

10 THINGS TO CONSIDER


# Before Buying an MDM Solution

For any company born in the cloud era, bring your own device (BYOD) is part of doing business. Cloud and mobility have changed the way we work, and created an environment where employees want access to corporate applications and data at any time, from anywhere and from whatever device they choose.

But allowing employees to use personal devices for work presents a unique security challenge: how can you be sure that access to corporate applications from an employee-owned device is secure without a) invading employee privacy by monitoring everything on their device, and b) creating a cumbersome access workstream that frustrates users?

For more than a decade, security practitioners have turned to traditional mobile device management (MDM) solutions to secure remote and personal mobile devices. MDM solutions, however, come with their own challenges. Users are skeptical about allowing an MDM on a personal device; they're concerned that admins can glean personal information and control how they use their devices. But admins without an MDM on user-owned devices fear they'll lack visibility. It's a cycle that stalls out BYOD security programs and can increase the risk of exposure to organizations.

**It begs the question:  
how do you minimize the risk  
associated with a BYOD program  
without an MDM solution?**



**Here, we'll examine  
10 things you  
should consider  
before buying an  
MDM solution.**

# 1

## Unified Endpoint Visibility

Once you allow BYOD in your organization, you open the door for your users to work with myriad devices across various platforms: iOS, Android, Windows, macOS, ChromeOS and more. However, most endpoint visibility solutions are siloed. They are designed exclusively for Windows or Macs or mobile devices. A solution specific to each platform results in a massive productivity drain and major administration headaches. Admins are forced to change BYOD policies to only support one or two different platforms, because the management hassles are simply too great. And the lack of platform choice frustrates users further.

Instead, consider a unified endpoint visibility solution to provide a comprehensive, global view on all end user devices from a single dashboard: managed devices, unmanaged devices, Windows, Macs, iOS, Android, ChromeOS and more.

Unified endpoint visibility improves admin productivity by providing a consolidated view into all devices and platforms from a single place.

It helps you better understand your user and endpoint inventory and activity. It also gives users the freedom and flexibility to use whatever device they choose, while you maintain control, which is the true spirit of a BYOD program.

# 2

## User Experience

Securing BYOD shouldn't get in your users' way. But most MDM solutions are considered intrusive. Users fear their privacy may be invaded and that they'll lose control of certain features and functions of their personal devices - cameras, messaging, etc...

**When it comes to security, if users don't trust it, they don't use it, which can be a major setback to a BYOD program.**

Consider a solution that collects only security information about devices – the less personal data collected, the better – and notify users what type of information will be collected and examined. And, if possible, provide an incentive for users to install the solution on their device. A BYOD security solution only works if it's actually used.

# 3

## Inventory Management

You have to know what devices are accessing your assets. Period. That's why a device inventory and inventory management are imperative - and many MDM solutions lack the ability to provide a detailed device inventory.

Consider a security solution that enables you to identify all devices that access your environment and also tag assets to specific users to understand who owns a device, how many devices they're using and what applications they access.

This reduces the burden of device lifecycle management while also eliminating the surprise of unknown devices accessing your applications. As the saying goes: you don't know what you don't know. A device inventory tells you what you may not already know and puts the power in your hands.



# 4

## Device Security Management

Now that you know which devices are accessing your environment and which operating systems (OSs) are most commonly used, it's time to assess the security risk to your environment, which is another area where traditional MDMs fall short.

Consider a security solution that can give insights into the security posture of all devices. For example: is the device using passcodes and biometrics? Is encryption turned on? What OS and browser versions are installed and are they up to date, properly configured and patched?

Device security status will help you detect and stop out-of-date and vulnerable devices from gaining access.

**Allowing only devices whose security posture is up to snuff to access applications and data reduces risk.**

# 5

## Policy Enforcement and Compliance

Any organization that allows BYOD must be able to enforce security policies to reduce the risk of data breaches and prevent vulnerable or unsecured devices from accessing sensitive data. Security policies are unique to each organization and you should be able to customize policies based on the risk associated with certain applications.

For example, your policy could only allow access to certain critical applications if devices have been updated with the latest patches and have encryption turned on, while devices could access less critical applications without as many checks.

Consider a solution that empowers you to enforce security policies rather than prescribing them on paper to ensure adherence. That way you can set consistent policies across applications, whether on-premises or in the cloud, to deliver a seamless user experience.



# 6

## Administration

What kind of administration time and resources are required when you allow employees to bring their own devices? MDM solutions often carry hefty administrative overhead. Your goal should be to keep that to a minimum, so you can focus your time on more pressing tasks.

Consider a cloud-based solution to manage and secure BYOD. This can reduce your total cost of ownership (TCO) because it's self-healing and fully available at all times. Also consider a solution from a provider that follows an agile development cycle, releasing updates in hours and days.

There's no overhead required to keep the application up to date - your users receive automatic updates to their devices to ensure they have the latest security patches and features.

It's also important to examine solutions through which you can manage access to applications based on user groups and individual roles and automate security patches and updates, further reducing your administration overhead. Along with reducing risk, this saves time and money.

# 7

## Audits and Reports

If your organization must adhere to strict compliance regulations, such as HIPAA, PCI DSS, NIST, SOC 2 or ISO 27001, you have to ensure employee-owned devices are always in compliance.

**Compliance starts with strong access security controls.**

Reduce the risk of data regulatory fines by aligning your corporate policies to ensure you don't allow out-of-date and out-of-compliance devices to access corporate applications.

Consider a BYOD security solution that enables you to generate user and device reports and security logs with just a few clicks to help meet compliance requirements for tracking and security event logging, as well as provides valuable assets for audits and incident response and recovery.

# 8

## Transparency

When it comes to BYOD security, if users don't know what actions a solution is taking, they're less likely to embrace it. That's one major opposition to traditional MDM solutions: users don't know what information is being collected or how it's being used.

Consider a solution that is transparent and provides your users insight into what information is collected. This gives users confidence in the solution and trust that they can verify the information collected at any time.

**Confident users are happy users, and user happiness goes a long way toward a smooth BYOD security experience.**

# 9

## User Onboarding

When selecting a BYOD security solution, it's important to investigate the user onboarding process. Is it clunky and cumbersome? Or is it streamlined and frictionless?

Consider a solution through which you can onboard users at the time of login and offer flexible onboarding options through different types of endpoints, like mobile devices or laptops. Some solutions also offer user self-enrollment, through which users can sign up and enroll their own devices with no training. With self-enrollment, admins can send out links via email to initiate onboarding, saving support time.

# 10

## Ecosystem and Integration

Does the BYOD security solution you're evaluating integrate easily with existing device management tools and vendors to share information on device state? How about with security identity event management (SIEM) and user behavior analytics (UBA) solutions to identify anomalous logins from devices?

**Smooth integration of a security solution into your ecosystem is imperative to protect existing technology investments and avoid rip and replace.**

Consider a BYOD security solution that helps you automate your security processes and also improves your organization's overall security posture by sharing data across tools.

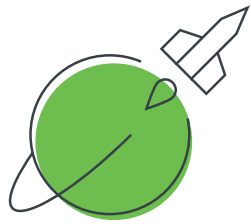


# Conclusion

Those are 10 key considerations to keep in mind before buying an MDM solution to secure your BYOD environment. Users today want access to corporate applications and data from their personal devices from wherever they choose. For admins, this presents a challenge: traditional MDMs are

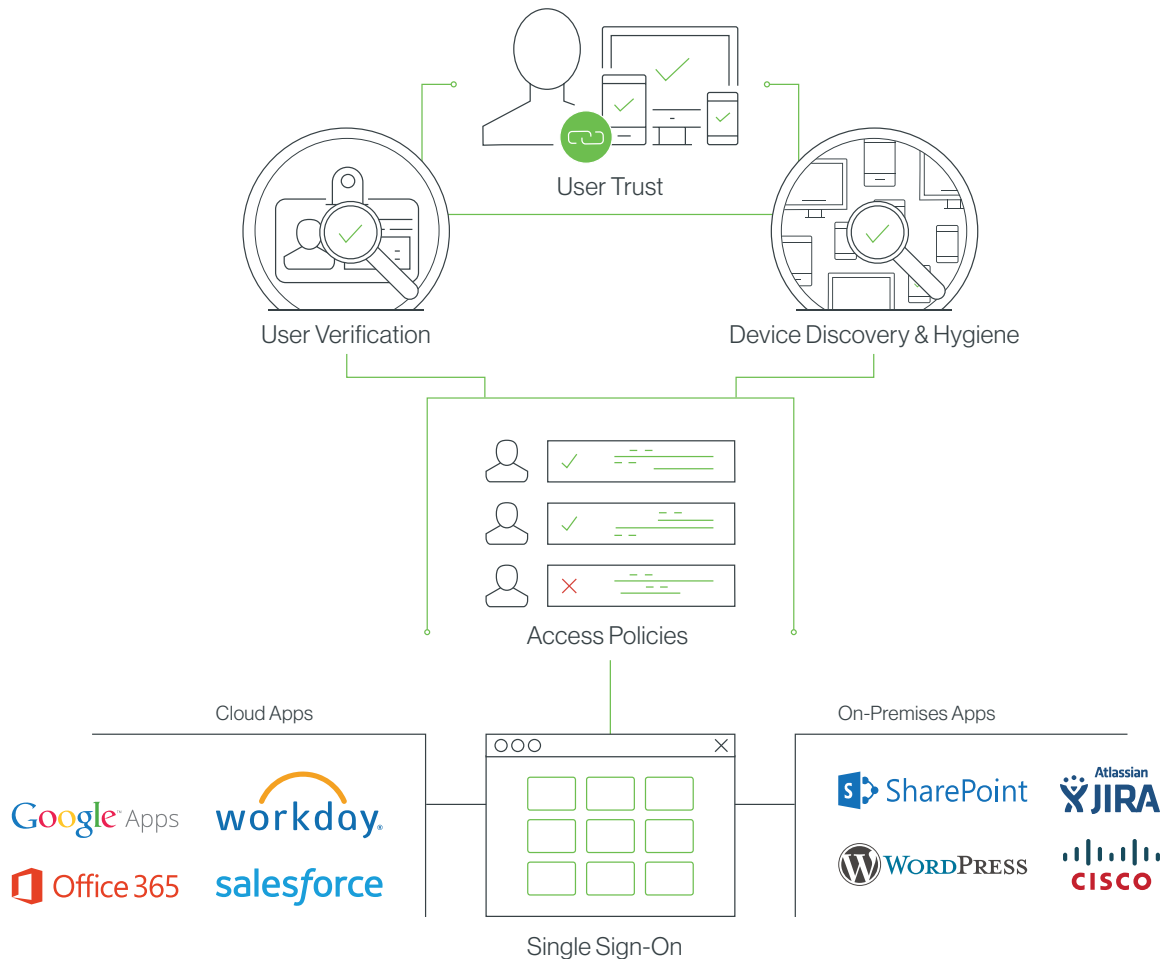
a hard sell to users, but without an MDM, there's no visibility and little control into who accesses what. Before you invest in an MDM solution, it's important to consider these 10 things to determine if an MDM is actually right for your business.





# Beyond

Trusted Users. Trusted Devices. Every Application.



**Duo Beyond**, our zero-trust security platform, helps you secure all mobile devices including BYOD without the management headaches and user resistance inherent with an MDM solution.

Duo Beyond secures access to all applications, for any user, from any device, and from anywhere. Cloud-first organizations and those looking for a secure, rapid transition to the cloud use Duo Beyond to protect their on-premises and hosted applications, while securing their mobile workforce and their chosen devices.

Duo Beyond delivers a zero-trust security platform that enables organizations to base application access decisions on the trust established in user identities and the trustworthiness of their devices, instead of the networks from where access originates. Duo delivers this capability from the cloud and without reliance on outdated, cumbersome, and costly technologies

Learn more about **Duo Beyond** and start your free 30-day trial at [duo.com/beyond](https://duo.com/beyond)



