1Password

1Password Device Trust

ENSURE DEVICES ARE KNOWN AND COMPLIANT

Can the devices accessing your sensitive apps and data be trusted? While MDMs can help enforce a limited number of security policies on some endpoints, they leave a critical gap when it comes to unmanaged devices and applications.

As part of Extended Access Management, 1Password Device Trust closes the security gap and ensures your data is protected by continuously verifying the identity and posture of each device before granting access to your applications.

Key features

DEVICE HEALTH CHECKS

Enforce a wide range of security and compliance policies with pre-built and custom health checks

- 100+ pre-built checks
- Support for custom checks
- osquery-based agent
- Cross-platform support, including Linux

GUIDED SELF-REMEDIATION

Empower end users to resolve device issues independently, at a time that's convenient for them —without IT assistance

- Included remediation guides
- Configurable remediation settings
- Snooze option for flexible resolution
- Transparent privacy center

IDENTITY PROVIDER INTEGRATIONS

Integrate with your IdP to ensure devices are known and healthy before they access SSO-protected apps

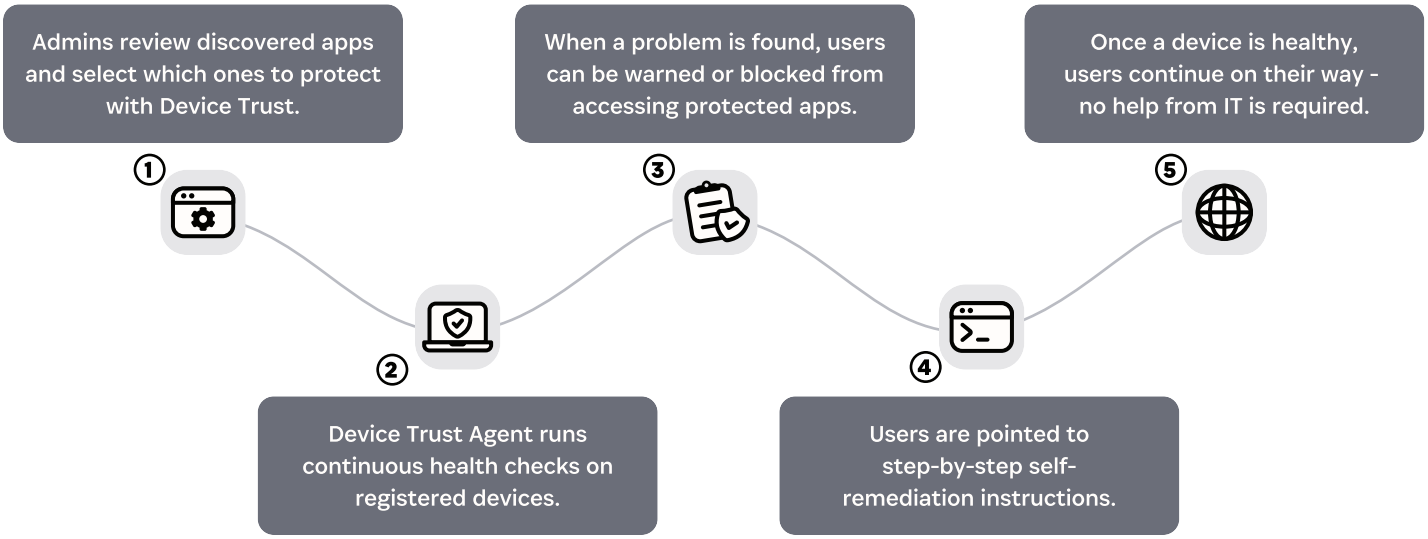
- Verify device identity
- Enforce device posture
- Sync users and groups

EXTENDED DEVICE COMPLIANCE

Get visibility into apps your employees use and expand enforcement of device health checks to all web apps

- Get visibility into all work-related apps
- Configure apps with Device Trust
- Enforce checks via 1Password browser extension

How 1Password Device Trust works



What version of Device Trust is right for you?

1Password Device Trust is available in two powerful versions to fit the needs of your business:

- **Device Trust Core:** Designed to secure web apps, Device Trust Core enforces device health checks via the 1Password browser extension and guides end users through self-remediation.
- **Device Trust Connect:** Includes everything in Core, and also integrates with leading IdPs to ensure every device is known and healthy before signing in to SSO-protected apps.

Unmatched capabilities of 1Password Device Trust

100+ PRE-BUILT DEVICE HEALTH CHECKS FOR REAL-TIME POSTURE MONITORING

Continuously verify that devices meet your security standards with over 100 pre-built health checks that can ensure encryption is enabled, apps are updated, security tools are working, and more. Go even further with custom checks.

DEVICE COMPLIANCE ENFORCEMENT THAT EXTENDS TO ALL WEB APPS

Use the 1Password browser extension to automatically block access to specific web apps when devices fail security checks. This ensures protection for sensitive information across the entire organization, not just managed apps.

CROSS-PLATFORM SUPPORT INCLUDING LINUX AND MOBILE

Secure all the devices your employees use, including Linux. Employees can safely use devices they're comfortable with without compromising organizational security standards.

Solutions

DEVICE SECURITY

- Address the challenges of untrusted MDM and BYO-devices by verifying every device is trustworthy and compliant.

COMPLIANCE AND CYBER INSURANCE

- Meet the requirements of cyber insurance carriers and common compliance frameworks such as SOC 2, ISO 27001, NIST, and more.

DEVELOPER SECURITY

- Take back control of developer secrets by eliminating secret sprawl and discovering unencrypted SSH keys on devices to secure them.

PASSWORDLESS

- Enforce modern authentication methods like device trust, passkeys, and MFA while guiding your team toward a passwordless future.

About 1Password Extended Access Management

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 unmanaged ones that legacy IAM, SSO, and MDM tools can’t reach. Over 165,000 leading companies rely on 1Password to close the Access-Trust Gap: the growing risk created when unmanaged apps, devices, and AI agents access sensitive company data and resources without proper governance controls. Learn more at 1Password.com.

Get in touch with us

For more information about Extended Access Management visit:
1password.com/extended-access-management