1Password

SMB SECURITY

Block unauthorized access to safeguard your data

Unauthorized access represents one of the biggest cybersecurity risks for small and medium businesses. Whether it's from compromised credentials or unhealthy devices, unauthorized access is one of the leading causes of security breaches and ransomware. When left unchecked, it can also become a blocker for earning and maintaining compliance, or qualifying for cyberinsurance.

Why it matters

Unauthorized access from compromised credentials and devices is a common way that organizations get breached. This can stem from weak or reused passwords, unhealthy or unmanaged devices, or credentials existing beyond an employee's tenure.

The impact of insecure credentials and devices is sizable:

- 92% of all successful ransomware compromises originate through unmanaged devices. (Microsoft Digital Defense Report, October 2024)
- 68% of breaches involved a human element such as compromised user credentials or phishing (Verizon 2024 Data Breach Investigations Report, Verizon, May 2024)
- 47% of SMB employees admit to using shadow IT (Balancing Act: Security and Productivity in the Age of AI, 1Password, April 2024)

Prioritizing credential and device security can:

- Reduce your risks of breaches and ransomware
- Meet key requirements for meeting and earning compliance, and qualify for cyberinsurance
- Reduce overhead and the number of IT tickets associated with passwords and devices

Eliminate unauthorized access to safeguard your organization's data

Preventing unauthorized access requires securing credentials and making sure devices are healthy–but in a way that makes work easier, not harder. Traditionally this has been extremely difficult to do, since many security tools and practices create barriers for employees, rather than empower them. Balancing security and productivity drives a need for security solutions and processes that simplify being secure while making sure that unauthorized access is blocked.

This approach has some critical requirements:

- Empowered employees that can use the solutions and devices that make them most productive
- Easy-to-use security tools that simplify employee access
- Visibility into how access is used in order to support meeting compliance mandates and minimize the cost of cyberinsurance

How 1Password Extended Access management helps secure your data

1Password prevents unauthorized access. We do that by securing credentials and validating that devices are secure. We empower your employees to be active participants in your cyber defense by guiding them through simple self-remediation steps whenever their device or credentials are not fully secure and trusted.

How 1Password Extended Access Management prevents unauthorized access:

- Securely manages credentials for every application that may host corporate data, including unmanaged applications or shadow IT
- Verifies that devices are secure before they are allowed to access corporate data
- Provides access audit trails to make it simple to achieve compliance objectives and qualify for cyberinsurance

Get started today

Experience 1Password Extended Access Management for yourself with one of our interactive demos today.