Enigma Vault Security Policy

Last updated: July 30, 2021

This security policy describes how we secure our Enigma Vault API services and your data.

Overview

Our primary responsibility at Enigma Vault is to secure your sensitive data. Our services were built from the ground up with privacy and security in mind. To learn more about our privacy practices, please review our privacy policy.

Application security

Static application security testing

The Enigma Vault API undergoes static application security testing (SAST) every time there's a code change. If a vulnerability is identified by the SAST service, the build fails, and all other development efforts are halted until resolution. Ensuring that code commits are high quality and defect free provides the cornerstone of our protection against cyber criminals and data loss.

Dynamic application security testing

Every three months the Enigma Vault API undergoes dynamic application security testing (DAST) by a trusted third-party assessor. A trusted third-party assessor also performs an annual penetration test using various security tools.

Web application firewall

A web application firewall (WAF) protects the Enigma Vault API during runtime. It is in block mode and stops malicious web requests. Its efficacy is continuously monitored, and all blocks are promptly investigated.

Authentication

We have chosen OAuth2/OpenID Connect as the Enigma Vault API authentication mechanism. All protected endpoints require a valid bearer token.

Developer Portal security

Multi-factor authentication

To access the developer portal where client credentials and reporting reside, the developer must configure multi-factor authentication (MFA). We have chosen time based one time passwords (TOTP) MFA using apps such as Google Authenticator or Cisco Duo instead of SMS. TOTP doesn't rely on cellular networks and has far fewer risks than SMS.

Advanced authentication security

While MFA provides a very strong layer of security, we didn't stop there. Passwords are checked against compromised lists and if the password has been involved in a previous breach, the developer will have to use a different password to login. We also use adaptative authentication techniques that determine if the login is of low/medium/high risk based on a multitude of factors.

Email notices

Whenever you login to the portal, you'll receive an email stating you just logged in. We can't imagine a scenario where a bad actor could gain control of your password, MFA TOTP, and slip by our advanced authentication security, but if they do, you will know with the email notice.

Data security

Encryption in motion

All traffic between the API and the client occurs over TLS 1.2 or higher. All internal traffic within our services uses TLS 1.2 or higher as well.

Encryption at rest

Besides disk and table level encryption, we take it one step further and use AES-256 client level encryption. All of the data provided to the API gets encrypted prior to being stored with our cloud services provider, AWS.

Infrastructure security

Enigma Vault's API operates on AWS' serverless compute, database, and storage offerings. They're responsible for OS/platform level updates, patch management, etc. This allows us to focus on code and high-level AWS management and provides you the most modern, secure data storage and processing API out there. We take advantage of AWS SecurityHub to map to various security frameworks and to identify any potential issues. We use AWS GuardDuty to alert us of any malicious account level activity.

Encryption key protection

Enigma Vault keys are using AES methods. The keys are stored within an encrypted enclave managed by our cloud services provider, AWS. The keys are rotated annually.

Disaster recovery

Multiple availability zones

We utilize AWS' multiple availability zones within a region. Think of an availability zone as a data center operating on its own power, network, and other resources. Barring something short of an apocalypse, multiple availability zones provide baked in high availability. Four horsemen appearing? No big deal, see multiple regions below.

Multiple regions

While we highly doubt something bad will happen to one of AWS' primary regions, we've planned for it. In the event of a catastrophe where one of the primary regions goes down, your data is safe. We replicate data and card vault data real time to another region. File vault replication happens near real time.

Compliance

We understand that security does not equal compliance, but we also understand the importance of assurance and attestation to you.

PCI compliance

Enigma Vault's card vault, data vault, and file vault have achieved PCI-DSS level 1 certification. The attestation of compliance (AOC) is available on request.

ISO 27001 compliance

We are currently in the process of obtaining ISO 27001 compliance certification.

Shared responsibility

We eat and breathe security, and we hope you do too. It is our job to protect your data and keep it safe. You have the responsibility of protecting your portal login credentials, API client credentials, and the systems and services that use Enigma Vault.

Reporting a potential issue

If you come across a potential vulnerability, please reach out to us immediately at support@enigmavault.io.

Data retention and secure disposal

Card Vault

Within the card vault, card tokens utilize a concept called time to live (ttl). The ttl is configurable by the app client up to 15 minutes. After 15 minutes, and the client app has not extended the ttl, the card is purged. If the user checks the box that they want their card saved, the card is saved permanently. For permanent cards, they can be deleted by the app client using the delete endpoint. Card data is point-in-time backed up for 35 days. While handled together through the API, the cvv is treated much differently behind the scenes because it is sensitive authentication data (SAD). The cvv has a static ttl of 15 minutes; it cannot be changed. If the card ttl is increased, the cvv ttl remains as it was. If the card ttl is decreased, the cvv ttl changes to the lesser ttl. When authorization occurs, the ttl is purged from the table. There are no backups taken of the cvv table.

Data and File Vaults

The data and file vaults require the app client to purge items using the delete endpoint. Deleted data will reside for 35 days.

Usage and application logs

Application and network level logs are stored for a minimum of 1 year per PCI-DSS. Usage logs related to billing are kept for 60 days.

Companywide Commitment

Nothing is more important to us than ensuring the privacy and security of your data. Each employee takes a pledge of excellence to ensure quality, reliability, privacy, and security.