sumologic

A Sumo Logic White Paper

Sumo Logic Security Model

Secure by Design

Entrusting your data to a third-party service provider requires rigorous security measures. At Sumo Logic, the security and integrity of our customers' data is critically important. That's why best-of-breed technologies and stringent operational processes are employed to ensure that customer data is completely safe at all times.

This white paper describes the technologies and processes used by Sumo Logic to secure customer data, and provides background on the company's deeply ingrained security culture.

Security Background and Culture

Securing customer data is not only an imperative at Sumo Logic, it's in the company DNA. Sumo Logic's founders and employees are veterans of some of the most respected security companies in the industry, including market- leading SIEM vendors, managed security service providers, and national laboratories.

The Security Team at Sumo Logic is heavily involved in the design and development of the company's log management and analytics service from the ground up. From product management through engineering and operations, the Security Team is intimately involved in the specifications process, the coding phase, code reviews, user acceptance, and operational practices.

Strategic security technologies and processes that are core to Sumo Logic include:

- Whole-disk encryption
- Access controls at per-thread granularity
- Whitelisting of individual processes, users, ports and addresses
- AES 256 encryption
- Regular penetration tests and vulnerability scans
- A strong Secure Development Life-Cycle (SDLC)

Compliance and Certifications

Sumo Logic is constantly working with global services firm Brightline to acquire and maintain a variety of certifications and attestations. We currently hold:

- A PCI/DSS 3.0 Service Level Provider Level 1 Certification
- A SOC 2, Type 2 attestation
- An attestation of HIPAA compliance
- FIPS-140 compliance

Additionally, Sumo Logic complies with the U.S.- EU Safe Harbor framework and the U.S.- Swiss Safe Harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal data from EU member countries and Switzerland.

Logical Data Separation

Data is kept logically separate on various layers throughout the entire Sumo

Logic service. First, all customer data is tagged throughout the data lifecycle and is enforced at every layer of the system. This restriction applies to all data and all processes/threads, both in memory and on disk.

Secondly, all customer data is kept for long-term storage in Amazon's Simple Storage Service (S3) and is encrypted using per-customer keys, which are rotated on a 24-hour basis. These per-customer, per-day keys are stored in S3.

Physical Security

Sumo Logic operates only in AWS data centers that have been certified as ISO 27001, PCI/DSS Service Provider Level 1, and which have authorization from the U.S. General Services Administration to operate at the FISMA Moderate level, and are also a certified platform for applications with Authority to Operate (ATOs) under the Defense Information Assurance Certification and Accreditation Program (DIACAP).

Physical data centers are located in secret locations across the globe. Physical security measures such as biometric access controls, 24 hour armed guards, and video surveillance are used to ensure that no unauthorized access is permitted.

Encryption in Transit

All customer data is transmitted from and to Sumo Logic in an encrypted fashion, with no exceptions. This includes data uploaded from a Sumo Logic Collector, as well as data retrieved from the service by a search query via the Sumo Logic UI, or via a Sumo Logic API.

Before logging in, users see an Extended Validation (EV) TLS 3.1 and higher certificate from GeoTrust. All user interaction with the Sumo Logic service will use this EV TLS Certificate for secure communications between their browser and Sumo Logic. Sumo Logic certificates are encrypted on FIPS- compliant storage media in an off-site location, just to maintain their integrity.

Encryption at Rest

All file systems that store customer data are encrypted.

Account Creation

As a cloud-based solution, Sumo Logic handles data collection, processing, storage, forensics, and analysis through a centralized and highly secure platform. From the very first interaction on any account, Sumo Logic utilizes best practices to ensure the security of customer data.

Sumo Logic automatically sends an email to a user in order to activate their account. During account activation a user is asked to create an account password. Sumo Logic has strong password standards that are outlined in the password dialog. It is strongly recommended that customers use complex and random generated passwords in order to maintain rigorous password protection for each Sumo Logic account. Customers are advised not to use the same password for their Sumo Logic account that is also used for any other service.

Advanced Enterprise Authentication Mechanisms

Cross Site Request Forgery (CSRF) is a serious threat to users of many web services, which is why Sumo Logic has proactively engineered a solution to ensure protection at every layer. When customers authenticate to the Sumo Logic service (either through a browser, or through Sumo Logic's API) there is a highly secure session-ID tracking mechanism that works transparently to ensure that only an authorized user is the initiator of any requests.

Additionally, Sumo Logic supports authentication via Security Association Markup Language (SAML), which allows for Single Sign On (SSO) from an enterprise intranet portal, extending our customers' enterprise authentication standards to Sumo Logic.

User level data security

Sumo Logic's Role Based Access Control (RBAC) features allow our customers to set per-user permissions to all of their data. This system allows for fine-grained access control based, enforcing segregation of duties within an organization to maintain compliance with internal and external data standards.

Node security

The Sumo Logic production system consists of many individual nodes running as a cluster. Each of these nodes is a hardened and well-protected system at the network and application layers.

All Sumo Logic cluster nodes are booted with the latest, up-to-the-minute security releases of Ubuntu. Each node is configured to automatically install any new security updates as they become available.

All OS, application, and security logs from each of the cluster-nodes are fed into a separate instance of the Sumo Logic environment for analysis.

Every node in the Sumo Logic cluster runs a default-deny host-firewall that white lists only the other cluster nodes with which it specifically needs to communicate, and only over the specific TCP and UDP ports which are required for that node to perform its function.

Each node in the cluster also runs the Snort Intrusion Detection System, with a policy that has been customized by the Sumo Logic Security Team. These logs (along with all of the other host logs) are fed into Sumo Logic for monitoring.

Vulnerability program

Sumo Logic implemented an industry leading vulnerability and incident response program.

Testing Program

- **Daily:** Sumo Logic security team uses Rapid 7 to run fully-credentialed scans of every new server.
- **Weekly:** Sumo Logic security team uses Rapid 7 to run fully-credentialed scans of every new build.
- **Quarterly:** Sumo Logic security team uses Rapid 7 to run ASV scans.
- **Every six months:** Sumo Logic security team engages a third party, IOActive, to perform penetration testing and Collector code review.

Sumo Logic implemented an incident response program based on RFC 2350, committing to the following SLAs:

- **Critical Issues:** Remediation efforts begin immediately, with a target to patch within 24 hours.
- **High Severity Issues:** Remediation within five days.
- **Medium Severity Issues:** Remediation within 60 days.
- **Low Severity Issues:** Addressed in accordance with their business and customer impact.

Access to data by Sumo Logic

Access to the production cluster is only allowed to Sumo Logic employees with a need to access the system. If a Sumo Logic employee requires access to a customer's UI screens for troubleshooting or technical support, this will only be granted with customer consent and only on and as-needed basis.

Protecting data is a critical component of every activity, product and service at Sumo Logic. Please feel free to contact us with any questions, suggestions or issues about any of the above, including our security policies. Please email them to security@sumologic.com.

Data Deletion

After a customer's data retention period (as specified in a customer contract) ends, customer data is deleted.

When customer log data is collected, it is divided between a raw data stream and an index stream; keys to the raw stream and keys to the indexes are generated. When data is deleted, indexes and keys are deleted rendering the data unrecoverable: the data cannot be found because the indexes were deleted, and the data cannot be decrypted because the keys were deleted. Next, our batch process deletes raw data and metadata in accordance with the DoD 5220.22-M data deletion standard.

305 Main Street
Redwood City, CA 94063
www.sumologic.com

© Copyright 2015 Sumo Logic, Inc. All rights reserved. Sumo Logic, Elastic Log Processing, LogReduce, Push Analytics and Big Data for Real-Time IT are trademarks of Sumo Logic, Inc. All other company and product names mentioned herein may be trademarks of their respective owners. | WP-0815