1Password

10 access management risks and how to overcome them

Practical security strategies for busy teams

Small and midsize businesses (SMBs) face many of the same cybersecurity challenges as giant enterprises; you're expected to protect sensitive data, manage secure access, and ensure compliance, all without hindering productivity. The only difference is that you have to achieve all these goals with a lean IT team and a limited budget, because neither the customers who trust you with their data nor the bad actors trying to steal it are grading on a curve.

So, in this guide, we'll explore the top 10 access risks that small businesses face today, including credential vulnerabilities, insecure devices, and uncontrolled app use. You'll also learn practical, achievable strategies to mitigate these risks – and discover how **1Password Extended Access Management** can help you achieve these goals.

10 Access Management Risks for SMBs and the costs of ignoring them

One of the most prominent areas where risk presents itself is access management. Access management is how you control who has access to which systems in your organization, and how that access is secured. Unsurprisingly, access management is an area of high security risk, especially for SMBs.

10 SMB access management risks

1. Stolen or compromised credentials
2. Weak passwords that AI can successfully guess
3. Lack of multi-factor authentication (MFA)
4. Risky credential storage and sharing practices

Credential risks

5. Employees can download anything to their devices
6. Endpoint protection is insufficient
7. Unpatched devices are susceptible to hackers

Device security risks

8. Unauthorized applications and AI use
9. Inability to track or audit who has access to what
10. Inability to fully offboard employees from applications and tools access permissions

Application risks

These risks can be segmented into three distinct categories: credential risks, device risks, and application risks. Let's break them down.

Credential risks

Weak, reused, AI-guessable, or compromised passwords make it easy for attackers to slip quietly into your systems and steal sensitive information or disrupt your operations.

Multi-factor authentication (MFA) is designed to mitigate password-related risks by adding a stronger form of authentication (like biometrics or one-time codes) into logins, but is often not used where it is available. Add to that the common but risky practice of sharing credentials via spreadsheets, emails, or chat apps, and it becomes that much easier for attackers to expand their foothold, and that much harder for IT to centrally govern access for employees.

1. **Stolen or compromised credentials**
   An attacker uses stolen credentials to gain unauthorized access to systems.
   Impact: Breaches, financial loss, and compromised sensitive data.

2. **Weak, common, or default passwords that AI can successfully guess**
   Easy-to-guess or default passwords that make it easy for attackers to gain unauthorized access.
   Impact: Increased vulnerability to phishing attacks and unauthorized access.

3. **Lack of multi-factor authentication (MFA)**
   Relying solely on a password to sign in, making it simple for attackers to gain access to systems.
   Impact: Easier exploitation of stolen or weak credentials.

4. **Poor credential storage and sharing practices**
   Storing or sharing passwords in unsecured ways, like spreadsheets, emails, or chat apps, making it easy for attackers or unauthorized users to gain access.
   Impact: Easier lateral movement and the ability for employees to retain access over time, such as after employment ends or a new role is taken.

Device security risks

Device security is another area where small businesses struggle to enforce policies. Bring-your-own-device (BYOD) policies introduce significant vulnerabilities, since these devices often lack basic security safeguards, and can be ideal targets for ransomware, malware, or unauthorized access. But even company-owned and managed devices can be at risk, since patch management is challenging for IT teams using traditional tools like mobile device management (MDM).

5. **Employees can download anything to their devices**
   Description: Personal devices used for work purposes without IT or security oversight.
   Impact: Unsecured and potentially compromised endpoints accessing sensitive company data.

6. **Endpoint protection is insufficient**
   Description: Managed devices used for work purposes are missing the checks to ensure that they are secure and trusted.
   Impact: Increased exposure to ransomware and malware.

7. **Outdated or unpatched devices**
   Description: Devices and the software on them haven't been updated or patched, and may become easy targets for attackers.
   Impact: Susceptibility to known vulnerabilities and exploits.

Application risks

> The challenge of access management has intensified with the explosion of software-as-a-service (SaaS) apps, often referred to as app sprawl.

Employees adopt new tools faster than admins can track them or secure them, leading to a rise in shadow IT and shadow AI – unauthorized apps that can contain sensitive and unprotected data, outside the visibility or control of IT. Without clear visibility, IT can't effectively manage software licenses or employee access to them, which hurts both security and budgets. On top of that, overly broad or mismanaged permissions give employees far greater access than they actually need, heightening the risk of data leaks and regulatory violations.

8. **Unauthorized applications and AI use**
   Description: Employees use unapproved applications or AI tools without IT or security's knowledge.
   Impact: Increased risk of breaches from unmonitored software and loss of control of corporate data.

9. **Inability to track or audit who has access to what**
   Description: IT and security teams can't track who is using which app when, making it more difficult to meet compliance requirements.
   Impact: Difficulty ensuring compliance.

10. **Inability to fully offboard employees from applications and tools**
    Description: Lack of visibility into all of the applications an employee has access to makes it difficult to ensure that each employee is fully offboarded when they leave a role or company.
    Impact: Data leaks, unauthorized access, compliance issues.

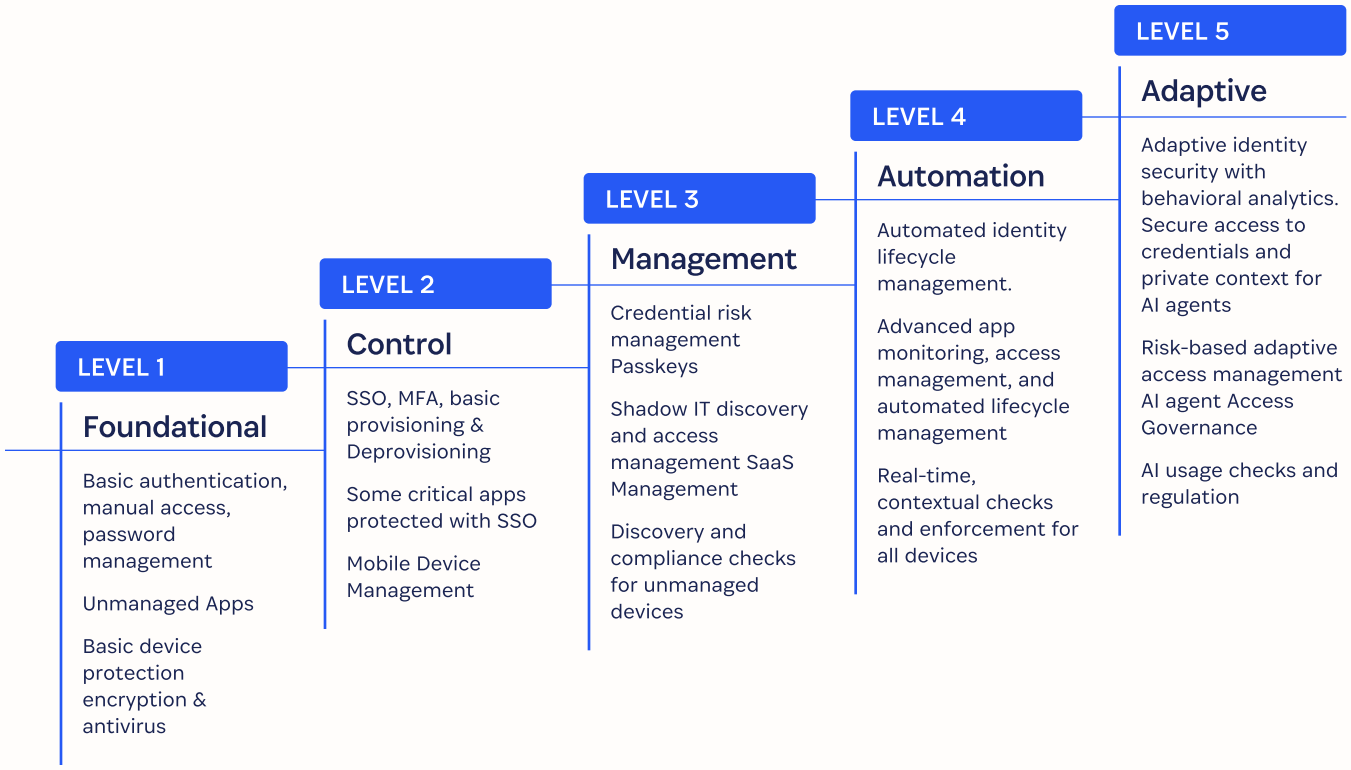
How to reduce risk with the 1Password Security Maturity Model

The path to strong security is a journey, and every step forward matters. Not every organization will be starting from the same place – and that's okay. Whether you're just getting your credential management practices in order, or already automating access controls, there are steps you can take to improve your security posture.

The good news? You don't need a large team or enterprise-grade budget to make meaningful progress. With the right tools in place, you can improve security without adding complexity for your IT team or friction for your employees.

The 1Password Security Maturity Model

1Password's Security Maturity Model outlines five levels of progression, from foundational to adaptive. This model was developed based on 1Password's experience working with more than 165,000 businesses and seeing how organizations move along this journey.



How to use the 1Password Security Maturity Model

The 1Password Security Maturity Model is intended to highlight the challenges you'll face from an identity, application, and device perspective as your organization grows. It should be used as a reference point for the steps you need to take to progress your security journey.

At **Level 1 (Foundational),** many teams rely on manual processes and basic tools: individual passwords managers, unfederated apps, antivirus software. But this setup is fragile, especially as your company scales or compliance requirements tighten.

The first big leap happens at **Level 2 (Control),** where SMBs begin to adopt single sign-on (SSO), enforce multi-factor authentication (MFA), and centralize provisioning and deprovisioning. Some apps may be protected, and a mobile device management (MDM) tool might be in place, but visibility is still limited, and gaps remain. Shadow IT continues to be a blind spot.

Progressing to **Level 3 (Management)** means shifting from reactive to proactive. Credential risk management becomes a priority. Teams start rolling out passkeys and reducing password reliance. You begin discovering which applications are being used (and by whom), and expanding access controls like SSO beyond your critical systems. Device security matures too: you're not just managing phones or laptops anymore – you're assessing the security posture of every device accessing your data, including personal or unmanaged ones.

At **Level 4 (Automation),** you introduce more advanced controls. Identity and access lifecycles become automated via tools that grant and revoke permissions with minimal manual interventions. Applications are continuously monitored for misuse or abnormal behavior. Devices undergo real-time, contextual security checks, and enforcement is dynamic and triggered by risk, not just static rules.

Today, few SMBs reach **Level 5 (Adaptive)** unless they work in highly specialized sectors such as defense, but this stage represents the future of access security: behavioral analytics, AI-aware governance, and risk-based controls that evolve as your organization grows.

Mitigating risk with 1Password Extended Access Management

Thus far, we've talked about the threats faced by small businesses, and outlined a pathway to addressing them as your company grows and matures. Now, we're going to talk about concrete solutions that can meet you where you are and address the most urgent access management risks your company faces. 1Password Extended Access Management enables your SMB to secure every sign-in, to every application, from any device your team uses. It’s composed of three products, each designed to solve credential, device security, and application risks:

Product	Risk addressed
Enterprise Password Manager	• Stolen or compromised credentials • Weak passwords that AI can successfully guess • Lack of multi-factor authentication (MFA) • Risky credential storage and sharing practices
1Password Device Trust	• Employees can download anything to their devices • Endpoint protection is insufficient • Unpatched devices are susceptible to hackers
Trelica by 1Password	• Unauthorized applications and AI use • Inability to track or audit who has access to what • Inability to fully offboard employees from applications and tools

Credential Risk Management with 1Password Enterprise Password Manager

Rolling out 1Password's Enterprise Password Manager (EPM) to your workforce is one of the simplest and most impactful steps you can take to secure access management – regardless of your company's maturity level. Instead of relying on employee memory or risky spreadsheets, your entire team can securely store, manage, and autofill strong, unique passwords across every application and website.

EPM not only secures passwords, it sets your team up for the next stages of credential security – identifying opportunities to implement MFA, enabling the transition to passkeys, and proactively identifying passwords that have been compromised in other breaches.

- Easily generate, store, and autofill unique passwords, eliminating risky credential management practices.
- Add multi-factor authentication to sign-ins across your organization effortlessly, significantly reducing risks from compromised credentials.
- Administer scalable password policies quickly and verify compliance at a glance.
- **Interactive demo:** Experience how 1Password EPM address credential risk management

Instead of relying on employee memory or risky spreadsheets, your entire team can securely store, manage, and autofill strong, unique passwords across every application and website.

Device Security with Device Trust

1Password Device Trust ensures that only **known, healthy,** and **compliant** devices can access your business apps. Devices failing critical security checks – such as outdated software or missing antivirus protection – are warned or blocked until users fix identified issues via clear, guided remediation steps. This automated self-remediation approach ensures minimal disruption for both end-users and IT, keeping your employees productive while significantly reducing your device-related risks.

1Password Device Trust ensures that only known, healthy, and compliant devices can access your business apps.

For SMBs, 1Password Device Trust can fulfill multiple functions at multiple maturity levels. If your organization has not invested in an MDM solution, device trust can help ensure compliance. But 1Password Device Trust also complements MDM, in that it can secure BYOD and provide richer, more comprehensive health checks than MDM alone.

- Gain real-time visibility across all managed and bring-your-own (BYO) devices.
- Use the library of over 100 posture checks and design your own custom checks to inspect operating system version, antivirus status, patch levels, and more.
- Block unhealthy devices from authenticating, and provide users with self-serve remediation steps to get back to work quickly.
- With Device Trust Connect, integration with popular IdPs like Okta, Microsoft Entra, and Google Workspace lets you gate all SSO sign-ins.
- Device Trust Core extends protection even to non-SSO web apps – any browser-based authentication attempt triggers posture checks via the 1Password extension.
- **Interactive demo:** Learn how 1Password Device Trust enables device security

App Visibility & Governance with Trelica by 1Password

Trelica by 1Password discovers and catalogs every app used across your organization, whether officially approved or unsanctioned shadow IT. With 350+ integrations, Trelica provides granular and automated control over app access and permissions, automatically aligning access rights to roles and responsibilities.

Trelica by 1Password discovers and catalogs every app used across your organization, whether officially approved or unsanctioned shadow IT.

Trelica by 1Password enables you to get to management (level 3) and beyond. It provides intelligent license management and helps uncover unused or redundant software, instantly reducing unnecessary spend. Compliance audits become simpler, too, with comprehensive activity tracking and detailed reporting readily available for SOC 2, GDPR, and other regulatory frameworks.

- Trelica by 1Password discovers all SaaS apps – managed and unmanaged – across your organization, giving you complete visibility into shadow IT.
- With over 350 direct integrations to identity, HR, finance, and app platforms, Trelica automates provisioning and de-provisioning workflows tied to personnel changes.
- Intelligent license management uncovers unused or redundant apps, helping reduce unnecessary spend.
- Automated onboarding, offboarding, and approval flows reduce risk from overly broad permissions.
- All activity is audited and tracked, streamlining compliance with SOC 2, ISO 27001, DORA, and GDPR.
- **Interactive demo:** See the visibility provided by Trelica in 1Password

Take Control of Your Business' Security

Mitigating access risks doesn't have to be complicated. By adopting clear security strategies and leveraging the right tools, your business can stay secure, compliant, and efficient.

Ready to secure and simplify your security management?

Request a Demo to see 1Password in action, or explore how we've empowered SMBs just like yours with our **Virtu Case Study**.

1Password

Trusted by over 165,000 businesses and millions of consumers, 1Password pioneered Extended Access Management, a new cybersecurity category built for the way people and AI agents work today. Our mission is to unleash productivity without compromising security. The 1Password Extended Access Management platform secures every sign-in, to every app, from every device, including the managed and unmanaged ones that legacy IAM, IGA, and MDM tools can't reach. Leading companies such as Asana, Associated Press, Aldo Group, Canva, IBM, MongoDB, MediaComm Communications, Octopus Energy, Slack, Salesforce, Stripe, Under Armour, and Wish rely on 1Password to close the Access-Trust Gap: the security risks posed by unfederated identities, unmanaged apps, devices, and AI agents accessing sensitive company data without proper governance controls.

Learn more about 1Password.