1Password

WHAT IS 1PASSWORD EXTENDED ACCESS MANAGEMENT?

The Business Case for Extended Access Management

Securing access across every device and app

With the **1Password Extended Access Management** platform, you can address the challenges of shadow IT applications, untrusted MDM devices, and BYO-devices by verifying every sign-in is trustworthy and compliant.

Security teams need to ensure that only trusted users on secure devices can access business applications and data. However, traditional Identity and Access Management (IAM) and Mobile Device Management (MDM) tools fall short – they can't dynamically assess device health, evaluate contextual risks, or enforce compliance every time a user accesses business applications and data.

With 1Password Extended Access Management, security and IT teams gain granular access control over every device and SaaS app. Gain real-time insights into your organization's security and compliance stance, and solutions to enforce modern authentication methods like device trust, passkeys, and MFA. By securing access across every device and app, 1Password empowers security and IT teams to focus on high-priority work while safeguarding your company's most critical assets.

The 1Password Extended Access Management Platform Benefits

Our Extended Access Management Platform is designed to enable employees to be productive while also securing every sign-in, to every application, from any device.

With our platform	Without 1Password Extended Access Management
Empower employees to securely use the tools and devices they need to be most productive.	Restrict employees to IT-approved tools that are slow to pass security reviews and SSO integration.
Secure all applications, including managed, shadow IT, and legacy applications.	Leave non-IT-managed apps unprotected and vulnerable.
Ensure the health of all devices, whether company-managed, unmanaged, or employee personal devices, and block or limit access attempts from untrusted devices.	Allow unhealthy or unverified devices to access sensitive data when using traditional IAM tools.
Allow only healthy devices to access applications, unlike IAM tools that cannot limit access from unhealthy devices.	Use of traditional IAM tools lack enforcement for device security, increasing exposure to threats.
Facilitate the transition from passwords to passwordless to reduce credential risk and improve employee experience.	Treat passwordless as a goal without visibility into which apps can move toward passkey or passwordless alternatives.
Earn and maintain security compliance with ease using policy enforcement and detailed audit reporting.	Struggle with manual audits, inconsistent policy enforcement, and compliance gaps.
Proactively mitigate risks by identifying, resolving, or blocking risks before they escalate.	React to security incidents after they've already caused damage.
Deliver an elegant, simple user experience that encourages employees to self-remediate and secure devices.	Rely on complex processes that employees bypass, risking business data on unsecured personal devices.

How 1Password can secure every sign-in to every application from any device

Fill in this section with examples of how 1Password Extended Access Management will support your business initiatives related to modern workforce security.

Business Outcomes	Potential Business Impact	What challenge is your organization experiencing?	Industry Proof Points
Example: Identify and resolve device and credential risks before they escalate	Reduce data breach likelihood rate by up to 22%.	IT teams lack insights to prioritize security vulnerabilities and are bogged down, delaying their response to critical threats which could lead to data breaches.	In 92% of cases where attacks progressed to the ransom stage, the attacker had leveraged unmanaged devices in the network. Source: Microsoft Digital Defense Report, Microsoft Threat Intelligence, October 2024). 68% of breaches involved a human element such as compromised user credentials or phishing. Source: Verizon Data Breach Report, May 2024.
Example: Enforce device compliance across your workforce	Reach 90% of devices adhering to compliance mandates using 1Password Device Trust policies.	Our IT and security teams are unable to consistently enforce OS versions, improve device security configurations, and align those policies with compliance mandates.	46% of employees don't update software immediately due to work interruptions, with 73% attributing the delay to being too busy or not wanting to disrupt their workflow. This delay in updates heightens risks on both personal and work devices. Source: Balancing Act: Security and Productivity in the Age of AI, 1Password, April 2024.
Example: Build a culture of security with self-remediation	Reduced IT workload and faster resolution of security risks with employee self-remediation.	Employees don't adhere to security best practices and are unable to resolve sign-in and device compliance issues, leading to IT bottlenecks.	62% of IT and security professionals report experiencing burnout due to reactive work environments, including addressing issues that could be self-remediated by employees. Source: Gartner Peer Community Survey, 2023.

Cost of doing nothing vs using 1Password

This table compares three scenarios for managing device compliance, data breach risk, IT support tickets, and overall security costs: doing nothing, hiring additional full-time employees (FTEs), or implementing 1Password. Use this data to assess your own organization's security posture and potential cost savings. In the "Your Impact" column, estimate how your organization could benefit from 1Password's Extended Access Management capabilities based on your current security and IT costs.

	Do nothing	Hire FTEs	Use 1Password (Example)	Your impact
Device compliance	No improvement; ~50% device compliance	Increase to ~70% device compliance	Reach up to 90%+ device compliance [1]	
Data breach risk from credentials [2]	Breach likelihood remains at 27%	Breach likelihood reduced from 27% → 15% 12% x $4.88M = $450K	Breach likelihood reduced by 22% (27% → 5%) 22% x $4.88M = $1.074M	
End user IT support tickets	~600 tickets/ month	Reduce tickets by 10%	Reduce IT tickets by up to 70% [3]	
Expense	$0 additional cost	~500k / year	~$150K/year	
Return	$0	~$450K/year saved from breach reductions	~$1.5M/year saved from breach and compliance costs	
ROI [4]	$0	-10%	900%	

Assumptions

[1] Assumed constant at $300K/year

[2] Breach savings formula: Breach savings = Likelihood reduction x IBM's Average Cost of a Data Breach

[3] Forrester Total Economic Impact of 1Password Business.

[4] ROI Formula: ROI = Return [Savings-Cost] x 100. Example for 1Password: Return=$1.374M - $150K=$1.224M and ROI=($1.224M/$150) x 100 = 900%

Conclusion

1Password is the ideal security provider for every organization. The 1Password Extended Access Management platform reduces risk by minimizing attack surface and helps you maintain compliance, instilling confidence in meeting or exceeding regulatory requirements. It empowers IT and security teams to focus on strategic priorities while enabling employees to work securely and resolve issues independently, enhancing efficiency and productivity.

For more information about how 1Password can support your security needs, please reach out to your sales representative or contact us.