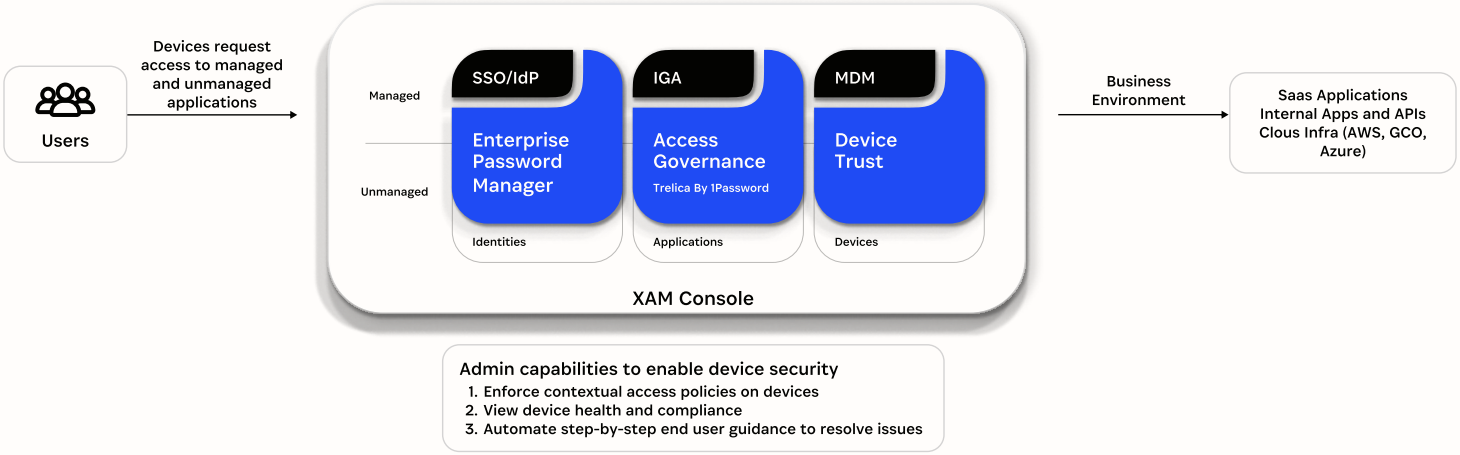
1Password

Secure every device, everywhere

Modern security requires that every sign-in from every device be trustworthy and secure. Doing so means organizations must check and validate device posture before they grant access across all devices, whether managed or bring your own device (BYOD). This can create a blind spot for organizations that use mobile device management (MDM) tools since these tools focus on managing the configuration of devices rather than validating if the device is in a secure state at the time of an access request. And MDM doesn't work on Linux devices often preferred by developers.

1Password Extended Access Management verifies that all access from managed and BYO devices is secure and compliant. This enables you to reduce the risk associated with unauthorized or unhealthy devices, get visibility into device health across managed and BYO devices, and simplify meeting compliance mandates.

1Password Extended Access Management enables device security



Why it matters

Whether it’s your policy or not, the reality is that access to your corporate systems happens on managed, unmanaged, personal, and contractor-owned devices. Securing them all requires more than traditional device management tools. If you can’t see or secure the devices your team is using, you can’t protect your data. That puts your business at risk.

- 92% of all successful ransomware compromises originate through unmanaged devices. (Microsoft Digital Defense Report, Microsoft Threat Intelligence, 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)

By solving for device security with 1Password, you can:

- Minimize the attack surface by ensuring secure, compliant access to resources.
- Free your security and IT teams from repetitive tasks, empowering them to focus on strategic priorities.
- Build confidence in maintaining and exceeding regulatory requirements for access controls and privacy across the organization.
- Enable employees to work securely and self-remediate issues without introducing friction.

1Password Extended Access Management

1Password Extended Access Management secures access from every device, whether IT manages it or not.

- **Gain visibility into every device:** See which devices access apps and data, even unmanaged ones.
- **Enforce device trust policies:** Set rules to allow access only from healthy, trusted devices.
- **Block risky devices:** Prevent access from compromised or jailbroken devices or those without up-to-date security controls.
- **Empower self-remediation:** Let employees fix issues, like outdated OS or missing antivirus, on their own, then regain access.
- **Secure BYOD:** Give employees flexibility without compromising security or visibility.

How 1Password products enable device security

1Password	How it contributes
1Password Device Trust	Ensures all managed and unmanaged devices are in a trusted state before allowing them to access business applications and sensitive data, including personal devices that employees may use to be most productive.
1Password Enterprise Password Manager	Secures passwords and provides multi-factor authentication to unmanaged apps and apps in the queue for federation.

Get in touch with us. Experience 1Password Extended Access Management by requesting a demo today.