DASHLANE

Security at a glance

Dashlane is built with zero-knowledge architecture. Vaults are encrypted and decrypted locally on each device, which means only end users have access to their data. Dashlane can't access or view this data.

To extend zero-knowledge protection into the cloud, Dashlane leverages confidential computing and secure cloud enclaves (AWS Nitro Enclaves). These enclaves isolate cryptographic operations and encryption key management from the underlying infrastructure, ensuring that even privileged access to servers can't expose sensitive data.

The full Dashlane product is zero knowledge: Vault, audit logs, integrations, and data flows. Even if Dashlane's infrastructure were compromised, everything would remain fully protected.

Cryptographic architecture and key management

- **Vault encryption:** AES256-CBC-HMAC mode for confidentiality and integrity
- **Key derivation:** Argon2d (3 iterations, 32 MB memory cost, 2 threads) for GPU-resistant password stretching
- **Key separation:** Distinct secrets for vault encryption and device authentication

Each new device generates a unique device key (40 bytes, random). This key authenticates to Dashlane servers independently from the vault encryption key. Device authorization requires explicit user verification: Either a one-time token (for password-based accounts) or secure device pairing using Curve25519 (for passwordless accounts). This ensures that only trusted endpoints can decrypt vault data.

Enterprise security features

- **Single sign-on (SSO):** Integrate with any SAML 2.0 identity provider (such as Okta or Entra ID); Dashlane's Confidential SSO uses AWS Nitro Enclaves to maintain zero knowledge
- **SCIM provisioning:** Automate onboarding and offboarding with identity providers to enforce least-privilege access
- **Activity logs:** Get full audit trails for admin actions, vault access, and policy enforcement; they're also exportable to SIEMs
- **Role-based access control:** Provide granular permissions and delegated admin controls
- **API and CLI:** Get additional customization, if needed

CONTINUED

DASHLANE

Compliance

- SOC 2 Type II and ISO 27001 certifications
- Yearly third-party penetration testing and bug bounty program
- Encrypted data hosted in AWS data centers in Ireland under the EU's GDPR framework
- Built under the CISA Secure by Design pledge

Why security teams trust Dashlane

Dashlane's security model combines state-of-the-art cryptography, enclave-based cloud isolation, and defense-in-depth architecture to maintain zero knowledge across all layers, from the client device to the cloud. Our zero-knowledge architecture and end-to-end encryption ensure maximum security and privacy.

Dive deeper into Dashlane's best-in-class security.
Learn more