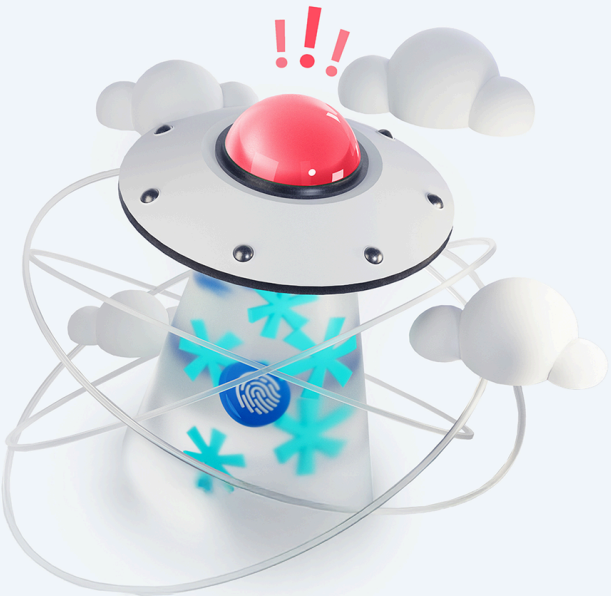
bitwarden



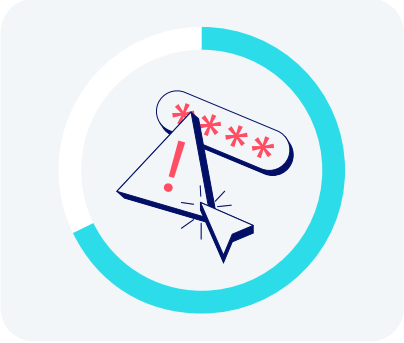
BITWARDEN SECURITY PERSPECTIVES

Data loss prevention

What you need to know

What exactly is data loss prevention?

Data Loss Prevention (DLP) refers to strategies and tools designed to identify, monitor, and protect sensitive data from threats like unauthorized disclosure, accidental leakage, or theft. One of the most important aspects is preventing the unauthorized transfer of sensitive information outside of secure environments. This is commonly known as data exfiltration.



Highlighting the risk DLP helps mitigate,

68% of data breaches

in 2024 involved non-malicious human actions, such as errors or falling for social engineering.

Source: Verizon 2024 DBIR

How does password management fit in here?

Password management plays a critical role in making Data Loss Prevention work. It helps an organization secure employee credentials, manage access to sensitive information, and mitigate human error. Specific features to look for:

- **Centralized credential management:** securely stores credentials in encrypted, centralized vaults. This prevents unauthorized access while minimizing risks from unmanaged accounts.
- **Role-Based Access Control (RBAC):** assigning credentials based on individual or group roles reduces insider threats by ensuring that employees can only access the specific information they need to get their work done.
- **Secure secrets management:** centralizing critical infrastructure credentials minimizes exposure of sensitive API keys and cloud tokens.
- **Encrypted passwords sharing:** secure methods for password sharing help prevent exposure risks posed by insecure channels like email or messaging apps.
- **Multi-Factor Authentication (MFA):** requiring additional verification adds a crucial layer of security. This significantly reduces the risk of credential theft.
- **Automated offboarding:** immediately revoking access when an employee leaves helps protect against data theft.
- **Audit and activity monitoring:** detailed logging of credential usage and access helps detect suspicious activities. This helps improve both incident response and compliance efforts.

Together, these features help maximize the effectiveness of Data Loss Prevention. These systems play a vital role by classifying critical data, monitoring its use, and enforcing policies that prevent improper sharing. They also help to ensure compliance with data protection regulations, maintaining confidentiality and safeguarding valuable intellectual property.

How data loss prevention keeps today's businesses safer

In this article

Using password management to implement Data Loss Prevention is a powerful way to protect against the growing risks posed by cyberthreats, insider breaches, and regulatory compliance pressures. It allows you to:

- **Protect sensitive information:** many businesses routinely handle sensitive data like financial records, customer information, or intellectual property. It's imperative to safeguard against unauthorized data leakage or theft.
- **Mitigate insider threats:** controlling data access through role-based permissions helps companies reduce the risk of any employee leaking data, either accidentally or intentionally.
- **Prevent cyberattacks:** an important component of any effective security strategy is protection against common breach threats like phishing, malware, and credential stuffing.
- **Ensure regulatory compliance:** by adhering closely to stringent regulations like GDPR, HIPAA, and PCI DSS, companies can avoid costly legal penalties.
- **Preserve reputation:** in today's world, maintaining customer trust and brand integrity are critical factors in ensuring business continuity.
- **Reduce costs:** data breach responses, regulatory fines, and lost productivity are all expenses that any business seeks to avoid.

How Bitwarden supports data loss prevention

Bitwarden helps achieve Data Loss prevention through a comprehensive set of password management and security solutions. These include:

- **Zero-Knowledge encryption:** encrypts data locally on users' devices, ensuring that only authorized users can access credentials.
- **Centralized credential vaults:** prevents credentials from being fragmented and exposed across insecure locations.
- **Advanced access control:** restricts credentials based on employee roles and responsibilities, minimizing over-permissioning.
- **Secure credential sharing:** facilitates encrypted and time-limited credential sharing, eliminating many unsafe sharing practices.
- **Proactive security monitoring:** quickly alerts users about compromised credentials, encouraging timely password rotations to prevent unauthorized data access.
- **Comprehensive audit trails:** logging credential access attempts, password changes, and unusual activity directly supports compliance audits and forensic investigations.
- **Robust MFA integration:** strengthens login processes, ensuring only verified users can gain access to critical data.
- **Automated credential management:** automates employee onboarding and succession, revoking access to prevent unauthorized access post-departure.

The bottom line

Now more than ever, organizations need to take a proactive approach toward securing their sensitive data. It's critical to minimize the risk of external cyberthreats, insider breaches, and regulatory compliance pressures.

Bitwarden offers a powerful, user-friendly platform with a robust feature set. Together, these tools can significantly strengthen Data Loss Prevention efforts while preventing data exfiltration. Just one more reason Bitwarden is regarded as the most trusted name in password management.

What makes Bitwarden stand out from the pack?

Bitwarden uniquely enables customers to implement effective Data Loss Prevention strategies through an intelligent combination of:

- A user-friendly approach and coverage across all device, to enhance broad employee adoption for maximum protection.
- Companies can choose from a wide variety of policies and deployment configurations designed to protect sensitive information. Options range from highly centralized to more flexible approaches.
- An option for centralized data ownership provides utmost protection and continuity for large organizations.