

Executive Summary

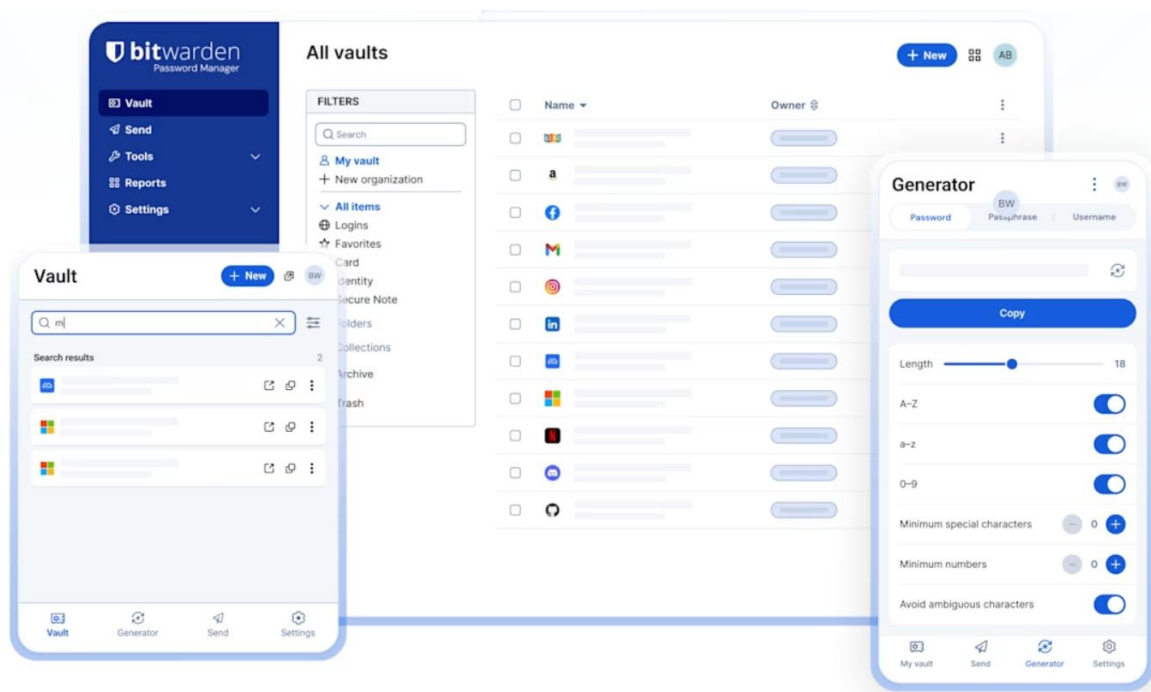
Qnetix Enterprise Password Management delivers a secure, user-friendly method to store, share, and govern business credentials and sensitive data. Built on Bitwarden, this solution provides end-to-end encrypted vaults, central policies, and strong authentication to reduce credential risk while improving employee access and productivity.

Business Benefits

- ✓ Reduce cyber risk by removing weak, reused, and exposed passwords
- ✓ Increase compliance confidence with audit logs and security reporting
- ✓ Improve user adoption with simple, cross-platform access
- ✓ Enable secure sharing across teams without email or chat risks
- ✓ Support modern access with SSO, MFA, and passkeys
- ✓ Scale securely for remote, hybrid, and global workforces

Problems Solved

- ✓ Password sprawl and inconsistent password hygiene
- ✓ Insecure sharing of credentials and sensitive files
- ✓ Limited visibility into credential risks and usage
- ✓ Shadow IT and unmanaged application access
- ✓ Secrets embedded in code and infrastructure tooling
- ✓ Slow onboarding and offboarding for employees and partners



Cloud
Modernise

Infrastructure
Consolidate

Data
Accelerate

Security
Protect

Monitoring
Optimise

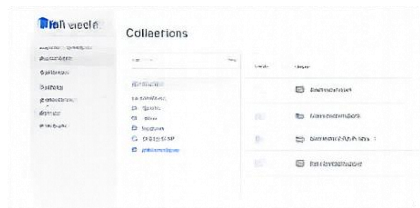
Technical Leader Summary

This solution combines zero-knowledge, end-to-end encryption with strong governance controls for enterprise scale. It supports flexible deployment options, integrates with identity providers and directories, and provides API and CLI access for automation. Open-source transparency and third-party assessments support assurance requirements, while audit logs and reporting improve operational oversight.



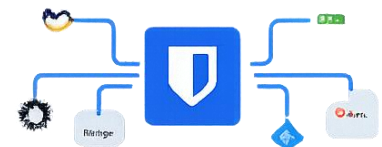
Generate, save, and autofill

Project every account with strong and unique passwords and passkeys, saved securely across unlimited devices, and autofill instantly.



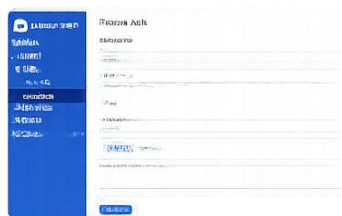
Centralized administration

Manage your representation with access controls, policies, centralized item ownership, and securely reassign all from one place.



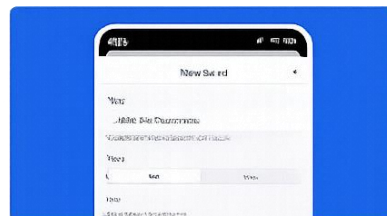
Integrate with your tools

Add Bitwarden seamlessly to your existing tech stack with easy integrations with your SSO, proxy, directory service, and tool and anything your business relies on.



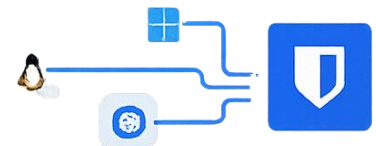
Easy imports

Move passwords from browsers or other managers to Bitwarden in minutes.



Share with others

Use organization collections to share with teammates or Bitwarden Send to transmit encrypted text and files to anyone.



Self-host option

Host Bitwarden on premises, or on your private cloud for full data sovereignty.

Solutions

Overview

Qnetix Enterprise Password Management provides a central, encrypted vault for passwords, passkeys, notes, and other sensitive data. The solution is available as cloud-hosted or self-hosted and supports secure access across desktop, browser, and mobile clients.

Cloud
Modernise

Infrastructure
Consolidate

Data
Accelerate

Security
Protect

Monitoring
Optimise

Core Platform Features

- ✓ Generate, store, share, and autofill passwords securely
- ✓ Password and passphrase generation to improve hygiene
- ✓ Vault health reports for exposed, reused, and weak passwords
- ✓ Cross-platform access with offline availability
- ✓ Biometric unlock for faster, safer access
- ✓ Encrypted exports and file attachments
- ✓ SSH key storage and management
- ✓ Integrated two-step login options
- ✓ Emergency access for business continuity

Core Platform Benefits

- ✓ Stronger protection against credential-based attacks
- ✓ Reduced risk from insecure sharing practices
- ✓ Clear visibility into credential health and access activity
- ✓ Improved user experience without weakening security

Enterprise Governance and Administration

- ✓ Centralised user management with role-based access control
- ✓ Enterprise policies to enforce security standards
- ✓ Directory integration and SCIM provisioning for user lifecycle management
- ✓ SSO support for streamlined authentication
- ✓ Role-based access and shared collections with least privilege controls
- ✓ Auditable event logs for compliance and investigations
- ✓ Account recovery administration for users
- ✓ API and CLI for automation and workflow integration
- ✓ Secure sharing with time-limited access controls

Secrets Manager

- ✓ Centralised secrets storage for DevOps and IT teams
- ✓ Store, collaborate, deploy, and audit secrets securely
- ✓ Replace hardcoded secrets with secure secret IDs
- ✓ Granular read and write permissions for people and machines
- ✓ Audit trails for secret access and changes
- ✓ CLI-based workflows and pre-built integrations

Passwordless Authentication

- ✓ Passkey authentication for customers and workforce users
- ✓ FIDO2 and WebAuthn-based phishing-resistant logins
- ✓ Integrates with existing authentication platforms
- ✓ Centralised passkey management and administration

Access Intelligence

- ✓ Uncover shadow IT and unknown application usage

Cloud
Modernise

Infrastructure
Consolidate

Data
Accelerate

Security
Protect

Monitoring
Optimise

- ✓ Prioritise business-critical applications for remediation
- ✓ Identify weak, reused, or exposed credentials across the organisation
- ✓ Automated alerts and guided remediation workflows
- ✓ Track security improvements through dashboards

Authenticator

- ✓ Open-source authenticator app for multi-factor authentication
- ✓ Generates time-based codes locally on device
- ✓ Provides stronger protection than SMS-based codes

Secure Send

- ✓ Encrypted sharing of passwords, files, and sensitive text
- ✓ Self-destructing messages to reduce exposure
- ✓ Share safely across desktop and mobile devices

Identity Provider Integrations

- ✓ SSO support for AWS, Microsoft Entra ID, Okta, Google, and Duo
- ✓ Additional integrations for Auth0, PingFederate, and JumpCloud
- ✓ Aligns authentication with existing enterprise tooling

Security and Compliance

- ✓ Zero-knowledge, end-to-end encryption protects data before it leaves user devices
- ✓ Open-source transparency enables community review and independent security assessments
- ✓ Regular third-party security audits and penetration tests
- ✓ Compliance support including GDPR, HIPAA, CCPA, and TAA

Service Delivery

The sections below describe the typical onboarding and support journey for Qnetix services. Each service is tailored to your scope, change windows, and operational priorities.

Onboarding and Setup

We designed onboarding to be fast, low-risk, and fully managed by Qnetix. You provide authorised contacts and access requirements, and we handle provisioning, configuration, validation, and documentation handover. Training is included where required. Standard onboarding and offboarding are included at no additional cost, with additional onboarding support available at a pre-agreed rate.

Typical onboarding phases include:

- ✓ Discovery and requirements validation
- ✓ Access provisioning and security alignment
- ✓ Service configuration and integration
- ✓ Testing, validation, and acceptance
- ✓ Go live and handover into steady state

Cloud
Modernise

Infrastructure
Consolidate

Data
Accelerate

Security
Protect

Monitoring
Optimise

The timeline is agreed with each customer and aligned to change windows and delivery priorities.

Ongoing Delivery and Support

Support is provided through email and online ticketing systems with clear priority-based response times:

- ✓ P1 (Critical - Service down or severely impacted): Within 4 hours
- ✓ P2 (High - Significant functionality impaired): Within 8 hours
- ✓ P3 (Medium - Minor functionality issue): Within 2 business days
- ✓ P4 (Low - General inquiry or enhancement request): Within 3 business days

Customers can set and adjust ticket priorities and track status through the full lifecycle.

Proactive service management includes monitoring, patching, planned maintenance, and continuous improvement. We operate ITIL-aligned practices for incident, problem, request, change, and capacity management to keep services secure, stable, and optimised.

Reporting and Reviews

Quarterly reporting and service reviews provide visibility and accountability. Reports typically cover:

- ✓ SLA performance and uptime
- ✓ Incident and change summaries
- ✓ Usage and capacity trends
- ✓ Risk, compliance, and improvement actions

Reviews focus on performance, planned improvements, and roadmap alignment with agreed action tracking and follow-ups.

Account Management

Each customer is assigned:

- ✓ Technical Account Manager for service oversight, escalation, and governance
- ✓ Principal Engineer for technical assurance, troubleshooting, and optimisation

Formal service reviews are quarterly, with ad hoc check-ins available as required. Governance aligns to ITIL principles, including service-level management, change enablement, and capacity planning.

About Qnetix

Qnetix is an outcome-driven IT managed service provider supporting startups, growing businesses and the UK public sector. We operate as an extension of leadership and technical teams, delivering measurable outcomes through technology innovation, structured runbooks, governance, and accountable service delivery.

Our mission is to improve customer operations with reliable, secure, and cost-efficient services backed by UK-based support. Our values are trusted, expert, and outcome driven.

Cloud
Modernise

Infrastructure
Consolidate

Data
Accelerate

Security
Protect

Monitoring
Optimise

We provide end-to-end IT services that scale with your business, including hosting, multi-cloud and private cloud services, security and compliance, DevOps and DevSecOps, Kubernetes, observability and monitoring, end-user support, SaaS applications, and AI systems management. We use AI to supplement engineering delivery and operate management systems that oversee service quality and risk.

Customers choose Qnetix for predictable delivery and clear governance, with a dedicated UK lead architect on every engagement and flexible commercial models, including outcome-based contracts. We provide a 24x7 command centre, ISO-aligned governance, and a global talent pool backed by strong vendor relationships. Rapid onboarding and continuous optimisation help customers move quickly while staying secure and compliant.

Cloud
Modernise

Infrastructure
Consolidate

Data
Accelerate

Security
Protect

Monitoring
Optimise