PIQUE SOLUTIONS

# Device and Application Management: Windows 10 versus Chrome OS and Android 8

## Manageability 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

Pique Solutions conducted a comparative analysis of the management capabilities of Microsoft Windows 10 and Google Android 8 (Oreo) and Chrome OS environments. The analysis assessed the level of functionality those capabilities provide, the utility of those capabilities, and their impact on the user experience.

As organizations of all sizes and types become increasingly dependent on mobile productivity, workers at those organizations require and demand “anytime, anywhere, any device” access to incorporate data and other information. This makes effective device management a critical success factor for IT and the business, as well as integrated device management capabilities key evaluation criteria when selecting operating environments.

Our study found Microsoft’s native management solutions superior to the native management capabilities of Google, primarily for the following reasons:

1. Manageability features of Windows 10 are easier to configure, deploy, and use than those of Google.

2. Windows 10 management processes are easily scalable and repeatable, without incurring additional fees or creating certificate management issues.

3. Windows 10 offers greater flexibility and support of modern management scenarios, such as bring-your-own-device (BYOD) programs and hybrid cloud deployments.

4. Microsoft Enterprise Mobility + Security (EMS) offers more intuitive enrollment and setup of policies, as well as superior patching, compliance, and application management capabilities as compared to Google’s management offerings.

5. To achieve the same level of functionality, Google customers are required to deploy, integrate, and manage third-party tools.

6. Overall, Windows 10 offers greater user productivity, lower total cost of subscribed deployment, and lower cost of ownership, as compared to both Android and Chrome OS.

A direct comparison between EMS and the Google Chrome OS Management Console was not possible, because of the management functionalities natively available in Windows 10 that are not offered by Google. While both management platforms have their strong points, and Google performed most tasks adequately, it would require the addition of one or more third-party tools to approach functional equivalence with Microsoft.

With Windows 10 and Windows 10 Mobile, Microsoft has unified its PC, tablet, and phone operating systems. Windows 10 Pro, Windows 10 Enterprise, Windows 10 Mobile, and Windows 10 Mobile Enterprise all share the same core, the same app model, and access to the same app store. Select Windows 10 variants support specific functionality, such as virtualization and telephony features; however, security, management, and apps built on the Universal Windows Platform are the same across PCs, tablets, and phones. This white paper will therefore refer to all Windows 10 variants collectively as “Windows 10” and note specific applicable differences throughout.

## Introduction to Device Management

Employees introduce personal devices to enterprise environments in the form of tablets, smartphones, and personal laptops. The issue becomes how does the enterprise manage mobile and personally owned devices and control the flow of information.

Deploying and using management solutions used to require significant technical training and certifications and consumed significant time and resources. With solutions such as Microsoft EMS and Windows AutoPilot, provisioning and managing devices has become significantly easier and faster, as most of the previously manual tasks are now fully automated and no reimaging is necessary. Using a combination of these tools will provide the enterprise with a scalable management solution that ties into existing user authentication and provisioning systems (e.g., Active Directory or a hybrid solution Azure Active Directory to fully facilitate cloud deployments), by providing the enterprise with a highly configurable solution that can fully automate device setup and configuration.

When using a personally enabled device or BYOD strategy, one can configure devices with a conditional access control policy before giving access to enterprise resources. Users enroll their devices with EMS, which auto-provisions the device based on policy settings that provide organizational settings and apps over the air, along with application and geographical restrictions. For devices purchased directly from Google or an Android device carrier, one can also take advantage of Microsoft Intune to automatically enroll new devices into the enterprise using EMS and put restrictions on the types of content available that a user can put on the mobile platform. If users lose their device or leaves the organization, they only leave with their device and personal data and not any sensitive organizational data.
EMS can enforce settings, monitor corporate compliance, and remove corporate data and apps, while leaving personal data and apps on each user's device intact.

Once configured, users can personalize their devices with their own applications and data in addition to any corporate account or applications provided by their employer. When devices are shared by several people or used for a single purpose (e.g., in a restaurant or a hotel), IT administrators typically configure and manage them centrally rather than relying on an individual user to perform the setup. With a nonpersonalized device deployment, users generally are not permitted to install apps or store any personal data on the device. EMS can place restrictive settings across multiple device types, not just those powered by Windows 10.

In the past, device management has relied on expensive third-party tools that are limited in features and functionality and often hold the enterprise hostage due to high licensing models and maintenance costs. Sadly, these solutions are still needed for granular control of Google's Android platform because the G Suite management solution from Google lacks the features and functionality to properly provide granular and transparent settings that enterprises require as more industries are dealing with higher compliance standards.

Workers are increasingly demanding to have the ability to use their personal devices for business without exposing their personal information. Mobile device management (MDM) vendors are responding to this with reversed enrollment flows, where a user can download the initial mobile portal without enrolling their device for management by their employer. However, if the user wants access to corporate data on their personal device, their only option is enrolling their device in an MDM solution.

With the continuous rise of IoT and connected devices where security risks are greater, the greatest challenge for MDM vendors is to integrate these devices into their existing MDM tools. Another challenge for MDM vendors is balancing security and productivity. When accessing corporate data on their personal devices becomes cumbersome due to security policies, user productivity decreases.

Most third-party MDM solutions support both corporate-owned and personal devices, including smartphones and tablets, and many cater to a variety of operating systems. However, each solution is unique, offering different levels of support, integration, management, and usability. Additionally, each MDM tool handles data security and privacy differently. There are pros and cons for deploying a third-party MDM solution. For the positive aspects, MDM solutions are highly scalable, a factor that becomes increasingly valuable with the growing number of devices used by the mobile workforce.

Below are some of the limitations of third-party MDM tools:

- Both cloud-based and on-premises MDM solutions can be complex to manage and very expensive.
- MDM solutions provide support for only the lowest common denominator due to the vast fragmentation of device OEM MDM application programming interfaces. This is especially true for Android, where device fragmentation is the greatest.
- The management and security controls of third-party MDM tools are sometimes not granular enough to address the unique management and security needs of a specific enterprise.

Android is a mobile operating system exclusively. While Chrome OS can now access additional functionality via Google Play Store, that marketplace is known to have numerous malicious apps that can place enterprises and users at extreme risk. Due to the fragmented nature of the Android platform, the ability of users to root Android devices, and the limitations of Google's native MDM capabilities outlined in this white paper, large corporations are often forced to deploy third-party MDM tools. Besides incurring significant additional capital and operational expenditures by doing so, they often realize that some features of their MDM solutions only work on some Android devices. To mitigate this, Google has been actively expanding its partnerships with third-party MDM vendors who have been steadily improving the compatibility of their solutions with the many varieties of the Android platform.

## Assessment Methodology

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

1. Based on product documentation and hands-on testing, we determined the management features and capabilities provided natively across Microsoft Windows 10, Google Chrome, and Google 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. The comparison of Google's and Microsoft's management features and functionality was based primarily on publicly available product documentation and other relevant public data.

4. When public data was not available or was not sufficient, hands-on testing was conducted 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 8, Pique Solutions researched the features and functionality across five main categories:

- **Device Enrollment:** Discovery, certificate, provisioning
- **Device Configuration and Policies Supported:** Network, device resources management, geo-fencing
- **App Management:** Delivery, update, configuration, app black-/whitelisting
- **Remote Assistance:** Asset management, OS and security updates, lost device, remote wipe
- **Monitoring:** Anomalous behavior detection, compliance, root detection

For the testing environment, we used the most widely adopted and common software in the enterprise market: Microsoft Windows Server, Microsoft Active Directory, Office 365 (documents and email), “Enterprise App” (a lightweight limited-functionality app to simulate an enterprise-provided app), “Personal App” (a lightweight limited-functionality app to simulate a personal app), and OneDrive.

The MDM system used was EMS E5 integrated with a set of Microsoft tools, Google apps, and ATA, DLP, and UBA.

# Key Findings

## Device Enrollment

The following table summarizes the results of our hands-on testing of the device enrollment capabilities provided by Microsoft and Google. Microsoft achieved the perfect score in all three categories (discovery, certificate, provisioning) while Google performed relatively worse, especially in the discovery category for Android 8 and the certificate category for both Android 8 and Chrome OS.

| Testing Scores | Baseline | Feature | Functionality |
|---|---|---|---|
| Windows 10 | 27 | 27 | 27 |
| Android 8 | 27 | 6 | 5 |
| Chrome OS | 27 | 12 | 10 |

A few things should be mentioned before discussing device enrollment. There are several different types of device enrollment use cases: BYOD, corporate-owned device (COD), and Device Enrollment Manager (DEM). An administrator is typically responsible for enrolling enterprise-owned devices before they are issued to the user. Below is a brief description of each:

- **Bring Your Own Device:** BYOD includes personal phones, tablets, and PCs. Users install and run the company portal app to enroll BYODs. This program lets users access company resources like email.
- **Corporate-Owned Device:** CODs include phones, tablets, and PCs owned by the organization and distributed to the workforce. COD enrollment supports scenarios like automatic enrollment, shared devices, and preauthorized enrollment requirements. A common way to enroll CODs is for an administrator or manager to use the DEM.
- **Device Enrollment Manager:** DEM is a special user account that allows enrollment and management of multiple CODs. Managers can install the company portal and enroll many userless devices.

Existing enterprise management tools, such as Group Policy Orchestrator (GPO), Windows Management Instrumentation (WMI), PowerShell scripts, and System Center Configuration Manager (SCCM), continue to work for Windows 10, and there is now a built-in agent for joining Microsoft's own EMS management solution.

After enrolling in the program, administrators can log into the EMS website, link the device to their EMS servers, and assign devices to users. Once assigned, users can go through the Setup Assistant on their devices; any enterprise-specified configurations, restrictions, and controls are automatically installed.

When users enroll themselves into the EMS management solution by logging into a new or existing device with their Azure credentials and accepting the enterprise policy, their device will be reconfigured with the settings approved and enforced by the enterprise. Some 400 common settings are available to the enterprise out-of-the-box, with support for additional PowerShell and WMI scripts that administrators can use to perform more granular settings, such as GPO security, network, hardware component restrictions, and the like.

Other methods of enrollment include conditional enrollment. This is an effective option for BYOD scenarios where employees and contractors use personal devices for business. The granular restrictions within conditional enrollment will ensure that when the employee or contractor leaves the organization, all email, contacts owned by the company, and business apps and data will be wiped.

EMS gives organizations the ability to securely enroll devices in the corporate environment, wirelessly configure and update settings, monitor policy compliance, deploy apps and books, and remotely wipe or lock managed devices. This is not limited to Windows 10 devices, as EMS can also be used to manage Android-, iOS-, and macOS-based devices.

In addition, Microsoft recently introduced a game-changing management tool, Windows AutoPilot. With AutoPilot, a user can take delivery of a new Windows 10 device straight from the vendor and the device will provision itself in a matter of minutes. The combination of EMS and AutoPilot provides unparalleled device enrollment capabilities especially to enterprises adopting the modern management principles empowered by the cloud. For those organizations that are yet to make that transition, Microsoft is developing processes to assist customers who currently do not utilize any cloud services but are interested in a shift to modern management. For example, co-management is a new concept that allows Windows 10 devices to be managed by Microsoft Intune MDM and the SCCM agent at the same time. It will provide a mechanism for organizations to migrate workloads to modern management at their preferred pace. A variety of third-party MDM solutions are available to support different server platforms. Each solution offers different management consoles, features, and pricing.

EMS provides a fast, streamlined way to deploy enterprise-owned devices, by using a simplified initial setup that automates enrollment and the supervision of devices without having to physically touch or prepare them before users get them. This process can be made even simpler for users, by removing specific steps in Setup Assistant, so users are up and running quickly, making the enrollment process quick and painless.

Auto-enroll and BYOD policies are very popular ways of enrolling devices and associating them with users when it comes to application management. Windows 10 enrollment can be performed using the auto-enroll or BYOD policies, although if an enterprise has several hundred or thousands of devices to enroll, bulk enrollment is always an option. Whether one is using the Azure-based auto-enrollment, bulk enrollment, or the Windows AutoPilot deployment program, numerous options and wizards are available for specific management requirements and device ecosystems.

Google recently introduced the extension of some of their MDM in G Suite for iOS. While this enhances Google's management capabilities, Microsoft EMS still commands a large advantage over G Suite with its device-agnostic framework and flexibility and its superior management capabilities for non-Windows devices. For example, EMS can provide full user behavior analytics, data loss prevention, and MDM of Android, iOS, and Windows 10 mobile devices (e.g., tablets, Surface, phones). It can also manage policies that impact Google Chrome and macOS. Google G Suite can only match a fraction of these capabilities.

The Chrome OS native management platform is the Google Chromebook management console. We found enrolling devices into the device manager to be time-consuming. First, one needs to buy all devices from Google directly and pay either a yearly or perpetual per-device licensing fee. Any devices purchased outside of Google need to be purchased through an approved partner at an undisclosed fee. The enrollment options for Chrome OS are Forced Re-enrollment, Verified Access, and Verified Mode. These are the only options for enrolling Google devices.

### Forced Re-enrollment

This setting forces a device to re-enroll into a domain after wiping by default. When this feature is disabled, the device is not forced to re-enroll after wiping. Once enabled, if the user does not want a Chrome device to re-enroll in a domain, he or she needs to deprovision or disable the device. When the Forced Re-Enrollment device policy in the Admin console is turned on and the user wipes or recovers the device, the enrollment screen is the first thing the user sees when he or she restarts the device.

### Verified Access

Verified Access is a Chrome device setting that enables a web service to request proof that its client is running an unmodified Chrome OS that is policy-compliant (running in Verified Mode if required by the administrator). The Verified Access setting includes the following controls:

- **Enable for Content Protection:** Ensures that Chrome devices in your organization will verify their identity to content providers using a unique key (the Trusted Platform Module). Also, with this feature enabled, Chromebooks can attest to content providers that they are running in Verified Boot mode.
- **Disable for Content Protection:** If disabled, some premium content may be unavailable to your users.
- **Enable for Enterprise Extensions:** Enables Verified Access for the devices in this organizational unit. If enabled, Chrome extensions can interact with the Trusted Platform Module on the device.
- **Disable for Enterprise Extensions:** If disabled, Chrome extensions attempting to perform Verified Access will receive a permissions error.

### Verified Mode

Verified Access is how a network service, such as a VPN gateway, a sensitive server, an Enterprise certificate authority, or an Enterprise Wi-Fi access point can get a hardware-backed cryptographic guarantee of the identity of the device and the user trying to access it. Verified Access ensures that a device connecting to your network has been unmodified and is policy-compliant. Verified Access uses the Trusted Platform Module present in every Chrome OS device to enable enterprise network services to cryptographically confirm the identity and status of verified boot and enterprise policy using a Google server-side API. The administrator needs to enable the Verified Access feature in the Google Admin console and force-install a Chrome extension on the user's Chrome devices. Once this is done, the network service talks to the Verified Access API to determine the policy compliance and talks to Google to (optionally) determine the identity of the client device. Service accounts that can receive a device ID will list email addresses of the service accounts that gain full access to the Google Verified Access API. Service accounts that can verify a device but do not receive a device ID will list email addresses of the service accounts that gain limited access to the Google Verified Access API. Most API access will need to be performed from the developer's console.

## Device Configuration

The following table summarizes the results of our hands-on testing of the device configuration capabilities provided by Microsoft and Google. Microsoft, again, achieved the perfect score in all four categories (network management, device policy, geo-fencing, remote wipe) while Google performed relatively worse, especially in the network management category for both Android 8 and Chrome OS and in the geo-fencing category for Android 8.

| Testing Scores | Baseline | Feature | Functionality |
|---|---|---|---|
| Windows 10 | 36 | 36 | 36 |
| Android 8 | 36 | 18 | 13 |
| Chrome OS | 36 | 25 | 20 |

When looking at configuring a Windows 10 device or Chrome OS or Android device, understanding the mixed-mode deployment structures is imperative to a successful deployment infrastructure. In our scoring process, Windows 10 devices were found to be the most configurable, down to the most granular components, with the click of a button. In contrast, Google requires significant configuration in this area because some corporate environments do not allow for camera, USB, card reader, or Thunderbolt access. While Windows 10 configuration profiles were very extensive and easy to deploy, this process was cumbersome and time-consuming for Google.

Configuration profiles automate settings, accounts, restrictions, and credentials. In Windows 10, they can be delivered through EMS if one needs to configure many devices and prefers a low-touch, over-the-air deployment. Profiles can also be sent as an email attachment, downloaded from a web page. These settings can also impose geo-fencing in regard to the types of service that will be available when an employee or contractor travels out of the country. Many enterprises have strict policies due to their industry affiliation that might require users to enroll in EMS to get email access and contacts. This can be achieved by using the EMS solution to automatically provide the email configuration and contact synchronization. Once a device is enrolled, an administrator can approve the device or simply leave it to the system to identify the user via Azure ID and let the policy automatically flow down to the device. Then the device receives notification of the policy via an established secure communication, and the devices can receive EMS policy updates and remote commands anywhere in the world.

Most enterprise mobility management solutions support basic mobile device and mobile app technologies. These are usually tied to the device being enrolled in your organization’s MDM solution. Microsoft Intune supports these scenarios and additionally supports many “without-enrollment” scenarios.

Organizations differ to the extent they will adopt “without-enrollment” scenarios. Some organizations standardize on it. Some allow it for companion devices such as a personal tablet. Others do not support it at all. Even in this last case, where an organization requires all employee devices to be enrolled in MDM, they typically support without-enrollment scenarios for contractors, vendors, and for those with devices that have a specific exemption.

In Windows 10, one can even use Microsoft Intune's without-enrollment technology on enrolled devices. For example, an iOS device enrolled in MDM may have "open-in" protections (protection feature of iOS that restricts one from opening a document from one app, such as Outlook, into another app, such as Word, unless both apps are managed by the MDM provider of the mobile operating system. In addition, IT may apply the app protection policy to EMS-managed mobile apps to control "save-as" or to provide multi-factor authentication. Regardless of an organization's position on enrolled and unenrolled mobile devices and apps, Intune, as a part of EMS, has tools that will help increase workforce productivity while effectively protecting corporate data.

Google Chrome OS presents many serious challenges in this area. Once the device is enrolled, Chrome OS provides an overly simplified management interface, which allows the administrator to set storage policy, location restrictions, sign-in settings, device updates, and kiosk settings. The trouble areas that administrators face are application usage and play store applications. This causes a bug issue for not only manageability in regard to not being able to whitelist and blacklist applications from both the Chrome OS Web Store and Google Play for Android available to most Chromebooks, but also for security and privacy over disclosure concerns of enterprise and user information.

## Application Management

The table below summarizes the results of our hands-on testing of the Application Management capabilities provided by Microsoft and Google. Again, Microsoft outperformed Google, especially in comparison to Android 8 in the update category.

| Testing Scores | Baseline | Feature | Functionality |
|---|---|---|---|
| Windows 10 | 36 | 36 | 35 |
| Android 8 | 36 | 26 | 20 |
| Chrome OS | 36 | 33 | 23 |

Today's complex device landscape presents an array of challenges to keep data secure on corporate-owned, employee-owned, and foreign-owned devices. Intune offers choices, allowing you to choose whether to use device management, application management, or a combination of the two—depending on your needs.

Being able to whitelist a set of applications from an app store for controlled images and licensing is important for any enterprise. Based on our testing, the Windows 10 whitelisting/blacklisting functionality is a more granular and configurable solution when compared to that of Google, and it allows custom app and full app store selections. In contrast, Google Chrome OS and Android offered limited access to marketplace restricted app store when white-/blacklisting, with poor restrictions on regular app store apps that left both Chrome OS and Android open to malicious and buggy applications.

Microsoft Intune provides device and application management and works seamlessly to deliver cross-EMS capabilities such as conditional access with Azure Active Directory Premium. Conditional access combines the power of Intune and Azure Active Directory Premium, allowing one to define policies that provide contextual controls at the user, location, device, and app levels. Natural prompts ensure that only verified users on compliant devices can access sensitive data.

Application configuration policies can help administrators eliminate these problems by allowing them to assign these settings to users in a policy before the users run the app. The settings are then supplied automatically, and users do not need to take action. Intune can also be configured to assign applications to devices whether or not Intune manages them. The following table outlines the various options for assigning apps to users and devices.

| Application Whitelist and Management | Devices Enrolled with Intune | Devices not Enrolled with Intune |
|---|---|---|
| Assign to users | Yes | Yes |
| Assign to devices | Yes | No |
| Assign wrapped apps | Yes | Yes |
| Assign apps as “Available” | Yes | Yes |
| Assign apps as “Required” | Yes | No |
| Uninstall apps | Yes | No |
| End users install apps from Company Portal app | Yes | No |
| End users install apps from web-based Company Portal | Yes | Yes |

In comparison, the Google Chromebook management console does not provide the administrators many options for whitelisting. The administrator can select the types of applications and extensions; however, he or she needs to use the device section to define which applications can be used for Android users.

In Windows 10, kiosk mode is normally a locked browser with limited accessibility to a specific web-based application. In Chrome OS—a web browser operating system—in kiosk mode the restrictions can be as broad as full screen locked into G Suite or another enterprise-specific application.

Although Google does reasonably whitelist applications for Android users, the list of apps available for whitelisting will not match the list of all available apps in the G Suite Marketplace. Instead, only apps that are available to nonadministrative users appear.  If there is a need for an app to be available to nonadministrators, an administrator will need to contact the app developer about enabling it for all users.

## Remote Administration

Being able to use remote administration from a central device management solution is very important, as this allows security professionals to perform investigations and helpdesk administrators to troubleshoot issues that a user may be experiencing. Except for the preceding Android 8 deficiencies, scoring on this section was somewhat even, as both Chrome OS and Windows 10 offer a solid remote administration solution. Where Windows 10 remote administration really made the difference was with remote administration of Android devices. The ability to have a remote interactive session with an Android phone or tablet from the Windows 10 management suite was an important factor that increased the lead for Microsoft over Google.

The following table summarizes the results of our hands-on testing of the remote administration capabilities provided by Microsoft and Google. Microsoft achieved the perfect score in all four categories (asset management, OS/firmware update, security update, lost device) while Google's main relative weaknesses were the OS/firmware update and security update functionality for Android 8.

| Testing Scores | Baseline | Feature | Functionality |
|---|---|---|---|
| **Windows 10** | **36** | **36** | **36** |
| **Android 8** | **36** | **20** | **17** |
| **Chrome OS** | **36** | **34** | **29** |

EMS can set policy to allow remote administration using Microsoft Intune. Intune is the preferred native tool that is part of the EMS suite, that provides many of the traditional MDM functions. With EMS, remote desktop functionality on the endpoint device is completely configurable and scalable in both on-premises and cloud solutions, including hybrid deployments. Having the remote desktop function available on Windows 10 desktops, laptops, and tablets, including 2-in-1 solutions, adds great value for the enterprise. Remote assistance and desktop can be enabled via policy within Intune. Using the TeamViewer service within EMS, administrators can remotely access Android devices and, with Google Chrome OS remote desktop app, Windows 10 administrators can also remotely manage Chrome OS devices in the enterprise.

Google also offers a remote desktop app that works within the Chrome browser user interface. This allows Chrome OS to remotely access multiple devices for administration purposes. The security of the protocol itself is unclear, although perhaps it is SSL/TLS encryption of something more lightweight. The app is also available on Android devices in a one-way capacity, but remote management of an Android device is not available from Google.

## Diagnostics and Monitoring

The following table summarizes the results of our hands-on testing of the diagnostics and monitoring capabilities provided by Microsoft and Google. We found this category to be the most significant positive differentiator for Windows 10 versus Chrome OS and Android 8.

| Testing Scores | Baseline | Feature | Functionality |
|---|---|---|---|
| **Windows 10** | **36** | **36** | **36** |
| **Android 8** | **36** | **3** | **3** |
| **Chrome OS** | **36** | **10** | **8** |

Scoring in this category leaned heavily on the Microsoft side of the score card, as the Windows 10 management suite offers full user behavioral analytics combined with application protection profiles and data leak prevention. Alternatively, Google has minimal analytics—for instance, configuration is almost nonexistent and documentation and references to any behavioral analytics is minimal.

The Google management console has a few settings for Chrome OS devices enrolled in your domain report, such as their current device state, including firmware, Chrome OS and platform version, and boot mode. This report also includes user information. Reporting on device use for the user regarding all devices that are registered to that user is also available.

For Microsoft, EMS reporting is somewhat more extensive, as EMS can also report on abnormal and anomalous traffic for compliance as well as identify potential insider threats, data leakage, and intellectual property theft. While providing the same types of reports provided by the Google management console solution. EMS can also provide reports based on device status, user status, and application monitor logs including geographical reports. The level of detail that is available from EMS application protection reporting is extremely detailed and precise with no details left out.

## Transparency and Granularity

The following table summarizes the results of our hands-on testing of transparency and granularity provided by Microsoft and Google.

| Testing Scores | Baseline | Feature | Functionality |
|---|---|---|---|
| **Windows 10** | **36** | **36** | **36** |
| **Android 8** | **36** | **7** | **4** |
| **Chrome OS** | **36** | **6** | **3** |

Windows 10 users are still able to maintain their own privacy settings under several device configuration policies. Many of the key management features regarding privacy are maintaining personal user privacy, as individuals have the right to access their personal data, correct errors in their personal data, and erase and export their personal data, as well as object to the processing of their personal data for purposes undisclosed. With a conditional enrollment policy for BYOD, users can have a certain amount of visibility into the settings maintained by enterprise policy, along with a limited capability in many cases to strengthen but never weaken the inherited policy enforced by the enterprise EMS.

Chrome OS does not currently provide a solution around user privacy and reports all activity back to the device administrator. This includes web browsing habits, email, and app and G Suite usage. If the vault facility is enabled, the G Suite administrator can view the email with the user’s consent. While Chrome OS has been hardened to protect the authentication identity and provide operating system sandboxing, user privacy has not been taken into great consideration.

Location awareness is equally covered by both Microsoft and Google, as both feature geo-fencing, essentially allowing access to enterprise resources of a specific nature based on the geographical locale of the user and device. Microsoft does go quite a bit further, however, with the ability to detect and alert on abnormal and anomalous user behavior. The data loss prevention and behavioral analytics capability further sets Microsoft apart from Google.

Microsoft’s EMS solution is outstanding in this area, offering a full-featured product suite that provides the administrator complete control over the entirety of the deployed infrastructure and endpoints. Microsoft Intune allows for full configurability of component management regarding the camera, the microphone, contacts, the calendar, and messaging parameters, while other parts of EMS can be configured to control and manage what data can be shared with people features for collaboration purposes.

## Compliance

The actions for noncompliance allow the administrator to configure a time-ordered sequence of actions that are applied to devices that do not meet the compliance policy criteria. By default, when a device is detected that does not meet the compliance policy criteria, Intune immediately marks it as noncompliant, and then Azure AD Conditional Access blocks the device. The actions for noncompliance give the administrator more flexibility to decide what to do when a device is not compliant. For example, he or she can decide to not block the device immediately and then give the user a grace period to be compliant.

There are two types of actions:

- **Notify End Users via Email:** The administrator can customize the email notification before sending it to the end user. Intune provides customization of the recipients, subject, and message body, including company logo and contact information.
- **Mark Device as Noncompliant:** The administrator can determine a schedule in number of days after the device is marked not compliant. He or she can configure the action to take effect immediately or give the user a grace period to be compliant with device compliance policies.

To make this work, the administrator will need to have created at least one device compliance policy to set up actions for noncompliance and learn how to create a device-compliance policy for each platform. When planning to use device-compliance policies to block devices from using corporate resources, the administrator is required to have Azure AD Conditional Access setup along with a notification message template.

The Windows 10 management suite delivers a comprehensive, well-integrated, and full-featured device management solution. While Google’s Chrome OS and Android management consoles are simple and easy to use, many features pertaining to compliance and reporting are glossed over. While Microsoft is actively working with customers to help them achieve compliance, Google has not addressed as many compliance issues and requires customers to request that information. Again, the scores for this section for the reasons previously stated are in Microsoft’s favor.

## Patch Management

Microsoft Intune can help secure managed computers in many ways, including the management of software updates that keep computers up to date by ensuring the latest patches and updates are quickly installed.

When new updates are available from Microsoft Update, or a user created a third-party update, when the update is applicable to the managed computers, a notification is displayed on the Overview page of the Updates workspace. After an administrator or user clicks this notification link, he or she can then perform various operations such as viewing more information about the update, approving or declining the update, and viewing the computers that will install the update if it is approved. One can also deploy updates for software that is not made by Microsoft. This can be achieved by using the Upload Update wizard to get the update into the Cloud Storage space, after which one can approve or decline the update just like with Microsoft software.

In comparison, Chrome OS devices update to the latest version of Chrome OS when it is available. There is a new release of Chrome OS approximately every 6 weeks. In addition, there might be security fixes or software updates. Administrators are recommended to keep the default auto-update settings for Chrome OS devices in the Google Admin console. That way, devices automatically update when the new release hits the Stable Channel. Like Windows 10, Chrome OS devices running Chrome OS version 40 or later can use peer-to-peer (P2P) automatic updating. This helps reduce external network traffic. Enrolled devices automatically update from nearby devices, if they're the same model and if the organization's network allows P2P connectivity. In addition, multicast DNS should not be filtered or blocked on the local area network. If P2P automatic updating fails or is not possible on the network, devices update through normal channels instead.

Both Microsoft's and Google's product suites are evenly matched when it comes to patch management, except for Android, a count against Google. According to research firm Bridgeway, while Android commands a large portion of the mobile device market, 24% of the devices are not only vulnerable to attack but cannot be updated. This is due to the market growing at exponential rates, while individual manufacturers and service providers are holding back software updates in anticipation of a new device that has the latest version of the Android operating system. This leaves the Android user base vulnerable and open to attacks, such as the most recent Skygofree, Android malware that also includes the ability to automatically record conversations and noise when an infected device enters a location specified by the person operating the malware. The latest feature of this malware is the ability to steal WhatsApp messages by abusing the Android Accessibility Service, which is designed to help users who have disabilities or who may temporarily be unable to fully interact with a device. The malware also can connect infected devices to Wi-Fi networks controlled by attackers.

## Conclusions

Based on Pique Solutions research, hands-on testing, and analysis, we found Microsoft to be a superior alternative to Google for device and application management because it delivers more effective and intuitive modern management features and a better user experience. With EMS, Windows 10 can manage disparate devices, report on every facet of each device and user, deliver detailed behavior analytics, prevent data leakage, and maintain user privacy and identity protection. With Windows AutoPilot, provisioning and configuring a device happens in an unprecedently short time and with very little effort. These capabilities make Windows 10 a very powerful management solution, one that is better positioned than Google Android and Chrome OS to respond to the management challenges associated with digital transformation, increasing worker mobility demands, and growing privacy, security, and compliance requirements.

One of the most notable differentiators of Windows 10 versus Android and Chrome OS is the ability of Windows 10 to provide management features that are flexible, granular, and comprehensive, yet nondisruptive to users, their productivity, and their creativity. Microsoft has been successful in identity management, authentication, and authorization while navigating the age of BYOD, cloud, and hybrid cloud environments. Google, on the other hand, appears to have myopically focused on cloud-based enterprises, offering stringent controls but little flexibility in terms of BYOD and forced enrollment of devices. Google's device and user management alternatives also come with higher licensing costs and total cost of ownership, as they require significantly more time to configure and administer.

Another important distinction between the management offerings from Google and Microsoft is that Windows 10 is natively able to manage most platforms, while Chrome OS can only manage Chrome OS devices and Android only manages Android devices. In comparison, the Windows 10 management platform provides a unified suite of tools that cover every facet of management. Windows 10 and EMS can provide and oversee user and device provisioning, identity management, application and data management, behavior analytics, and data loss prevention. With Windows 10, EMS, and Windows AutoPilot, Microsoft looks at the challenges of enterprise device management more broadly, providing a solution that is more comprehensive, more cohesive, and easier to deploy and use.

To conclude, Pique Solutions analysis and hands-on testing found that, compared to Android 8 and Chrome OS, Windows 10 provides superior management capabilities that are easier to implement and use. As a result, Windows 10 facilitates higher productivity gains at a lower total cost of ownership.