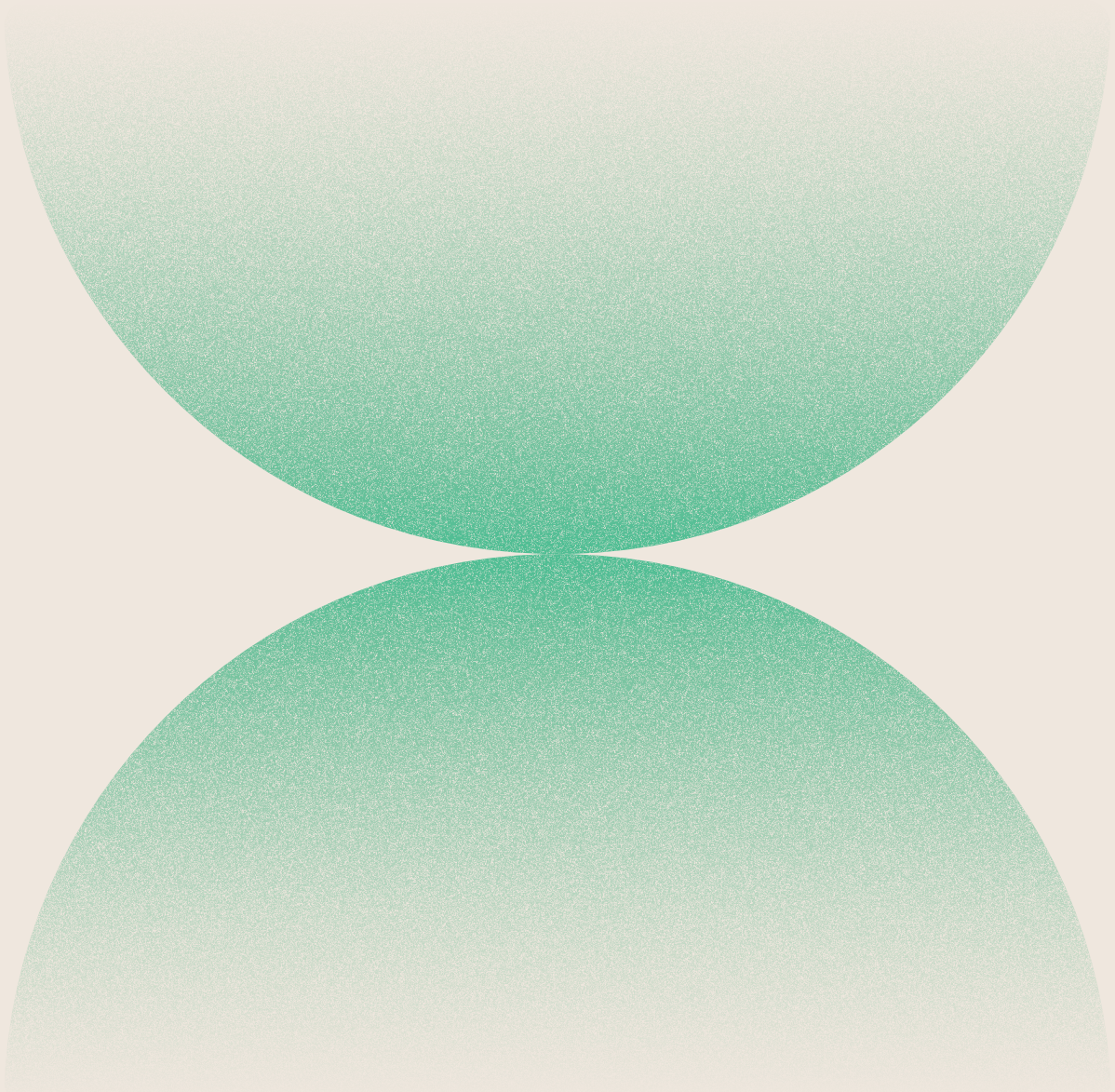
Island

The Importance of **an Enterprise Password Manager**

Solution Brief | May 2023



Introduction

The password as an authentication tool was introduced at the dawn of the computer era and we're still using them today. Improvements in cryptography for hashing passwords, passwordless authentication strategies, and federated identity management have reduced our reliance on passwords as a single point of failure. But the constant drum of breaches and successful hacking attempts shows that passwords remain a significant source of risk — particularly in an enterprise environment where a breach can cause massive reputational and financial damages.

Strong password policies require that users maintain complex, unique passwords for each service or website they use, and update passwords periodically. Even with an enterprise identity provider, users need to manage dozens of passwords for legacy or third party systems that fall outside the scope of IDP. A good password manager is no longer a luxury, but increasingly a critical tool for good password hygiene. This paper outlines the challenges and vulnerabilities for password management and why enterprise security necessitates an enterprise password manager.

Password Vulnerabilities

The first hurdle to clear for strong passwords is complexity. As raw computing power continues to increase along Moore's law, the cost of brute-force attacks on passwords decreases. Today, a password with eight or fewer characters (or a word found in a dictionary) can be cracked in minutes — making a simple password little better than no password at all. The solution to this is password complexity: using longer passwords with a mix of uppercase and lowercase, numbers, and symbols. The same attributes that make strong passwords resistant to computer-based attack also make them difficult for humans to memorize.

A related class of password failure is the breach of the database or service that stores passwords for an application or web service. Sadly, this is all too common: the online password breach tracking site Have I Been Pwned tracks a running tally of over 650 websites and some 12.4 million accounts that have been compromised. The danger for a breach is two-fold: first, all the accounts on that site are immediately vulnerable to exploitation. Second, and more troubling, is the risk to completely unrelated sites or applications if those passwords are reused elsewhere. Once a password dump is breached, malicious attackers will attempt to use the same email & password on other sites and services. This underscores the critical importance of maintaining passwords that are both complex *and unique* across every service.

The next risk to password failure is direct disclosure: handing over passwords to a malicious attacker. Phishing and Man-in-the-Middle attacks are two common avenues for intercepting credentials, and both are frequently exploited for credential compromise. Malware often achieves the same result by infecting a host system and recording keystrokes, exfiltrating working memory, or using other advanced techniques to capture passwords. Web browser cookies can be used to directly hijack an authenticated session and masquerade as a user, without even requiring password disclosure directly. These threats are categorically different in that they are immune to password complexity and uniqueness — even the strongest password will fail if it's directly disclosed to an adversary or a session is hijacked.

Last, a word on multi-factor authentication (MFA): Requiring additional factors beyond a password is an important step to protecting accounts. But, just like passwords themselves, other factors can fail with a determined attacker. The most common MFA approach is SMS-based text messages with a one-time code. While far better than a password alone, SMS-based MFA is far from bulletproof. Attackers can use social engineering to hijack a phone number through the mobile carrier, or convince a user to share the code directly as part of an advanced phishing attack. Fortunately, MFA technology advancements offer much stronger solutions such as FIDO2 and WebAuthn that greatly improve the security posture of the login flow and make use of biometrics and cryptographically-signed challenges to greatly improve login security.

A Password Manager Address Some — But Not All — Concerns

A good password manager is a de facto requirement for any online activity, whether personal or in the workplace. Thankfully, password managers are now commonplace. These range from free services included with most web browsers and operating systems to paid services like 1Password or LastPass that add valuable features like password health checks syncing across devices and browsers. The most important feature of a password manager is the relative ease for generating long, complex passwords that are unique for each website or application. When used as intended, this effectively addresses the first two challenges of weak passwords and password breaches.

> The danger for a simple password manager is that it can instill a false sense of security across two dimensions: password storage and password usage.

By its nature, a password manager is the ultimate prize for a malicious attacker. If an adversary can compromise a device and gain access to locally stored passwords, or breach the online service that stores passwords for syncing and retrieval, all is lost. Some services go to great lengths to protect the password store, offering strong encryption methods that can only be unlocked by a user with a password they alone know. Others are tragically incomplete in their password storage scheme and have been exploited by attackers. And as we've seen in repeated stories over the past many years, adversaries prize exploitation of a password manager's services.

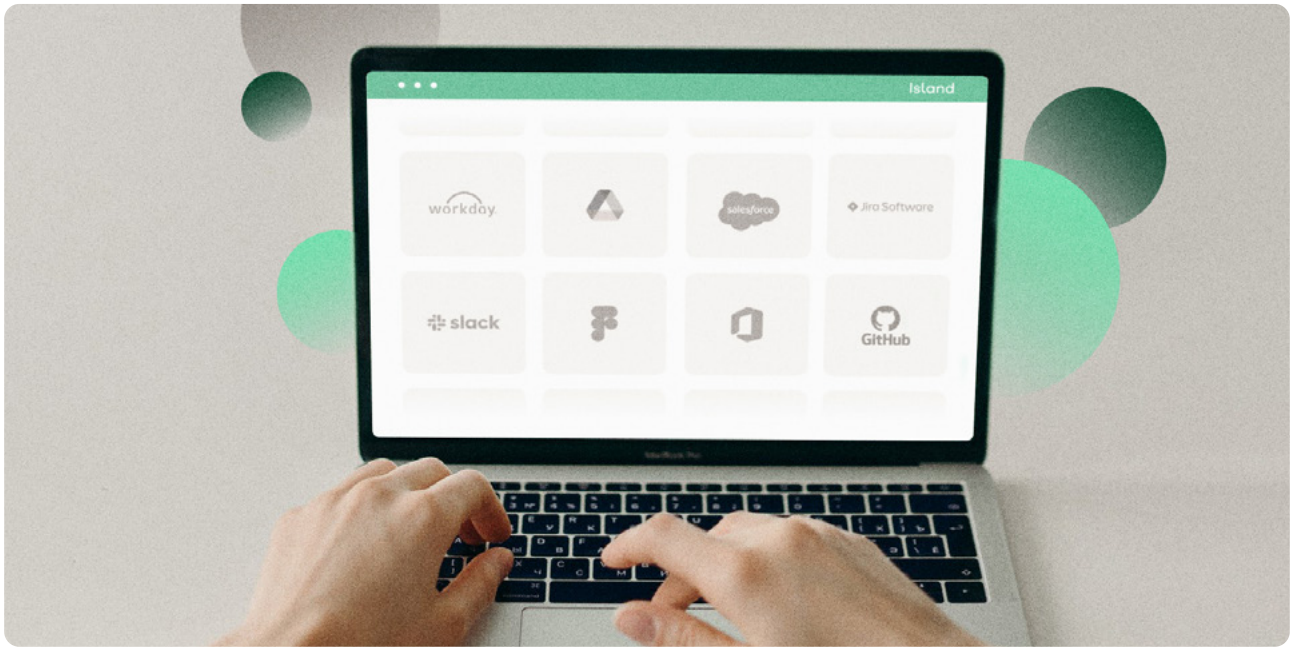
The more immediate risk to consider is password usage itself. As outlined above, even the strongest password manager alone cannot stop phishing or MitM attacks from stealing passwords. The web browser where passwords are used is an equally critical aspect for maintaining security. An outdated or vulnerable web browser can be exploited to hijack a session directly through cookie exfiltration or memory dump. Each layer in the stack, from device and OS, to web browser, to the network itself must work together with the password manager to ensure full protection of the user and their credentials. Worse yet, exfiltrating passwords from the existing password managers in browsers such as Chrome are trivial through the use of readily available online tools.

The Island Enterprise Browser with Island Password Manager Delivers a Complete Enterprise Password Management Solution

Island, the Enterprise Browser, completes the enterprise password management challenge. At baseline, Island offers the same password creation and retrieval capabilities that encourage good password hygiene with complex, unique passwords. What separates the Island Password Manager from commonplace consumer-oriented password managers is its inclusion within the Island Enterprise Browser.

Every user who uses the Enterprise Browser authenticates with their organization's enterprise identity provider — meaning all access to the browser and the password manager is protected with enterprise-grade authentication. This includes strong MFA strategies like WebAuthn to gracefully include biometric identity challenges as part of the login flow. Island also evaluates device posture to ensure that Island can only be used on devices that meet organizational standards, such as requiring OS patching and full disk encryption. Unlike consumer password managers, the only way to access the Island Password Manager is through the Island Enterprise Browser. When a user leaves the organization, or if their device is lost or stolen, access can be immediately revoked to eliminate the risk of compromise.

Going further, the Enterprise Browser offers a unique set of security controls to protect the browser footprint and everything it engages with. Island goes beyond consumer browsers to protect against known and unknown web-based as well as physically-local threats. Working memory, cache, cookies, and even keystrokes are protected against tampering or exfiltration. This means passwords and applications within the Enterprise Browser are secure, even if the device they're accessed on is unmanaged.



All web activity within the Enterprise Browser, including every login flow, is protected against the full range of threats. As outlined above, the threats to passwords and the applications they protect are varied and always changing. Effective protections must be broad as well, across every layer of interaction from the passwords themselves, to the browser environment, to the OS and device configuration.

Common Password Attacks

Threat Type	How Adversaries Attack	Island Enterprise Browser Protections
Password complexity	Simple passwords can be brute-force guessed	Require complex passwords
Password uniqueness	One breach can disclose passwords used on other sites & services	Require unique passwords
MFA Weakness	SMS hijack via mobile phone number porting; advanced phishing	Use strong MFA techniques like WebAuthn
Unpatched OS	Exploit known vulnerabilities in OS	Require minimum OS patch level and secure device posture (EPP, encryption, location, etc.)
Unpatched browser	Exploit known vulnerabilities in a consumer browser	Force browser updates automatically
Stolen device	Use local password data saved on the device	Require full disk encryption; no local password storage; block lost or stolen devices from accessing Island
Phishing	Convince a user to enter a password on a spoofed login page	Warn users and block untrusted login pages
MitM Attack	Intercept passwords over the network by inserting a malicious intermediary between the device and their intended destination	Block Man-in-the-Middle attempts
MitB Attack	Intercept passwords within the browser by inserting malware on the device	Block Man-in-the-Browser attempts
Session hijack	Use malware to exfiltrate cookies & cache to hijack an authenticated session	Encrypt cookies and cache
Keystroke logging	Use malware to intercept keystrokes and steal passwords	Encrypt keystroke buffer
Advanced Threats	Myriad known and unknown attack vectors	Protect all browser activity from both web-based and physically-local attack; collect analytics for security researchers & incident response

Going beyond the security benefits of the Enterprise Browser with Island Password Manager, users also benefit from a native in-browser user experience that can't be replicated by third-party extensions or applications. There is nothing extra to install or configure, and the Island Password Manager is displayed as a side-panel that doesn't overlay or block any screen real estate. Strong, unique passwords are automatically generated and suggested when registering an account and automatically offered on login pages.

> **By combining the Enterprise Password Manager with the Enterprise Browser, Island delivers a uniquely elegant experience for end-users and administrators alike.**

Conclusion

Strong password management is critical to building a complete enterprise security architecture. A password manager is an important leg of the stool, but passwords are only as strong as the browser and device posture where they're used. By combining the Enterprise Password Manager with the self-protecting Enterprise Browser, Island offers a complete solution that is impossible to replicate with a collection of disparate tools.