of cloud-based email is the loss of control and visibility. This has placed a heavy burden on security vendors tasked with protecting hybrid cloud environments.

The benefits of having native security controls that span from the operating system to the cloud are compelling for many reasons. One of them is reduced investment in third-party security tools. A defensive, in-depth approach is considered a reasonable one, and Microsoft already offers the same security controls natively with O365. Apple does not have a comprehensive security offering for enterprise cloud email. In addition, Apple does not provide any details on how they protect user information from being compromised. It is only assumed that Apple follows security best practices that can be outlined in NIST 800-53.

Although many security controls can be selected for Infrastructure as a Service (IaaS) and Platform as a Service (PaaS), the gateway to those services requires some form of SaaS. As more enterprises embrace public, private, hybrid, and multivendor cloud deployments, native control of data, whether at rest or in motion, is becoming increasingly important. These granular native controls working in concert to provide security orchestration from the endpoint to the cloud truly separate Microsoft from Apple and provide the Windows 10 platform—and the organizations that choose it—with a significantly higher level of security.

Microsoft's ability to respond quickly and effectively to threats with security updates was recently demonstrated by its response to hardware processor vulnerabilities of Spectre and Meltdown. These are a newly discovered class of vulnerability based on a common chip architecture that, when originally designed, was created to speed up computers. Apple has taken a different approach to address the processor vulnerabilities by offering a level of granular control and malware scanning for applications from the App Store that limit the ability of the attacks to succeed. Apple also claims that since the release of this vulnerability there are no known exploits impacting macOS.

Assessment Methodology

The overall assessment methodology used by Pique Solutions was as follows:

1. Based on product documentation and limited hands-on testing, we compared the security features and capabilities provided natively across Windows 10, macOS and iOS. Additionally, for those platforms that are unable to address the features natively, we identified and assessed the functionality of third-party tools needed to supplement the native functions.

2. We conducted interviews with subject matter experts to verify assumptions and platform capabilities.

3. We based our feature and functionality comparisons primarily on publicly available product documentation and other relevant public data.

4. When public data was unavailable or insufficient, we conducted hands-on testing to compare specific features or functionality.

Pique Solutions applied the following scoring methodology. The baseline was calculated as the maximum score attainable, multiplied by the number of features evaluated in each category.

Feature	Functionality
1 - Requires 3rd-Party SW	1 - Not Intuitive
3 - 25% Integrated	3 - Slightly Intuitive
6 - 50% Integrated	6 - Moderately Intuitive
9 - 100% Integrated	9 - Highly Intuitive

To assess Windows 10, macOS, and iOS, we researched the security features and functionality across the six main categories listed here.

1. Identity and Authorization

- Authentication: Local authentication of user to device and apps, remote authentication of user, remote authentication of device, FIDO
- Ecosystem of third-party security and management tools
- Biometric Support: Methods, store, use

2. Information Protection

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

3. 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
- Built-in Exploit Protection
- Built-in Anti-Virus Protection

4. Encryption

- Automatic disk encryption

5. Hardware-Rooted Security

- VBS

6. App Store

- App Store Security Policy
- Application Vetting
- Application developer vetting

Our research addressed the following OS versions:

- Microsoft Windows 10 (Pro, Enterprise, Mobile, S)
- Apple macOS High Sierra
- Apple iOS 11

Key Findings

Based on Pique Solutions' comparative analysis of Windows 10 versus macOS and iOS, we found that Windows 10 provides users with a larger set of native and granular controls for every area of security functionality reviewed in this comparison. In comparison to Windows 10, macOS and iOS require the implementation of third-party tools to reach parity with the native security functionality in Windows 10. Windows 10 security controls enable an organization to reduce their attack surface with a defensive, in-depth approach, from the endpoint to the cloud. Apple macOS and iOS also provide native security controls; however, they are limited to browser, application isolation, and strict control to the application within their app store. The following are the key findings that demonstrate the superiority of Windows 10 security controls as compared to those of macOS and iOS.

Identity and Authorization

- Windows 10 is the first major OS with Fast ID Online (FIDO) 2.0 support for the enterprise. Apple also provides FIDO support starting with iOS 9 touch ID.
- Apple macOS and iOS do not natively provide two-factor authentication and require third-party biometrics or smart cards for older MacBooks. They do provide a two-step authentication, but this is targeted to the consumer market.
- Windows 10 biometrics replaces passwords to improve both security and usability.
- Apple macOS and iOS provide touch ID support and Face ID with iPhone X.
- Apple has a closed system that focuses on the consumer user of both macOS and iOS, and they leave any enterprise security controls to third-party products.

Information Protection

- Microsoft Windows Information Protection (WIP) secures critical data by providing device-side protection, data separation, data-leakage prevention, and information sharing. It also eliminates the need for a secure container or for app wrapping.
- Apple macOS and iOS do not provide data-leakage prevention natively. To get the same level of protection as WIP, additional investment is required for other data protection technology.

Threat Resistance

- Windows 10 Measured Boot uses hardware to measure the system boot process for integrity.
- Apple provides a custom (Closed) hardware security module for encryption and integrity validation.
- Windows 10 has strong application protection through Windows Defender Application Guard, which provides strong sandboxing, memory isolation, and trusted execution of an application.
- Windows 10 provides built-in protection for exploits through Windows Defender Exploit Guard and provides a level of antivirus protection that utilizes machine learning without the need for signatures.

- Apple requires third-party EDR tools like Cylance to provide the same level of protection.

Encryption

- Windows 10 provides full disk encryption natively with BitLocker. Apple also provides the same level of full disk encryption using FileVault within macOS and provides the same for iPhone once a passcode or biometric authentication is set up on the iPhone.
- Apple does not provide the ability to utilize RAID with FileVault, whereas BitLocker provides this natively. This is a huge differentiation in determining capabilities that separate consumer from enterprise clients.

Hardware-Rooted Security

- Windows 10 provides virtualization-based security (VBS) using Windows Defender Device Guard.

- Apple provides hardware-level security through isolation. This provides Apple the ability to isolate applications so they have no access to system resources, including the network, user documents, opening and saving files, peripherals such as printers and cameras, and locations, address books, calendars, and similar central services.

App Store

- Microsoft and Apple provide a similar user experience within their respective app stores. In terms of security and vetted applications, they both screen every application for the presence of malware before it is released to the public. This provides enterprise and consumer users a much higher level of assurance and confidence that they are deploying safe applications.

Feature and Functionality Comparison

Identity and Authorization

Testing Scores	Baseline	Feature	Functionality
Windows 10	**81**	**72**	**72**
iOS	**81**	**65**	**65**
macOS	**81**	**65**	**65**

IAM provides the right people access to the resources they need when they need them for the right reasons. Enterprises need IAM capabilities that address agility in managing distributed systems where users maintain access across multiple device types. IAM should ensure the 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.

The most common form of identity is a user name and password. Most users need to remember on average at least several passwords. This limits their desire or ability to use and remember highly complex passwords, thus rendering those passwords 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 their complexity factor. Although not strong, passwords and PINs 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 can be effective and convenient. Even better, by leveraging biometrics, user identity becomes truly unique, more personal, and more convenient to the user and the enterprise.

Authentication

Windows 10 provides two-factor authentication for remote enterprise domain authentication of the user to device and apps. Windows Hello technology replaces passwords with the combination of a specific device and a biometric gesture or PIN. This technology also supports Microsoft accounts, Active Directory (AD), Azure AD, and any non-Microsoft service that supports FIDO 2.0 authentication. Windows 10 is the first operating system to utilize FIDO 2.0 in an enterprise environment—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.

Microsoft and Apple both participate with FIDO (Fast Identity Online) Alliance, a consortium that supports an open and scalable authentication standard to enable simpler and more secure user authentication experiences across many websites and mobile services. FIDO is viewed as the strongest form of authentication available today, with the intent to replace easily compromised passwords with other forms of authentication, like hardware keys and biometrics. While Microsoft has already fully implemented FIDO 2.0 support in Windows 10, including multiple methods of biometrics and two-factor authentication, macOS and iOS have

implemented FIDO and use a PIN-based authentication system with biometrics as a convenience feature along with two-step authentication.

While not FIDO 2.0, both macOS and iOS support local and network-based (party vendor required) authentication, including the use of biometric readers, smart cards, and tokens for two-factor authentication.

Biometric Support

Windows Hello is an extensible framework that enables the use of biometric sign-in options for Windows 10. The user's unique biometric identifier enables authenticated access to the device. While Windows Hello supports fingerprints, facial recognition, and iris scanning, new hardware may expand these currently supported biometrics.

Windows 10 integrates and supports biometrics with the other security components of biometric-enabled devices. 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 TPM that is required on every Windows 10 device. Never storing biometric images eliminates the risk of the use of those images to gain illicit access to corporate resources from another device. Built-in anti-spoofing and liveness detection prevents the use of simulated biometrics, such as a photograph of the user's eye, to access a device.

Apple macOS supports biometrics on its latest MacBooks. Additionally, iOS supports biometrics (Touch ID and Face ID) but depends on the mobile device, as the iPhone X is the only Apple mobile phone that provides Face ID.

Windows 10 scores higher than macOS and iOS on every measurable capability related to authentication. Windows 10 provides two-factor domain authentication without a password or a secondary device, like a token. Furthermore, Windows 10 supports domain accounts for local authentication. Keys are stored in hardware with Windows 10 Enterprise, providing an additional layer of protection by storing authentication credentials in a limited-access isolated virtual container. Windows 10 provides an integrated framework with support for the latest methods of authentication, including FIDO. Windows 10 biometric authentication has strong anti-spoofing protection. Apple does not provide a suitable authentication system for enterprise use without the implementation of third-party tools.

Information Protection

Testing Scores	Baseline	Feature	Functionality
Windows 10	**36**	**36**	**36**
iOS	**36**	**28**	**28**
macOS	**36**	**28**	**25**

As defined with data loss prevention, data controls relate to three functional groupings that correspond to the data life cycle. These are 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 to the data as possible. 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 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 with RAID support. It automatically applies encryption 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-bit 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.

Similar to how Microsoft uses TPM, Apple uses their Secure Enclave. This is a coprocessor fabricated in the Apple T1, Apple S2, Apple S3, Apple A7, and later A-series processors. It uses encrypted memory and includes a hardware random number generator. Secure Enclave provides all cryptographic operations for data protection key management and maintains the integrity of data protection even if the kernel has been compromised. Communication between Secure Enclave and the application processor is isolated to an interrupt-driven mailbox and shared memory data buffers.

Secure Enclave runs an Apple-customized version of the L4 microkernel. This microkernel is signed by Apple, verified as part of the iOS secure boot chain, and updated through a personalized software update process.

When the device starts up, an ephemeral key is created, entangled with the device's UID, and used to encrypt Secure Enclave's portion of the device's memory space. Except on the Apple A7, Secure Enclave's memory is also authenticated with the ephemeral key. On the Apple A11, an integrity tree is used to prevent replay of security-critical Secure Enclave memory, authenticated by the ephemeral key and stored in on-chip SRAM.

Additionally, data saved to the file system by Secure Enclave is encrypted with a key entangled with the UID and an anti-replay counter. Anti-replay services on Secure Enclave are used for revocation of data over events that mark anti-replay boundaries including, but not limited to, the following:

- Passcode change
- Touch ID or Face ID enable/disable
- Fingerprint add/delete
- Face ID reset

- Apple Pay card add/remove
- Erase All Content and Settings

Secure Enclave is also responsible for processing fingerprint and face data from the Touch ID, Face ID sensors, and pin code, determining whether a match exists, and then enabling access or purchases that require Touch ID, Face ID, or pin code on behalf of the user. An important fact to note is that Apple's FileVault is unable to provide RAID and is limited to full disk encryption with only one drive.

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.

Windows 10 comes with a VPN platform that includes two types of VPN connections:

- INBOX Protocols
    - IKEv2, PPTP, and L2TP (with L2TP both PSK and Certificate)–based VPNs are supported
    - Inbox VPN uses EAP for authentication. The supported EAP methods are:
        - MSCHAPV2
        - TLS (uses certificate-based authentication including Windows Hello, virtual smart cards, and certificates)
        - TTLS (Outer Method)
          With the following inner methods:
            - PAP/Chap/MSCHAP/SCHAPv2
            - EAP MSCHAPv2
            - EAP TLS
        - PEAP
          With the following inner methods:
            - EAP MSCHAPv2
            - EAP TLS

- VPN Plug-in Platform for TLS/SSL
    - The VPN plug-in platform allows third-party developers to write downloadable VPN apps from the Microsoft Store.

Apple provides a native VPN client and provides most of their VPN interoperability via Cisco technology:

- Apple provides a built-in VPN, which is limited to the following VPN types:
    - IKEv2, Cisco IPsec, and L2TP over IPsec
- Apple VPN IKEv2 authentication is limited to:
    - Username

    - Certificate
- Apple VPN Cisco IPsec authentication supports:
    - Shared Secret
    - Certificate
- Apple VPN L2TP user authentication supports the following:
    - RSA Secure ID
    - Certificate
    - Kerberos
    - Crypto Card
- Apple VPN L2TP machine authentication supports the following:
    - Shared Secret
    - Certificate

Windows 10 supports many on-demand and enforcement methods to simplify and secure the VPN connection. 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 application 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 traffic filtering based on host destination attributes with both app-based and traffic-based rules. Apple macOS can use third-party VPN clients like Cisco AnyConnect.

Apple macOS works with VPN servers that support the following protocols and authentication methods:

- IKEv2/IPsec with user authentication by shared secret and certificates
- Cisco and AirWatch which can be purchased from the Apple App Store

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 unintentional data loss. The only exception to this rule is a witting malicious authorized user. 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 be protected. This can be achieved by several means. Executing in protected memory space is one way of protecting secrets in memory from disclosure. Other ways might allow sensitive data in regular memory during normal execution but then ensure that it is nonpageable memory (so it is not persisted to disk), or removing keys from memory when the screen is locked, or, as is most often the case, simply encrypt memory contents when they are swapped to disk or crash-dumped (e.g., with BitLocker).

Windows 10 WIP implements the most effective method for data protection. Because it integrates with the operating system, WIP does not require separate secure containers or

duplicate apps to protect data. WIP encrypts data dynamically based on defined organization policies. By focusing on managing enterprise data regardless of app, WIP provides the enterprise visibility into sanctioned applications and control of enterprise data without impacting the personal user experience. WIP can be configured to classify 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 mobile device management to specify which apps are allowed and/or disallowed, manages app classification sans app wrapping or app modification. This means admins can leverage existing apps and do not need to add or remove any special version of a business-classified app from a device, including when wiping enterprise information. WIP does not tamper with personal apps and data.

Trusted apps are those designated for corporate use that can access protected work data as well as personal data. Apps that are not part of the trusted app list will not be able to access corporate information stored on the device or on a corporate share. That data remains encrypted when saved to an untrusted location like a USB drive or personal cloud storage account. Furthermore, the keys are under organizational control, so when a user leaves the organization, or the device is no longer managed through mobile device management, his or her keys are revoked, and the user can no longer decrypt that data regardless of its location or remotely accessible organizational resources. Restricting remote access to corporate resources to only managed devices is a server-side feature called Conditional Access. It is complementary to, but separate from, WIP. If you engage Conditional Access, then you require users to be managed to get access to work data there; they cannot just use their credentials on a random machine. If you set WIP as part of the management policy, then you also get device-side selective wipe ability. A key feature of WIP is that it allows Windows 10 apps, whether involving personal or corporate data (e.g., contacts, Outlook), to work in parallel while still providing the necessary controls and encryption to work data. For example, documents in Microsoft Word for enterprise clients could disallow copying and pasting into personal documents or locations while still allowing personal documents to be shared.

WIP enables IT to set four levels of protections for devices accessing corporate resources:

- **Hide Overrides:** WIP looks for inappropriate data sharing and prevents the user from completing the action. WIP clipboard/sharing prompts, dialogs, and inbox save experiences do not offer personal options for work data when in this mode, hence “Hide Overrides.”
- **Allow Overrides:** WIP looks for inappropriate data sharing and alerts the user when he or she does something that may be a policy violation. This protection level lets users override the policy and share the data anyway, but it logs the action to an audit log.
- **Silent:** WIP runs silently, encrypting data and logging when users do something potentially inappropriate, but it does not prompt users or block their actions. It enables IT to learn about apps and sites used for work and have confidence that policy is correct before raising the enforcement level. This is the minimum level needed to enable the selective wipe scenario.
- **Off:** WIP is not active and does not protect data on the device.

WIP allows the managing organization (IT Pro "user") to specify their corporate network:

- Enterprise Cloud Resources
- Enterprise Local Area Network Domain Names
- Enterprise Proxy Servers
- Enterprise Internal Proxy Servers (to forced-tunnel work resources outside the LAN)
- Enterprise IPv4 Ranges
- Enterprise IPv6 Ranges
- Neutral Resources

Organizations can choose to either block unapproved data sharing (e.g., copying and pasting) outright or allow auditable sharing. With auditable sharing, users can override the WIP-defined restrictions, but if a user attempts unauthorized data sharing, an alert provides the user with a warning. The user can then proceed, and an EMM system will either log or cancel the action. When users create new documents, they can manually change the classification from a "corporate" classification to a "personal" classification within any allowed app. When a user classifies a new document as "personal," he or she will not be able to copy and paste information from a corporate document into that new personal document. Classification events for changing from corporate to personal are logged for review. It is important to note that Microsoft does not log when a document is marked as "corporate."

Apple macOS and iOS do not provide a native data protection for data management like Windows 10 beyond FDE. Therefore, investment in third-party data management technology will be required to address data management in macOS and iOS. Apple's data protection also requires third-party products, as Apple does not provide the functionality natively.

Windows 10 excels at information protection, predominantly due to using a hardware security module for encryption and WIP to manage business data without the need for secure containers or app wrapping. Apple macOS and iOS are not clear on hardware-based encryption management, due to the proprietary nature of those platforms. What can be deduced from Apple's public documents is that it uses a keying system to protect files and directories, but it does not offer native data management capabilities.

Secure management of business information within macOS and iOS requires an additional investment of third-party enterprise-level data protection tools. While macOS can scale in large enterprise environments, to achieve security functionality parity with Microsoft, it requires significant capital and operational expenses related to procurement, implementation, and management of several third-party tools. Microsoft WIP provides a comprehensive approach to data security natively that extends from the endpoint to the cloud. This provides enterprises with more granular controls and options for protecting their data without the need of third-party solutions that required significant orchestration.

Threat Resistance

Testing Scores	Baseline	Feature	Functionality
Windows 10	90	90	87
iOS	90	34	31
macOS	90	34	31

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

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.

Device Integrity

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.

Trusted Boot verifies that the remaining Windows boot-related components are trustworthy and have integrity. Trusted Boot will detect any file modifications and attempt to restore those files to a known good state. Trusted Boot requires that Microsoft signs all code in the operating system, including OEM drivers and the antivirus solution, thereby providing the next layer of integrity validation. Windows Store or a trusted enterprise store must digitally sign all Windows 10 apps.

Microsoft extends the primary integrity validation process by including a second hardware-backed process called Measured Boot. This uses TPM hardware to baseline the boot process for critical startup-related components, including firmware, Windows boot components, and drivers. TPM provides isolation and protection of the baseline data against tampering attacks.

Apple macOS provides System Integrity Protection, which is a security technology that was released in OS X El Capitan and later. Apple designed System Integrity Protection to help prevent potentially malicious software from modifying protected files and folders on a Mac. System Integrity Protection restricts the root user account and limits the actions that the root user can perform on protected parts of the Mac operating system.

Before System Integrity Protection, the root user had no permission restrictions, so it could access any system folder or app on the Mac. Software that obtains root-level access when you entered your administrator name and password to install the software can modify or overwrite any system file or app.

System Integrity Protection includes protection for these parts of the system:

- /System
- /usr
- /bin
- /sbin
- Apps that are preinstalled with OS X

Paths and apps that third-party apps and installers can continue to write to include:

- /Applications
- /Library
- /usr/local

System Integrity Protection is designed to allow modification of these protected parts only by processes that are signed by Apple and have special entitlements to write to system files, such as Apple software updates and Apple installers. Apps that you download from the Mac App Store already work with System Integrity Protection. Other third-party software, if it conflicts with System Integrity Protection, might be set aside when you upgrade to OS X El Capitan or later.

System Integrity Protection also helps prevent software from selecting a startup disk. To select a startup disk, choose System Preferences on the Apple menu, then click Startup Disk, or hold down the Option key while you restart, then choose from the list of startup disks. In short, Apple is limited to restricting unwanted access to folders and files unless the adversary has root/admin credentials that could allow them to install an unsigned, unvetted application that can access folders and files as well as system level directories and processes.

Application Protection

The threat landscape is constantly growing and becoming more complicated to defend without a layered defense. Additionally, the threat surface creates more opportunities for the adversary to gain access. Most attacks start in the inbox and about 80% of those attacks will use the browser to access malware. Microsoft provides Office 365 Advanced Threat Protection in the cloud that focuses on email security for business accounts. For the endpoint, the Windows 10 first layer of security is Application Guard, which enforces container and browser isolation. In the event a user accesses a site that contains malware, that incident is isolated and will not affect the host PC. The second layer of defense is AppControl. This provides the ability to block unrecognized applications and only trust those application that

have been vetted. Microsoft Defender AV is a built-in anti-malware solution that can remove malicious binaries without the use of signatures. Microsoft Defender AV uses machine learning and heuristics to identify the threat. Lastly, Microsoft provides Windows Defender Exploit Guard. There are four features that are key in exploit guard that expand beyond the endpoint to include network protection:

- Exploit protection can apply exploit mitigation techniques to apps the organization uses, both individually and to all apps.
- Attack surface reduction rules can reduce the attack surface of your applications with intelligent rules that stop the vectors used by Office-, script-, and mail-based malware.
- Network protection extends the malware and social engineering protection offered by Windows Defender SmartScreen in Microsoft Edge to cover network traffic and connectivity on your organization's devices.
- Controlled folder access helps protect files in key system folders from changes made by malicious and suspicious apps, including file-encrypting ransomware malware.

Windows 10 provides multiple additional threat-resistance features that are absent in macOS and iOS. The ability of macOS and iOS to protect a system from malware, or any exploitation for that matter, can only be achieved by deploying third-party security tools, and by allowing access only to applications from the App Store and from approved developers.

Although macOS and iOS have application isolation, they do not have any native security controls that will protect against exploitation, and they require a third-party product to reduce their attack surface such as an EDR solution like Cylance. For Apple customers who have enrolled in Apple's consumer email (@icloud.com), it is unclear whether Apple provides any protection around SPAM, phishing (except for accessing web-based email from Safari), and malware. Because O365 is an enterprise-level email solution, this is an unfair comparison, but it indicates that Apple is not investing in native enterprise security controls that are provided with O365 with ATP. At least they provide the ability to subscribe to O365 via their email client, thus an Apple BYOD device can be provided the highest level of security from Microsoft. However, most enterprises have limited security budgets and little security expertise needed to operate multiple third-party products with different management infrastructures. Microsoft's O365 ATP can fill the void for enterprises that use Apple MacBook and iOS for email. This will limit Apple's ability to serve large enterprise clients, especially those that have hybrid cloud environments. For those companies, the ability to have fluid security controls from the endpoint to the cloud is becoming increasingly important.

Encryption

Testing Scores	Baseline	Feature	Functionality
Windows 10	**9**	**9**	**9**
iOS	**9**	**9**	**9**
macOS OS	**9**	**6**	**6**

Windows 10 provides the user with the ability to enable full disk encryption (FDE) natively with BitLocker. BitLocker uses TPM to ensure that its keys are only released to the booting system when it matches the expected values, which ensures there is no malicious boot

program capturing keys or controlling memory before Windows boots. Microsoft's approach to FDE is not unique, as Apple provides the same capability using Secure Enclave.

Windows 10 does provide the capability to encrypt selected folders and files using their encrypted file system (EFS), which is also used by WIP. The main difference between FDE and EFS is that the latter stores the encryption keys in the user profile on the operating system instead of wrapped by the TPM chip. Full disk encryption is mandatory in most enterprises today whether it is driven by corporate policy or regulatory compliance. Apple macOS requires the user to invoke FDE, and iOS automatically provides full disk encryption once a user provides a passcode, Touch ID, or Face ID. Windows 10 provides the option for full disk encryption, which can be required through policy, and folder/file encryption. With these options, Windows 10 enterprise customers can make a choice on what they want to encrypt.

Hardware-Rooted Security

Testing Scores	Baseline	Feature	Functionality
Windows 10	**9**	**9**	**9**
iOS	**9**	**9**	**9**
macOS	**9**	**9**	**9**

Windows 10 provides VBS using Windows Defender Device Guard. This provides the ability to run the code integrity service alongside the kernel in a Windows hypervisor-protected container. Device Guard can be used in concert with Application Control to a defined set of approved applications to further reduce the attack surface. Apple macOS and iOS provide a feature like VBS, but it is exclusively tied to application isolation. The Windows 10 advantage over macOS and iOS for enterprise customers is that this protection can expand to include application control. For this, Apple relies on System Integrity Protection and Gatekeeper to assure that one is not downloading compromised apps from the Mac App Store.

App Store

Testing Scores	Baseline	Feature	Functionality
Windows 10	**36**	**21**	**18**
iOS	**36**	**27**	**27**
macOS	**36**	**27**	**27**

Microsoft and Apple provide a similar user experience within their app stores. Users can purchase applications, movies, songs, and books. Both Microsoft and Apple screen every application for the presence of malware before being published and will also perform periodic checks of already published apps. Apple achieves this with its developer program, which outlines their methodology for testing and vetting applications. There is literally no difference between how the app stores approach ensuring the security of applications within their app stores. The reason for Apple's higher score is that Apple has published more information on how they vet developers and effectively enforces that installed apps are from an identified developer, which implies that those applications are secure.

Conclusions

Based on Pique Solutions in-depth review of product documentation and hands-on testing, we found that Windows 10 in the enterprise natively offers a more comprehensive set of security controls that spans multiple security domains when compared to macOS and iOS. We found that Apple is lacking key threat resistance and information protection functionality critical to enterprise security and that macOS and iOS require the implementation of additional third-party security controls to achieve parity with the native security controls of Windows 10. Apple's heavy reliance on third-party tools increases complexity as well as capital and operational expenditures for Apple customers. Windows 10, macOS, and iOS all offer similar levels of functionality for container and application isolation and full disk encryption. However, macOS does not provide redundant array of independent disks (RAID), a technique enabling enterprises to store the same data on multiple hard disks to increase read performance and fault tolerance.

Where Apple's approach also differs from that of Microsoft is in application control. While Apple does this on a per-device basis, without native centralized security management and orchestration capabilities this capability is integrated into Windows 10. Here, too, macOS and iOS are dependent on the use of third-party products for management and configuration. Outside of next-generation firewall, Windows 10 natively delivers a turn-key security solution that provides full interoperability across their technology stack.

Windows 10, macOS, and iOS scored almost identically in the application protection, encryption, hardware-rooted security, and app stores categories. Having similar security capabilities across these four areas are table stakes for the consumer market, which should naturally transfer to the enterprise environment. However, Apple is not investing in the enterprise market outside of providing third-party enterprise applications from their App Store and leaving it to enterprise customers to integrate and orchestrate these products.

Additionally, Apple lacks a native cloud offering for enterprises such as Microsoft Azure. Again, Apple's iCloud is only sufficient for the consumer market, as it does not include IaaS, PaaS, or enterprise-level SaaS applications beyond creating content that can be used in the enterprise with Apple Keynote, Pages, Numbers, and third-party applications.

Pique Solutions' feature and functionality comparison found the largest advantage of Windows 10 vs. macOS and iOS in the identity and authorization, information protection, and threat resistance categories. An example worth noting in the identity and authorization category is Windows Hello. Windows Hello supports Microsoft accounts, Active Directory (AD), and Azure AD, as well as non-Microsoft services that support FIDO 2.0 authentication. In the information protection category, Microsoft provides a more comprehensive solution than Apple with WIP, which natively provides an effective method for data protection. Because it is integrated in the operating system, WIP does not require separate secure containers or duplicate apps to protect data. WIP encrypts data dynamically based on defined organization policies. Last, in the threat resistance category, Microsoft offers multiple layers of security that not only address known threats but also possess machine learning capabilities for identifying new potential and actual threats.