VAULT ONE
A JUMPCLOUD COMPANY

Privileged Access Built for Modern Security

Support Zero Trust strategies by enforcing least privilege with granular conditions and real-time session oversight. Minimize insider and lateral movement risk with access that's narrowly scoped, time-bound, and fully observable.

Designed to meet the needs of a broad range of international standards, JumpCloud's VaultOne enables: GDPR, ISO 27001, HIPAA, FedRAMP, SOC 1, SOC 2, and LGPD (Brazilian General Data Protection Law).

Security & Data Encryption:

Data Encryption: VaultOne utilizes the AES-256 algorithm for isolated encryption of data in transit and at rest. For password hashing, the PBKDF2-HMAC-SHA256 algorithm is used.

Private Keys: Each customer has unique encryption keys, with support for third-party key management.

Secure Storage: Sensitive data, such as passwords and keys, are stored in FIPS 140-2-compliant HSM hardware for maximum security.

Connection Protection: Connections are protected via Transport Layer Security (TLS), and communications from the Distributed Engine have an additional, unique encryption key.

Data Handling and Processing: Data for Brazilian customers are processed in Brazil, while data for international customers are processed in the United States.

Delivery and Availability: VaultOne is delivered from multi-regional data centers leveraging automatic management and built-in geo-redundancy, creating three copies of each customer's database on fault-tolerant nodes to ensure high availability and rapid disaster recovery.

Threat Mitigation and Management: VaultOne leverages the latest threat-protection protocols, including intrusion detection, DDoS prevention, anti-malware, penetration testing, and advanced analytics and machine-learning tools.

Data Backup: Full backups are performed hourly, and transaction-log backups are done every five minutes.

Login & Password Protection:

VaultOne protects local user passwords by using a randomly generated code and the SCRYPT-PBKDF2HMAC-SHA256 hashing algorithm to split and combine passwords. Active Directory logins are authenticated directly against the domain, and their passwords are not stored in VaultOne.

Multi-Factor Authentication (MFA): VaultOne reinforces security with its native MFA and integrates with other MFA solutions like Google and Microsoft Authenticator, as well as sending an OTP code to the login email.

User Authentication Controls:

Restricts access to trusted IP addresses: Logins are only allowed from previously authorized IPs.

Sets a login attempt limit: The maximum number of login failures is defined before an account is temporarily locked or marked as inactive.

Implements CAPTCHA in the login process: CAPTCHA verification is added to protect against automated attempts and bots.

Applies the security policy before login: Users must accept and understand the login policy terms before accessing the system.

Privileged Access for Every Critical Asset

IT and security teams shouldn't be missing critical visibility gaps in their authentication and auditing. Legacy providers just aren't built for modern security environments or Zero Trust frameworks. JumpCloud provides the clarity and control you need to secure your environment and meet compliance demands in a Zero Trust world, by leveraging deep telemetry and granting secure access with clear, immutable attestations of who did what, and when, for each resource.

© 2025 JumpCloud Inc. All rights reserved.