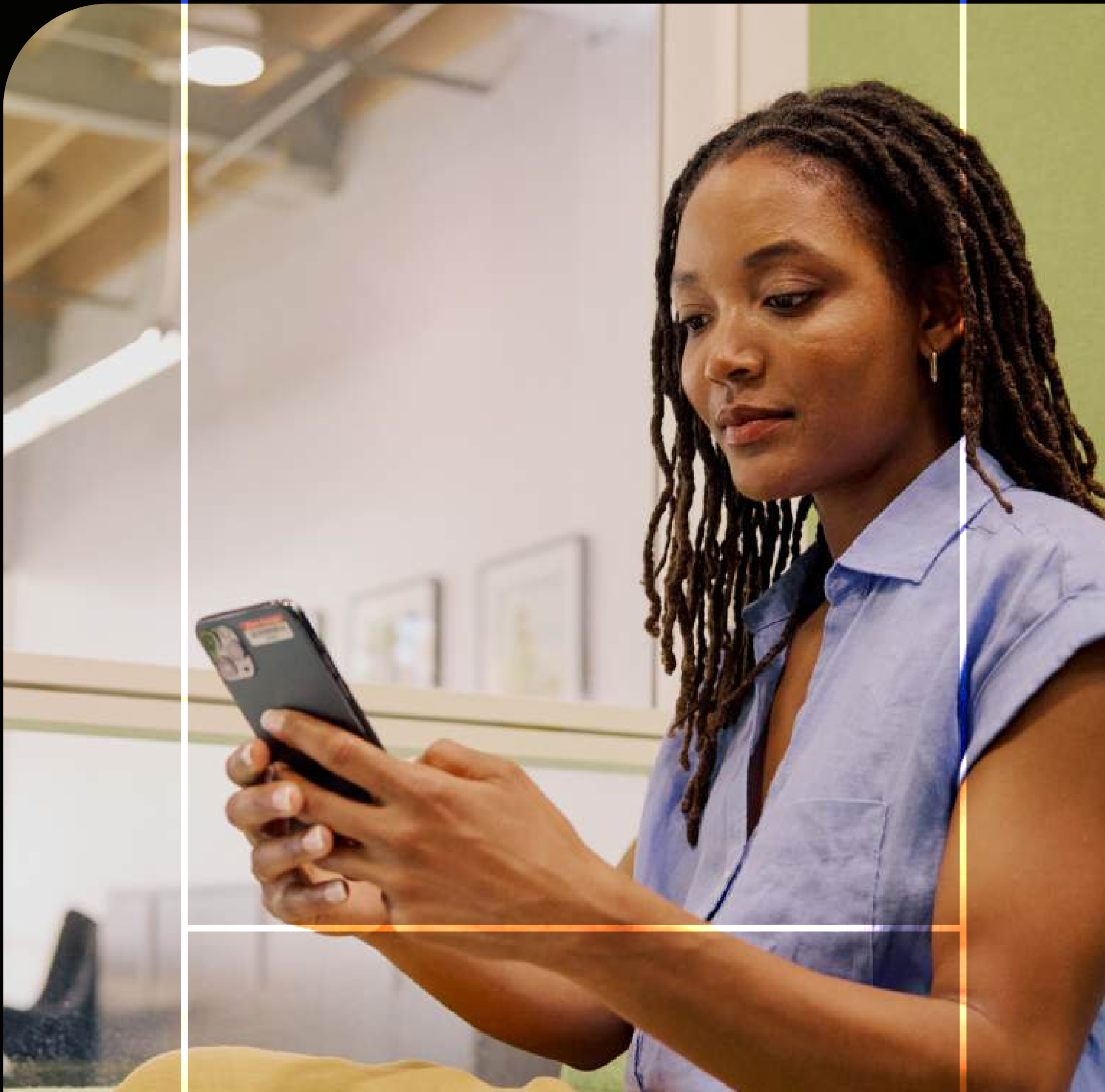
1Password

EBOOK

Why MDM isn’t enough for device security



Contents

Introduction

For years, mobile device management (MDM) solutions have been all but ubiquitous in corporate cybersecurity – often considered the primary or even singular tool necessary to secure a company's devices. Devices enrolled in MDM are commonly referred to as "managed," which reflects the tendency of companies to consider a device functionally secure as long as it has MDM installed. Yet, there are serious security concerns that MDMs cannot manage at all.

If an IT or security professional wants to find every Mac in their fleet with System Integrity Protection disabled and require users to enable it, MDM cannot help. If they want to find unencrypted SSH keys on developer hard drives and encrypt them, MDM cannot help. The same is true for sensitive files, malicious browser extensions, and a laundry list of other device properties which can expose companies to data breaches and attacks.

And this is to say nothing of the many types of devices not managed by MDMs. Unmanaged devices run rampant in many companies, and introduce enormous risk; Microsoft reported[1] that 92% of successful ransomware attacks originated from unmanaged devices.

Recent years have seen an onslaught of ransomware attacks, phishing schemes, and evolving regulatory and compliance standards. They have also seen new security and compliance challenges posed by remote and hybrid workforces, and the increasing use of personal devices in corporate environments. These changes require IT and security teams to gain more visibility into "unmanaged" devices (those not enrolled in MDM) and call for more robust security on managed devices.

In light of MDM's shortcomings, many security leaders are seeking to shore up their endpoint security by embracing alternative or complementary solutions. Among the most prominent categories is device trust.

This ebook provides an overview of the many factors that companies should consider in securing their end-users' devices, and the relative abilities of MDM and device trust to suit those needs. This analysis underscores a critical insight: Security programs must utilize a variety of tools to protect a company's entire attack surface. Both MDM and device trust are crucial for addressing the diverse risks posed by end-user devices.

Device trust solutions allow admins to enforce device compliance as part of access management; they ensure that a device is both known and in a secure state before it is permitted to access company resources.

[1] Microsoft Digital Defense Report, Microsoft Security Insider, September 2024

What are the differences between MDM & device trust?

MDM and device trust are commonly positioned in contrast to each other, but it's something of an apples-and-oranges comparison. MDM and device trust share overlapping core capabilities, as both offer visibility and control over end-user devices that remotely access company resources. However, even a broad definition of each term reveals foundational distinctions.

MDMs enable IT admins to remotely enforce certain foundational policies on devices like laptops, desktops, and smartphones. MDMs can push certain updates, prevent users from altering baseline security settings, and allow administrators to remotely wipe and lock devices. This helps ensure that devices follow company security policies and can help prove a company's compliance with security and data privacy laws and guidelines.

Device trust solutions for security leaders: to safeguard sensitive company information by ensuring that only secure, compliant devices can access critical resources. To accomplish this, admins install a device trust agent on a user's device, where it continually monitors a device's posture to detect when it has fallen out of compliance. Devices that are missing the agent or are in violation of a company's security policy are blocked from authenticating until the issue is resolved. This ability to restrict access based on whether a device is trusted is why device trust falls under the Zero Trust framework.

Even these definitions come with some caveats, owing to the fact that MDM is an older category and device trust is a newer innovation in security.

MDM is an older technology

MDM has been well established since the early aughts, giving the category time to standardize and mature. While there are certainly differences in the services individual MDM products offer, it's rare to find MDM solutions that lack certain representative features, like the ones we'll be overviewing in this article.

Device trust is continually innovating

Device trust is built on the principles of Zero Trust Access (ZTA), a concept which gained traction in the early 2000s. But device trust has only recently begun building momentum as a solution category within the Zero Trust framework.

As such, there's still a good deal of variation among device trust solutions. All of them meet the two essential requirements of device trust: that a device is both known and in a secure state before it can access protected resources. But different device trust providers use different methods to accomplish these goals, and device trust products have a wider range of capabilities than MDM. Companies looking into device trust will need to do deeper research to ensure that any given product delivers on all their "must-haves."

Since 1Password offers a device trust product, (1Password® Device Trust, as part of the 1Password® Extended Access Management platform) this ebook will use it as an example throughout this discussion.

Large disparities in device telemetry & posture enforcement

Both MDM and device trust collect information on the security posture of devices. But there's a stark difference in the level of detail each product can report – and what they can do with that information.

MDM offers broad oversight

MDMs have fairly limited abilities to report on and enforce device posture, usually by acting as an admin over basic settings. There is some variation in those capabilities between vendors, but some of the most common abilities include:

Restricting access to public Wi-Fi networks	Requiring that screenlock be turned on	Requiring that firewall be enabled
Restricting camera usage	Forcefully installing or uninstalling apps	Pushing out OS updatest
Requiring that a device be password-protected	App management, such as forcing app updates, allowlisting or blocklisting apps, or requiring the use of an enterprise app store	Enforcing disk encryption

MDMs work, in essence, by cutting the user out of the equation, using forceful methods without regard for employee productivity or agency. In the case of OS updates, MDM pushes the updates to end-users and then forcibly restarts their devices to install them. This can be immensely disruptive to employee workflows, reducing productivity at a company-wide scale. And these losses to productivity don't always come with commensurate gains in overall security. MDM can do very little for compliance issues that can't be solved through blunt automation.

That leaves teams with no solution for – or even awareness of – major risks to their fleet, like unencrypted SSH keys, malicious browser extensions, or the storage of sensitive corporate data on devices.

On the whole, MDM was built to provide the kind of broad oversight that was needed when it was first designed. As industry needs have evolved, some enterprise MDM solutions have attempted to achieve more granular data collection through compensatory features like extensions. In practice, such features are complex to access and manage for real-time reporting.

Device trust offers granular insights

Most device trust solutions provide insight that goes beyond the limited telemetry offered by MDM.

For instance, 1Password Device Trust is built using osquery, which allows admins to query their fleets based on thousands of device properties. This lets admins have a complete device inventory with real-time insights into each device's health and security.

For example, when a critical vulnerability is identified in a piece of commonly used software, teams need to ensure that it's patched. With this solution, admins can query their whole fleet to see which machines are running that software. Then, they can configure a Check requiring those users to install the update before they can authenticate again.

The ability to query across thousands of properties lets device trust solutions enforce more varied and granular policies than MDM typically can. 1Password Device Trust comes with 100 pre-built Checks based on common security and compliance concerns. On top of that, it allows admins to write their own custom Checks.

This enables device trust admins to do things like:

- Identify sensitive data on a hard drive
- Ensure the timely deletion of sensitive data
- Detect unsafe browser extensions
- List Mac system extensions
- Detect the storage of plain-text credentials and SSH keys
- Require updates for OS, browsers, and other software
- Require that MDM and EDR tools are present and functioning properly

That list is only a small subset of 1Password Device Trust's capabilities, and device trust solutions can also check for the same baseline telemetry as MDMs.

This level of granularity is possible precisely because device trust doesn't rely on the kind of brute force enforcement of MDM. Most device trust solutions don't attempt to remediate issues themselves, and many rely on end-users to resolve compliance issues. This is a boon for productivity and also enables device trust to function on devices outside the scope of MDM (topics subsequent sections of this piece will explore in more detail).

1Password Device Trust offers granular insights that help teams solve for the risks that MDM can't.

How MDM and device trust meet compliance needs

No single security solution can ensure device compliance with the complex and varied landscape of global regulations and standards. MDM and device trust both bring critical capabilities to the picture.

MDM is a compliance necessity

Compliance standards are a primary driver of MDM's use in the workplace today. This is thanks to its ability to force managed devices, en-masse, into meeting basic levels of compliance.

Most crucial is MDM's ability to remotely lock or wipe devices. This greatly reduces the risk of sensitive data being taken from stolen or lost devices, and is a major asset when securely offboarding employees. This capability is explicitly necessary to pass many compliance audits. Examples include:

PCI DSS requires that compliant companies have various protections related to lost or stolen devices. This includes the requirement that, "If a device is presumed to be lost or stolen, the merchant should immediately disable and securely wipe the device remotely."

ISO 27001:2022 requires the installation of remote wipe capabilities.

HIPAA requires the enablement of remote wipe.

SOC 2 compliance requires that "Policies and procedures are in place to automatically or manually erase or otherwise destroy confidential information that has been identified for destruction."

NIST is not a compliance standard, but a broader set of guidelines that other standards follow. And their guidelines for enterprise mobile device security also recommend remote wipe capabilities.

These compliance requirements mean that MDM is a necessity for most companies once they reach a certain size. Even so, the previously mentioned limitations to MDM's telemetry mean that it is far from enough to achieve total compliance with any one of those standards.

Device trust fills MDM compliance gaps

Most device trust solutions lack the ability to remotely lock or wipe devices. However, the capabilities of device trust make it particularly well-suited to compensate for many of the compliance gaps left by MDM:

PCI DSS requires that processes or mechanisms must be in place to guard against phishing attacks.

ISO 27001:2022 requires that companies "Take proactive measures to prevent data from being leaked," such as "...adequate authorisation techniques." They also require systems to delete downloaded data according to specified timeline retention policies.

HIPAA requires oversight and mapping of data flows across devices.

SOC 2 has confidentiality requirements dictating that companies "Have procedures to identify confidential information when it is created or received" and "Ensure secure destruction of confidential data after retention periods expire."

GDPR and CPRA/CCPA require that companies take steps to ensure that employees do not process protected data "...except on instructions from the controller..."

We'll detail throughout this article how device trust suits these different requirements. And once again, this is far from an exhaustive list.

Compliance and privacy: 1Password Device Trust is built on the principles of honest security. This is why we include a privacy dashboard for each employee that shows what data our agent collects, and its potential impact on user privacy. This can help companies prove their commitment to meeting GDPR and CCPA requirements related to transparency and data minimization.

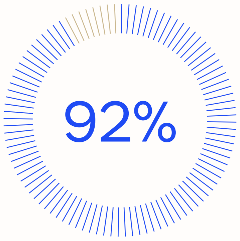
Overcoming MDM's limitations for BYOD & unmanaged devices

MDM and device trust both have a lot to offer company-owned, “managed” devices. But modern companies also have to deal with the threat of unmanaged devices that aren’t enrolled in MDM. 47% of companies in 2023 allowed employees remote access to company resources from completely unmanaged devices.[2]

These unmanaged devices present enormous risk; they might be carrying malware, running outdated software, or belong to bad actors using stolen employee credentials. In fact, Microsoft reported[1] that 92% of successful ransomware attacks originated from unmanaged devices.

MDM can’t secure BYOD

MDM’s capabilities are best suited to company-owned devices, where a company has a right (and even an obligation) to aggressively enforce policy. But there are many devices that fall outside that scope, and on which MDM is either impossible or inadvisable.



92% of successful ransomware attacks originated from unmanaged devices.

BYOD (bring your own device) is a common phenomenon in the modern workplace, but few organizations attempt to deploy MDM onto BYO-devices. Employees are reluctant to accept a tool that can remotely wipe (and otherwise control) a device that they own and use for their personal affairs. Attempts to deploy it can invite pushback from employees and admins alike.

In many ways, MDM’s data wipe capabilities can be as much a compliance problem as a solution. NIST[3] is quite clear that, “Wiping data not owned by the enterprise can cause legal issues.”

Even if a company decides to deploy MDM on personal devices, it will have to contend with additional limitations enforced by MDM vendors. Microsoft Intune’s documentation[4] specifies that “Your organization can view the location of a lost corporate-owned device. They can't view the location of a personal device.”

[2] The Shadow IT Report, Kolide, September 2023, [3] Guidelines for Managing the Security of Mobile Devices in the Enterprise, National Institute of Standards and Technology, May 2023, [4] Intune User Help, Microsoft, January 2025

MDM is also not suited for managing contractor or partner devices. In fact, it may even be impossible – a device cannot be enrolled in more than one MDM at a time, and contractor and partner devices are likely to have another MDM installed.

Finally, MDMs that can cover Linux devices are few and far between, and will often only be able to manage certain Linux distributions. Even then, Linux MDMs often have limited controls over those devices – for instance, some cannot support remote wipe for Linux.

Device trust reduces the attack surface

Device trust solutions offer a less invasive form of management that is suitable for securing personal and contractor devices. Device trust prevents noncompliant devices from authenticating via SSO without subjecting employees to forced updates and remote wipes.

1Password Device Trust offers unique capabilities to reduce many of the fears related to user privacy. Employees are assured that their company can't access any information beyond that which is explicitly listed in users' Privacy Center. This enables companies to securely enable BYOD without compromising either security or privacy.

Still, as popular as BYOD is, it won't suit many organizations. For instance, BYOD is not advised for healthcare settings, where it can add even deeper complications to the already complex task of complying with HIPAA guidelines. In cases like these, device trust enables teams to ban personal devices outright. Admins can refuse registration from devices that aren't company-owned or enrolled in MDM, and block authentication from any device that isn't registered to a user.

Osquery's read-only capabilities also lets 1Password Device Trust provide more comprehensive management for Linux endpoints; it offers Debian and RPM installers for Linux-based systems, and tests that all official Checks work on those devices.

1Password Device Trust offers unique capabilities to reduce many of the fears related to user privacy.

MDM inhibits productivity

Security works best when it succeeds on a cultural and technical level. CISOs famously struggle with finding the right balance between security and productivity since security tools inherently introduce some friction into workflows. But too much friction can impede employee productivity to such a degree that the broader organization suffers. Furthermore, tools that frustrate or antagonize users are likely to drive them toward workarounds like shadow IT.

As such, the end-user experience is a critical element to consider in securing employee adoption and support for security programs.

MDM disrupts workflows

MDM has a well-known tendency to frustrate end-users. Forced updates and device restarts alone are a significant disruption, since nobody likes having their device updated without their permission.

MDM's brute-force approach can also get in the way of users – especially more technical users – doing their jobs. For instance, an engineer might need to temporarily disable their firewall in order to run tests. MDM doesn't give them that option; it works by graying out checkboxes and limiting a user's agency over a device.

This reputation – as well as the aforementioned privacy concerns – often incites resistance from employees when companies roll out MDM. This can result in an uneven and lengthy deployment.

> “
>
> Tools that frustrate or antagonize users are likely to drive them toward workarounds like shadow IT.

A 2022 report published by HAL Open Science[5] summarized the issue: “Studies have indicated that MDM adoption varies among levels and roles of the employees, and successful implementation is influenced by the perceptions of the fairness of the decisions.”

Because of these user-experience drawbacks, MDMs very often have long exemption lists populated with executives who don't want to deal with them. A 2023 survey[2] shows that executives and managers are most likely to use unmanaged devices to access company resources, often to get around obstructive security policies.

[5] Effects of MDM Adoption on Employee in the Context of Consumerization of IT, HAL Open Science, August 2022

Device trust enables productivity without compromising security

Unlike MDM, device trust solutions give admins and users more options than auto-blocking or auto-updating, letting them better account for the nuances of user workflows.

When 1Password Device Trust's agent detects an issue, the menubar app:

🔔	**Proactively notifies users of the issue**
📋	**Gives them detailed instructions on how to fix that issue**
📅	**Tells them how long they have to remediate the problem before they'll be blocked from authenticating**

For instance, if the firewall is disabled on a device, its user will be told how to turn it back on and given a deadline to do so. After that deadline, they'll be blocked from authenticating. But until then, users have the flexibility to remediate the problem on their own time – or to run needed tests before enabling it again.

This flow greatly reduces some of the frustrations that make MDM so controversial among users, allowing them to stay productive while keeping their devices secure.

Device trust solutions give admins and users more options.

The IT admin experience

Endpoint security can only succeed if it serves the needs of administrators. One goal of both MDM and device trust is to give admins some ability to automate the enforcement of security policies across their whole fleet.

On the administrative side, however, MDM and device trust have significant differences in terms of how much work will be needed to manage them.

MDM introduces complexity

The limitations of MDM's telemetry mean that it has limited capabilities for vulnerability management. Expanding those capabilities can represent a significant challenge for admins, who have to write and push out custom shell scripts to oversee critical aspects of their fleet.

A 2022 survey from Samsung Business Insights[6] revealed some telling statistics related to MDM usage. "For more than half of the companies in our survey (53%), management of mobile devices is outsourced (either fully or in part)."

They also pointed out that smaller organizations are more likely to outsource mobile device management, "...likely because they do not have the internal IT expertise to manage and secure devices."

Managing MDM can be challenging and resource intensive. Its rigid enforcement often leads to an uptick in help desk tickets, as users seek exemptions or assistance navigating its complexities.

53%

For more than half of the companies in our survey, management of mobile devices is outsourced.[6]

[6] Maximizing Mobile Value, Samsung, April 2022

Device trust reduces admin burdens

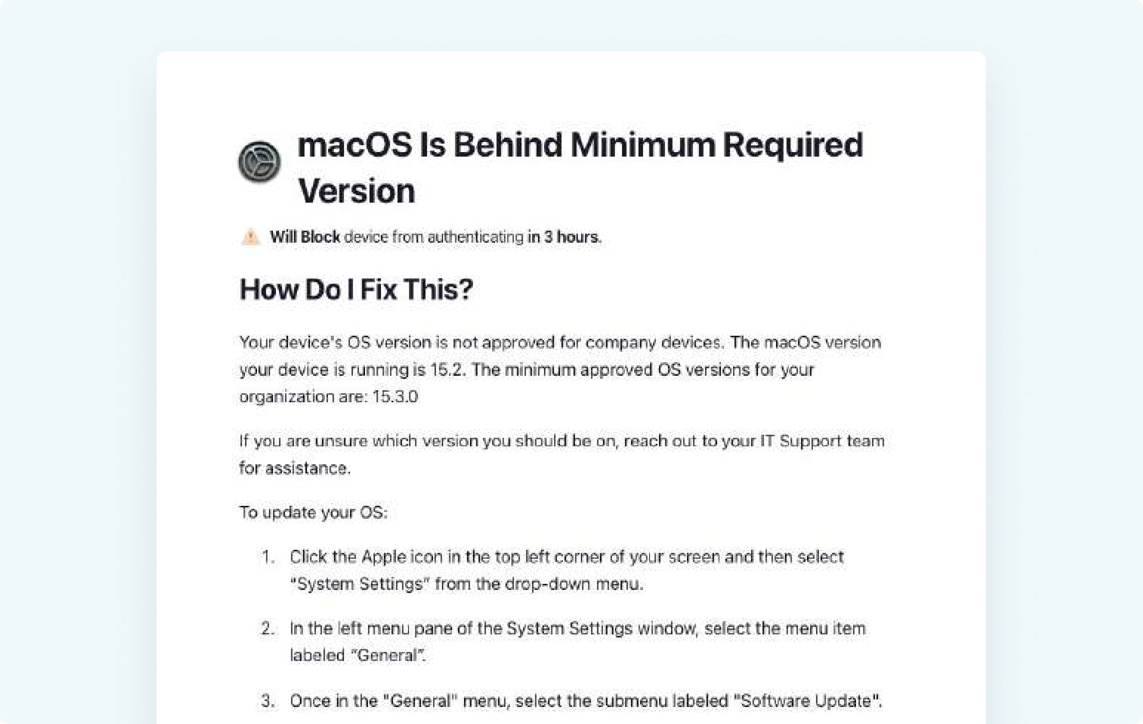
It would be an oversimplification to say that device trust solutions are inherently easier to maintain than MDMs, but they certainly can be. The major differentiator here is how a solution handles end-user blocking, and whether it impedes the productivity of end-users and IT admins.

Many device trust solutions simply block authentication and then direct users to IT in order to get unblocked. This can lead to mountains of support tickets when frustrated users are locked out of their applications.

However, certain device trust solutions – including 1Password Device Trust – offer “end-user remediation,” which provides users with instructions to let them solve issues themselves. This substantially lightens the burden on admins, as users can resolve problems without the need for IT support.

Teams interested in this capability should be sure to examine the specifics of how different device trust solutions achieve it. Many only offer self-remediation instructions for specific issues, or offer limited detail in their remediation instructions, which limits their usefulness. In other words, self-remediation is only effective insofar as it is deeply built into a solution, and not merely treated as an afterthought.

1Password Device Trust writes end-user remediation instructions for all pre-built Checks and requires them for custom Checks. This helps reduce the number of IT support tickets, since employees have agency over their devices and workflows and are never locked out without warning.



macOS Is Behind Minimum Required Version

⚠ **Will Block** device from authenticating **in 3 hours.**

How Do I Fix This?

Your device's OS version is not approved for company devices. The macOS version your device is running is 15.2. The minimum approved OS versions for your organization are: 15.3.0

If you are unsure which version you should be on, reach out to your IT Support team for assistance.

To update your OS:

1. Click the Apple icon in the top left corner of your screen and then select “System Settings” from the drop-down menu.
2. In the left menu pane of the System Settings window, select the menu item labeled “General”.
3. Once in the "General" menu, select the submenu labeled "Software Update".

Deployment challenges for admins & end-users

Once a company has considered what MDM and device trust can offer toward meeting security and compliance goals, they next need to consider the time and effort needed to deploy the solutions across the organization.

MDM deployment is uneven

Deploying MDMs on company-owned devices before they are given to end-users is fairly simple. Part of this is due to the sheer ubiquity of MDM solutions; OS vendors make it particularly easy to ship out devices that are pre-enrolled in their proprietary MDM.

For instance, Apple has Apple Business Essentials and Windows has Microsoft Intune. These allow IT to ensure that certain security features – like each operating system's built-in antivirus or encryption – are enabled by default. IT can pre-configure each device before it's sent out to an employee.

Remote deployment is also possible and most MDM companies provide various options for automatic, manual, self-guided, or even bulk enrollment. But these options are more complex, or may be dependent on other services from the vendor. Either way, enrollment issues are quite common, and at the end of the day, security and IT teams may still not be entirely certain that every device is enrolled and the MDM is working properly.

MDM deployment is uneven and enrollment issues are common.

Device trust requires IdP integration

When it comes to deploying device trust, leadership and admins are likely to lack the familiarity they have with MDM.

Furthermore, device trust only works when it can block authentication, meaning it must interact with a company's identity provider (IdP). 1Password Device Trust achieves this by integrating with SSO providers like Okta. However, the solution can't be deployed to companies that don't use a supported SSO provider

This issue is common across the device trust category. For instance, many other device trust solutions, like Okta's and Cisco's, come bundled with their other identity and access management products. They may even require further integrations; many of Okta's device trust capabilities require that devices already have an MDM installed as a prerequisite.

These dependencies can introduce challenges, but for companies with the necessary infrastructure, device trust is otherwise straightforward to roll out. 1Password Device Trust offers a particularly simple self-enrollment flow for end-users. Teams can even use their existing MDM solutions to automatically push it to managed devices.

1Password Device Trust offers a particularly simple self-enrollment flow for end-users.

Comprehensive security needs complementary solutions

To summarize, MDM is indispensable for enforcing baseline security policies, particularly on company-owned devices. But it's far from a silver bullet, and teams would be mistaken to ignore unmanaged devices or assume that "managed" means secure.

The good news is that MDM doesn't have to do everything, and companies don't need to accept its shortcomings and assume all the risks that come with untrusted devices.

Device trust solutions address challenges that MDM alone cannot resolve. For company-owned devices, they act as a powerful complement, ensuring MDM operates effectively while strengthening security beyond MDM capabilities. In BYOD scenarios, device trust can replace MDM, offering a secure alternative for personal devices.

Ultimately, comparing apples and oranges isn't the best metaphor for endpoint security tools. Comparing MDM to device trust is more like comparing walls and ceilings. If you want to ensure that everything is protected, you'll probably need both.

Want to learn more about how 1Password Device Trust can enhance your existing security solutions? Reach out for a demo!