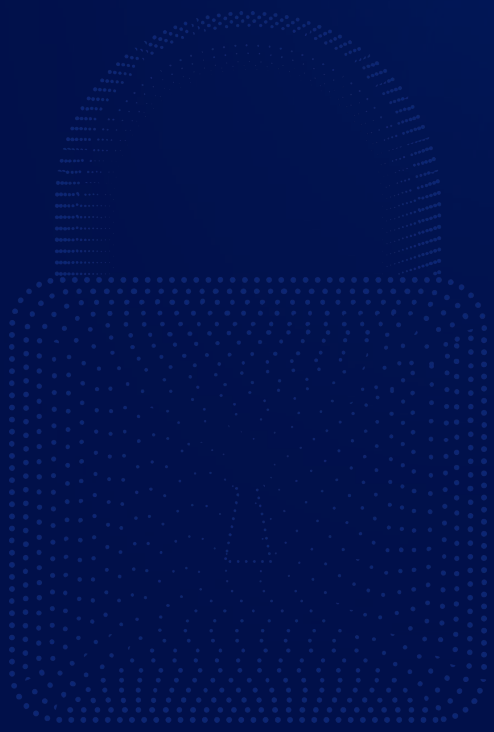
Safe Securities, Inc.

SAFE

Security Statement



www.safe.security

Introduction

At Safe Security, we make cyber risk an informed business decision.

As a pioneer in the "Cybersecurity and Digital Business Risk Quantification" space, Safe Security is enabling businesses to objectively measure and mitigate cyber risk across the enterprise. We are fundamentally changing how digital risk is managed with our ML Enabled API-First SAFE Platform, which aggregates automated signals across people, process, and technology, both for 1st and 3rd Party to dynamically predict the breach likelihood (SAFE Score) & $$ risk of an organization.

With security being at the heart of everything we do, we go the extra mile to ensure that our customers' data is secure. We implement best in class and industry-leading security programs and measures to secure our cloud-based platforms and processes.

Our approach to security

Our approach to security is based on the following objectives:

01

Best-in-class SaaS product security

02

Satisfy customers' cloud security requirements

03

Fulfill industry security standards

04

Proactively identify security threats to the product

Compliance with Laws, Regulations, and Standards

01

SOC 2 Type 2 and SOC 3

02

Veracode Verified

03

ISO 27001:2013

04

ISO 9001:2015

05

SG:D Accredited

Data Security

SAFE is a cloud-based SaaS platform.

01
Data Centers

Our product - SAFE - and our customers' data are hosted on the cloud hosting service, Amazon Web Services (AWS).

SAFE product and customers' data can be hosted on any of the supported AWS regions worldwide. As a customer, when you sign up for SAFE, you are essentially allocated a tenant. As part of this process, you can select a region where the application data is stored. There are different types of data collected, processed, and managed by SAFE.

Refer to Data Residency in SAFE for more details.

Currently, SAFE is hosted in the following AWS regions:

Geography	Region
US	N Virginia
EU	Frankfurt, Germany
Middle- East	Bahrain
APAC	Singapore
	Sydney, Australia
	Mumbai, India
UK	London

Data Security

SAFE is a cloud-based SaaS platform.

02
Encryption of data

Data in transit:

SAFE encrypts the customers' data in transit over public networks using **TLS 1.2** to protect it from unauthorized disclosure or modification.

Data at rest:

SAFE encrypts the customers' data at rest using the AES **256-bit AWS KMS** key.

Key Management:

SAFE uses AWS Key Management Service (KMS) for storing encryption keys. We allow our customers to provide their own AWS KMS key, and in such cases, the key generation and management access will completely be with the customer.

Securing the SAFE application

We follow a defense in-depth approach wherein the application code undergoes a series of security assessments. The vulnerabilities are prioritized based on their severity and are addressed before the application is deployed to production. The activities that take place under the application security program is outlined below:

01

Secure Coding Practices

We at SAFE Securities, Inc. follow a rigorous, industry best practice approach to secure our software development. We endeavor to provide a secure product with a continuous process of security testing and review. Our secure coding practice includes:

1. Input Validation.
2. Output Encoding
3. Authentication and Password Management
4. Session Management
5. Access Control
6. Cryptographic Practices
7. Error Handling and Logging
8. Communication Security
9. System Configuration
10. Database Security
11. File Management
12. Memory Management

Securing the SAFE application

02
Vulnerability Assessment & Penetration Testing

We perform continuous SAST and DAST scans of the product as a part of our DevSecOps practices. Any vulnerabilities found during these scans or other vulnerability discovery activities are patched with the highest priority before the product's final release. In addition, our internal security team performs the manual and automated testing of the application for the business logic flaws before each release.

Daily Scans through our CI pipeline using Veracode among many other tools

- **01** Static Application Security Testing (SAST)
- **02** Software Composition Analysis

Per sprint assessment using commercial tools and in-house checklist

- **03** Dynamic Application Security Testing (DAST)
- **04** Business Logic Validations

Securing the SAFE application

03
Production Infrastructure Security

The AWS production environment where SAFE is deployed undergoes continuous security assessment. Some key activities include:

- Configuration assessment of all PaaS services
- Daily Vulnerability Assessment scans
- Continuous logs and alerts monitoring
- Periodic patch management and access review

The production endpoints that are accessible over the internet undergo security assessments as a part of our 'due diligence' approach to ensure only essential services are allowed over the internet.

Third-Party Assessment

Third-party Security Assessment is performed using a 4-tier approach defined under Vendor Management Policy and Process. All the third parties are categorized based on the area of focus and criticality of business. A Questionnaire-based security assessment is performed for each of the third-party, and if the assessment report is found satisfactory, only then is the vendor allowed.

In addition, we perform Third-party Vendor Risk assessment for each third party using the SAFE. The assessment includes digital attack surface discovery based on their domain name, assessment via 100+ automated Outside-In assessment controls for Email Security, Network Security, DNS security, System Security, Application Security, Malware Servers, Breach Exposure, and more.

Securing our Employees

01
Security awareness training

Cybersecurity is in our DNA. We have implemented security awareness and secure coding practice training campaigns continuously to ensure that security is top of mind' and not 'an afterthought.'

Additionally, we ensure cybersecurity awareness of our employees through the SAFE Me mobile application. SAFE Me performs mobile device assessment, scans for exposures on the dark web in real-time, and provides cybersecurity awareness training to our employees.

02
Background verification of new recruits

We perform the background verification for all new recruits, according to local laws.

Privacy Policy

We care about the privacy of your personal information.

Click here read our privacy policy

Reporting Security Issues

We have implemented an easy process to report any bug or security issues found in our system. If you find any security issues, please write to us at bugs@safe.security with all the related information.

If you are our existing customer:

Click here to create a support ticket

www.safe.security | info@safe.security

Palo Alto
3000, El Camino Real,
Building 4, Suite 200, CA
94306