Imprivata Knowledge Hub:

Credential Vault

What is a Credential Vault? Learn about this term and more with our expansive website glossary that explores topics related to access management security.

Video Transcript:

Kayleigh Flemming: Hi, I'm Kayleigh with Imprivata!

A credential vault is a feature of privileged access management applications that protect and manage sensitive login information and access credentials.

A credential vault serves as a centralized repository where users can securely store: Usernames, passwords, tokens, and digital certificates.

Credential vaulting is a best practice in account security that eliminates the use of traditional username and password entry, or the insecure storing of important credentials to local applications - such as the notes app on your phone - or physical material, such as notepads.

Today, passwords are still being shared, compromised, and ineffectively managed, which creates an inherent risk for phishing and account breaches.

Credential vaults are not to be confused with password managers. Password managers provide secure storage for individual credentials, while credential vaults store much more sensitive data, and are often adopted by enterprise organizations who need advanced controls for managing privileges and account level permissions. For example, an individual user may use the "Passwords" manager app on their iPhone for storing login information for apps such as Netflix, but for larger applications like Salesforce, companies need to exercise more privileged access control using a Credential Vault.

Credential vaults protect sensitive data from unauthorized access, such as risky user practices including password sharing. They also protect privileged credentials from attacks including phishing schemes. Credentials vaults are built to manage types of access that are less routine, and more high-risk access to assets like servers, databases, systems, networks, and data.

The benefits of a credential vault include improved security, as they keep passwords out of sight of non-privileged users. Anyone needing to access sensitive data must validate their identity with a form of multifactor authentication (MFA) before accessing login information. Vaults can also automate password rotation so that credentials can be randomized for each login attempt. In addition, a credential vault eliminates error-prone manual password entering and simplifies the login process for end users to access the applications they need.

Contact Imprivata to learn more about privileged access security and enterprise-level credential vaulting.

Thanks for watching!
