storecove

Security

Principles

2022-11-18

www.storecove.com

Contents

1 Security

1.1 Certifications

1.1.1 ISO 27001

With this certification we demonstrate that we comply with the International Standard for Information Security (ISO 27001), and have taken all necessary precautions to protect sensitive information against unauthorized access and processing. This applies to all our products, to the benefit of all our customers.

ISO 27001 demands that the company meet high standards of risk management and security control on an on-going basis. The certification also guarantees that all relevant networks are protected against any systemic vulnerabilities.

1.1.2 PCI DDS

Storecove uses Amazon's AWS platform and infrastructure. The environment is protected according to the PCI DSS hardware standard. Storecove employees do not have any physical access to our production environment.

1.1.3 AWS Security

In addition to physical security, being on AWS platform also provides us significant protection against traditional network security issues on the infrastructure including,

- Distributed Denial Of Service (DDoS) Attacks
- Man In the Middle (MITM) Attacks
- Port Scanning
- Packet sniffing by other tenants

Storecove obtains the SOC 1 and SOC 2 report from AWS for the services rendered by them and validates the same for the effectiveness of the opinion of the third party auditor.

1.2 Data Encryption

1.2.1 Data At Rest

We store our data securely in several ways. First, we use AWS RDS and that runs on AES-256 encrypted servers. We also have data in AWS S3 which is encrypted using AES-256. Our server fleet consists of Docker containers that run on AES-256 encrypted volumes.

1.2.2 Data In Flight

All data exchanged with the outside world as well as selected relevant internal data is transferred inside TLS tunnels using AES-256 encryption.

1.3 Vulnerability Management

Storecove uses modern web frameworks and follows those frameworks' best practices for securing access. We monitor for bugs and security patches in all the systems we use and apply updates religiously.

We periodically proactively rotate our docker containers to ensure we always have a fleet of fresh instances.

In addition, we've engaged external security firms to perform weekly penetration tests and source code audits on Storecove's systems, and we will continue with those tests and audits regularly in the future.

1.4 Application Security

Our application servers can be accessed only via HTTPS. We use industry standard encryption for data traversing to and from the application servers.

We provide two factor- and SAML SSO authentication for users and we support multiple users with different roles to restrict access to sensitive data.

1.5 GDPR

All servers and data storage are located inside the EU.

We retain your document data for 365 days by default for us to be able to effectively troubleshoot and diagnose problems. However, we can retain your data for longer or shorter time periods if you so desire.

When you delete a sender/receiver identity, by default all data pertaining to that identity is deleted as well.

1.6 Responsible Disclosure

We want to hear from you! We're grateful for security researchers who practice responsible disclosure. Please contact us at security@storecove.com with the details of the problem you've found. We treat these reports as our highest priority, and we'll get back to you immediately. And we promise not to seek legal action against those who fully disclose security issues to Storecove and do not maliciously exploit those vulnerabilities.

storecove

www.storecove.com