PIQUE SOLUTIONS

Security: Windows 10 versus Chrome OS and Android 8

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.

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

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

Pique Solutions conducted a comparative analysis of the protection and resilience capabilities of Microsoft Windows 10 and Google Android 8 (Oreo) and Chrome OS operating systems. The analysis assessed the level of assurance those capabilities provide an organization, the utility of those capabilities, and their impact on the user experience. Our analysis included an in-depth review of product documentation as well as hands-on testing.

Pique solutions found that Windows 10 provides more native and integrated security controls when compared to Android 8 and Chrome OS. To achieve similar levels of protection and resilience security controls provided by Microsoft, Google enterprise clients would have to purchase and integrate multiple third-party security products and tools. In fact, Google just recently expanded their security partnerships to fill the native security gaps, adding 11 new third-party security partners to its ecosystem. This complex layering of different products and services creates fragmentation across multiple products and services. The relative cohesiveness and completeness of the Windows 10 platform is a compelling differentiator against Google, as it directly affects not only data security but also user productivity and total cost of ownership for enterprise customers.

Pique Solutions concluded that Microsoft's security capabilities are superior to those of Google, not only for large enterprises but also for small and midsized businesses and consumers. Microsoft's security controls are more intuitive than those of Google and provide a stronger level of defense via a comprehensive, multifaceted security approach that is natively available. In contrast, Google does not natively provide some critical security capabilities, such as protection of data flowing between applications or between on-premises and cloud-based resources. Deploying, integrating, and managing third-party tools to gain these capabilities lowers productivity and increases total cost of ownership for Google customers.

One of the most important facets of operating system security is the ability to remotely update the OS when a new threat arises. With the notorious fragmentation of Android, this becomes extremely difficult to achieve. While users can initiate the operating system update on their own for Android, mobile carriers control the process. Their record for pushing out updates for users is very poor, due in large to the fragmentation of Android. The perfect example of this are Meltdown and Spectre vulnerabilities and Google's and Microsoft's relative ability to quickly mitigate them. Both Microsoft and Google issued security updates for Meltdown and Spectre; however, most Android users are using version 6.0, which will not be patched because this version isn't currently supported. Google Android version 8.0 does have security updates that address Meltdown and Spectre but only 1% of Android users are on version 8.0. Enterprises that are not on Android version 8.0 continue to face a high risk of their systems being compromised.

As more enterprises embrace public, private, hybrid, and multivendor cloud deployments, native control of data wherever it is, at rest or in motion, is becoming increasingly important. Granular native controls working in concert from the endpoint to the cloud is what truly separates Microsoft from Google and equips the Windows 10 platform—and organizations that choose it—with a significant competitive advantage.

Introduction to Security

Cybersecurity is becoming an important topic for enterprises striving to remain resilient in the wake of an attack that could lead to a breach of sensitive data. Most enterprises rely on multiple third-party security controls to detect and prevent threats. With third-party security products, enterprises have many options depending on what type of data they are defending. For example, protecting sensitive intellectual property requires a robust data leakage prevention (DLP) 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 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:** Nonintrusive, 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 k. 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. Many third-party security vendors are moving away from signature-based detection to machine learning and artificial intelligence to keep up with the adversary.

Having a comprehensive and layered security solution is extremely important. Microsoft provides a comprehensive data protection solution but also has robust security controls that address the endpoint and the cloud, such as O365. Microsoft's Windows Defender security suite and Advanced Threat Protection (ATP) offerings are monitoring for malware, vulnerabilities/malware, phishing, and spam. Microsoft also provides full disk encryption, file-based encryption, virtual-based security controls, and application/web browser protection through isolation. Although *some* of these security controls can be provided by many third-party security vendors, Microsoft provides all this natively. In comparison, Chrome OS and Android provide a fraction of these security controls natively. They are limited to full disk encryption (only applies to Android), application/browser isolation, and addressing security vulnerabilities within Chrome OS and Android. To achieve the same level of security controls, Google customers are required to implement, use, and manage many third-party security controls, which directly increases total cost of ownership and complexity.

Google recently announced enhancements to G Suite Enterprise that include anti-phishing and malware detection/prevention for Gmail. Until recently, Microsoft O365 with ATP was leading G Suite Enterprise for Gmail in providing protection for the largest attack vector, which is email. With Google's latest release on March 21, 2018, Google rolled out almost identical countermeasures for hosted enterprise email. They provide the ability to configure multiple countermeasures, but this requires a security expert to configure. Additionally, on the same day, Google expanded their Google Cloud security partnerships to offer the following capabilities:

- Auth0 offers the ability to secure cloud endpoints and seamlessly implement secure identity management into customer products and services.
- Check Point can now secure multiple VPCs using a single CloudGuard security gateway to protect customer applications.
- Cloudflare Web Application Firewall helps to prevent attackers from compromising sensitive customer data.
- Dome9 has developed a compliance test suite for the Payment Card Industry Data Security Standard (PCI DSS) in the Dome9 Compliance Engine.
- Fortinet provides scalable network protection for workloads in Google Cloud Platform(GCP).
- Palo Alto Networks VM-Series Next Generation Firewall helps customers to securely migrate their applications and data to GCP, protecting them through application whitelisting and threat prevention policies.
- Qualys provides vulnerability assessments for Google Compute Engine instances.
- Rackspace Managed Security and Compliance Assistance provides additional active security on GCP to detect and respond to advanced cyber threats.

- RedLock Cloud 360 Platform is a cloud threat defense security and compliance solution that provides additional visibility and control for GCP.
- StackRox augments Google Kubernetes Engine's built-in security functions with a deep focus on securing the container runtime environment.
- Sumo Logic Machine Data Analytics Platform offers enterprise-class monitoring, troubleshooting, and security for mission-critical cloud applications.

This partner ecosystem will be managed within Google's Cloud Security Command Center, which helps security teams gather data, identify threats, and act on them before they result in business damage or loss. Although Google's Cloud Security Command Center is in alpha stage, this backs up the claims that Google requires multiple third-party products to achieve the same level of native security controls that Microsoft provides.

Assessment Methodology

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

1. Based on product documentation and hands-on testing, we compared the security features and capabilities provided natively across Windows 10, Chrome, and Android 8. 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.

When scoring the relative feature and functionality of the three platforms, 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, Chrome OS, and Android, 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
- Third-party ecosystem
- 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

- Virtualization-based security (VBS)

6. App Store

- App Store Security Policy
- Application Vetting
- Application developer vetting
- Android apps running on Chrome OS

Our research addressed the following OS versions:

- Windows 10 (Pro, Enterprise, Mobile, S)
- Google Chrome OS 62
- Google Android 8 (Oreo)

Key Findings

Based on Pique Solutions comparative analysis of Windows 10 versus Android 8 and Chrome OS 62, we have 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. As opposed to Android 8 and Chrome OS, which both require the implementation of third-party tools to address specific areas of security, Windows 10 offers all the required security functionality natively. Overall, the native security controls provided in Windows 10 allow an organization to reduce their attack surface with a defensive in-depth approach, from the endpoint to the cloud. Google does provide a set of native security controls; however, they are limited to browser and application isolation. The following are the key findings that demonstrate the superior effectiveness of Windows 10 security controls as compared to Android 8 and Chrome OS.

Identity and Authorization

- Windows 10 is the first major OS with Fast ID Online (FIDO) 2.0 support for the enterprise, and Google also provides FIDO support.
- Chrome OS and Android do not natively provide two-factor authentication and require third-party biometrics or smart cards.
- Windows 10 biometrics replaces passwords to improve both security and usability.
- Chrome OS and Android provide fingerprint ID support if it is available with the hardware platform they are running on.

Information Protection

- Microsoft Windows Information Protection (WIP) secures critical data by providing device-side protection, data separation, data-leakage prevention, and information sharing without the need for redundant workspace and apps. It also eliminates the need for a secure container or for app wrapping.
- Chrome OS and Android provide rudimentary data-leakage prevention within Gmail for users who subscribe to G Suite Enterprise. To get the same level of protection as WIP requires, 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.
- Depending on the hardware platform, Google provides a 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 anti-virus protection that utilizes machine learning without the need for signatures.

- Google G Suite provides anti-phishing and malware protection for enterprise Gmail clients.

Encryption

- Windows 10 provides full disk encryption natively with BitLocker.
- Chrome OS only provides file-based encryption using eCryptfs.
- Chrome OS encrypts each user's cached user data.
- Android has provided full disk encryption in version 5.0 and higher.
- Android has provided file-based encryption in version 7.0 and higher.

Hardware-Rooted Security

- Windows 10 provides VBS using Windows Defender Device Guard. Google's answer to VBS is strictly tied to the browser by using site isolation.

App Store

- Microsoft and Google provide a similar user experience within their respective app stores. In terms of security and vetted applications, Microsoft screens every application for the presence of malware before it is released to the public. Google also screens every application for malware with Google Play Protect; however, hackers continue to target Google and are often successful in their efforts.

Feature and Functionality Comparison

Identity and Authorization

Testing Scores	Baseline	Feature	Functionality
Windows 10	81	72	72
Android 8	81	40	57
Chrome OS	81	41	63

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 three 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. Yet, while 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 have the potential to 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 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 Google are both core sponsors of the 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, Android 8 and Chrome OS are still limited to a PIN-based authentication system with biometrics as a convenience feature. Google has announced their intent to provide support in the future for

FIDO authentication, starting with the use of fingerprint biometrics for web-based apps, but the timeline for deployment is unknown.

While not FIDO 2.0, both Chrome OS and Android 8 support local and network-based 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 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 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.

Chrome OS supports biometrics through third-party hardware. Additionally, Android supports biometrics but is dependent on the mobile device. Google also has the capability of unlocking the phone and applications with its Trusted Voice functionality.

Windows 10 scores higher than Google 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. The Google identity management system lacks any level of assurance beyond protection against malicious intent using simple methods. Google 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
Android 8	36	20	20
Chrome OS	36	20	20

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 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 operating system and data storage partitions. 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.

Chrome OS provides tamper-resistant hardware (TPM Chip) that makes it difficult to gain unauthorized access to files. Android 8 devices with the required supporting hardware have encryption enabled by default. Low-end devices that do not have fast flash storage nor use 32-bit chips that do not support accelerated AES encryption are exempt from the default encryption requirement. A device can adopt removable media and apply block-level encryption to that media. Dm-crypt is the basis of Android disk encryption, which is a kernel feature that works at the block device layer. The default encryption algorithm is 128-bit AES. Those devices that do not have the supporting hardware, which includes all but the newest high-end Android devices, will continue to store the key in software.

It should be noted that exhaustive key search techniques on a key space of 128 bits, using the latest streamlining processes, require resources (e.g., MIPS, memory, power, time) many orders of magnitude beyond current capabilities. Any unforeseen breakthroughs could certainly apply to 256-bit as well as 128-bit. Leveraging 256-bit does not necessarily mean better but may lead to a positive impact on system resources and utilization for processing key algorithms.

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

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.

Chrome OS and Android require the use of third-party VPN clients like Cisco AnyConnect. Google relies heavily on the use of Transport Layer Security (TLS) to ensure data is protected in transit.

Android 8 works with VPN servers that support the following protocols and authentication methods:

- IKEv2/IPsec with user authentication by shared secret and certificates, PEAP-MSCHAPv2, EAP-TLS, or EAP-TTLS
- Pulse Secure, Cisco, SonicWALL, Check Point, Open VPN, AirWatch, MobileIron, and F5 Networks SSL-VPN using the appropriate client app from the Google Play app store
- L2TP/IPSec with user authentication by MS-CHAPV2 Password, virtual smart card, one-time password, or certificate, and machine authentication by shared secret
- PPTP with user authentication by MS-CHAPV2 Password, virtual smart card, one-time password, or certificate

Android supports 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. Android 8 provides support to facilitate VPN connections on allowed apps and prevents 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 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).

WIP implements the most effective method for data protection. Because it integrates with the OS, 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 MDM to specify which apps are allowed 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 MDM, 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 some random machine. If you set WIP as part of the management policy, then you also get this 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."

Chrome OS and Android 8 do not provide a native data protection for data management like Windows 10 beyond file system access controls and a data container—Android for Work.

Investment in third-party data management technology will be required to address data management. Google's focus for data protection is wrapped within their G Suite for Enterprise offering. Google's data protection is limited to only Gmail and provides light-weight DLP controls. They have many predefined content detectors depending on what geography you want to apply to the predefined content detectors. For example, if you select the United States, you can choose from the following:

- Social Security Number
- Driver's License Number
- Drug Enforcement Administration (DEA) Number
- ABA Routing Number
- National Provider Identifier (NPI)
- CUSIP
- FDA Approved Prescription Drugs
- Passport

While for Google this feature is limited to email, Microsoft can apply these controls beyond email.

Android for Work is a secure container for Android 8. It creates a segregated workspace, called a work profile, in which managed data resides. The administrator of the profile has full control over scope, ingress, and egress of data as well as its lifetime. Apps, notifications, and widgets from the managed profile are marked with a red badge to distinguish them from personal apps and are presented in the primary user interface. Apps inherit their own segregated data space when the same app exists in the primary user and managed profile. Apps cannot communicate directly with one another across the profile–user boundary, unless allowed by the organization. They act independently of one another unless allowed by the administrator using profile configuration settings. Accounts in the managed profile are unique from the primary user. There is no way to access credentials across the profile–user boundary. Only apps in their respective context can access their respective accounts. Work apps that are copies of personal apps duplicate network connectivity, storage, and memory, requiring users to pay attention to resource management on all but the most powerful devices.

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. Chrome OS and Android are not clear about hardware-based encryption management and do not seem to provide native data management capabilities. While some versions of Android (e.g., Lollipop) seem to support hardware encryption, it is turned off by default by OEMs.

Secure management of business information with Google would require an additional investment of third-party enterprise-level data protection. Additionally, Chrome OS does not scale in large enterprise environments due to the cost and complexity of multiple solutions. 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.

Threat Resistance

Testing Scores	Baseline	Feature	Functionality
Windows 10	90	90	87
Android 8	90	52	75
Chrome OS	90	68	75

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 then 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 OS, 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.

Android provides the SafetyNet Attestation API. This API assesses and assists with the compatibility and security of your apps that run in an Android environment. The API assesses the integrity of the device and app. This is an additional layer to identify whether or not the device has been modified or tampered with. It is not clear that Google provides this API for Chrome OS outside the verified boot process.

Chrome OS and Android 8 implement what Google 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, 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

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.
- Google Android Enterprise guarantees security patches within 90 days, which could put millions of mobile devices at risk.
- Microsoft releases security patches every 30 days.

Windows 10 provides multiple additional threat-resistance features that Chrome OS and Android 8 do not. Chrome OS and Android 8 rely on their web browser and known bad sites to protect a system from malware and other exploitations. Although Chrome OS and Android 8 have application isolation, they do not have any native security controls that will protect against exploitation—thus, a third-party product is required to reduce their attack surface. Most enterprises are not only limited by minimal security budgets but also by in-house security expertise needed to operate multiple third-party products with multiple management infrastructures. This will limit Google’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.

Google just recently announced enhancements to G Suite Enterprise that include anti-phishing and malware detection/prevention for Gmail. New default-on protections include flagging emails from untrusted senders who attach suspicious attachments, warning against email spoofing, and the ability to scan images and expand shortened URLs for malicious indicators and links. With these recent enhancements, Google G Suite users receive the same level of anti-phishing and malware protection with Gmail as do Microsoft customers with O365 ATP. For enterprises, Google Team Drives can now better protect highly sensitive content through new controls, such as limiting file access privileges and Information Rights Management (IRM), which prevents users from printing, downloading, and copying files.

Encryption

Testing Scores	Baseline	Feature	Functionality
Windows 10	9	9	9
Android 8	9	9	6
Chrome OS	9	9	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 Google provides the same capability using eCryptfs.

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. Chrome OS can only provide file-based encryption and Android 8 provides full disk encryption and file-based encryption. 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 encrypt.

Hardware-Rooted Security

Testing Scores	Baseline	Feature	Functionality
Windows 10	9	9	9
Android 8	9	6	9
Chrome OS	9	6	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. Chrome OS and Android provide a similar feature to VBS; however, it is exclusively tied to the web browser using site isolation. This capability is consistent across multiple operating systems and is necessary in providing isolation. One of the important advantages of Windows 10 to enterprise customers is that they can expand this protection to include application control. This increases the security efficacy of Windows 10 well beyond that of Chrome OS and Android.

App Store

Testing Scores	Baseline	Feature	Functionality
Windows 10	**36**	**21**	**18**
Android 8	**36**	**20**	**14**
Chrome OS	**36**	**20**	**14**

Microsoft and Google provide a similar user experience within their app stores. Users can purchase application, movies, songs, and books. Both Microsoft and Google screen every application for the presence of malware before being published and will also perform periodic checks of already published apps. Google achieves this with Google Play Protect, which outlines their methodology for testing and vetting applications. There is literally no difference in both app stores with respect to what they offer customers and flexibility when rolling out custom-based applications for enterprises. Despite Google's Potentially Harmful Application scanning tool, Google Play has been plagued with malware. In Google's "Android Security 2017 Year in Review" paper, they reported 383,000 applications had the presence of malware. This is not evident with Microsoft's store and large enterprise organizations should consider this when thinking about Chrome OS and Android in their environments.

Conclusions

Based on in-depth review of product documentation and hands-on testing, Pique Solutions found that the Microsoft Windows 10 platform offers a more cohesive and comprehensive security solution than Google Android and Chrome OS. While Microsoft provides a complete set of security controls natively in Windows 10 and supporting Microsoft tools, Google relies heavily on third-party tools to offer analogous security capabilities. As a result, Android and Chrome OS struggled across all key areas of our analysis to deliver a seamless security offering. The only two areas where Google natively achieved parity with Microsoft in our evaluation were container and application isolation and full disk encryption.

To achieve parity with Microsoft in the remaining areas, Google customers would be required to deploy, integrate, and manage many third-party tools. This layered approach to security increases complexity and increases the risk of leaving vulnerabilities exposed. In addition, the reliance on third-party tools significantly increases total cost of ownership. Given the fact that most organizations have limited budgets allocated to security (on average 5% of the overall IT budget), the additional investment needed to integrate and manage these third-party tools for Google to achieve security parity with Microsoft consumes precious resources and may force IT to make harmful trade-offs due to budget limitations.

While Google's approach to security is essentially tied to cloud-based security countermeasures for threats that have already been defined, Microsoft's security ecosystem extends from the cloud to the data center and the user's device and includes powerful machine-learning capabilities. As a result, Microsoft can address the security threats associated with public and hybrid cloud deployments that are increasingly popular among enterprises more effectively than Google. While the comprehensive suite of security controls provided by Windows Defender and Windows Information Protection include DLP that extends to applications, folders, files, and network infrastructure, Google's DLP framework extends no further than Gmail, with the ability to scan messages, message subjects, and attachments for keywords.

Effectively executing security updates is a critical function of enterprise security strategy. While Windows Store can push updates to any Windows 10 device, allowing all Windows 10 devices to stay current with the latest security updates, Android relies on device manufacturers to maintain accountability for updates to their active devices. Given the vast number of Android devices and the popularity of rooting them makes this approach ineffective. This is further exacerbated by the vast fragmentation of the Android operating system and the slow adoption of new Android versions.

In conclusion, based on the analysis presented in this white paper, for enterprises striving to significantly reduce the cost, complexity, and vulnerability of their security infrastructures, Windows 10 is a superior alternative to Chrome OS, Android, and G Suite Enterprise due to its superior functionality and lower cost of ownership.