Securing the Sumo Logic™ Service

A Sumo Logic White Paper

Introduction

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 specification process, the coding phase, as well as in code reviews, penetration testing, user acceptance and operational practices.

Some strategic security technologies and processes that are core to the Sumo Logic service include:

- Centrally managed, FIPS-140 two-factor authentication devices for operations personnel
- Biometric access controls
- Whole-disk encryption
- Thread-level access controls
- Whitelisting of individual processes, users, ports and addresses

- Strong AES 256 encryption
- Regular penetration tests and vulnerability scans
- A strong Secure Development Life-Cycle (SDLC)
- Threat intelligence and managed vulnerability feeds to stay current with the constantly evolving threatscape and security trends

Compliance and Certifications

Sumo Logic is constantly working with our CPA partners at Brightline CPAs and Associates to acquire and maintain a variety of certifications and attestations. We currently hold:

- A SOC 2, Type 2 attestation
- An attestation of HIPAA compliance
- A PCI/DSS 3.1 Service Provider Level 1 Certification
- Sumo Logic complies with the U.S. – E.U. 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 European Union member countries and Switzerland
- The service is also FIPS-140 compliant

Logical Data Separation

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

First- all customer data is tagged per organization, and this tagging persists throughout the data lifecycle and is enforced at every layer of the system. For instance-only processes and threads such as queries within an authenticated organization's context may access that organization's data. 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 encrypted using per-customer keys, which are rotated on a 24-hour basis. These per-customer-per-day keys are stored on a highly secured node separate from S3. Because each customer's data is stored in separate S3 buckets, with unique encryption keys for each customer/day there is no logical co-mngling of data at this layer.

Physical Security

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

Physical data centers are located in secret locations with only key personnel even aware of their address. Additionally, many physical security measures, such as biometric access controls, twenty-four-hour armed guards and video surveillance, are used to ensure that no unauthorized access is permitted.

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

Encryption in Transit

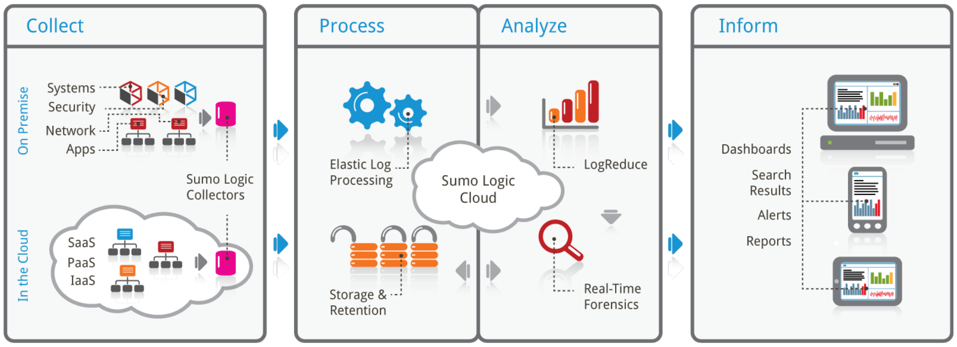
Upon logging in at https://service.sumologic.com, users will see an Extended Validation (EV) SSL certificate from GeoTrust. All user interactions with the Sumo Logic service will use this EV SSL Certificate for secure communications between their browser and Sumo Logic. Sumo Logic's certificates are encrypted on FIPS- compliant storage media in an off-site location, just to maintain their integrity. Once collectors are installed and reporting to Sumo Logic, they will send chosen log data to the Sumo Logic service through an SSL encrypted session to https://collectors.sumologic.com.

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

Encryption at Rest

All data at rest within the Sumo Logic system is encrypted using strong AES 256 bit encryption. All spinning disks are encrypted at the OS level and all long term data storage is encrypted using per-customer keys which are rotated every 24 hours.

Account Creation



As a cloud-based solution Sumo logic service handles data collection, processing, storage, forensic and analysis through a centralized and highly security platform.

As a cloud-based solution Sumo logic service handles data collection, processing, storage, forensic and analysis through a centralized and highly security platform. From the very first interaction on any account, Sumo Logic utilizes best practices to ensure the security of customer data. The Sumo Logic Security service automatically creates and issues a strong temporary password. This strong password is only temporary, and must be reset the first time a user logs in. Sumo Logic has password standards that are outlined in the password dialog. A password-management solution is strongly recommended 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 into the service 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 to the Sumo Logic service.

Additionally, Sumo Logic supports your organizations authentication needs through the use of the Security Association Markup Language (SAML), which allows our customers to extend their enterprise authentication standards to the Sumo Logic Service, and allows for Single Sign On (SSO) from your enterprise intranet portal.

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 from their Sumo Logic console. This system allows for fine-grained access-control based on filters defined by the customer. This allows you to enforce segregation of duties within your organization and allows you to maintain compliance with your internal and external data standards.

Authenticated Collector Download

After logging in and changing the temporary password, customers download Sumo Logic's collector software. In order to securely register the collector, a customer must provide the one-time collector registration ID that the collector will generate upon installation. (The collector will connect with collectors.sumologic.com over SSL on port 443 for verification and will request a onetime token.) This one-time registration is only valid for fifteen minutes; the collector should only be installed when users are ready to register it.

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 Maverick. 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 copy of the Sumo Logic environment for analysis.

Every node in the Sumo Logic cluster runs a default-deny host-firewall that has white lists only for the other cluster-nodes with which it specifically needs to communicate, and only over the specific TCP 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 the Sumo Logic service for monitoring.

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, and only through a highly secure two-factor authentication mechanism utilizing centrally managed and tracked IronKeys. 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.