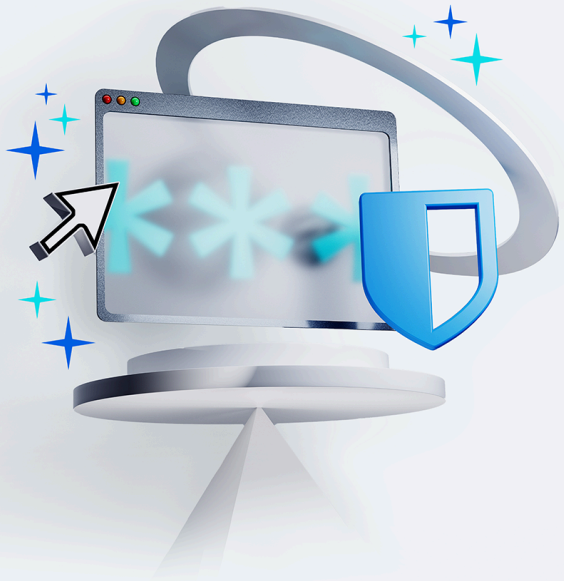
bitwarden

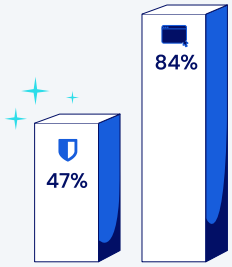


BITWARDEN SECURITY PERSPECTIVES

Evolving beyond browser-based

Why leave browser-based password management behind?

Browser-based password managers have long provided basic convenience. But by modern standards, they lack the robust security, functionality, and scalability that today's businesses require. Limitations include vulnerability to browser exploits, inadequate encryption, poor cross-platform compatibility, and lack of centralized management controls. Fortunately, credential management has come a long way.



Users of third-party (dedicated) password managers are significantly less likely to reuse passwords compared to those relying on browser-based managers. One study found that **only 47% of dedicated password manager users reported reusing passwords**, whereas 84% of those using browser-based managers admitted to the practice.

Source: USENIX Association

In this article

What makes the dedicated password manager a better alternative?

Dedicated password management platforms overcome the shortcomings of browser-based solutions. They also introduce important new features, enhanced security, and portability. Specific features to look for:

- **Advanced encryption**: end-to-end AES-256 encryption and zero-knowledge principles can protect credentials far more effectively.
- **Cross-platform support**: seamless integration extends across all major browsers, mobile devices, and operating systems.
- **Centralized credential vault**: provides secure storage and management for passwords, credit cards, secure notes, and infrastructure secrets like API keys.
- **Secure credential sharing**: encrypted and controlled sharing options include secure transmission to anyone.
- **Enhanced security features**: robust MFA integration, phishing-resistant auto-fill protection, and breach reports all help proactively manage security risks.
- **Role-based access control (RBAC)**: allows precise control of credential access based on specific user roles and responsibilities.
- **Comprehensive audit and reporting**: detailed activity logs and compliance reporting improves visibility and regulatory adherence.
- **Secrets management**: secure handling of DevOps credentials, API keys, and other infrastructure secrets is critical within development pipelines.

How dedicated password managers keep today's businesses safer

The password managers built into browsers like Chrome, Firefox, and Safari may offer basic password-saving features. But dedicated password managers provide far more comprehensive, secure, and efficient solutions for managing credentials. Today's leading solutions allow you to:

- **Strengthen cybersecurity**: safeguard against browser vulnerabilities, malware, phishing, and credential theft.
- **Improve credential habits**: encourage stronger password practices and proactive management of weak or compromised passwords.
- **Enhance credential control**: provide IT teams with centralized management, visibility, and enforcement capabilities.
- **Facilitate secure collaboration**: enable secure credential sharing within teams, including the option to share hidden passwords.
- **Ensure regulatory compliance**: simplify adherence to standards like ISO 27001 SOC 2, HIPAA, and GDPR through audit-ready security practices.
- **Support operational continuity**: ensure ongoing access to critical credentials, minimizing operational disruptions.
- **Reduce IT overhead**: minimize password-related support requests by adding automation and self-service capabilities.
- **Secure infrastructure credentials**: leverage specialized solutions for secure management and automated injection of DevOps secrets.

Adopting best practices for password and credential management allows a business to address security gaps, improve access control, and enhance employee productivity.

How Bitwarden helps support modernization

Bitwarden offers a comprehensive, secure, scalable solution. They also provide businesses with a clear path for embracing a more robust, enterprise-grade approach to credential security. Bitwarden facilitates a seamless, secure, successful transition by:

- **Offering a centralized, secure vault**: securely storing and managing credentials, infrastructure secrets, and sensitive information with AES-256 encryption.
- **Ensuring cross-browser and device compatibility**: allowing users consistent, secure access across diverse devices and platforms.
- **Enabling secure credential sharing**: providing robust tools like Bitwarden Send for encrypted credential sharing to anyone.
- **Implementing strong security measures**: leveraging MFA, domain matching, and breach monitoring to protect against credential theft and phishing.
- **Automating credential management**: integrating with directory services like AD and SCIM for efficient employee onboarding, offboarding, and automated credential provisioning.
- **Providing detailed audit and compliance tools**: comprehensive logging and reporting enhances security oversight and regulatory compliance.
- **Securing DevOps and IT credentials**: specialized management of DevOps secrets, including automated rotation and secure injection in development pipelines.

The bottom line

By migrating to the enterprise-grade protection of Bitwarden, businesses can significantly improve their security posture within a very short time frame. This represents an opportunity to address security gaps, improve access control, and enhance employee productivity.

You'll also be streamlining every facet of the credential management processes. Just one more reason Bitwarden is regarded as the most trusted name in password management.

What makes Bitwarden stand out from the pack?

Bitwarden provides administrators a seamless, secure way to wean employees off of browser-based password managers in favor of a centrally-managed enterprise password manager. Unlike other password management offerings:

- Bitwarden's browser plugin supports nine browsers: Chrome, Edge, Firefox, Safari, Opera, Brave, Vivaldi, Tor, and DuckDuckGo. This represents the largest number of supported browsers for a password manager's browser-based plugin.
- Administrators can automate the deployment of Bitwarden browser extensions to end users via Microsoft Intune. Read more about this option in our deep dive: Deploy Browser Extensions with Intune.