VAULT ONE

VAULTONE CLOUD SECURITY

Microsoft Azure

AICPA SOC

All VaultOne customers benefit from an infrastructure and platform built to meet the requirements of the most security-sensitive organizations. We're committed to preserving the confidentiality, integrity, and availability of our customers' privileged account management workloads and assets. VaultOne was architected on the highly secure Microsoft Azure Cloud Platform and meets a broad set of international and industry-specific compliance standards, including General Data Protection Regulation (GDPR), ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2.

SECURITY FEATURES

- 100% isolation and encryption of all customer data both in-transit and at rest, using the AES-256 standard encryption algorithm and PBKDF2-HMAC-SHA256 hashing algorithm.
- Private encryption keys for each customer, with third-party key management support (Azure KeyVault).
- All sensitive data (passwords, secrets, keys) are stored in the most appropriate place for this type of information, a FIPS compliant HSM hardware.
- All connections to VaultOne are protected via Transport Layer Security (TLS). Distributed Engine communications are also secured with an additional encryption key unique to the tenant.
- All customer databases are continuously backed up every hour, with a transaction log backup performed every five minutes.
- VaultOne undergoes an ongoing bug-bounty program with industry experts recognised worldwide.
- VaultOne is delivered from the hardened Microsoft Azure US-WEST, Brazil-South, and many other datacenter locations.
- VaultOne takes advantage of Microsoft Azure's auto-scaling and built-in geo-redundancy, which generates three copies of each customer's database, maintained across fault tolerant nodes to ensure continuous availability and facilitate swift disaster failover and recovery.
- VaultOne leverages Microsoft's latest threat management and mitigation protocols, including intrusion detection, denial-of-service (DDoS) attack prevention, anti-malware, penetration testing, and analytics and machine learning tools to help mitigate threats.

ADDITIONAL INFORMATION

Login Password Protection

VaultOne hashes and salts local user passwords using a randomly generated salt and the SCRYPT-PBKDF2-HMAC-SHA256 hashing algorithm. Active Directory logins authenticate directly against the domain and their passwords are not stored in the VaultOne.

Tighten user authentication security even further with these built in options:

- Restrict logins to trusted IP Addresses
- Set the number of login failures before a user is marked as inactive.
- Require CAPTCHA on login.
- Enforce login policy agreement before sign in.
- Enforce two factor authentication using Google Authentication, or Email.

How secure is AES 256 bit encryption?

Advanced Encryption Standard is the strongest encryption there is. Governments, the military and banks use 256 bit encryption to protect highly sensitive information; universities use it protect privileged student data; the healthcare industry uses it to keep patients' medical records secure. Today, organizations worldwide look to advanced data encryption standards to protect themselves from hackers and cyber crime.

As you're interested in advanced encryption techniques… check out the range of security and compliance solutions VaultOne provides for organizations that need to meet industry security standards.