1Password

Access management checklist for CISOs and security leaders

Security professionals are routinely asked to prioritize the initiatives that will be most impactful to bolster security while also improving business outcomes. However, choosing where to focus your attention and resources can be a challenge.

The following checklists are designed to assist CISOs and other security leaders in improving access management at their organizations and patching the holes left by unmanaged devices, applications, and users. These checklists are adapted from the IDC report “The Future of Access Management: Identity Security Requirements for a Modern Application Access Approach” and written with the collaboration of Dave Lewis, 1Password’s Global Advisory CISO.

The goals and tactics we suggest here address problems found in every region and industry, as well as at companies of every size. They are built to support a zero trust architecture, the CIS Controls Framework, and the principle of least access: restricting the flow of data to the devices, applications, and users that are meant to have it.

Device trust

Goal: Only permit known devices to access company resources.

Outcome: Prevent bad actors from accessing company data with phished credentials, prevent data exfiltration onto unknown devices, and either securely enable or effectively block BYOD.

Actions	Things to consider	Current Status
Implement MDM on all company-owned devices.	MDMs are often a compliance requirement, but they lack the ability to enforce granular policies and are not suitable for all devices.	
Implement a device trust solution on devices not enrolled in MDM (personal devices, third-party contractors, Linux machines).	Device trust solutions can also go on MDM-enrolled devices to provide more comprehensive posture checks.	
Block authentication to company resources to devices missing the device trust agent and/or MDM.	Requires integration with your SSO provider to make device trust part of the authentication flow.	

Goal: Only permit devices in a secure, compliant state to access company resources.

Outcome: Prevent malware-infected devices from accessing company data, fulfill contractual and compliance obligations, and locate and erase sensitive data from devices.

Actions	Things to consider	Current Status
Continually monitor key device health properties, including: • OS updated • Browser updated • Applications patched • No malicious browser extensions installed • Firewall turned on • EDR present and working correctly • No unencrypted credentials • No unencrypted SSH keys • Disk encrypted • Screenlock on	Assess device trust solutions on the number of checks they provide out-of-the-box, as well as the ability to write your own custom checks.	
Enable real-time queries and reporting on fleet status.	Look for the ability to export device events and send them to log aggregation software or SIEM for advanced alerting and incident response.	

Goal: Limit employee disruption, IT bottlenecks, and privacy concerns.

Outcome: Improved productivity, increased IT bandwidth, and positive user experience.

Actions	Things to consider	Current Status
Be transparent about all data collected on a user's device.	Transparency is a precondition for employees and contractors to consent to put an agent on their personal devices.	
Provide users with a path to self-remediation whenever they are blocked from authenticating.	When assessing vendors, assess the quality of fix instructions. They only work when they are detailed and easy to follow for all users, regardless of technical skill level.	
Avoid surprise forced restarts and blocking.	Warn users as soon as a problem is detected, and give them advance warning before any disruption to their work.	

User identity

Goal: Enable secure sign-in.

Outcome: Prevent credential-based and phishing attacks, centrally manage access permissions, reduce end-user friction.

Actions	Things to consider	Current Status
Implement and require the use of a password manager.	A password manager can facilitate your transition to more secure forms of authentication and encourage better password hygiene in the meantime.	
Implement SSO when possible.	Budget concerns may make it impossible to put all applications behind SSO, so be strategic about the ones you choose to protect.	
Implement phishing-resistant MFA.	When possible, ditch passwords and SMS notifications in favor of biometric authentication, hardware keys, and passkeys.	
Grant access based on contextual signals, such as: • Impossible travel • Credential strength • Device identity • Device health	Look for automated solutions that will either block authentication or step up to more secure forms of authentication based on these signals.	

Goal: Manage all identities throughout the user lifecycle.

Outcome: Easily manage onboarding and offboarding and prevent unauthorized access.

Actions	Things to consider	Current Status
Centralize onboarding and offboarding for employees, contractors, and vendors.	Consolidate all applications into a single universal sign-on system, allowing administrators to manage access by granting or revoking permissions, irrespective of the organization's identity provider enrollment.	
Programmatically identify dormant credentials and accounts.	Revoke access when it is no longer needed, not just when someone leaves the organization.	

Application visibility

Goal: Manage Shadow IT.

Outcome: Reduce IT spend for unapproved applications, prevent data leakage.

Actions	Things to consider	Current Status
Identify all applications on which work is taking place. This will a require a multipronged approach, potentially including: • Querying devices • Scanning work emails • Scanning password vaults • Network monitoring	Take into account user privacy considerations, search for known enterprise applications rather than collecting data on all applications in use.	
Prohibit unsafe and unapproved applications.	Achieve through automation (such as blocking authentication from devices with prohibited apps) and direct outreach from IT.	
Identify and eliminate unused licenses.	Realize significant cost savings. Reallocate funds to achieve the goals outlined in this checklist.	
Protect approved applications	Bring acceptable applications under IT management via SSO or an enterprise password manager	

1Password is among the most trusted brands in cybersecurity, having built its reputation with a best-in-class password manager. Today, 1Password supports companies of every size and in every industry through 1Password Extended Access Management. This comprehensive security solution solves persistent IT and security challenges by bringing visibility and control to unmanaged applications, devices, and identities.

To learn more or schedule a demo, please visit 1Password.com