1Password

BUYER'S GUIDE

How to choose a device security solution

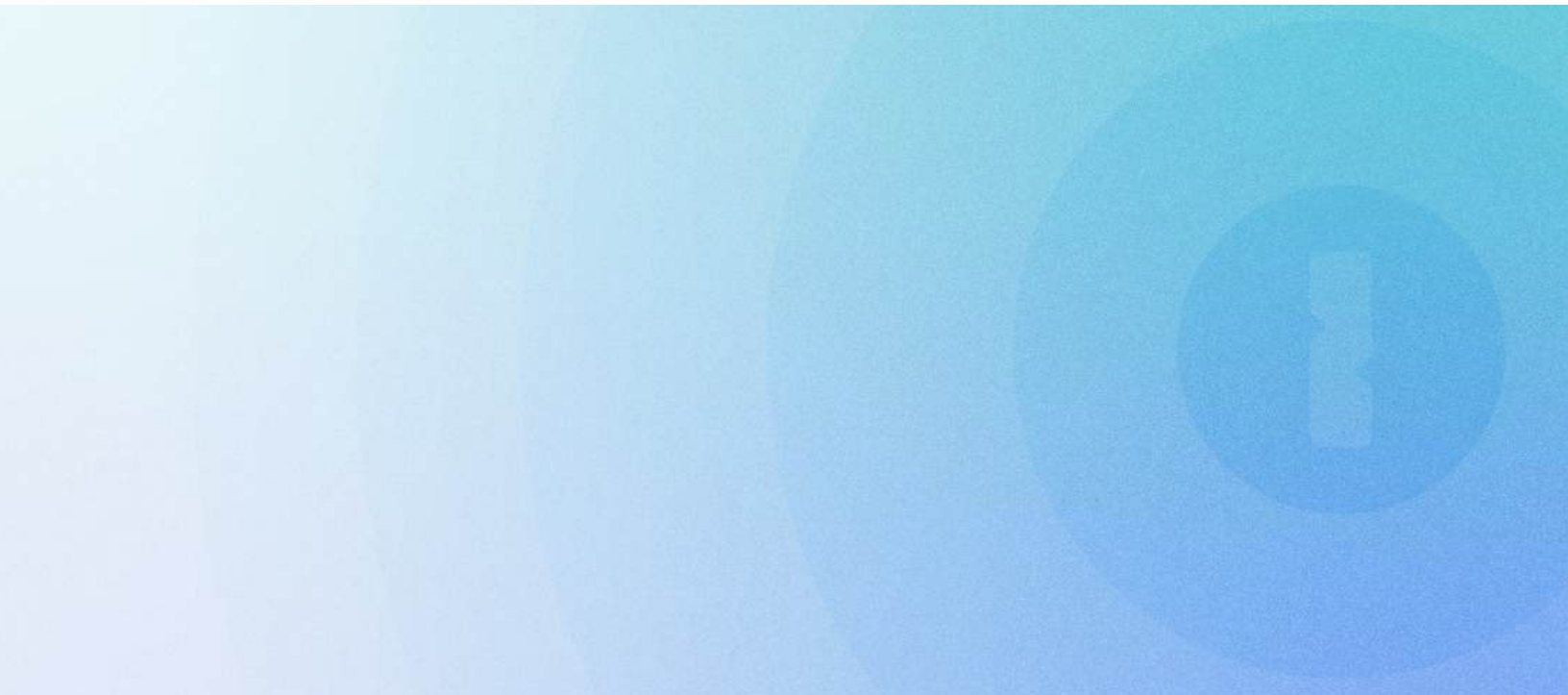

Table of contents

Introduction

Device security is foundational to every cybersecurity program. However, traditional approaches to device security have focused primarily on managing known devices, not necessarily securing them. This approach has left critical security gaps that can be exploited by bad actors. The impact can be significant–in fact, according to Microsoft, 92% of all successful ransomware compromises originate through unmanaged devices (Microsoft Digital Defense Report, October 2024).

In order to address modern device security, there are a variety of requirements that must be addressed in order to secure your organization. These include:

- The ability to manage or secure third-party of BYO (bring-your-own) devices
- Visibility into how data is being accessed or used on devices
- Processes and tools that enhance employee workflows and do not hinder productivity
- Ensuring that managed devices do not fall out compliance or violate company security policy

Traditional approaches to device security fall short of meeting these new requirements, and addressing these challenges must be top of mind as you develop a strategy for securing every device in your organization and when evaluating device security solutions. This guide will walk you through the needs of modern device security and lays out the key requirements when considering device security solutions.

The role of device security in a modern organization

The needs of securing devices have evolved. While traditionally it was enough to manage and secure company-provided devices, the proliferation of BYO devices and flexible work arrangements have fundamentally shifted how organizations need to secure devices. Furthermore, addressing ransomware attacks, phishing schemes, and evolving regulatory and compliance standards have added considerable complexity to device security.

It's not possible for legacy device security products to meet the needs of modern device security. Security teams need Device Trust solutions whether or not they employ MDM solutions, especially when taking third-party or BYOD into consideration. Security leaders must have a comprehensive understanding of device security in totality when evaluating solutions. One good example is how mobile device management (MDM) and device trust play complementary roles in enabling device security.

Why can’t MDM meet all of my needs?

MDM has become a staple for managing devices in many organizations. It is often the first tool adopted when securing a company’s devices. Unfortunately, when it comes to unmanaged and untrusted devices, focusing primarily on MDM leaves significant gaps. For example:

> *If an IT or security professional wants to find every Mac in their fleet with System Integrity Protection disabled and require them 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.*

That is not to say that MDM does not have a role to play in securing an organization's devices. It is simply recognition that organizations must do more than manage corporate devices in order to be secure. Device trust, for example, is focused on ensuring that every device is in a known and secure state before access to company resources is permitted. This is inclusive of unmanaged and BYO devices.

Device trust, and MDM – what’s the difference?	
MDMs enable IT admins to remotely enforce certain foundational policies on devices, such as laptops, desktops and smartphones. MDMs are specifically used on company-managed devices.	**Device trust** enables admins to enforce granular policies and device compliance as part of a broader access management strategy, ensuring that access to corporate data and systems is secure, regardless if a personal or managed device is used.

1 Key requirements for device security solutions

The needs of device security have changed

Modern device security requires going beyond the simple management of corporate devices. Today, device security must incorporate the context of access, verify that only healthy and trusted devices access applications and data, and do all of this while ensuring that employee productivity is not hindered or slowed.

These requirements can best be summed up by focusing on security needs of modern workforce security:

Jobs to be done	Description
Safeguard sensitive company information	Verify that only secure, compliant devices can access corporate resources, whether managed, third-party, or BYOD.
Enforce security best practices	Empower employees to self-remediate and follow organizational security policies consistently and effectively, reducing the risk of data breaches and compliance violations.
Build a security-first culture	Embed security issue self-remediation into everyday employee workflows, turning it immediately into a shared responsibility across teams.
Earn and maintain compliance	Prove your business is security compliant with minimal effort, using policy enforcement and audit reporting.
Proactively mitigate risks	Identify and resolve device and sign-in risks before they escalate. Empower employees to resolve common device and credential issues to reduce the window of opportunity for attackers to exploit weaknesses.
Protect sensitive data and prevent ransomware	Proactively defend against ransomware threats that exploit weak credentials, phishing vulnerabilities, and untrusted devices to gain access to critical systems, applications, and data.

Core requirements for modern security that must be supported by device security solutions.

Breakdown: The needs of device security

Each of these needs can be broken out into specific capabilities that are required in a device security solution. The following section details each need, the capabilities required, and how they contribute towards establishing strong workforce security while also contributing to the needs of modern enterprise security.

Use case	Requirement
Safeguard sensitive customer information	Requires and enforces updates for OS, browsers, and other software
	Detects the storage of plain-text credentials and SSH keys
	Policies - Ensure the platform allows the creation of tailored security policies for specific user groups (e.g., executives, contractors, remote employees)
	Ability to query across thousands of properties to enforce varied and granular policies
Enforce security best practices	Require that MDM and EDR tools are present and functioning prior to authentication
	Provide a path for secure access for third-party and contractor devices
	Control device registration to ensure BYO and Unmanaged devices are not used in specific environments (healthcare, for example)
Build a security-first culture	Enables self-remediation of issues by the employee
	Proactively notifies employees of issues
	Provides employees with detailed instructions on how to fix that issue
	Informs employees on how long they have to remediate the problem before they'll be blocked from authenticating
	Provides security without disrupting workflows or inhibiting productivity
	Security and transparency - visibility into who has access to data on BYO and unmanaged devices

Continues on next page...

Use case	Requirement
Earn and maintain compliance with ease	Automated compliance checks for industry standards like GDPR, SOC 2, PCI DSS, and HIPAA.
	Audit-ready reporting that simplifies compliance.
	Processes/mechanisms to guard against phishing
	Ensure destruction of confidential data after retention period expires
Proactively mitigate risks	Ability to prevent authentication via SSO if devices are non-compliant
	Comprehensive telemetry that tracks device posture, application usage, and access patterns.
	Ability to show or provide consolidated insights to a single dashboard or tool
	Ability to search across an entire fleet to identify vulnerabilities and require necessary updates prior to authentication
Protect sensitive data and prevent ransomware	Proactively defend against threats that exploit: weak credentials
	Proactively defend against threats that exploit: phishing vulnerabilities
	Proactively defend against threats that exploit: access to corporate systems from untrusted and unhealthy devices

Overview of the needs and requirements of device security solutions.

2 Device security: evaluation criteria

The evaluation criteria below are designed to help you meet the device security requirements of a modern workforce. When used as part of the buying process, these requirements will ensure that you have considered the most critical aspects needed for an industry-leading device security tool.

Safeguard sensitive company information

Safeguarding data and other sensitive company information has long been table stakes for security teams. However, due to the challenges of securing every device, especially those not managed by your organization, traditional approaches to device security have left gaps in addressing this fundamental need. As a result, modern device security requires that additional steps be taken to verify that devices are in a secure state before permitting access.

Require updates for operating systems (OSes), browsers, and other software

Requiring that software updates and patches have been implemented is a crucial aspect to securing your organization as new threat vectors are identified. Device security solutions must be able to validate that these updates have been made, and prevent access as necessary when they have not.

Detect the storage of plain-text credentials and SSH keys

Mismanaging credentials and secrets can lead to significant risk to your organization. Understanding where credentials and SSH keys may have been stored in plain-text can enable your security team to take action and proactively mitigate the risk.

The platform allows the creation of tailored security policies for specific user groups (e.g., executives, contractors, remote employees)

Device security solutions need to have granular access controls in order to provide the appropriate levels of security based on the end user. This can be a combination of features, such as role-based access controls (RBAC), automated policy assignment, or granular policy customization.

Ability to query across thousands of properties to enforce varied and granular policies

Given the sheer number of devices many organizations must secure, a device security solution must have the ability to identify issues across thousands of devices, and be able to provide a path towards remediation for each one.

Enforce security best practices

When it comes to device security, it should be no surprise that there are simple best practices that must be followed and can be enabled by a solution. While this seems obvious, some of the best practices can be deceptively difficult. For example, finding a way to secure third-party or contractor devices can be exceptionally challenging.

Require that MDM and EDR tools are present and functioning prior to authentication

MDM and EDR tools are only impactful when deployed and functioning properly on a corporate device. Organizations must be able to validate that these tools are implemented and working properly before access is approved. In the case that the MDM or EDR check fails, organizations must have the ability to stop access from taking place.

Provide a path for secure access for third-party and contractor devices

Third-party and contractor devices represent a significant risk to organizations. Because these devices are not managed by your organization, it is virtually impossible to implement MDM or EDR tools on these devices (much less be able to validate that the device is healthy). Due to the risk associated with unhealthy device access, device security solutions must provide a path for securing access from these devices.

Control device registration to ensure BYO and Unmanaged devices are not used in specific environments (healthcare, for example)

While there has been a rise in the use of BYO devices, there are specific cases where unmanaged devices cannot be used. Device security requires the flexibility to secure unmanaged and BYO devices–but also prevent their usage where necessary.

Build a security-first culture

Building a security-first culture is a cornerstone of modern cybersecurity. In the case of device security, the focus must be on solutions that empower your employees to self-remediate issues on their devices. By taking this approach, security teams are able to reduce the strain felt by their department, while also enabling employees with the flexibility to adhere to security updates in a way that doesn't impede productivity.

Enables self-remediation of issues

Empowering employees to self-remediate reduces reliance on IT and security teams while al so providing front-line defense and ownership of security issues. This is especially true as it relates to personal or BYO devices, where your organization may not provide a direct line of support to remediate issues.

Proactively notifies employees of issues

When an issue is discovered, the device security solution must immediately notify employees that their device has been flagged as unhealthy and either restrict or allow access depending on the policies you set.

Provide employees with detailed instructions on how to fix that issue

It is imperative that employees be provided with guided instructions on how to remediate issues when they occur. The instructions must be clear, concise, and provide a path to secure access in the event that access is blocked as a result of the issue.

Informs users on how long they have to remediate the problem before they'll be blocked from authenticating

Employees must be informed about how long they have to remediate any issues before access will be blocked. While not always possible, giving users adequate time to address issues empowers them to become secure when it is most convenient for the employee and not hinder productivity.

Provides security without disrupting workflows or inhibiting productivity

Device security solutions must enable employees to be secure while not being a hindrance to workflows and productivity. It is critical to understand the employee experience and the impact that security tools will have on productivity.

Security and transparency - visibility into who internally has access to data on BYO and unmanaged devices

Employee privacy is paramount, especially when considering security on personal devices. Providing transparency into who has access to data on the device, and what data they have access to, is critically important to employee adoption of device security solutions.

Earn and maintain compliance

Earning and maintaining compliance is a pillar of every cybersecurity strategy. When it comes to devices, there are a variety of requirements that must be met in order for your organization to be compliant. While the specific requirements may differ based on your industry or location, the below are high-level requirements that should be considered when evaluating device security solutions.

Automated compliance checks for industry standards like GDPR, SOC 2, PCI DSS, and HIPAA

Device security tools need to continuously monitor and evaluate a device's configuration, software, and access controls against predefined compliance standards. These checks ensure that devices meet the security and privacy requirements mandated by these regulations.

Audit-ready reporting that simplifies compliance

Audit-ready reporting provides clear documentation of device security posture and compliance status. This helps to reduce the time and effort spent on audits.

Processes/mechanisms to guard against phishing

While many mechanisms are required to address phishing, device security solutions can help to address it by providing features such as two-factor authentication (2FA) or identifying passwords and replacing them with phishing-resistant passkeys.

Proactively mitigate risks

Proactive mitigation is designed to find and stop cybersecurity issues before they escalate. In terms of device security, proactively mitigating risks is focused on identifying unhealthy or non-compliant devices, and enabling the appropriate remediation steps to be taken before your corporate systems can be compromised.

Ability to prevent authentication via SSO if devices are non-compliant

In the event that a device is found to be unhealthy, device security solutions must be able to block access to corporate applications that are available via SSO. Allowing access to these applications while the device is unhealthy can create a risk of breach or compromise.

Comprehensive telemetry that tracks device posture, application usage, and access patterns

Device security solutions must provide telemetry across thousands of devices. In addition, this telemetry must provide granular insights into posture, application usage, and access patterns.

Ability to show or provide consolidated insights to a single dashboard or tool

Device security solutions must provide visibility into common security and compliance metrics in order to provide insight into the overall security posture of devices.

Ability to search across an entire fleet to identify vulnerabilities and require necessary updates prior to authentication

Device security tools must have methods for security teams to identify vulnerabilities across their entire fleet. Furthermore, should a vulnerability be found, the tool must be capable of preventing authentication until the issue is remediated.

Protect sensitive data and prevent ransomware

According to Microsoft, 92% of successful ransomware attacks originate from unmanaged devices. Due to this risk, any approach to device security must consider how organizations can protect themselves and their data from ransomware attacks.

Proactively defend against threats that exploit access to corporate systems from untrusted and unhealthy devices

Organizations must have the ability to dynamically verify the security status of each device at the time of access, and only approve access if the device is healthy and trusted.

Proactively defend against threats that exploit weak credentials

According to Verizon, credentials are responsible for 38% of breaches. Device security requires tools that enable employees to easily create, manage, and store strong credentials.

Proactively defend against threats that exploit phishing vulnerabilities

Device security solutions must provide mechanisms or processes to guard against phishing attacks.

3 Checklist and questions

Comparison Checklist

Use case	Requirement	Device Trust (1Password XAM)	MDM (MS Intune, Google Workspace)
Safeguard sensitive customer information	Requires and enforces updates for OS, browsers, and other software	✓	✓
	Detects the storage of plain-text credentials and SSH keys	✓	✗
	Ensure the platform allows the creation of tailored security policies for specific user groups (e.g., executives, contractors, remote employees)	✓	✗
	Ability to query across thousands of properties to enforce varied and granular policies	✓	✗
Enforce security best practices	Require that MDM and EDR tools are present and functioning prior to authentication	✓	✗
	Provide a path for secure access for third-party and contractor devices	✓	✗
	Control device registration to ensure BYO and Unmanaged devices are not used in specific environments (healthcare, for example)	✓	**Limited**
Build a security-first culture	Enables self-remediation of issues by the employee	✓	✗
	Proactively notifies employees of issues	✓	✗
	Provides employees with detailed instructions on how to fix that issue	✓	✗
	Informs employees on how long they have to remediate the problem before they'll be blocked from authenticating	✓	✗
	Provides security without disrupting workflows or inhibiting productivity	✓	✗
	Security and transparency - visibility into who has access to data on BYO and unmanaged devices	✓	✗

Continues on next page...

Use case	Requirement	Device Trust (1Password XAM)	MDM (MS Intune, Google Workspace)
Earn and maintain compliance with ease	Automated compliance checks for industry standards like GDPR, SOC 2, PCI DSS, and HIPAA	✓	Limited
	Audit-ready reporting that simplifies compliance	✓	✗
	Processes/mechanisms to guard against phishing	✓	✗
Proactively mitigate risks	Ability to prevent authentication via SSO if devices are non-compliant	✓	Limited
	Comprehensive telemetry that tracks device posture, application usage, and access patterns	✓	✗
	Ability to show or provide consolidated insights to a single dashboard or tool	✓	✓
	Ability to search across an entire fleet to identify vulnerabilities and require necessary updates prior to authenticationAbility to search across an entire fleet to identify vulnerabilities and require necessary updates prior to authentication	✓	Limited
Protect sensitive data and prevent ransomware	Proactively defend against threats that exploit: weak credentials	✓	✗
	Proactively defend against threats that exploit: phishing vulnerabilities	✓	✗
	Proactively defend against threats that exploit: phishing vulnerabilities	✓	Limited

Questions to ask vendors

Based on the defined evaluation criteria, there are a variety of questions that are critical to answer when evaluating device security solutions. Every vendor included in the evaluation process should answer these questions and provide a detailed response to how their specific platform can address each use case.

Use case	Questions to ask vendors
Safeguard sensitive customer information	Can the platform require and enforce updates for operating systems, browsers, and other software?
	Can the platform prevent access to applications and data if trust fails?
	Does the platform support custom access controls for specified groups (executives, contractors, partners, etc.)?
	Can the platform find vulnerabilities and enforce granular access policies across thousands of properties and devices?
	Does the platform have dynamic access controls that take the context of access into account at the time of authentication?
Enforce security best practices	Can the platform verify that MDM and EDR tools are present and functioning prior to authentication?
	Does the platform provide a path for secure access for third-party and contractor devices?
	Does the platform respect employee privacy and prevent access to personal information?
	Does the platform control device registration to ensure BYO and unmanaged devices are not used in specific environments (healthcare, for example)?
Build a security-first culture	Does the platform enable self-remediation of issues by the user?
	Can the platform proactively notify users of issues?
	Does the platform provide users with detailed instructions on how to address issues?
	Does the platform inform users of how long they have to remediate the problem before they'll be blocked from authenticating?
	Can the platform provide security without disrupting workflows or inhibiting productivity?
	Does the platform provide transparency, and provide users with visibility into who has access to data on BYO and unmanaged devices?

Continues on next page...

Use case	Questions to ask vendors
Earn and maintain compliance with ease	Does the platform provide automated compliance checks for industry standards like GDPR, SOC 2, PCI DSS, and HIPAA?
	What audit-ready reports are available for compliance purposes?
	Does the platform have mechanisms to guard against phishing?
Proactively mitigate risks	Can the platform prevent authentication via SSO when devices are non-compliant?
	Does the platform provide comprehensive telemetry that tracks device posture, application usage, and access patterns?
	Does the platform have the ability to show or provide consolidated insights to a single dashboard or tool?
	Can the platform search across an entire fleet to identify vulnerabilities and require necessary updates prior to authentication?
Protect sensitive data and prevent ransomware	Can the platform proactively defend against threats that exploit **weak credentials?**
	Can the platform proactively defend against threats that exploit **phishing vulnerabilities?**
	Can the platform proactively defend against threats that exploit **access to corporate systems from untrusted and unhealthy devices?**

4 Device security: How 1Password helps

1Password Device Trust ensures that every device is known, secure, and compliant before allowing access to your corporate applications. In addition to validating the health of managed devices, 1Password Device Trust enables security teams to extend that validation to unmanaged and BYO devices.

With 1Password Device Trust you can:

- See an inventory of all corporate and BYO devices used by your team.
- Check the health and compliance of all devices accessing your applications from a single dashboard.
- Block access to apps based on device health checks. Choose from a library of more than 100 pre-written device checks, or write your own.
- Provide your team with self-serve remediation instructions. Empower team members to resolve issues with their devices on their own without help from IT.

1Password Device Trust is part of the 1Password Extended Access Management platform. When fully deployed, the platform provides your security team with a comprehensive security solution that secures access from any device, to any application, from any location.

A note on 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.

5 Conclusion

Securing the modern workforce has become a major challenge for every organization. As a result, it's had a major impact on how devices must be secured going forward. While traditional tools like MDM have a role to play, fully implementing device security means going beyond simply managing corporate devices. Today, organizations must take a comprehensive approach to device security inclusive of unmanaged and BYO devices. The path forward is to embrace device trust and ensure that access to your corporate systems only comes from secure, healthy devices.

Want to see how 1Password can support your device security needs? Register for a demo today.

1Password

Trusted by over 150,000 businesses and millions of consumers, 1Password offers identity security and access management solutions built for the way people work and live today. 1Password is on a mission to eliminate the conflict between security and productivity while securing every sign-in for every app on every device. As the provider of the most-used enterprise password manager, 1Password continues to innovate on its strong foundation to offer security solutions relied upon by companies of all sizes, including Associated Press, Salesforce, GitLab, Under Armour, and Intercom.

Learn more about 1Password.