Seliom

Report

Seliom Security Overview

Last Updated: June, 2020

Seliom Data Center & Network Security

Physical Security

NAME	DETAILS
Facilities (Amazon Web Services)	Most of Seliom's physical infrastructure is hosted and managed within Amazon's secure data centers and utilizes the Amazon Web Service (AWS) technology. Amazon continually manages risk and undergoes recurring assessments to ensure compliance according to the industry's standards. Amazon's data center operations have been accredited under: • ISO 27001 • SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II) • PCI Level 1 • FISMA Moderate • Sarbanes-Oxley (SOX)
Facilities (Google Cloud Storage)	A small part of Seliom's physical infrastructure is hosted and managed within Google's secure data centers and utilizes the Google Cloud Storage technology. Google continually manages risk and undergoes recurring assessments to ensure compliance according to the industry's standards. Google's data center operations have been accredited under: • ISO/IEC 27001 • ISO/IEC 27017 • ISO/IEC 27018 • SOC 1/2/3 • PCI DSS • CSA Star

On-site Security	Seliom utilizes ISO 27001 and FISMA certified data centers managed by Amazon and Google. Amazon data centers are housed in nondescript facilities, and critical facilities have extensive setback and military grade perimeter control berms as well as other natural boundary protection. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication no fewer than three times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. Google has a global scale technical infrastructure designed to provide security through the entire information processing lifecycle at their data centers. This infrastructure provides secure deployment of services, secure storage of data with end user privacy safeguards, secure communications between services, secure and private communication with customers over the internet, and safe operation by administrators. Google uses multiple physical security layers to protect their data center floors and technologies like biometric identification, metal detection, cameras, vehicle barriers, and laser-based intrusion detection systems.
Location	Seliom's data centers are located in Europe.

Network Security

NAME	DETAILS
Security Response Team	Our team is on call to respond to security alerts and events and can be reached at support@seliom.com
Protection	PAll firewalls infrastructure and management are provided by our service providers. Firewalls are utilized to restrict access to systems from external networks and between systems internally. By default, all access is denied and only explicitly allowed ports and protocols are allowed based on business need. Each system is assigned to a firewall security group based on the system's function. Security groups restrict access to the ports and protocols required for a system's specific function in order to mitigate risk. Host-based firewalls also provide the ability to further limit inbound and outbound connections as needed.
Vulnerability Scanning	Our service providers' managed firewalls prevent IP, MAC, and ARP spoofing on the network and between virtual hosts to ensure spoofing is not possible. Packet sniffing is prevented by infrastructure including the hypervisor which will not deliver traffic to an interface which it is not addressed to. Our service providers utilize application isolation, operating system restrictions, and encrypted connections to further ensure risk is mitigated at all levels. Port scanning is prohibited and every reported instance is investigated by our infrastructure providers. When port scans are detected, they are stopped and access is blocked.
Penetration Testing and Vulnerability Assessments	Third party security testing of our service providers is performed by independent and reputable security consulting firms. Findings from each assessment are reviewed with the assessors, risk ranked, and assigned to the responsible team

Security Incident Event and Response	In the event of a security incident, our engineering team is called in to gather extensive logs from critical host systems and analyze them to respond to the incident in the most appropriate way possible. Gathering and analyzing log information is critical for troubleshooting and investigating issues. Our service provider allows us to analyze three main log types: system, application, and API logs.
DDoS Mitigation	Our service providers infrastructure provides DDoS mitigation techniques including TCP Syn cookies and connection rate limiting in addition to maintaining multiple backbone connections and internal bandwidth capacity that exceeds the Internet carrier supplied bandwidth. We work closely with our providers to quickly respond to events and enable advanced DDoS mitigation controls when needed.
Logical Access	Access to Seliom's Production Network is restricted by an explicit need-to-know basis. It utilizes least privilege, is frequently audited, and is closely controlled by our engineering team. Employees accessing Seliom's Production Network are required to use multiple factors of authentication

Encryption and Authentication Requests

POLICY	DETAILS
Encryption in Transfer	All internal and external communication is done through a secure connection with SHA-256 encryption using RSA Encryption algorithm. Emails are sent by Postmark through a secure TLS connection.
Encryption at Rest and in Backups	Data at rest is encrypted via AES-256 algorithm. The backup is done through snapshots, also with AES-256 encryption.

Availability and Continuity

POLICY	DETAILS
Uptime	Although we strive for 100% availability, there are certain cases in which routine maintenance, deployments and unexpected errors may briefly interrupt our services. To the best of our ability, our customers will be notified ahead of time when such interruptions may occur. In any event, our team is constantly monitoring our services to ensure the highest uptime possible.
Redundancy	Our service providers clustering and network redundancies eliminate single points of failure.
Disaster Recovery	Our service provider's platform automatically restores customer applications and databases in the case of an outage. The provider's platform is designed to dynamically deploy applications within its cloud, monitor for failures, and recover failed platform components including customer applications and databases.

Application Security

Secure Development (SDLC)

POLICY	DETAILS
Ruby on Rails Framework Security Controls	We utilize Ruby on Rails framework security controls to limit exposure to OWASP Top 10 security flaws. These include inherent controls that reduce our exposure to Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), and SQL Injection (SQLi), among others
QA	We have a QA process in place to continuously review and test our code base. We identify, test, and triage security vulnerabilities in code.
Separate Environments	Testing and staging environments are separated from the production environment. No actual customer data is used in the development or test environments.

Application Vulnerabilities

POLICY	DETAILS
Code Analysis	Our source code repositories are continuously scanned for security issues.

Product Security Features

Secure Development (SDLC)

FEATURE	DETAILS
Authentication Options	Seliom supports logging in via email and password. In the future, we will provide SSO and Google Authentication.
Secure Credential Storage	Seliom follows secure credential storage best practices by never storing passwords in human readable format.
API Security and Authentication	Seliom's API is SSL-only and you must be a verified user to make API requests. Upon signing in, users are granted with an authentication token that will be able to make requests only within the organisation to which they have been granted access. All documents, process definitions, cases, and other relevant information is securely stored and can only be accessed through the use of these tokens.

Additional Product Security Features

POLICY	DETAILS
Access Privileges and Roles	Access to data within your Seliom account is governed by access rights, and can be configured to define access privileges. Seliom uses role-based action control (RBAC), providing customizable permission levels for your organization users.
Transmission Security	All communications with our service provider servers are encrypted using industry standard HTTPS. This ensures that all traffic between you and Seliom is secure during transit.

Additional Security Methodologies

Security Awareness

METHODOLOGY	DETAILS
Policies	Seliom has developed a comprehensive set of security policies covering a range of topics. These policies are shared with, and made available to all employees and contractors with access to Seliom information assets.
Training	All employees at Seliom are well-versed in software security best practices. New employees are given hands-on training once a year based on OWASP TOP 10 and SANS 25. Security Awareness is also part of Seliom's routine as updates are shared to all team members during internal events.

Employee Vetting

METHODOLOGY	DETAILS
Background Checks	Seliom performs background checks on all new employees in accordance to local laws. The background check includes Criminal, Education and Employment verification.
Confidentiality Agreements	All new hires are screened through the hiring process and required to sign Non-Disclosure and Confidentiality agreements in accordance to local laws.