Data sheet

Island

Password management, *built for the enterprise.*

Island Enterprise Password Manager (IPM) brings credential security into the heart of the enterprise, governed by the same policy engine, posture controls, and real-time enforcement that already protect every session, app, and user in your organization.

Overview

Traditional password managers were designed for individual users storing personal logins, not enterprises protecting company data. Over time, they added "business features," but the architecture stayed the same: operating outside your security stack, disconnected from enterprise policy and real-time risk signals. IPM is powered by the same Island Enterprise Platform foundation. Every credential inherits the same protections before every use: device posture validation, domain trust, phishing defense, DLP enforcement, and runtime protection. All applied automatically, and in real time.

Key outcomes

- Protect credentials at the moment of use
- Enforce policy to every browser & device
- Replace standalone password tools
- Block phishing and enforce device posture
- Share access without exposing the password
- Surface hygiene risk for every credential
- Deploy across the entire org with one toggle
- Reduce license overhead and lower IT burden

The challenge

Enterprises rely on consumer-grade password managers or browser-native tools that weren't designed for the enterprise:

Security control ends at autofill

Once a password fills, there's no visibility into device posture, phishing risk, or in-session exposure. Enterprises are blind the moment a credential is used.

Fragmented tools, fragmented policy

Password managers sit outside the IAM: separate consoles, separate policies, inconsistent enforcement across users, browsers, and devices.

Credential sprawl beyond SSO

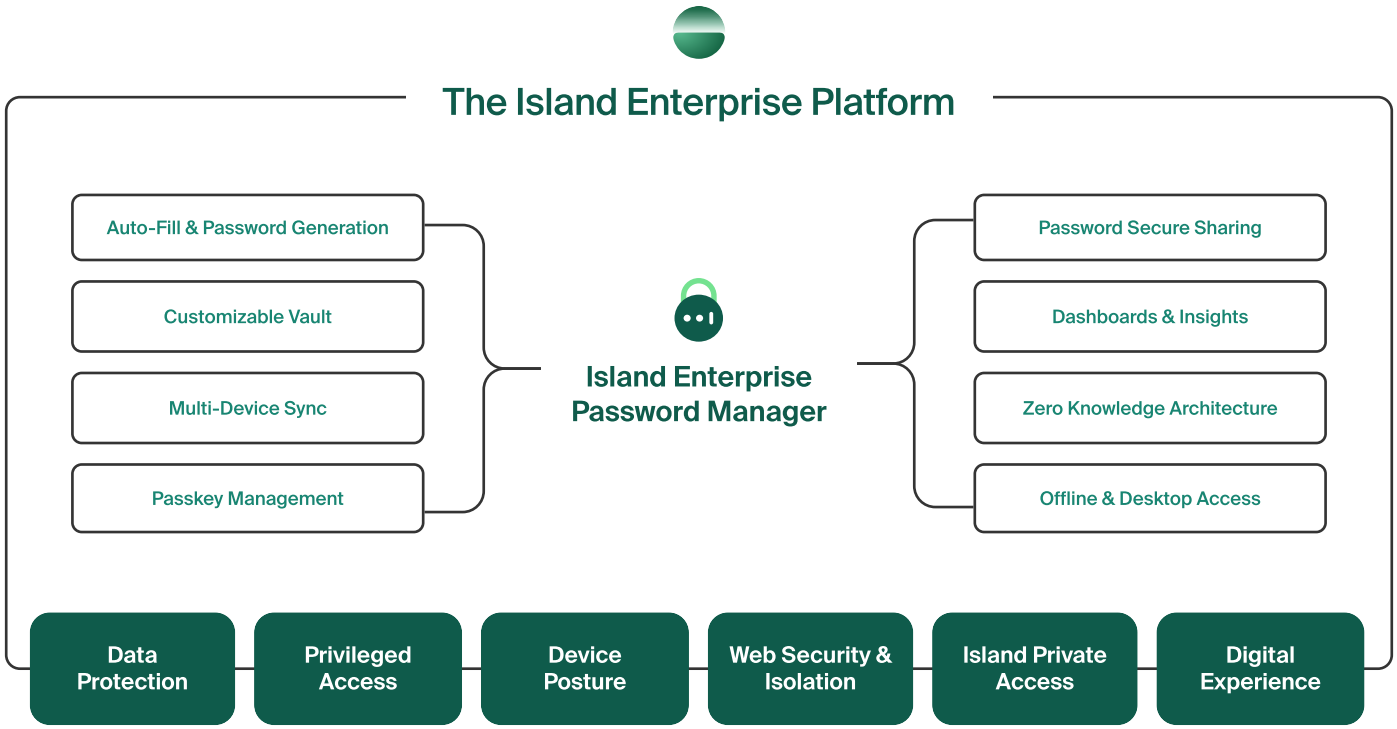
Many enterprise applications still operate outside SSO, leaving credentials unmanaged and outside policy the moment they are used.

Shadow password storage

Credentials saved in consumer browsers evade enterprise controls entirely, creating unmanaged risk that grows silently over time.

How it works

Island Enterprise Password Manager runs natively on the Island Enterprise Platform. Credentials are validated against policy and device posture in real time. Activity is logged and data is encrypted using Island's cloud with optional BYOK or zero-knowledge architecture for complete key ownership and isolation.



1 Access from any environment

A user accesses any supported environment: the Island Enterprise Browser, the Island extension (Chrome/Edge), the desktop app (PWA), or on mobile. IPM is present without any setup or installation.

2 Real-time pre-autofill validation

Before autofill, Island validates device posture, domain trust, and user identity. On unrecognized or unverified domains, credentials are not offered, and access is blocked on non-compliant devices.

3 Secure credential injection

Credentials are injected at the point of use. For protected sharing, Island transforms them at the network layer so passwords never appear in the DOM or user memory, with TOTP codes auto-filled during MFA.

4 Full session audit logging

Every credential interaction is logged with complete context: user, device, session state, and action. Audit data flows natively to SIEM and surfaces in admin dashboards and through the IPM Security Report.

5 Centralized policy management

All password policy, hygiene alerts, sharing rules, and encryption settings are managed from the same Island Management Console used for DLP, access, and device controls.

Key use cases

Secure credentials of shared accounts

Share access to social media, admin consoles, or service accounts without exposing passwords. Protected sharing injects credentials at the network layer, never revealing them to the DOM or user memory.

Privileged access governance

Tie every privileged credential to device posture, user identity, and session context. Set time-bound sharing with automatic expiration. Restrict copy, export, or screenshot of sensitive credentials with built-in DLP.

BYOD & contractor access

Extend password governance to unmanaged devices and consumer browsers without requiring managed endpoints. Enforce posture and policy before allowing credential use across distributed environments.

Password hygiene at scale

Surface weak, reused, old, and compromised passwords through the Security Dashboard and End User Security Report. Admins see org-wide hygiene scores; users get in-vault alerts with one-click remediation.

Phishing & credential theft prevention

Autofill is restricted to policy-approved, verified domains. Spoofed sites are blocked automatically. Keylogger and memory protection neutralize credential capture attempts in real time.

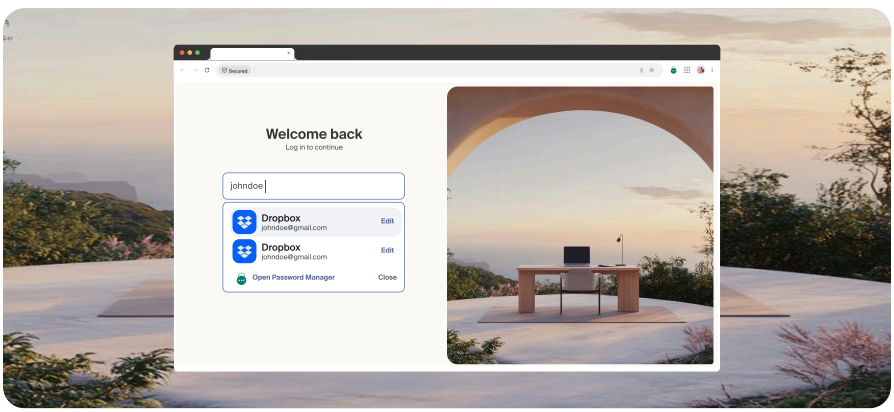
Compliance & audit readiness

Every credential interaction is logged and auditable. Native SIEM export. Align to NIST 800-53, PCI DSS, HIPAA, and SOX with encryption models (Cloud, BYOK, ZKA) that meet data sovereignty requirements.

Core capabilities

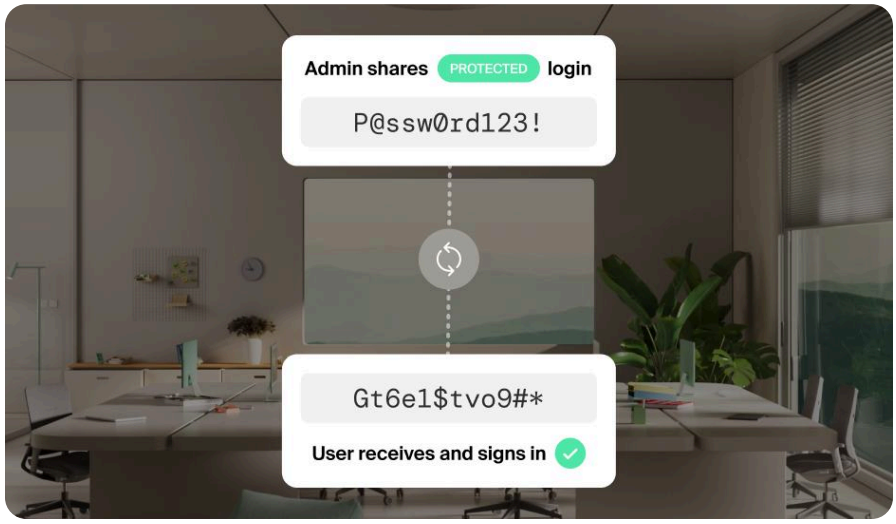
Credential storage & autofill

- **Auto-fill & password generation** - Generates, saves, and auto-fills policy-governed passwords, credit cards, identity data, and API credentials across web, SaaS, and desktop. Prompts to save at sign-up; injects securely on login. One vault for every credential type.
- **Multiple URL support** - A single vault item supports up to 5 associated URLs, reducing duplicate entries for multi-environment or subdomain-based credentials.
- **Passkey management** - Generates and stores passkeys for FIDO2-supported apps. Phishing-resistant, device-bound, and synced across environments..
- **Offline vault access** - An encrypted local vault keeps credentials available without connectivity. User-set offline password is never stored or transmitted in plain text.



Sharing & collaboration

- **Secure password sharing** - Share individual items or entire folders with individuals or groups at three permission levels – Admin, Protected, or Viewer. Group-level encryption ensures only authorized members can decrypt. Full audit trails included.
- **Protected sharing** - Share credentials without revealing the plaintext password. Island transforms credentials at the network layer, hidden from the DOM and user memory. *Unique to Island.*
- **Sharing expiration** - Shared credentials auto-revoke after a configurable time period (1 hour to 30 days). Owners can revoke manually at any time; recipients see a countdown.

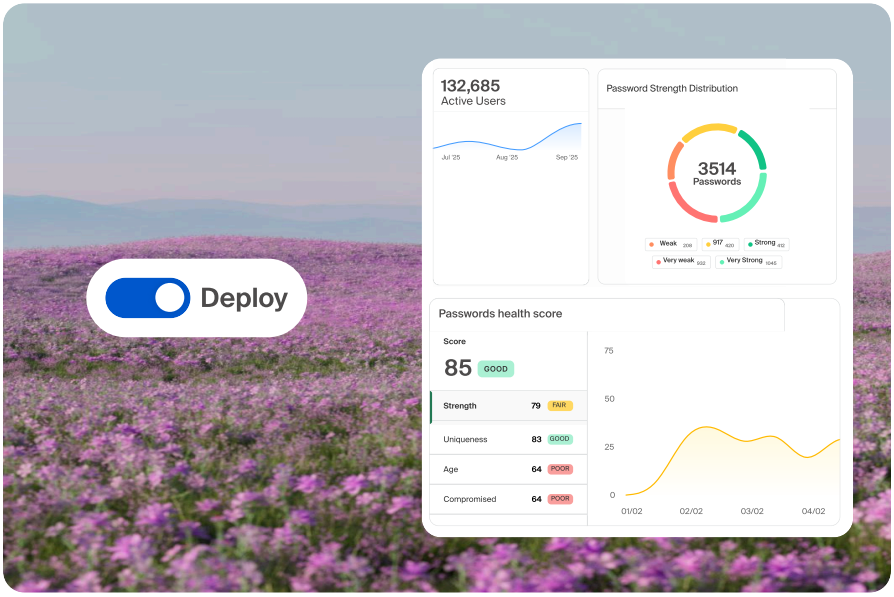


Security & threat protection

- **Exposed password detection** - Integration with "Have I Been Pwned" flags stored passwords found in known breach databases. Visible in admin dashboards and end-user security reports.
- **Compromised credential detection** - Extended breach checks cover passwords stored in IPM, surfacing risk across the Password Hygiene dashboard and in-vault alerts for both admins and users.
- **Device posture enforcement** - Vault access and autofill are restricted by real-time device state: EDR status, OS version, network trust, and geolocation. Non-compliant devices are locked out.
- **Phishing & domain validation** - Autofill is limited to policy-approved, verified domains. Credentials are never offered on spoofed or look-alike sites. Blocked before any interaction.
- **Keylogger & memory protection** - Obfuscates keystrokes, encrypts working memory, and favors autofill over manual entry, neutralizing credential capture attempts without user action.
- **Fast Login (PIN/biometrics) & MFA** - Users re-authenticate to the vault using biometrics, device PIN, or MFA, online or offline. Requires step-up verification before viewing, copying, or autofilling sensitive credentials.
- **Built-in TOTP support -** IPM generates, stores, autofills, and supports secure credential sharing with two-factor authentication, all without leaving the browser.

Admin visibility & control

- **Admin dashboards** - Full admin dashboards covering adoption trends, password hygiene scores, sharing behavior, at-risk users, and compromised credential visibility. Offering a full audit trail and insights.
- **End-user security report & alerting** - A Security Dashboard shows users their password health: weak, reused, old, and compromised passwords with in-vault alerts with direct remediation.
- **Filter personal credentials** - Admins configure dashboards to show only corporate credentials, filtering personal accounts based on organization domain configuration.
- **IdP, SCIM, & SIEM integration** - Native integrations with Okta, Microsoft Entra, Ping, and other IdPs. SCIM for automated provisioning and deprovisioning; SIEM export and full audit stream.
- **Unified policy. One control plane** - All password policy, sharing rules, hygiene alerts, and encryption settings managed from the same Island Management Console.



Deployment & encryption

- **Single-toggle deployment** - Activate across the full organization or targeted user groups with one policy toggle. No agents, no installs, no parallel systems.
- **Cross-platform support**- Available as part of the Island extension for consumer browsers as well as mobile, extending IPM to non-managed environments.
- **Cross-device sync** - Credentials sync across the Enterprise Browser, standalone desktop app (PWA), mobile (iOS/Android), and consumer browser extension. No setup required.
- **Data import** - One-click import from Chrome or Edge. CSV import from other password manager tools. Credentials mapped and policy applied automatically.
- **Encryption flexibility** - Choose your encryption model: Cloud, BYOK, or zero-knowledge architecture.

Why Island

1 Built in, not bolted on

Part of the Island Enterprise Platform, allowing you to govern every credential with the same engine managing your identity, access ,and data policies. One console, one policy, consistent enforcement.

2 Enterprise-grade security, everywhere

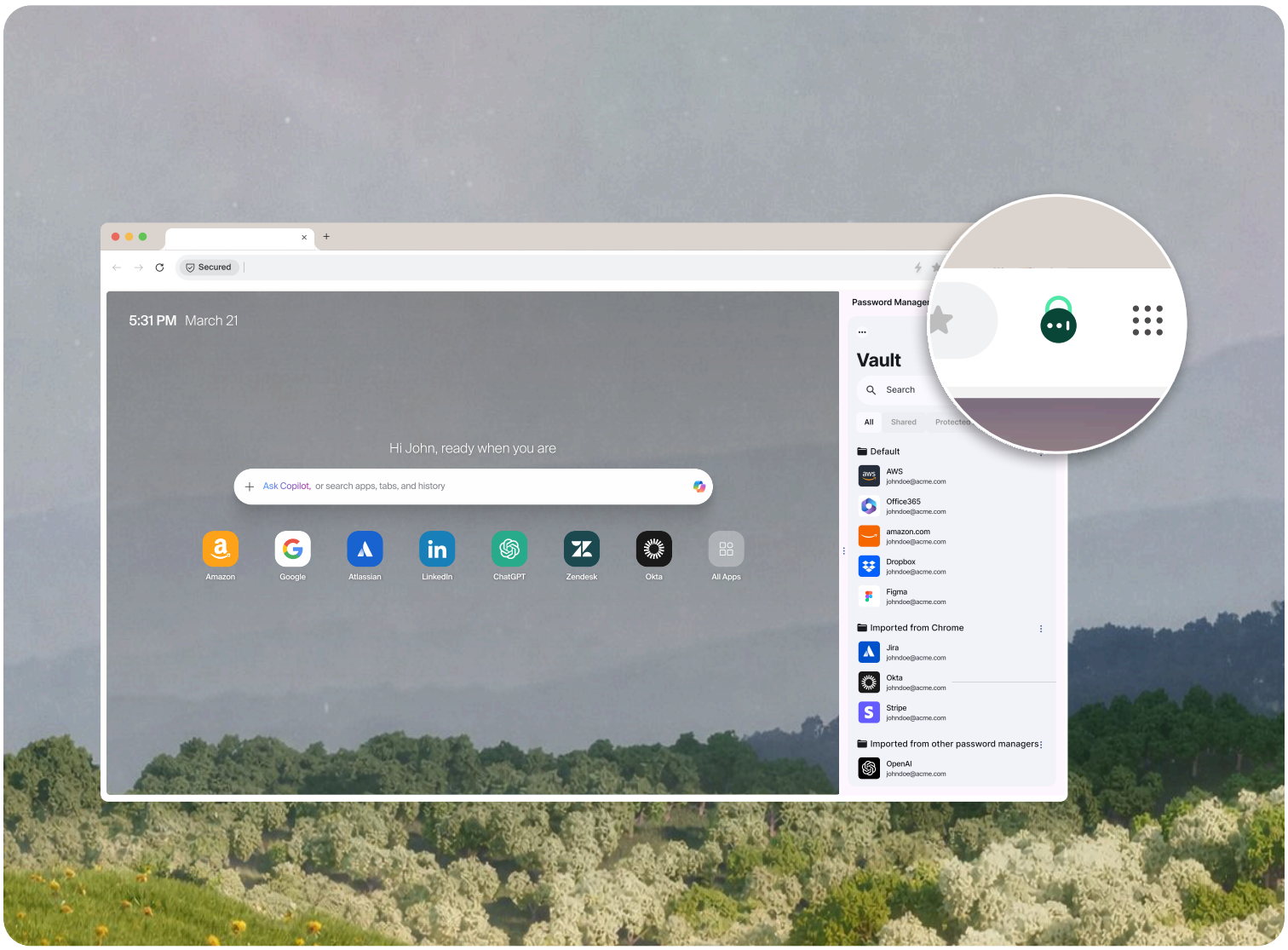
Island protects credential interactions. Real-time posture checks, domain validation, and session context govern every autofill while protection extends to the moment a password is used.

3 Deploy once. Protect everywhere

One toggle activates protection across the Enterprise Browser, desktop app, consumer browser extension (Chrome/Edge), and mobile. No parallel deployment. No user setup required. No separate license to renew.

4 Zero-friction user experience

Fast login and instant autofill, with automatic password generation and a seamless experience across every device. No friction. No training required. Enterprise-safe by design. Simple for employees to use.



> "As a bonus, the Island Enterprise Browser includes a built-in password manager rolled out to 100% of our end users, something only about 5% of users had access to before."

– William Dougherty
CISO, Omada Health

Why it matters?

63%
of employees store work passwords insecurely
Innovation Insight: Workforce Password Management Tools 2025

67%
reuse passwords across accounts
Innovation Insight: Workforce Password Management Tools 2025

81%
of hacking-related breaches involve stolen or weak passwords
IBM 2025 Cost of a Data Breach Report

1 in 2
share work passwords with people who shouldn't have access
Innovation Insight: Workforce Password Management Tools 2025

1 in 3
people experienced credential or identity theft in the last year
Identity Theft Resource Center

$4.8M
average cost of a breach initiated by phishing
IBM 2025 Cost of a Data Breach Report

About Island

Island is the ideal environment for enterprise work. Its Enterprise Platform unifies and embeds core modern work requirements like enterprise AI, network, and data protection directly into the browser, desktop, or anywhere work happens. With it, organizations see, control, and protect all work activity while users enjoy a smooth, seamless, AI-powered experience. Learn more at island.io.

amazon · CHIPOTLE · citi · lululemon · COSTCO WHOLESALE · SwissLife · Epidemic Sound · fiverr. · Marriott International · Teleperformance · T-Mobile · Pfizer · American Airlines · TaskUs · brightline · CWAN

See what password governance looks like when it's built for the enterprise. Get in touch

Island

The Enterprise Workspace