bitwarden

BITWARDEN SECURITY PERSPECTIVES

Least privilege access

What you need to know

What exactly is Least Privilege Access?

Least Privilege Access (LPA), also known as the Principle of Least Privilege, is a security approach designed to limit permissions for users, processes, and applications. The idea is to allow access to only the specific items needed to accomplish a task. One of the most effective ways to implement this is through Role-Based Access Control.

75%

of security failures predicted to stem from poor identity/privilege management.

Source: Gartner

In this article

What exactly is Least Privilege Access?

How does Password Management fit in here?

How Least Privilege Access keeps today's businesses safer

How Bitwarden supports Least Privilege Access

The bottom line

Why Does Bitwarden Stand Out Among Alternatives?

How does Password Management fit in here?

Password management plays a critical role in making Least Privilege Access work. It helps ensure that individual users aren't inadvertently given unnecessary access to sensitive information. Specific features to look for:

- **Role-based access control (RBAC) framework:** a robust password manager will provide a comprehensive RBAC framework, assigning appropriate access levels.
- **Granular permission control:** advanced password managers allow fine-tuning of permissions for shared credentials. Examples include read-only access, write access, and managerial access.
- **Credential sharing with hidden passwords:** a password manager can facilitate secure sharing by letting users autofill passwords without actually seeing them.
- **Encrypted secure ephemeral sharing:** some password managers allow for sharing of sensitive items with specified people for a limited time.
- **Audit trails and monitoring:** by logging events, a password manager can help pinpoint details of unauthorized activities.
- **Enforced strong passwords:** this feature reduces the risk of compromise by generating only complex passwords.
- **Zero-knowledge principles:** ensures the highest level of protection by enforcing complete end-to-end encryption for all items in a vault.

Together, these features help maximize the effectiveness of Least Privilege Access. They help you reduce security risks while ensuring that employees have whatever access they need to get their work done.

How Least Privilege Access keeps today's businesses safer

Using password management to implement Least Privilege Access is a proven approach to enhance security, minimize risk, and streamline access control. It allows you to:

- **Reduce the risk of data breaches:** limiting access reduces the attack surface. Even if one individual is compromised, potential damage is contained.
- **Prevent insider threats:** restricting the access of any individual reduces the risk and scope of internal data theft or sabotage.
- **Strengthen compliance and auditing:** providing audit logs for monitoring access promotes compliance with regulations like ISO270001, GDPR, HIPAA, and SOC 2.
- **Limit credential sharing risks:** using end-to-end encryption when sharing credentials limits access to specifically selected recipients.
- **Streamline employee onboarding and succession**: simplify access management while providing for immediate revocation of credential access.
- **Enhance productivity:** reduce time spent on password issues, including forgotten passwords and time-consuming password resets.
- **Support remote and hybrid workforces:** easily secure access across any device, anywhere.
- **Protect against credential reuse attacks**: reduce exploitation risks by encouraging strong, unique passwords.

Least Privilege Access is a powerful way for businesses and organizations to reduce security risks, improve efficiency, and ensure regulatory compliance.

How Bitwarden supports Least Privilege Access

Bitwarden helps achieve Least Privilege Access through a comprehensive set of security features, access controls, and management tools. These include:

- **Role-based access control:** offers custom roles and granular permissions, assigning minimum necessary privileges. Roles include Admin, Owner, and User, along with a full set of options for Custom Roles
- **Collections for grouped access:** organizes credentials by function, granting access only to those teams, departments, or individuals who need it.
- **Granular sharing controls:** allows admins to assign permissions for Read-Only, Read and Write, or Manager.
- **Encrypted vaults for secure storage:** all data is end-to-end encrypted.
- **Audit logs and activity monitoring:** provides detailed logs for every access event.
- **Account recovery:** allows approved administrators to gain critical credentials in emergencies.
- **SSO integration:** helps strengthen identity verification.
- **Enforced security policies:** supports policies like master password strength and 2FA requirements.
- **Administrator access limiting:** allows a range of options for limiting admin visibility to stored shared items.

The bottom line

Even in an age of increasingly sophisticated cyberthreats, it's possible to improve security without compromising productivity. Now you can ensure that employees have precisely the

access they need to get the job done.

Bitwarden offers a thoughtful combination of role-based controls, secure sharing, and robust monitoring. Together, they directly support today's best practices for Least Privilege Access principles. Just one more reason Bitwarden is regarded as the most trusted name in password management.

Why Does Bitwarden Stand Out Among Alternatives?

Bitwarden Password Manager is built with the needs of modern enterprises in mind, including, scalability, wide integration compatibility, centralized management, and flexibility to enact a principle of least privilege:

- Bitwarden allows organizations to choose the level of least privilege that works for them with options for adjusting administrator visibility to shared items.
- All items shared in Bitwarden are owned by the organization, providing centralized management access control.
- Powerful APIs allow for integration into other tools, including SIEM tools for real-time security alerts.
- Reporting to easily spot over-privileged users for streamlined auditing and remediation.