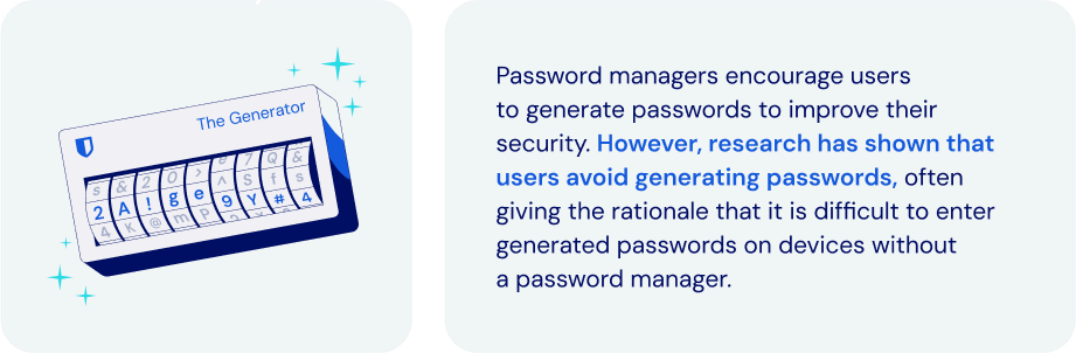
bitwarden

BITWARDEN SECURITY PERSPECTIVES

Application and employee-centric

What exactly is application and employee-centric credential management?

Application and Employee-Centric Credential Management is an integrated strategy for securely managing passwords and credentials. IT teams can use it to efficiently provision, manage, and update credentials while providing employees with intuitive self-service tools. The idea is to enhance security, improve productivity, and reduce credential-related risks.



Source: https://arxiv.org/abs/2409.03044

How does password management fit in here?

Password management solutions play a crucial role in enabling both application-centric and employee-centric credential management. This helps ensure security, efficiency, and compliance. Specific features to look for:

- **Centralized credential storage**: provides a secure, encrypted vault for both shared application logins and individual employee credentials.
- **Granular role-based access control (RBAC)**: minimizes unauthorized usage by restricting credential access based on clearly defined roles.
- **Application-specific credential organization**: uses collections or folders to categorize credentials by application, department, or project.
- **Secure credential sharing**: allows secure access to specific groups or individuals, including sharing of credentials to anyone.
- **Employee-Specific credential management**: provides secure vaults for individual employees' private work-related credentials.
- **Automated onboarding and succession**: integrates with directory services like SCIM or Active Directory, streamlining credential management throughout the employee experience.
- **Credential management for DevOps pipelines**: manages sensitive credentials like API keys and database passwords securely within CI/CD pipelines.
- **Multi-factor authentication (MFA)**: enhances security by integrating MFA for both application and employee account access.
- **Detailed audit logs**: maintains comprehensive tracking of credential access, changes, and sharing to support compliance and investigations.
- **Secure password generation**: automatically generates strong, unique passwords to comply with company policies that prevent reused and weak passwords.

In this article

- **Employee education**: promotes strong credential habits through integrated security awareness training within password managers.

This approach is designed with flexibility in mind—it can easily be tailored to fit the needs of both individual employees and specific business applications. A modern password management platform should be capable of supporting and enhancing these efforts.

How application and employee-centric credential management keeps today's businesses safer

Modern businesses rely on a growing number of applications, platforms, and user accounts to manage operations successfully. Unfortunately, this introduces new challenges in securing credentials across teams, departments, and individual employees. Sound credential management is crucial for businesses because it:

- **Enhances security**: centralized control and secure credential practices protect against phishing, credential stuffing, and unauthorized access.
- **Protects critical business applications**: reduces risk associated with manual or insecure credential handling by securing sensitive application logins.
- **Improves operational efficiency**: automated onboarding/succession and simplified credential management reduce administrative overhead.
- **Supports regulatory compliance**: comprehensive audit logging and security enforcement ensure adherence to compliance and protection regulations including ISO 27001, GDPR, HIPAA, and SOC 2.
- **Reduces IT support costs**: self-service recovery and auto-generated passwords minimize common credential issues like forgotten passwords.
- **Boosts employee productivity**: auto-fill and secure access across multiple applications/platforms streamlines workflows.
- **Facilitates secure collaboration**: allows teams to securely share and manage credentials for shared resources without compromising security.
- **Minimizes insider threats**: mitigates potential internal risks by instantly revoking credential access whenever an employee leaves or changes roles.
- **Supports remote workforce security**: secures credential access across remote and hybrid work environments.

By adopting a robust password manager, businesses can protect sensitive credentials, reduce security risks, and improve productivity across both applications and employees. It's an effective way to keep a digital ecosystem secure, organized, and scalable.

How Bitwarden supports credential management

By combining centralized storage, granular access control, and automated management features, Bitwarden streamlines credential security across internal teams and external applications alike. The platform effectively manages application and employee-centric credentials by providing:

- **Unified central vault**: easily manage and administer important credentials across employees.

- **Shared passwords**: share security with simple mechanisms for ongoing or one-time access.
- **Option for individual employee vaults**: provide employees with individual vaults for their own specific logins if desired.
- **Role-based and collection-based access control**: precise credential access can be tailored to specific roles and departments.
- **Automated lifecycle management**: helps at every stage, from streamlined onboarding to immediate credential revocation upon employee transition.
- **Secure DevOps secrets management**: provides for secure handling and automated rotation of sensitive infrastructure and API credentials.
- **Advanced security features**: best-in-class security includes comprehensive MFA integration, secure credential sharing, multifactor encryption, and phishing-resistant domain matching.
- **Comprehensive audit and compliance support**: detailed activity logs assist with regulatory compliance.
- **Cross-device access**: helps ensure business continuity and secure credential access across various platforms and devices.

The bottom line

As organizations continue to adopt more cloud-based tools, SaaS platforms, and remote work environments, managing user credentials securely becomes increasingly complex. It also becomes more important than ever.

Bitwarden can help any organization secure their valuable credential ecosystem. It's a great way to quickly achieve robust protection, improved productivity, and regulatory compliance. 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 value to both companies and their employees. From an administrative perspective, IT and security teams using Bitwarden have an option to dig deeper into the most important applications employees are using. This allows them to better understand the strength of credentials used, implementing mechanisms that encourage users to maintain the most secure behavior. Bitwarden refers to this approach as Access Intelligence and Risk Insights. Bitwarden offers:

- The option to provide employees with individual vaults, along with access or an organization vault.
- Client applications translated into over 50 languages, creating a smooth user experience for all employees—especially those within global organizations.
- Friendly expert support for millions of users at businesses worldwide.