STACKSI SECURITY BRIEF

STACKSI

INTRODUCTION

Stacksi saves your best people’s time and gets important deals closed faster by automating the process of responding to security questionnaires. Our system takes your known-good security documentation, the customer’s questionnaire and extracts relevant data from both. We then enable you to quickly and accurately generate a response, approve it, and send it back to the client.

Security is quite literally top-of-mind for us every day at Stacksi. We work to be good stewards of our customers’ data and take our own advice to heart. In this white paper, we detail our approach to security which starts from a philosophy of defense-in-depth. This document includes information about our application security, identity and access management, network security, and corporate security efforts.

GOVERNANCE

Security of customer data is an essential part of Stacksi's operations. Each employee must complete a background check, provide verifiable employment references, sign a security policy acknowledgement and a non-disclosure agreement. Once onboarded, all employees receive annual security training.

Individuals who have completed this process are given role-based, least-privilege access to Stacksi's systems. Access to Stacksi's production environment is limited to those with need-to-know and two-factor authentication is required through authenticator credentials or a hardware device. Firewall configuration and administrator permissions are given to a limited number of individuals. All records of access, configuration, and resource management are logged, and remote access is both regulated and monitored. To further enforce least privilege and auditability, all administrative access requires users to assume a specific role after successful administrator authentication.

Stacksi's security team actively reviews, audits, and improves our security practices to keep up to date with the latest developments in DevSecOps. As new threats arise, our security team ensures that our processes and systems continue to be updated. We believe in 'shift-left' security, and make sure that members of our development team have the knowledge necessary to make it real.

PRODUCT OVERVIEW

Document NLP Engine

Stacksi uses known good documentation to support the rapid answering of security questionnaires. At the heart of our system is our document NLP engine, which efficiently manages an index of customer information that can be used to answer security questionnaires.

Stacksi's NLP engine is entirely contained within Stacksi's network environment; customer documentation is not sent outside of the network.

Infrastructure Monitoring

Stacksi has the optional ability to monitor the network configuration of customer environments and use data from customers' network configuration to answer security questionnaires. All connections are optional, read-only, and use minimal privileges necessary to accomplish the necessary tasks.

Policy Manager

Stacksi's policy manager enables companies to maintain evergreen policies with the requisite version control and necessary process-related documentation. Automated reminders ensure that documentation is reviewed and kept up-to-date.

DATA PRACTICES

Data In Transit

All data is transmitted to Stacksi servers using Secure Sockets Layer (SSL)/Transport Layer Security (TLS 1.2), which is encrypted using Advanced Encryption Standard (AES) with a 256 bit or higher key (AES-256) using Elliptic-Curve Diffie-Hellman key exchange.

Communication between internal systems is also governed by least privilege. Our multi-tier architecture limits all communication to explicitly authorized security groups and ports specified within our firewall settings. Application and database tiers are not accessible via the public internet.

To prevent man-in-the-middle attacks, we ensure that authentication succeeds and an encrypted connection is established prior to any data transfer.

Data At Rest

Stacksi uses Amazon's S3 storage architecture to store customer data in an encrypted state. Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a key that it rotates regularly. Amazon S3 server-side encryption uses one of the strongest block ciphers available to encrypt your data, 256-bit Advanced Encryption Standard (AES-256).

Authentication to all systems storing customer information requires MFA. In particular, Stacksi leverages AWS IAM roles and permissions to support just-in-time least privilege access that can be audited and monitored effectively.

User Authentication

INFRASTRUCTURE ACCESS

Authentication to all systems storing customer information requires MFA. In particular, Stacksi leverages AWS IAM roles and permissions to support just-in-time least privilege access that can be audited and monitored effectively.

CUSTOMER ACCESS

Stacksi supports MFA and SSO. SSO is currently supported via Google SSO. Stacksi supports MFA for all users regardless of the authentication method used, either using an authenticator application like Google Authenticator or Duo (recommended) or as a last resort, SMS-based authentication. Role-based access within the application allows a least-privilege approach to information shared within the application.

Input Validation

All customer data uploaded to Stacksi is logically separated in separate S3 buckets, and scanned for viruses prior to being added to customer indices. Inputs are type checked and validated prior to being accepted.

VULNERABILITY MANAGEMENT

Vulnerability Scanning

Stacksi has built a network configuration scanner that it provides to customers and uses internally to ensure that network configurations - including database and bucket policies, identity and access management rights, firewall configurations, server communication policies, and backup settings - are securely architected.

In addition to internal monitoring, Stacksi also runs daily scans using Detectify against our application and API to proactively identify any vulnerabilities.

Stacksi also operates a public vulnerability disclosure program through Federacy, wherein security researchers can securely report any identified vulnerabilities in a structured fashion to Stacksi.

Identified vulnerabilities are patched based on severity and in line with commitments detailed in our Vulnerability & Patch Management Policies.

LOGGING PRACTICES

Stacksi logs all encryption / decryption and server requests, times, actions, response statuses, and error codes, keeping a verifiable trail of information for at least 5 years. Object-level logging verifies (before execution) that objects uploaded to our servers are sufficiently encrypted, even without explicit encryption headers. We additionally log, trace, and monitor procedures in EC2, S3, and RDS that interact with data.

ENDPOINT SECURITY

Application Servers

Servers are provisioned using known-good base images and configured using Terraform templates (IaC) that go through the same version control process as our application code. Permissionless default roles within our network support traceability of changes and limit the ability of network intruders to make modifications to resources.

User Endpoints

User endpoints are standardized and required to enable key security features, including firewall enabled, full disk encryption, antivirus and automatic logouts.

MALICIOUS ATTACKS

Distributed Denial of Service (DDoS): Through AWS, Stacksi protects against 96% of the most common attacks today, including SYN/ACK floods, Reflection attacks, and HTTP slow reads.

Man-in-the-middle: Secure TLS 1.2 implementation across our data transmission tech stack prevents MITM attacks.

Cross-site scripting: All platform inputs are sanitized and metadata logged, and secure coding guidelines are enforced company-wide.

Birthday Attack: By default, we disable usage of the insecure 3DESCBC cipher across all components of our application stack.

Dictionary Attack: High password entropy with a large minimum character count is strictly enforced for users interacting with the system.

Brute Force: Consecutive failed login attempts result in time-based lockouts and alerts in our IDS.

INTRUSION DETECTION

Stacksi only stores data on its servers in an encrypted format. We employ network-level next-gen IDS through AWS GuardDuty, in addition to alerts configured for suspicious events (e.g. failed SSH attempts into our systems).

STACKSI

Book a 30 min product demo at

www.stacksi.com