PIQUE SOLUTIONS

Device and Application Management

Windows 10 versus Chrome OS and Android

Manageability Feature and Functionality Comparison

PIQUE SOLUTIONS

April 2019

MICROSOFT SPONSORED THE DEVELOPMENT OF THIS WHITE PAPER.

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

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

Contents

Executive Summary

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 on mobile devices and on desktops that often run on disparate operating systems. 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.

While most OS vendors offer a management solution, their approaches vary. It is up to the enterprises to find a solution that accommodates their processes and management methods, while offering the highest security, functionality, and flexibility possible. Given their cost advantages and their positive impact on productivity, many leading organizations are increasingly adopting Unified Endpoint Management (UEM) solutions instead of trying to assemble, integrate, and manage several third-party multidevice management (MDM), multiplatform application management (MAM), and enterprise mobility management tools.

Moreover, many organizations today are moving parts of their IT infrastructure to the cloud to lower costs and increase productivity. This added complexity further changes the requirements for effective management, and the ability of the OS vendors to support these requirements becomes an important differentiator.

An effective management solution should offer the following capabilities:

- MDM capability.
- MAM capability.
- Self-service capabilities (i.e., password/PIN reset, installation of corporate-approved apps, and ability to join and manage groups).
- Ability to control access and protect corporate data.
- Support for a bring-your-own-device (BYOD) infrastructure and maintaining separation of ownership.
- UEM, including desktop management.

Pique Solutions was commissioned by Microsoft to conduct a comparative analysis of the management capabilities of Windows 10 against those of Google’s Chrome OS and Android. The analysis will assess the level of assurance those capabilities provide an organization and the utility of those capabilities.

Microsoft offers a full suite of management tools that support on-premises, hybrid, and cloud environments. The key components of Microsoft’s management suite are Intune, Systems Center Configuration Manager (SCCM), part of Enterprise Mobility + Security (EMS), which is fully integrated with Office 365 and Windows 10 under the Microsoft 365 solution umbrella. These tools provide security and IT operations teams with granular, native controls over all devices within the enterprise, as well as devices that connect to the enterprise, regardless of the OS they run.

Although Google’s management tool, the Admin console within G Suite, features many similarities to Microsoft’s EMS, our analysis identified several important limitations, including lack of support for multiple OS environments, the need for implementing third-party tools to achieve the level of functionality that Microsoft provides out of the box, and limited scalability.

Study Approach

The methodology developed by Pique Solutions is as follows:

1. Determine the management characteristics and capabilities required to perform daily operations, as well as the ability to manage access to enterprise resources, including storage and sharing.
2. Evaluate through research how selected devices and operating systems used in conjunction with those devices are managed, and compare their relative strengths and limitations.
3. Publish a detailed assessment of findings.

To assess Microsoft Windows 10 and Google Chrome OS and Android using industry-accepted standards and definitions, Pique Solutions referenced the manageability and required capabilities founded in the principles identified in Special Publication (SP) 1800-18 that cover privileged account management. Also referenced were industry best practices from the Data Interchange Standards Association (DISA), all correlated with various management techniques and capabilities as described by vendors. Keeping within the normal operating parameters of an enterprise-grade organization, based on practicality and functional management, enterprise management is not about being difficult or completely insecure but rather about balancing a functional enterprise operating system base while meeting enterprise goals.

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

Device Management

- Device Enrollment: Ease of enrollment, controls, compliance.
- Supported enrollment methodology, flexibility and functionality vs. strict.
- Management of Multifactor Authentication: Methods, store, use.
- Application management and restrictions.

Configuration and Policy

- Configuration Profiles: Roaming, geolocation, trust zones.
- Supported Encryption: Implementation of user and device roles for authentication and BYOD partitioning, software token storage, TPM support.
- Application Profiles: Group-specific allowed applications supported.

Administration

- Remote Administration: Application profile policy enforcement, OS policy and verification.
- Hardware Controls and Compliance: Hardware management, monitoring, and reporting.
- Monitoring and Ownership: Services, application, usage.

For scoring, the criteria are defined based on Pique's subject matter expertise and, where appropriate, based on the preceding guidance of the NIST and DISA for management and configuration best practices.

We used the following scoring system (maximum score = 15).

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

This white paper compares Windows 10 version 1809 to Google Android 9 Pie and Chrome OS 71.

Device Management

Device management has become a mainstay in everyday IT operations. As more companies introduce mobile platforms to enhance workforce productivity, the network perimeter has become something that users hold in their hands. Mobile devices available today allow access to every part of the enterprise infrastructure and enable employees to work from anywhere.

Policy management is one of the most efficient methods to control access to data, but only after exploring multiple solutions and what they offer in terms of compliance, policy enforcement, and flexibility can we determine the best device and application management solution for the enterprise.

Google unfortunately only shares Microsoft's vision in the realm of mobility and Chrome OS. Google's mobile management solution is limited to Android and Apple iOS devices, leaning heavily on Android device management. This approach limits the capabilities of the Google Admin console for compliance and patch management and can only address vulnerabilities in Chrome OS. Although managing Chrome OS using the Admin console is easy with the updated user functionality, it offers limited options for configuration.

Looking at management from the perspective of operating environment security, while provisioning of user management to CAC or PIV card authentication makes Chrome OS secure, it is difficult to manage, as authentication to the device is now managed outside of Chrome OS.

Windows 10 seamlessly integrates multiple authentication methods and standards, making it a robust operating system that can be easily deployed to most IT environments and effectively managed.

Intune has seen continual improvement in features and overall functionality for managing not just Windows 10 devices, but all mobile devices regardless of the operating system on which they run.

The Google Admin console provides limited functionality, as it can only manage Android, registered Google Chrome OS devices (e.g., Chromebooks, tablets), Android, and Apple iOS. Google only addresses its own operating systems and productivity suite (G Suite). Google completely fails to address management of multiple desktop operating systems, such as Windows 10 and macOS.

As the cloud becomes a more commonplace operating environment, vendors need to adapt. IT administrators will always expect the same levels of security, policy enforcement, and compliance to be afforded to them.

The fact that Windows has become the standard operating system for most enterprises motivates Microsoft to continue producing a best-of-breed management solution that can scale while also maintaining security, compliance, and policy enforcement.

While the significantly smaller presence of Chrome OS in the enterprise makes the demand for managing it low, Chrome OS management capabilities extend past device management by also covering G Suite applications. **Table 1** provides a summary of scoring for Device Management features and functionality.

Table 1. Summary of Scoring Results for Device Management

OS	Feature	Native Functionality	Granularity of Controls	Functionality vs. "Ideal"
Windows 10	●	●	●	●
Chrome OS	◑	◕	◑	◑
Android 9	◑	◕	◕	◑

Poor ○ ◔ ◑ ◕ ● *Excellent*

Mobile Policy

Being able to define a policy to protect enterprise devices, regardless of the operating system, is one key foundation of being able to enforce policies such as geographical resource restrictions, remote device wiping, data restrictions based on risk, and multifactor authentication.

While it's not always practical to restrict every part of a mobile device, as it limits its overall usability, in many cases a restricted device will save an enterprise from falling a victim to malware or a botnet.

The most common policies are BYOD and corporate-owned device (COD). Enterprises rely on both BYOD and COD when they do not have the budgets to support a COD policy alone or they allow employees to use their own devices and subsidize the monthly fees to compensate for restrictions placed on personal property to protect the enterprise.

Not only can Microsoft Intune manage device policies across all Windows 10 devices, as well as Android 9 (Pie) and Apple macOS and iOS devices, but the platform also offers many options for policy enforcement with many moving parts around device enrollment, user authentication to restricted data, and geolocation risk policies. This creates a complex and somewhat complicated user experience at both the interactive and API levels.

Google has maintained a simple and easy-to-navigate admin console experience with a software development kit that allows administrators with little to no coding experience to develop applications for the enterprise, easing the facilitation of management tasks.

Microsoft's new software APIs for EMS still prove slightly cumbersome and require intermediate programing skills to effectively create additional applications to enhance the management experience.

Application Policy Restrictions and Profiles

Application policy is more than just determining the limits of the user's ability to side-load unauthorized applications. It allows IT operations teams to set restrictions on circumstances that would put the enterprise at risk, based on user type (e.g., executive, privileged admin user, contractor), geographical location, user behavior, or a combination of all three.

Microsoft EMS enables IT operations and security teams to define multiple policies based on location, behavior, and general authorized application policies, allowing enterprises to create more dynamic policies that can be activated based on user risk, geolocation, and user types.

Google has made similar advancements in this space but has failed to address more than just Chrome OS and has since focused on access to their collaborative productivity suite (G Suite) and the Android platform.

Intune provides device and application management and works seamlessly to deliver cross-EMS capabilities such as conditional access with Azure Active Directory (AD) Premium. Conditional access leverages the power of Intune and Azure AD Premium together by allowing one to define policies that provide contextual controls at the user, location, device, and app levels. Natural prompts ensure that only authorized users on compliant devices can access sensitive data while providing self-service requesting access to applications and data using built-in forms and click-throughs. This flexible and scalable management solution allows enterprises to maintain a leaner IT operations team. A self-servicing management environment allows the end user to make requests to enterprise data and applications, providing an auditable solution that holds data owners accountable for access and puts less demand on IT operations.

Remote Administration

Remote desktop and device administration has seen an increase in the use of third-party products that offer secure multifactor administration, with recordings of user interactions, password management for privileged accounts, and a combination of both depending on the sensitivity of the system. Many of these third-party applications offer secondary logging options for authentication mechanisms to enhance and validate the system-based logging.

Being able to use remote administration from a central device management solution is especially important, as this allows security professionals to perform security investigations and helpdesk administrators to troubleshoot issues that a user may be experiencing. Both Chrome OS and Windows 10 offer a solid remote administration solution. Where Windows 10 remote administration really makes a difference is with its remote administration of Android devices. The ability to have a remote interactive session on an Android phone or tablet from the Windows 10 management suite illustrates the flexibility of the Windows 10 operating system. Using Intune, EMS can set policy to allow remote administration.

Remote desktop functionality on the endpoint device is completely configurable and scalable in both on-premise and cloud solutions, including hybrid deployments. Having the remote desktop function available to Windows 10 desktops, laptops, and tablets, including various PC manufacturers' 2-in-1 systems, has proven invaluable to the enterprise. Remote assistance and remote desktop can be enabled via policy within Intune. Using TeamViewer, administrators can remotely access Android devices and, with the recently added support for Chrome OS in Intune, Windows 10 administrators can also remotely manage Chrome OS devices.

This is not to be confused with Remote Desktop Protocol or any local remote desktop application, as it's regarding the manageability of the operating system using an agent or API via the management console of each respective management platform.

The closest solution that natively fits into the ideal scenario in this case is Microsoft's EMS suite tied in to Azure and Office 365 services.

Configuration and Policy

While many organizations see configuration and policy as a compliance and governance issue, they are also closely tied to security and asset management. For compliance management to be truly effective, identifying the business and technical owners who manage and maintain each program (e.g., the network, email, device management) is imperative to the success of policy enforcement and device configuration.

Both the business and technical owners' requirements for successful outcomes are guidelines for the configuration and policy, as it complies with security and organizational privacy restrictions. Internet technology system management (ITSM) platforms provide additional clarity when paired with compliance, vulnerability, and operating system management. Using vendor-provided management solutions with an ITSM can remove the risk of untested changes, inaccurate archives, and unforeseen consequences. **Table 2** provides a summary of scoring for Configuration and Policy features and functionality.

Table 2. Summary of Scoring Results for Configuration and Policy

OS	Feature	Native Functionality	Granularity of Controls	Functionality vs. "Ideal"
Windows 10	●	●	●	●
Chrome OS	◕	◕	●	◑
Android 9	◕	◕	◕	◑

Poor ○ ◔ ◑ ◕ ● *Excellent*

Profiles

As a best practice, configuration profiles are traditionally administered at an organizational and group level, because individual configuration profiles are neither scalable nor manageable. Microsoft supports this model by providing a flexible solution that accommodates the various role-based access and discretionary models of authentication and authorization.

Google has neglected to address role-based access, as its profile configuration is focused on end-user personalization and control over the endpoint device. Group policy is only taken into consideration in a data access G Suite storage scenario, because Google does not support a non-cloud solution.

Authentication policies that are initially defined on Google Chrome OS devices can be modified at the user level, allowing the end user to change or modify the authentication mechanism outside of the predefined policy.

Encryption

Choosing the right encryption solution can be difficult with a myriad of unseen pitfalls that do not often present themselves until after deployment. What most organizations don't realize is that most operating systems offer some form of built-in device encryption. Vendor-supported encryption

methods are mostly found to be supported in the management platform for the operating system, with dynamic key management and rotation policies available. Many security administrators argue that third-party encryption solutions are the only way to secure desktops and mobile devices, as they are always running optimized encryption algorithms of the highest standard. The fact of the matter is that the natively supported encryption methods and tools, which are optimized for the operating system, are a more effective approach to management.

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.

In the environments offered by Google and Microsoft, from administration to mobile device management to messaging, the encryption standards vary greatly. In regard to email messaging, Google not only offers S/MIME, which is an accepted industry standard for sending encrypted mail, but also provides the option to enable GAME, which is Google's own brand of PGP encryption. Branding and supporting a proprietary encryption algorithm introduces additional unknown risks that need to be assessed by any enterprise before adopting it.

Windows 10 management allows for x509 certificates combined with an industry-supported FIPS algorithm, along with AES-CBC algorithms, which are commonly used within the enterprise today. This approach from Microsoft enables enterprises to use a single platform to manage users, data access, and devices.

Windows 10 Enterprise allows multiple authentication types to be deployed, taking advantage of smartcard technology and biometrics.

Application Profiles

Managing application profiles can limit abuse and fraud waste management. Administrators taking advantage of application profiles can effectively manage application licenses and lower the security risks at a group level within an organization by limiting application security exposures.

Both Microsoft and Google provide administrators with the ability to create application profiles that contain a list of both acceptable and unwanted applications. Microsoft's UEM lends itself to AI and machine learning, as all behavior is modeled, analyzed, and retained for future events. This is extremely useful when looking at application profiles involving risk, which can be tied to user behavior, geographical location, and user actions.

Although the Google G Suite Admin Console gives administrators basic controls to manage their domains, its user interface can be difficult to understand and use and is not scalable for larger organizations. The lack of geographic-based application profiles combined with risk-based profiles leaves the platform missing key components that are necessary for successful large-scale deployments.

As Microsoft has been building user access models for quite some time, they provide a richer management environment that looks at many of the possible scenarios and enables system and security operations teams to take advantage of every possible configuration setting.

Using the Microsoft application profiler and insight products, administrators can quickly define the parameters of what version of the application will be made available to the end user along with in what region and under what circumstances a user can use an application.

Google has failed to achieve this level of control due to device adoption in the enterprise space, along with limited application control within the G Suite and Android platforms. Google's limited use cases on the Android platform reflect numerous device administration profiles with limited restrictions.

Microsoft is clearly making the most advancements in this area of Windows 10 device management, with an agnostic approach toward flexible application profiles available across multiple device and OS types.

BYOD Enrollment and Quarantine Policy Management

Recognizing that employees often work best when they're allowed to choose their own tools, BYOD policies let people use their own devices, whether occasionally, primarily, or exclusively, for work.

One of the most obvious challenges is how people are going to be able to access enterprise applications and corporate data and files on their personal devices. Simply installing apps directly on the device would raise serious security, privacy, and compliance risks, license management issues, and support complications, as well as restrict employees' choices to Windows-based devices.

Ideally, a flexible management frame lends itself to a BYOD model and either a choose your own device, a COD, or a personally enabled device. A combination of all three strategies allows for greater flexibility and can lower abuse from a fraud and waste management perspective. Other capabilities that should be taken into consideration are as follows:

- Management of multiple device types.
- Partitioning of corporate and personal data.
- Enablement of self-service provisioning of services.
- Mobile device quarantine capability.
- Policy enforcement.

Device quarantining allows organizations to limit their exposure to high-risk individuals who are traveling to unfriendly environments that are known for corporate espionage and stealing of intellectual property. Quarantining also limits malicious software and noncompliance with corporate policy.

Other methods of enrollment include conditional access. This method is ideal for BYOD solutions where employees and contractors can use personal devices for business with granular restrictions that will occur when the employee or contractor leaves the organization. Email will be wiped along with all contacts owned by the company, in addition to any associated apps installed by the company along with content and settings.

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 platforms.

In addition, using Windows AutoPilot, a user can take delivery of his or her 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 for enterprises adopting the modern management principles empowered by the cloud. For those organizations that are yet to make that transition, Microsoft has tools and processes in place to assist customers who currently do not utilize any cloud services but are interested in a shift to modern management. For

example, a co-management method using Intune and SCCM lets users attach their existing SCCM deployment to the Microsoft 365 cloud. It helps users unlock additional cloud-powered capabilities like conditional access.

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 an annual or a 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, and they are the only means of enrolling the devices after the initial hurdles toward device procurement.

Google's G Suite/Management Console recently introduced the extension of their MDM for iOS. While this is a step in the right direction for Google, Microsoft still commands a significant advantage with its device-agnostic framework and flexibility.

Cloud Management

Perimeter system management does not have a common topology in today's enterprise landscape. Enterprises are becoming more agile, lean, and mobile. Being able to keep up with the demand of a modern enterprise from an on-premises architecture means personnel will always be required in the office or datacenter. Today's solutions need to be flexible and allow administrators to take advantage of lower-cost infrastructure and improve the overall user experience. Using cloud-based vendor services that enable the system administrators to enforce policy across multiple device types with the click of a button becomes a priceless feature.

To reduce the impact of misconfiguration and external exposure, vendors can help place account restrictions on access to cloud services and provide device administrator profiles to accommodate organizational policies and corporate standards.

Cloud management has traditionally lent itself to a managed security service provider model. Today, cloud providers are offering cost-effective pure cloud and hybrid solutions that let enterprises maintain critical assets within their well-protected perimeter, while moving other services such as directory services, mail, and application and mobile device management to the cloud, often retaining the ability to fall back onto the on-premises solutions if necessary.

Google's own cloud offering is completely separate from the device management and does not allow for any cross-pollination of services in the Google cloud and G Suite Admin console.

While the Google Cloud platform has made advancements in features and functionality, its focus appears to be on direct competition such as Amazon Web Services and not on a combination of hosting and supporting integration with the G Suite Admin console.

Microsoft has been able to build a complete cloud-based infrastructure that incorporates directory services, policy, device, and mobility management in a single entity.

Table 3 provides a summary of scoring for Cloud Management features and functionality.

Table 3. Summary of Scoring Results for Cloud Management

OS	Feature	Native Functionality	Granularity of Controls	Functionality vs. "Ideal"
Windows 10	●	●	●	◕
Chrome OS	◕	◑	●	◑
Android 9	◕	◑	◕	◑

Poor ○ ◔ ◑ ◕ ● *Excellent*

Compliance and ITMS Governance

Device management is not just about adherence to corporate policies and security. It's also about being able to audit for compliance checks and, in many cases, about asset management. Assessing the additional risks from BYOD and allowing for personal enablement of corporate devices pose several risks and can open up a company to many new issues it had not considered before the rise of BYOD.

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

There are two types of actions are the following:

- **Notify End Users via Email:** Customize an email notification before sending it to the end-user. Intune provides customization for the recipients, subject line, and message body, including company logo and contact information.
- **Mark Device Noncompliant:** Determine a schedule in number of days after the device is marked not compliant, and then configure the action to take effect immediately or give the user a grace period to become compliant with device compliance policies.

To make this work, the administrator needs to create at least one device compliance policy to set up actions for noncompliance and then create a device compliance policy for each platform. Azure AD conditional access should be set up when planning to use device compliance policies to block devices from using corporate resources. A notification message template is also created, which is later used when determining actions for noncompliance to send to users via email.

Google's Admin console is designed specifically with strict privacy and security standards based on industry-wide best practices. For organizations with compliance standards, the Admin console is fully adherent. Google backs up these compliance promises with strong user contracts to ensure compliant environments are maintained.

Google holds the following compliance certifications:

- ISO 27001, 27018
- SOC 2, SOC 3
- HIPAA
- FERPA
- COPPA
- EU Data Protection Directive and GDPR

Initially, Google offered a very limited set of security management features for IT administrators from within the Admin console. Even now, businesses should carefully examine Google's user controls to ensure they cover the individual needs of different organizations.

However, Google has made great advancements in improving administrative control and they continue to work on new strategies. Administrators can now more easily manage user accounts and control access and user permissions. This helps prevent access to and sharing of sensitive company information by employees with unauthorized third parties.

Microsoft holds the same compliance certifications as Google. Administrators have full control to review and establish security policies around sharing content and inviting external users across various applications. This allows administrators to create customized policy infrastructures to meet the unique security demands of their organization.

An ideal solution would be a single entity that can reach into asset management, provide audit logs, and report on the state of current controls that are in place. The major problem is finding a vendor that can do this, keep within budget requirements, and maintain a low total cost of ownership.

The Windows 10 management suite clearly defines what a full-featured device management solution should offer. 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, whereas Microsoft put focused effort on customers achieving their compliance strategy. Google, on the other hand, appears transparent about many compliance issues and requires customers to request that information from Google.

Conclusions

Driven by corporate BYOD programs, hardware management has become increasingly diverse and includes Windows, iOS, macOS, and Android devices. Companies that perceive technology as a source of competitive advantage have started to move from traditional MDM and MAM tools to UEM and, by doing so, are reaping efficiency, productivity, and cost benefits.

Based on our research and analysis with regards to the device and application management capabilities of Windows 10 and Google Chrome OS and Android 9 devices, Microsoft has proven to be significantly better positioned than Google to respond to the changing needs and requirements of modern management. While Microsoft's management portfolio might seem complex, it is also the most comprehensive management solution in the market in terms of features, functionality, and flexibility.

Google has taken a pure MDM solution approach to managing Chrome OS and Android devices. This leaves the Admin Console platform lacking key functionality and forces the user to deploy, integrate, and manage various third-party tools. Microsoft, on the other hand, provides all the key functionality natively and in ways that simplify management, boost efficiency, and increase productivity. Our research identified several key advantages of Microsoft over Google, including the following:

- Unlike Google, Microsoft provides a single console to configure, manage, and monitor traditional mobile devices, PCs, and IoT assets, regardless of the OS on which they run.
- Microsoft Intune unifies the application of data protection, device configuration, and usage policies. Google natively lacks these capabilities.
- Microsoft Intune and Microsoft EMS orchestrate and coordinate the activities of related endpoint technologies such as identity services and security infrastructure more effectively than Google's Admin Console and related third-party tools.
- Google lacks capabilities required to scale to a larger enterprise environment. While the combination of Chrome OS and G Suite can be suitable for many start-ups or educational institutions, as the demand for web-based applications diminishes, so does the practicality of Chrome OS.

Other key differentiators include Microsoft's use of behavioral analytics combined with risk and geography-based access policies across multiple operating systems and devices, where Google's limited reach fails to address management needs in environments where multiple device types and operating systems coexist.

It is Microsoft's operating system and device-agnostic approach and comprehensive native UEM capabilities that set it apart from Google by providing a comprehensive, scalable management solution for enterprises of all sizes and IT environments without the need for costly implementations and management of third-party tools.