RESOURCE CENTER

# The credential lifecycle: Stay ahead to strengthen your security and access management

Get the full interactive view at
https://bitwarden.com/resources/credential-lifecycle-management/

bitwarden

## Credential lifecycle management starts with centralized ownership

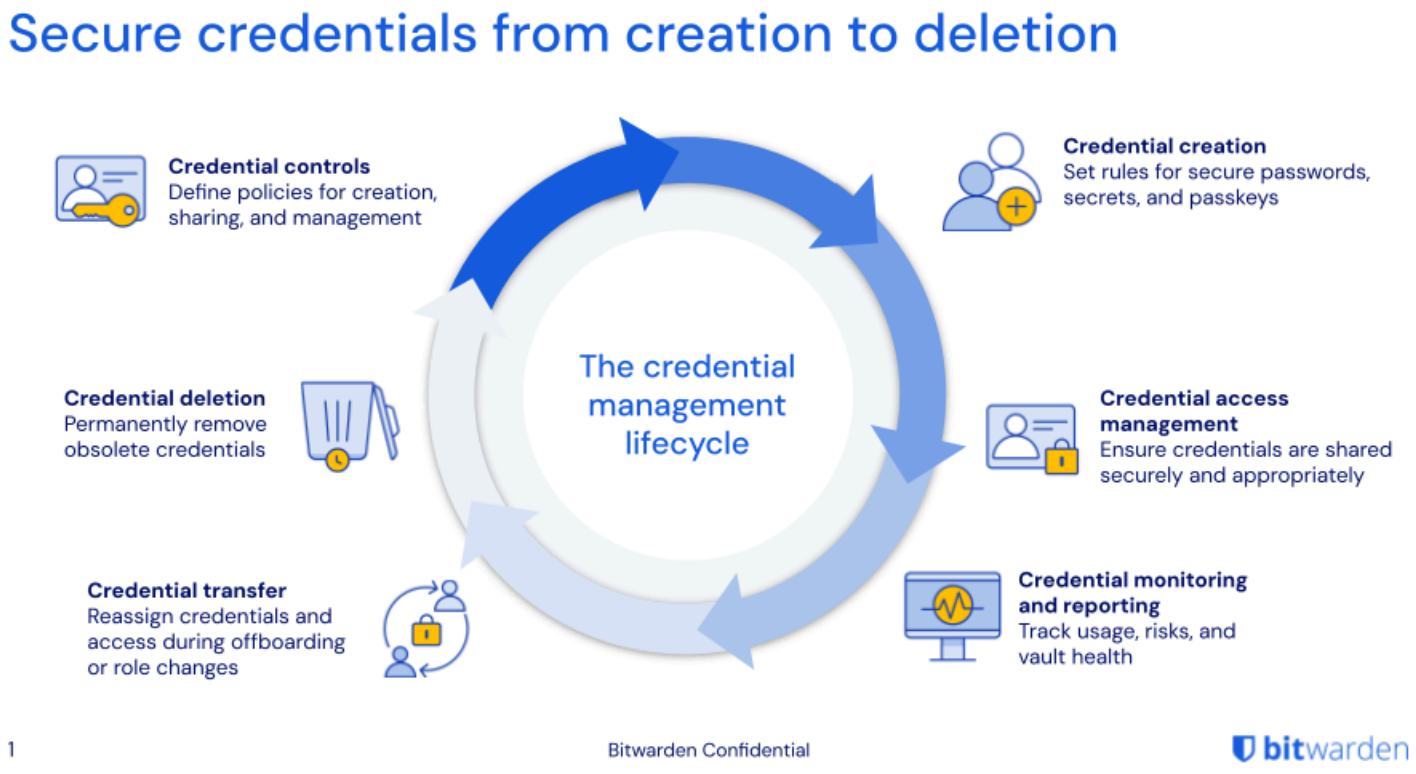
Managing credentials is one of the most important aspects of maintaining and safeguarding business security and data. However, many organizations are still struggling with how to handle credentials beyond their initial creation.

Just as every employee experiences a user "lifecycle" that starts with hiring and onboarding, credentials also have a life cycle, from creation to deletion. This is part of a comprehensive process known as identity lifecycle management, which is also a key component of maintaining security and access control, ensuring authorized users have proper access to digital assets, systems, tools, applications, and resources to be successful and secure.

The first step in establishing effective credential management is establishing centralized credential ownership. Without a clear ownership structure, credentials become scattered, untracked, or even lost when employees change roles or leave.

**By centralizing ownership, organizations gain:**

- Full visibility to make sure all user credentials are accounted for and meet security policies
- Comprehensive reporting where insights into all credentials are available for audits and compliance
- Complete event logging where every action taken on credential usage is tracked
- Seamless offboarding so credentials are easily transferred to another user when an employee leaves, preventing orphaned or inaccessible credentials




## What is the credential lifecycle?

Much like every employee has a journey within their organization, digital credentials also undergo a journey that starts with creation,

with several stages in between, and ends in deletion.

**The main phases of the credential lifecycle include:**

Credential controls

- Build a centralized approach to credential management. Define key policies for how credentials are created, shared, and managed. These include policies around collection management, individual vault policies so credentials are organized and compliant from the start.

Credential creation

- Creating any credential – whether it's a password, secret, SSH key, API key, passkey, or any other sensitive information. For example, setting a policy around password length ensures credentials follow standard and secure creation processes.

Credential management

- Ensure your users and teams are sharing credentials that follow secure guidelines and policies. This means, only the right people have the right credentials at the right time.

Credential monitoring and reporting

- Monitor for risks by tracking how credentials are used, accessed, and any other patterns that could signal security risks. Bitwarden vault health and member access reports help you stay on top of credential health.

Credential transfers

- For offloaded users or users changing departments, their credentials may need to be transferred to new owners. This is an important part of the offboarding, deprovisioning, or departmental change process to ensure access is reassigned quickly.

Credential deletion

- When a credential is no longer needed, it needs to be properly and permanently deleted so it's not lingering in the system without admin oversight.

## Challenges for companies without centralized controls

Without a well defined credential management strategy that starts with centralized credential control, many organizations leave themselves vulnerable to data breaches, credential misuse, and unauthorized access. Here are some examples:

### Lack of visibility and oversight

According to Forrester, 80% of data breaches are caused by misusing privileged accounts. Imagine your organization has just experienced a data breach – what happens if you need to conduct a security audit of the access rights of users inside and outside your organization? Mismanaging digital credentials can lead to significant security risks, making it crucial to have robust policies and tools in place to protect and manage these credentials effectively.

### The SSO security gap

The credential lifecycle takes into account that not all applications support SSO. Many legacy systems, third party services, and cloud applications do not integrate with SSO providers. Employees also often need to access external vendor portals, partner sites, or other SaaS tools that are not connected to their organization's SSO system. Not to mention unapproved applications – employees often sign up for SaaS tools independently, without admin approval. As such, these applications wouldn't be integrated with the SSO system. This

is where credential management provides redundancy and business continuity, ensuring full coverage and admin oversight across all applications and use cases.

### Offboarding risk

A recent study by Wing Security found that 63% of businesses may have former employees with access to organizational data. Offboarding employees may at surface seem like a simple admin task. But without proper processes that take into account not only data but credential access, organizations are at risk for:

- Data breaches
- Intellectual property theft
- Offboarded users who still have access to credentials
- Lost or forgotten credentials left by offboarded users
- Shared credentials that can no longer be accessed by current users

By controlling ownership from the start, organizations can proactively manage security risks, streamline access, and maintain complete oversight throughout the entire credential lifecycle.

## Credential lifecycle management with Bitwarden

### A modern approach to secure sharing

Competing password managers fail to treat credentials as dynamic pieces of data. For example, some vendors force users into a rigid sharing model, making it impossible to assign individual vault credentials to multiple vaults. A marketing team that needs just one credential from the product team will need to be assigned to the entire product team vault.

Others completely lack the ability for centralized vault control and management. This de-centralized model where every credential is owned by an individual user means users may have private credentials not visible to admins, leading to orphaned records and posing major security risks. Managing all of this – while fine for smaller companies – becomes nearly impossible to scale on the enterprise level.

Bitwarden offers a better way, one that takes into account the fact that enterprise credentials are vital, dynamic sources of data and that enterprises require both security and flexibility for credential management. By emphasizing the importance of digital credentials in secure sharing practices, Bitwarden ensures that sensitive information is protected from cyber threats through robust policies and tools.

Unlike competitors with rigid sharing models or completely de-centralized vaults, Bitwarden allows credentials to securely live in multiple vaults simultaneously, without compromising security. This means teams can access the credentials they need without unnecessary exposure to entire vaults. In addition, Bitwarden offers comprehensive administrative controls, so organizations can centrally manage credentials while still allowing user-centric usage as needed. This balance makes Bitwarden more enterprise-friendly, scalable, and adaptable.

## Full control with Bitwarden

### Start of the lifecycle

#### Full control from day one

Bitwarden enterprise and collection management policies give you an opportunity at initial set up to immediately determine who has access to what. Establishing these policies right at the start sets you up for greater consistency down the road. For example, customers who choose to turn on the **remove individual vault policy** prevents employees from saving vault items to a personal vault, giving admins complete oversight over credentials.

With the Bitwarden **password generator**, admins can enforce strong password policies and enable end users to easily and securely create those passwords that align with those policies. Likewise, the password generator works seamlessly with the browser extension autofill feature, allowing users to create a strong and unique password right at account set up and saved directly within their vaults. As users visit a login page, Bitwarden immediately recognizes the stored credential - now, instead of manually typing passwords, the autofill feature inserts credentials securely.

## Everything in between the lifecycle

### Secure sharing

Bitwarden offers the most comprehensive and robust **collection management settings** on the market. These collection settings offer a range of management strategies for collections and vault items. Want complete control over all organizational credentials and full administrative oversight? Or is your strategy to lean more into a flexible, user self-serve experience that supports least privilege? These settings allow you to adjust according to your company's policies.

### Monitoring and reporting

With Bitwarden vault health reports, member access reports, and event logs, admins gain full visibility into all credentials in use, including details such as which have been shared, who's accessing them, and whether they are at risk (weak, reused, breach-related passwords, missing MFA, and more)

## End of the lifecycle

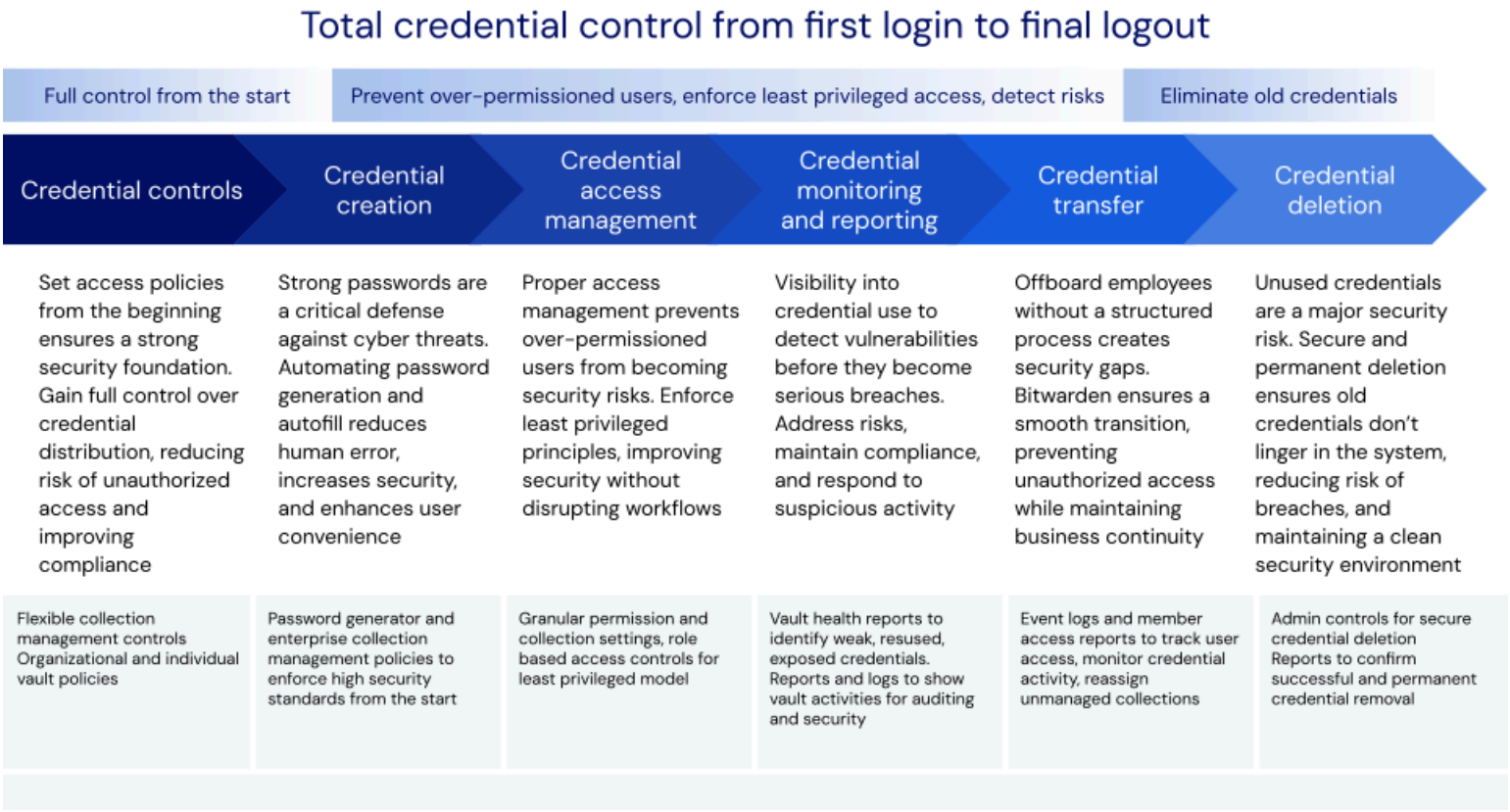
### Offboarding credential recovery and transfer

When a user offboards, their accounts are revoked to prevent unauthorized access. The following Bitwarden features give admins full visibility and control over how to reassign or transfer credentials when an employee leaves the company or changes departments:

- Member access reports provide details on all items a user had access to
- Event logs and SIEM show what credentials a user recently accessed
- Unmanaged collections are presented so admins know what needs to be reassigned, minimizing orphaned credentials
- Remove individual vault policy ensure all collections and items are under admin oversight

### Credential deletion

When a credential is no longer needed, the Bitwarden functionalities around least privilege access, robust credential management, and administrative control make it easy to securely delete credentials from the system, ensuring no unused credentials are left to compromise security. Use the Bitwarden event log feature to track and confirm that a credential was successfully and permanently deleted.




## Credential lifecycle planning starts today

Don't let credential lifecycle management planning be an afterthought – many organizations fail to address it until an employee leaves or a data breach occurs. Think ahead to stay ahead. Here are tips to get your teams started.

### Ask questions

- How do we currently manage credentials when an employee leaves the company or moves to a new role?
- How do we track shared credentials across teams?
- How do we know what applications are being accessed outside our identity provider? Are we able to prevent unauthorized access?
- What happens if a credential is mishandled or shared with the wrong person?

### Consider long-term benefits

- Establishing a credential lifecycle plan can save time and reduce security risks, especially during high-risk events such as offboarding.
- Credential management helps enforce zero trust, which trusts no one and assumes a breach is constantly imminent or has occurred, requiring every user to pass a verification process before they are given access.
- In a time when employee turnover is reaching heights (a recent Fast Company article calls it an "employee exodus,") your team needs to consider how you manage your workforce, their security, and – most importantly – their credentials. This isn't just an HR shift, but an organizational security concern.

**Bitwarden prepares you for today, tomorrow, and beyond**

## Bitwarden offers the most structured offboarding

| Offboarding process | Bitwarden | 1Password | Keeper |
|---|---|---|---|
| Credential recovery and removal | Remove individual vault policy prevents personal storage, ensuring admins retain access to all collections | Warning: Employee private vaults cannot be disabled, admins have extra steps to recover or remove credentials | Warning: All items are saved on individual level, admins must manually ensure owned items are re-assigned before deactivation. |
| Vault clean up | Admins retain access to all credentials, preventing orphaned or unassigned credentials | Warning: Vaults can store multiple copies of the same credential and duplicates can exist in multiple vaults, requiring manual clean up | Warning: Deleting a vault record doesn't remove shortcuts, creating security risks |
| **The bottom line** | **Best for full admin control in offboarding** | **Risk of unmanaged private employee vaults** | **Requires manual planning to avoid orphaned or unassigned credentials** |

3 Bitwarden Confidential bitwarden

Bitwarden stands out with credential lifecycle management

The credential lifecycle is too often overlooked and conversations around who owns organization credentials start too late. In reality, these are essential aspects of identity and access management. Bitwarden provides built-in functionalities for enterprise password management that helps organizations prepare well beyond merely credential creation and deletion. Bitwarden also integrates modern credential management tools to enhance security and flexibility. These enterprise features help establish best practices around reporting, sharing, and transferring, ensuring organizations protect their data from beginning to end. Learn more by starting a free 7-day business trial.

## Definitions

### Privileged access management (PAM)

Privileged access management (PAM) is a critical component of credential management that focuses on controlling and monitoring access to sensitive systems and data. PAM solutions provide granular access control, ensuring that only authorized users can perform specific actions within systems. They also track and log all activities, creating an audit trail for security and compliance purposes. By implementing PAM, organizations can mitigate security risks, protect sensitive data, and ensure that user access is limited to only the permissions necessary to perform their job functions. This approach not only enhances security but also helps organizations comply with regulatory requirements and maintain a robust security posture.

### Access management and credential management

Access management and credential management are closely related concepts that work together to ensure secure access to systems and data. Access management involves controlling who can access which digital assets and what they can do within systems once authenticated. Credential management, on the other hand, involves the secure handling of user credentials, including passwords, certificates, tokens, and keys. By implementing a credential management system and access management policies, organizations can ensure that user identities are verified, access privileges are limited, and sensitive data is protected from unauthorized access. This

integrated approach helps maintain a secure and efficient environment, reducing the risk of data breaches and ensuring that only authorized users can access critical systems and information.