Competitors & Alternatives

When buyers evaluate EPM, they're often comparing tools — but also trying to solve broader problems like visibility, compliance, or consolidation. This section helps position 1Password not just as a "better password manager," but as a more complete identity and access solution. 1Password is a future-ready platform that grows with your organization with offerings across Extended Access Management, more to come on this for MSPs.

Category Competitors

Competitor	Where 1Password Wins	Where 1Password Expands
Bitwarden	- Simpler, consumer-style tool - Limited admin controls - No native secrets management or device trust	- Highlight 1Password's enterprise-grade UX + SCIM, audit logging, and end-to-end encryption
Keeper	- Strong in privileged access - Overkill or complex for most teams - High total cost of ownership (TCO) at scale	- Position EPM for broader team access and usability
LastPass	- Security trust erosion with past breaches - Dated architecture (no 2SKD) - Painful rollout history	- Emphasize 1Password's zero-knowledge model, seamless onboarding, and high adoption rates
Dashlane Business	- Basic features for small teams - Not built for enterprise controls - Limited secrets support	- Win on scalability, admin experience, and extensibility - SSH keys, API tokens, passkeys, secrets, and policy controls

PRIVATE & CONFIDENTIAL - This content is for MSP internal use only and should not be shared

SSO / IAM Tools (with Credential Gaps)

Examples: Okta, Microsoft Entra ID, Ping Identity

Area	IAM Tools Alone	1Password
Credential Coverage	Only supports SAML/SCIM-managed apps	Secures shared credentials, non-SAML, unmanaged, and long-tail SaaS
Policy Enforcement	Enforces access at login layer only	Extends enforcement to credential storage and usage
Shared Logins	No built-in solution	Vault-based, auditable sharing with access control
Visibility	Limited post-login insight	Track what's stored, used, reused, and shared
Differentiator	IAM protects identities. 1Password protects what happens *after* login — and secures what IAM can't reach.	

Workarounds & Shadow IT

Examples: Google Sheets, Notion, Slack, Confluence, internal wikis

Area	Workarounds	1Password
Security Posture	No encryption, access controls, or audit logs	Encrypted, vaulted, and policy-driven
User Behavior	Encourages credential sprawl and "copy/paste" culture	Encourages secure-by-default usage patterns
Visibility & Revocation	None	Centralized access, activity logs, and role-based controls

PRIVATE & CONFIDENTIAL - This content is for MSP internal use only and should not be shared

Differentiator	We turn insecure habits into auditable, compliant credential workflows — with zero friction for employees.	

Secrets Managers (Developer-Focused)

Examples: HashiCorp Vault, CyberArk, AWS Secrets Manager

Area	Secrets Managers	1Password
Audience	DevOps teams, infra and security engineers	End users, IT, security, and developers alike
Usability	CLI/API-first, complex UI, limited collaboration	Human-friendly vaults with developer-grade access controls
Scope	Focus on machines and systems	Secure both machine and human credentials in a unified platform
Bridge Use Case	Doesn't support shared logins or vaulting	Secrets Automation + EPM covers both secrets and access behavior
Differentiator	We give developers AND end users a secure, auditable way to manage credentials — and scale it org-wide.	

PRIVATE & CONFIDENTIAL - This content is for MSP internal use only and should not be shared