DASHLANE

Credential coverage self-assessment

Use this checklist to assess your organization's credential coverage. Share it internally with IT, security, and compliance stakeholders.

SSO and applications

- [ ] Do you have a complete and current inventory of all applications employees access for work?
- [ ] Do you know what percentage of those applications fall outside SSO?
- [ ] Can you demonstrate that non-SSO applications have alternative credential controls in place?
- [ ] Do you have visibility into shadow SaaS applications adopted without IT approval?

Vault and password management

- [ ] Do you know what percentage of your workforce has enrolled in your password manager?
- [ ] Can you produce credential hygiene evidence, such as password strength and compromised credential status, for employees outside the vault?
- [ ] Can you demonstrate MFA enrollment status for non-SSO applications for the full workforce?
- [ ] Can you produce a complete credential health report for every employee within 24 hours if an examiner requests it today?

Shared and privileged credentials

- [ ] Do you have a documented process for how shared credentials are distributed and rotated?
- [ ] Can you confirm that shared credentials are revoked promptly when employees leave or change roles?
- [ ] Are privileged accounts reviewed regularly for excessive permissions and inactive access?

AI agent access

- [ ] Do you have a complete inventory of AI agents operating in your environment?
- [ ] Do you have a governance framework defining how credentials are delegated to AI agents?

Have an expert conduct a full credential coverage assessment

Request an assessment