1Password

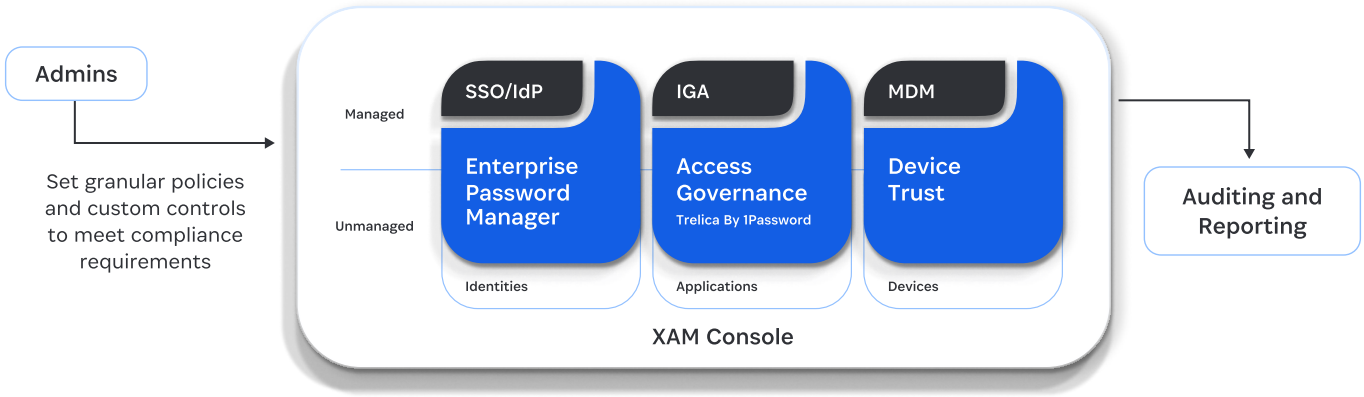
Extended Access Management for Compliance

In the era of SaaS, identity, and device sprawl, organizations continue to take on the responsibility of maintaining compliance with standards such as ISO 27001, SOC 2, PCIDSS, and NIST 800-53. Each major compliance standard typically requires controls for controlling access, enforcing strong authentication, securing devices, and providing detailed security reporting. Alongside these standards, cyber insurance providers often use these controls as a baseline to determine eligibility for coverage. But while proving compliance has never been easy, it's even more complex when users frequently access sensitive data on unmanaged devices and apps, outside the reach of traditional security and compliance tools.

1Password Extended Access Management helps organizations meet these requirements by enforcing security policies on every device, application, and identity, even those considered "out of scope" by other solutions.

1Password Extended Access Management's platform and products are compliant with ISO 27001 and SOC 2 frameworks by default, helping organizations simplify audit readiness, reduce access risks, and accelerate certification processes in cases where use of compliant solutions is required. In addition, we complement and integrate with Governance, Risk and Compliance (GRC) solutions like Drata to extend governance across identity, devices, and applications securely while meeting compliance framework requirements.

1Password Extended Access Management supports your compliance journey



Admin capabilities to support compliance needs

1. View real-time insights, logs, and anomalies
2. Enforce customizable access policies and controls
3. Automate user SaaS lifecycle management and access
4. Integrate with leading SIEM and GRC solutions

Why it matters

Failing to meet compliance standards exposes businesses to data breaches, regulatory penalties, or being unable to operate in specific industries or serve customers. Insurance companies are also looking for organizations to have certain security measures in place such as MFA, role based access controls, and access management enforcements before being eligible for cyberinsurance coverage. 1Password Extended Access Management mitigates credential risks, enforces device compliance, and gives you visibility and control on SaaS access privileges, while supporting your cyberinsurance requirements.

- Organizations that fail to centrally manage SaaS life cycles will be 5x more susceptible to a cyber incident or data loss due to incomplete visibility into SaaS usage and configuration. (Gartner Magic Quadrant for SaaS Management Platforms, 2024)
- $220,000 additional cost per breach is attributed to non-compliance with regulatory requirements. (IBM Cost of a Data Breach Report)
- There were more than $5.6 billion in total GDPR fines across more than 2,500 fines as of March 2025 and that number continues to grow. (GDPR Enforcement Tracker, March 2025)

How to support your compliance journey with 1Password

- Strengthen credential risk management through real-time security monitoring, activity logs, and strengthened authentication via MFA, SSO, or passkeys.
- Enforce device compliance by ensuring all organizational devices have anti-malware enabled, OS patches, hard drive encryption, customizable device health requirements, and robust audit logs.
- Ensure holistic SaaS governance and visibility with automated user offboarding, app discovery, customizable application access policies, and automated access reviews.

1Password's partnership and integration with Drata

1Password works with compliance solutions such as Drata to simplify and automate compliance, helping your team scale securely while meeting framework requirements.

The integration between Drata and 1Password Device Trust streamlines compliance processes through automated evidence collection and insights into security posture. Drata's integration with 1Password Device Trust continuously monitors five key Device Trust Checks that are particularly important for meeting compliance frameworks such as SOC 2, ISO 27001, NIST, and more.

These Checks validate that an end user's device has:

- A password manager installed
- Antivirus software installed and running
- Hard drive encryption enabled
- An updated operating system with the latest security patches
- Screensaver lock properly configured

The integration then enables Drata to retrieve detailed 1Password Device Trust Check results from all devices. From there, Drata can provide insights into device compliance and overall security posture.

How 1Password products support compliance requirements

1Password	How it contributes
1Password Device Trust	Ensure every device is known and compliant before granting access to work applications and sensitive data. Enforce over 100 pre-built health checks across managed or unmanaged devices to verify posture, and guide users to self-remediate any issues without IT assistance. Implement a wide range of device security policies related to software patching, disk encryption, firewall status, and more with pre-built checks, or build your own with our custom Checks editor to fit the specific compliance needs of your organization.
Trelica by 1Password	Secure and manage access to SaaS applications across the employee lifecycle, from onboarding to offboarding, with automated workflows to manage access requests and identify orphaned accounts. Govern user access to SaaS applications with regular access reviews that remove leaver access and ensure users have the correct level of access.
1Password Enterprise Password Manager	Protect sensitive data by enforcing secure authentication practices across all accounts, including those not covered by SSO. Meet compliance requirements through controls for identity and access by generating strong, unique credentials, enabling passkeys and MFA, and storing secrets in encrypted vaults. Provide visibility into credential usage and access patterns across the organization. Real-time alerts and exportable audit logs help meet compliance requirements and support faster remediation of credential-related risks.

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