RESOURCE CENTER

Critical Capabilities for Enterprise Password Management

Get the full interactive view at https://bitwarden.com/resources/critical-capabilities-for-enterprise-password-management/

bitwarden

Table of Contents

Critical Capabilities for Enterprise Password Management

Set yourself up for success by including all of the following in an evaluation of enterprise password management.

Integrate with your existing environment(s)

Feature	Detail	Impact
Broad SSO compatibility	SAML	Support wide range of existing identity providers
	OIDC	Support modern identity systems

Feature	Detail	Impact
	Login with SSO (and decrypt with password manager password)	Additional security via authenticating with SSO and decrypting with main password
	SSO with trusted devices	Use trusted devices to store users' password manager passwords for easy retention
	Customer managed encryption	Complete control with a key connector to retain user vault encryption locally with self-hosted deployments
	Clear role mapping for users	Tightly managed role assignment for onboarding to ensure utmost security
SCIM provisioning	SCIM endpoint for onboarding	Automate user rollout to accelerate your security posture. Operate natively without requiring a bridge
Principal User Names	Support accounts without an email address	Establish accounts by User Principal Name (UPN) where desired without requiring a user email ID

Deployment options

Feature	Detail	Impact
Cloud deployment	Simple SaaS service	Easily launch password management for any size organization
Self-hosted deployment	On-premises option	Complete control over password management in a private environment

Feature	Detail	Impact
Centralized client configuration options	Desktop and mobile deployment and configuration options, compatibility with device and mobility management systems	Central configuration and roll out of the Mac App and extension, the Windows App, the Linux App, the managed Chrome/Edge/Firefox browser extensions, and the mobile apps (preconfigured with optional self-hosted server URL) delivers the enterprise administration companies expect Full client list at bitwarden.com/download

Corporate Password Policies

Feature	Detail	Impact
Generate passwords	Abide by company policy	Ensure employee generated passwords meet company policies
Policy options	Length, min numbers, min special chars, upper case, lower case, passphrase options	Maintain compliance with existing company policies
Main password manager password policy	Policy for master passwords	Ensure employees' passwords for their password manager is strong
Account recovery administration	Automatic enrollment	Guarantee that administrators have the ability to help employees when needed with account recovery, ensuring all individual credentials remain accessible

Client compatibility

Feature	Detail	Impact
Comprehensive browser extension support	Supports all major browsers	Delivers maximum flexibility for broad adoption within any organization, including options to deploy centrally for company-controlled browsers

Feature	Detail	Impact
	Chrome	
	Firefox	
	Safari	
	Edge	
	Brave	
	Opera	
	Vivaldi	
	DuckDuckGo for Mac	
	Tor	
Comprehensive mobile app support	Support all major platforms and application download paths	Deliver maximum flexibility for the highest adoption
	iOS Apple App Store	
	Android Google Play Store	

Feature	Detail	Impact
	F-Droid	
	Direct from GitHub	
Comprehensive desktop app support	Supports all major desktop operating systems	Deliver maximum flexibility for the highest adoption
	Windows	
	MacOS	
	Linux	
Web app support	Functions available in stand alone web app	Ensure credential access securely in any environment
Command Line Interface (CLI)	Fully featured CLI	Easily enable programmatic actions and integration to fit existing enterprise workflows

Security and Encryption

Feature	Detail	Impact
Trusted open source architecture	Ability to see and examine codebase	Provide the utmost in trust and transparency for a mission critical software solution
Minimum vault encryption 256-bit (AES-CBC or similar)	Including PBKDF2 SHA-256 or Argon2	Strong encryption protects data should it get into the wrong hands. Advanced algorithms such as Argon 2 provide advanced encryption methods

Feature	Detail	Impact
Zero-knowledge encryption	Entire Vault is encrypted	
Breach reports	Integrate with services like HIBP	Breach reports help identify potential risk areas, warning users of breached sites and reused passwords
	Exposed Passwords report	Identifies passwords that have been uncovered in known data breaches that were released publicly or sold on the dark web by hackers
	Reused Passwords report	Identifies non-unique passwords in your vault
	Weak Passwords report	Identifies weak passwords that can easily be guessed by hackers and automated tools that are used to crack passwords
	Unsecured Websites report	Identifies login items that use unsecured (http://) schemes in URIs/URLs
	Inactive 2FA report	Identifies login items where: Two-factor authentication (2FA) via TOTP is available from the service, and you have not stored a TOTP authenticator key

Auditing and Logging

Feature	Detail	Impact
Full audit trail	Viewable and exportable logs of relevant events	Comprehensive event coverage ensures detail to identify auditable steps
SIEM Integration	Easy API access	Integrate with existing systems to collect event log information for fast analysis

Integration

Feature	Detail	Impact
Fully featured CLI	Command Line Interface	Enable programmatic integrations with existing company workflows, including handling of encrypted items. Easily handle bulk operations
Robust API	Application Programming Interface	Enable programmatic integrations for managing members, collections, groups, event logs, and policies

Authentication

Feature	Detail	Impact
Multifactor authentication for the password manager	Including authenticator app, WebAuthn, Yubico, email, Duo	Adding multifactor authentication delivers an additional layer of security
Ability to store MFA tokens	Store TOTP codes within password manager	Allow for multifactor authentication logins to be easily shared while retaining MFA
Integration with Duo	Out of box functionality	Additional security with existing multifactor solutions

Import and Export

Feature	Detail	Impact
Import Passwords	Import from all major password managers across .csv and .json formats	Quickly consolidate disparate solutions into a unified enterprise password manager
Encrypted Exports	Export in account encrypted, independently encrypted, and unencrypted formats	Robust export mechanisms serve as backups and freedom to migrate if desired

Secure Sharing

Feature	Detail	Impact
Share items with a user or a group of users	Include organization of multiple items in shared folders	Secure sharing keeps sensitive information protected with controlled access
Send and receive encrypted passwords externally with a limited lifespan	Handle encrypted sensitive information with automatic removal	Sensitive information shared through email and messaging channels is not encrypted and could be exposed. Using encrypted, limited lifespan methods reduces risk
Quickly revoke access when needed	Disassociate user from company credentials	With employee succession, removing access quickly ensures smoother transitions

Useability, Autofill and Biometrics, Offline access, Search

Feature	Detail	Impact
Client app localization	Language support	
Browser extension and mobile apps can autofill username and password	Including options for managing Uniform Resource Identifiers (URIs)	Autofill provides user convenience and serves as a means to recognize and prevent phishing
Browser extension and mobile apps can autofill MFA tokens	For accounts with integrated multifactor authentication	For fast, secure logins
Biometric access across mobile, browser extension and desktop apps	Fingerprint or face identification	Convenience and security of biometrics leads to broader adoption and more use
Account switching	In-App account selector	Provide simple switching between multiple Bitwarden accounts

Feature	Detail	Impact
Offline vault access	Vault remains accessible offline in browser extension, mobile, and desktop apps	Ensure business continuity with read access to the vault even if connection to the server is interrupted
Intelligent Search	Including options for advanced search	Detailed search including wildcards allows for quick retrieval of logins within a large vault
Individual vault	User-specific credentials	Allow for an individual vault that cannot be accessed by others

Secrets Management

Feature	Detail	Impact
Secrets Management Option	i.e. non human interaction for certificates or API key handling	Availability of a secrets management platform for use cases beyond general password management

Passwordless for developers

Feature	Detail	Impact
Passwordless and passkey infrastructure	Passkey software development kit to enable websites and enterprise apps	Rapidly transform your company to a passwordless organization, freeing employee and IT time to focus on their primary objectives

Compliance

Feature	Detail	Impact
SOC 2 and SOC 3 reports	Third party audits	Audited validation of business practices

Feature	Detail	Impact
HIPAA	Including the option to sign a business associates agreement	Compliance for healthcare related companies
GDPR	Data privacy	Assure data privacy
Annual security assessments	Network and security scans	Audited security reports showcase detailed attention to security
Independent security researcher program	Such as HackerOne	Proactively identify potential issues

Purchasing

Feature	Detail	Impact
Simple purchasing process	Direct or through channel	Easy to procure
Billed via invoice	30-day terms	Flexibility of an invoiced model
Complimentary Family plan for Enterprise users	Employee benefit	Security at work and at home leads to better overall habits

Implementation

Feature	Detail	Impact
Comprehensive documentation	Publicly accessible on web	Easily understand product operations and self-serve product knowledge

Feature	Detail	Impact
Online training	Pre-recorded and live	Provide accelerated ramp for administrators as well as end users
Onboarding templates	Admin enablement	Pre-built email templates facilitate employee onboarding
24x7x365 Support	Business and end user	Support for Administrators and Users around the clock
Integration support	Deployment success	Detailed technical expertise ensures smooth deployments

Have questions or comments on this list? Please contact us via bitwarden.com/help.

Want to see Bitwarden in action? Join our live demo via bitwarden.com/weekly.