PIQUE SOLUTIONS

Security: Windows 10 versus Google Chrome OS and Android

Security Feature and Functionality Comparison

PIQUE SOLUTIONS

MICROSOFT SPONSORED THE DEVELOPMENT OF THIS WHITE PAPER.

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

795 Folsom Street, 1st Floor | San Francisco, CA 94107 | Tel.: 415.685.3392 | www.piquesolutions.com

Contents

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

All other trademarks are property of their respective owners.

© 2020 Pique Solutions. All rights reserved.

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 Google's operating systems. The resulting analysis assesses the level of assurance those capabilities provide an organization and their utility.

For this white paper, we reviewed Microsoft's Windows 10 version 1809, referred to hereafter as Windows 10. For Google, we reviewed Android 9 and Chrome OS 72.0.3626, referred to hereafter as Android and Chrome OS, 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 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.
- Android and Chrome OS support hardware-based fingerprint biometric authentication but lack support for any other biometric type, leaving third-party vendors to install less secure methods of facial recognition.

Information Protection

- Windows 10, Android, and Chrome OS all support default drive encryption with trusted key storage.
- Windows 10, Android, and Chrome OS 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. Android supports encrypted files for its secure container environment, whereas Chrome OS relies on storing files in cloud storage.

Threat Resistance

- Windows 10, Android, and Chrome OS 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.

© 2020 Pique Solutions. All rights reserved.

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, Android, and Chrome OS 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.

© 2020 Pique Solutions. All rights reserved.

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

© 2020 Pique Solutions. All rights reserved.

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 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 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.

Android supports multiple user profiles, such as guest, work, and second home user accounts. These are all local user-to-device accounts with pattern/password authentication in a trusted execution environment (TEE) for PIN/pattern/password authentication and fingerprint authentication. Chrome does offer support for up to seven Google accounts to authenticate to a device with the same support for pattern/password and fingerprint authentication methods.

Android supports domain user authentication to apps with domain authentication support including multifactor authentication. Because Chrome supports Android apps, the same level of domain user-to-app authentication is supported for both Chrome and Android. FIDO Alliance and Google announced that version 7.0 and later of Android that has the latest Google Play services is FIDO2 certified; however, FIDO integration is for apps and not the device.

© 2020 Pique Solutions. All rights reserved.

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 by using third-party hardware with any Windows 10 device.

Android 9 and later includes a biometric API that app developers can use to integrate biometric authentication into their applications in a device- and modality-agnostic fashion. Biometric support, however, is currently for fingerprint only. Google claims that integrated support for other biometric modalities are forthcoming. Third-party hardware manufacturers have included biometric authentication for other forms, such as facial recognition, that have proven to be easier to bypass and weaken the device authentication. For Chrome OS, the Pixel Slate is currently the first and only Chrome device with any biometric support, specifically fingerprint. Both Google operating systems store the fingerprint in a hardware root of trust. **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	●	●	●	●
Android	◔	◔	◑	◔
Chrome OS	◕	◕	◑	◕

Poor ○ ◔ ◑ ◕ ● *Excellent*

Windows 10 is still the only operating system to support native two-factor domain user-to-device authentication with universal biometric support using the Windows Hello framework. Although Google has made strides in supporting FIDO for better authentication and introducing a framework for biometrics, the support is still not as robust. Google biometric support is limited to fingerprint authentication and lacks support for any other biometric types, leaving third-party vendors to install less secure methods of facial recognition.

© 2020 Pique Solutions. All rights reserved.

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 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 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.

Google operating systems leverage full-disk encryption with a hardware-based TEE. Full-disk encryption uses a single key protected with the user's device password to encrypt the whole of a device's user data partition. Upon boot, users must provide their credentials before any part of the disk is accessible. The encryption algorithm is 128-bit AES with cipher-block chaining and SHA256.

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.

© 2020 Pique Solutions. All rights reserved.

Android and Chrome OS support always-on VPN to disallow apps access to the network until a VPN connection is established. On multiuser devices, VPNs are applied per user, so the device routes network traffic specific to the user through a VPN without affecting other users. Per-profile VPNs configure the work profile to allow only enterprise network traffic through the enterprise work profile VPN. Google operating systems provide support to facilitate VPN connections on allowed apps and prevent VPN connections on disallowed apps.

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 mobile device management 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.

Android supports file-based encryption, which allows different files to be encrypted with different keys that can be unlocked independently. File-based encryption enables a new feature introduced in Android 7.0 called Direct Boot, which allows encrypted devices to boot straight to the lock screen. Previously, on encrypted devices using full-disk encryption, users needed to provide credentials before any data could be accessed, preventing the phone from performing all but the most basic of operations. For example, alarms could not operate, accessibility services were unavailable, and phones could not receive calls and were limited to only basic emergency dialer operations. This separation makes work profiles more secure because it allows more than one user to be protected at a time, as the encryption is no longer based solely on a boot time password.

Chromebooks are designed around the concept of cloud storage for file storage with the local drive primarily used as a local storage cache. This means file access security is browser-based and dependent on the addition of extensions to the Chrome browser. These extensions vary widely and can support multiple formats of encryption. Both Chrome OS and Android support extensions of WIP specifically for Microsoft Office apps.

© 2020 Pique Solutions. All rights reserved.

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	●	●	●	●
Android	◕	◑	◑	◑
Chrome OS	◕	◑	◑	◑

Poor ○ ◔ ◑ ◕ ● *Excellent*

Windows 10 and Google operating systems all support default drive encryption with trusted key storage. This has become standard in every major operating system by all leveraging at least AES-128 encryption. The same is true for support for all major VPN technology across every major operating system today. Where Windows 10 shows an advantage is in how it 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 Android supports file encryption for work profiles and Chrome OS depends on cloud storage file encryption.

© 2020 Pique Solutions. All rights reserved.

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

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.

Chrome OS initiates verified boot at startup. If it detects that the system has been tampered with or corrupted in any way, typically it will repair itself without any effort, taking the Chromebook back to an operating system that's as good as new.

Android implements what it defines as verified boot to validate device integrity. Android verified boot, based on the Linux kernel dm-verity, will perform a multistage platform verification on each boot sequence. Verified boot validates each stage, starting with a hardware key in the TEE that is the root of trust, for integrity and authenticity of all bytes before code execution can occur in the next stage. The verification goes all the way up to the system partition. Devices that ship without verified boot will not be able to upgrade to a supported version, because at that point the device cannot be fully trusted.

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 holistically across the OS to help mitigate the risks of sandbox escapes.

Android and Chrome OS apps run in a kernel-level app sandbox. The Android and Chrome OS systems assign a unique user ID to each app and runs it as that user in a separate process. The Android and Chrome sandboxes use Security-Enhanced Linux to enforce mandatory access control over all processes. By default, a Google app can only access a limited range of system resources. The system

© 2020 Pique Solutions. All rights reserved.

manages app access to resources that, if used incorrectly or maliciously, could adversely affect the user experience, the network, or data on the device. Restriction techniques include an intentional lack of APIs, a separation of roles, and restricted APIs for use by trusted apps. **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	●	●	◕	●
Android	◕	●	◕	◕
Chrome OS	◕	●	◕	◕

Poor ○ ◔ ◑ ◕ ● *Excellent*

Windows 10 and Google operating systems all support a form of secure boot to ensure a device's hardware and software have not been tampered with. Also, sandboxing has become the standard method of running applications across all the operating systems evaluated, including memory isolation techniques. Chrome OS, in particular, is strong here, as the operating system is based on the Chrome browser, meaning that sandbox functionality is native to the core OS. Windows 10 provides one distinct threat resistance feature over both Android and Chrome OS. Its Measured Boot uses hardware to evaluate the system boot process for integrity.

© 2020 Pique Solutions. All rights reserved.

Conclusion

Measured against the key criteria for this analysis, Pique Solutions found that Microsoft Windows 10 provides a higher level of capabilities compared to Google Android and Chrome OS 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	●	●	●
Android	◕	◑	◕
Chrome OS	◕	◑	◕

Poor ○ ◔ ◑ ◕ ● *Excellent*

Windows 10 provides native two-factor authentication for mobile devices, tablets, and PCs, whereas Google only supports two-factor for applications and not the device. Microsoft and Google are founding partners of the FIDO alliance, with Microsoft being an early adopter of FIDO authentication and Google recently announcing support. The difference in implementation is Microsoft supports FIDO for device authentication and Google supports FIDO for application authentication.

Windows 10 provides biometric support with Windows Hello that can be implemented for any kind of biometric authentication based on OEM implementation. Google has strong biometric support for fingerprint biometrics but lacks support for facial recognition, leaving vendors to implement less secure methods.

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. Android leverages file encryption for a work container, whereas Chrome OS depends on file encryption in cloud storage vendors. Secure management of business information with either Google operating system requires an additional investment of enterprise-level data protection, usually in the form of apps like Microsoft Office, which extends the WIP framework to Android and Chrome OS within the apps.

Windows 10 provides one distinct threat resistance feature over both Android and Chrome OS. Its Measured Boot uses hardware to measure the system boot process for integrity. Google devices have hardware root-of-trust by leveraging the TEE, 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 Google operating systems.

Overall, although Google Android and Chrome OS have strong security features, Microsoft Windows 10 scored higher for security due to native functionality and better implementation of those security features, particularly around authentication and secure file management.

© 2020 Pique Solutions. All rights reserved.