SignalFx

SignalFx Platform:
Security and Compliance

MARZENA FULLER
Chief Security Officer

SignalFx

SignalFx Platform:
Security and Compliance

Introduction

SignalFx offers the only in-stream monitoring platform for ingesting, processing, storing, analyzing, visualizing, and alerting on metrics data at massive scale in *real* real-time.

The service was designed from the beginning with security as a key tenet, using best-in-class technologies, infrastructure, and development practices to safeguard customer data while delivering low latency, real-time performance. The company's dedicated security function is led by our Chief Security Officer, who works with engineering and product management to deliver enterprise-level product security and continuously improve internal security controls and processes.

SignalFx security program is founded on these principles:

Secure by Design | The SignalFx platform was designed for comprehensive security from the ground up.

Defense in Depth | SignalFx implements preventive and detective security controls at every layer: data, application, host, and network.

Proactive Protection | SignalFx leverages best-in-class technologies to ensure that configurations are secure by default and continuously monitored.

Intentional development | Our teams meet and exceed regulatory compliance standards for software development and regulated client data access.

Compliance Program

SignalFx undertakes a rigorous annual audit to provide our customers and ourselves with an independent evaluation of our security controls and processes. The audit is conducted by the independent public accounting firm of Schellman & Company, LLC, registered with the Public Company Accounting Oversight Board (PCAOB) and is subject to strict auditing standards, inspections, and enforcement. SignalFx currently holds a SOC 2 Type 2 attestation.

General Data Protection Regulation (GDPR)

GDPR imposes rules on companies, government agencies, non-profits, and all other organizations that offer goods and services to people in the European Union (EU), or that collect and analyze Personally Identifiable Information (PII) tied to EU residents. GDPR is not geographically binding and applies to all parties regardless of location.

SignalFx has implemented data protection measures following specific GDPR guidance**:**

- Our customers can submit a Subject Access Request (SAR) to correct inaccuracies and/or erase their personal data maintained by SignalFx.
- SignalFx protects sensitive PII data in transit and at rest with TLS 1.2 and AES 256 algorithms.
- SignalFx performs impact assessments to help mitigate the risk of breaches by identifying vulnerabilities and how to resolve them. Our breach notification process complies with GDPR.

Data Security

DATA TYPES AND CLASSIFICATION

Data ingested, processed, and stored by SignalFx falls into two categories:

Customer secrets | passwords and tokens that customers provide during SignalFx setup.

Metadata | a key-value store mapping object IDs to a set of properties describing these objects. Metadata is used to allow SignalFx users to find, filter, and aggregate the metrics that they want to graph or alert on.

SignalFx supports four types of metadata: dimensions, properties, tags, and time-series metrics.

Dimensions are key-value pairs included as part of a datapoint, and are applied to the datapoint when it is sent to SignalFx. Each combination of dimensions and metric names is used by SignalFx to uniquely identify a metric time series and the data points that comprise it.

Example dimensions key-value pairs:

Aws_availability_zone : <availability zone of an instance>

Aws_instance_type : <instance type>

Aws_public_ip_address : <address of the elastic IP address bound to a network interface>

Properties are key-value pairs added to dimensions, metrics, and other objects after they have already been sent in or created.

Tags are labels or keywords assigned to dimensions, metrics and other objects. They are not key-value pairs.

Time-series metrics are data points over a period of time. Examples include: CPU utilization, API call response time, and include the metric value and a timestamp.

SignalFx developed its Data Classification policy based on the level of data sensitivity and impact of potential unauthorized disclosure. Security controls were designed and implemented to balance risk with the demands of real-time data streaming and analytics.

ENCRYPTION IN TRANSIT

All data sent to SignalFx via metric ingest, API, the app, or backfill, is encrypted with TLS 1.2. Any communication between a user's browser and SignalFx requires an extended validation SSL certificate. All requests come through the AWS Elastic Load Balancer (ELB) on port 443. The ELB uses SSL (X.509 certificate) to terminate the connection and then decrypt requests from clients.

Data is sent to SignalFx through a managed collection of open source agents (e.g. collectd, statsd, telegraf, etc), our open source Smart Agent, our Metric Proxy, through a connection to our customer's cloud infrastructure (e.g. AWS CloudWatch), as well as custom integrations built with SignalFx client libraries.

DATA INGEST

The **SignalFx Smart Agent** is a metric agent written in Go for monitoring infrastructure and application services in a variety of different environments. Customers can install either a standalone agent or a containerized version.

The SignalFx Smart Agent installed on customer infrastructure does not receive any inbound connections. The agent does not have the ability to auto-update, hence all updates must be manually installed and configured by customers.

Smart Agent Permissions | The Smart Agent runs as a signalfx-agent user. To use host observer (host discovery) the agent requires `DAC _ READ _ SEARCH` and `SYS _ PTRACE` to determine which processes are listening on network ports. Customers should not run Smart Agent with `root` privileges.

Cloud infrastructure integrations for AWS, Azure, and GCP use a restricted set of permissions.

- Access to AWS is set up via an AWS IAM role.
  The role requires `list` and `describe` permissions only.
- Access to Google Cloud is set up via a GCP Project Viewer role.
  The role requires `get` and `list` on monitoring `metricDescriptors` and `timeSeries`.
- Access to Azure is set up via an IAM role.
  The role requires Monitoring Reader permissions on the subscriptions being monitored.

For detailed permission requirements please refer to the SignalFx User Guide.

ENCRYPTION AT REST

SignalFx encrypts customer secrets at rest with AES 256 bit encryption. Each secret is encrypted with a dynamic key which is then encrypted with a root key.

DATA SEGREGATION

Customer data is tagged per organization with a unique 64-bit identifier.

The Data Model Library includes an ID generator which is used to generate IDs for common objects. The generator uses SHA-256 to generate a unique, 128-bit value based on the logical coordinates that uniquely identify the object. The most general form of this hashes a customer ID (most objects are associated with a customer), a *type hint* and a *name key* to produce a 128-bit value.

DATA REPLICATION AND BACKUP

SignalFx replicates its persistent data-stores to three Amazon Availability Zones (AZ) to address the risk of a single AZ failure, and backs them up to an encrypted S3 bucket in Amazon US-West to address a total AWS region failure.

SignalFx tests its backup and recovery procedures annually.

DATA RETENTION AND DELETION

SignalFx by default retains metric data for 13 months at the 1-hr aggregation, and implements an automated process to delete customer data 30 days upon account termination.

Application security

The SignalFx streaming platform is operated as a continuous deployment environment with a continuous testing and release pipeline. SignalFx uses Gerrit, a web-based code review tool on top of Git, to facilitate code reviews. Each change must be reviewed and approved by at least one other engineer before it can be submitted.

Customer-facing changes are communicated to customers via the 'What's New' section of the SignalFx product.

APPLICATION VULNERABILITY SCANS

SignalFx performs monthly Qualys web application security scans against OWASP Top 10 risks such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF) and unvalidated redirection. All findings are reviewed, validated, and remediated by SignalFx.

PENETRATION TESTING AND CODE REVIEW

SignalFx engages AppSec Consulting to conduct an annual penetration test and code review. During the pen test, AppSec tests SignalFx for platform vulnerabilities (server misconfigurations, published vulnerabilities, buffer overflow) and application vulnerabilities (authentication, authorization, permission escalation, cross-site scripting, session management). All findings are reviewed, validated, and remediated by SignalFx.

AUTHENTICATION

SSO

SignalFx provides single sign-on (SSO) for customers to use their existing identity providers for employee authentication. SignalFx provides supported integrations to certain SAML SSO providers (Okta, OneLogin, PingOne, ADFS, Azure Active Directory, Bitium, Google, Google Cloud Identity). If a customer's SAML SSO provider is not on our list of supported integrations, SignalFx can make available (upon administrator request) a generic integration for SAML SSO connection. Using this generic SAML SSO integration, administrators in a customer account can direct SignalFx to use any publicly available SSO endpoint to authenticate users.

Username and password

Customers who do not use SSO can authenticate with an email address and password. Passwords must be a minimum of eight characters and must include at least one number or special character. Password expiration requirements are also enforced. User passwords are stored in an industry standard encrypted hash format.

USER MANAGEMENT

SignalFx provides admin, user, and team application access control.

- Admins can manage users and teams.
- User access is controlled via team membership.
- Team management in the context of monitoring a subset of systems most companies organize users into multiple teams based on a general area of responsibility, such as Operations, DevOps, or Infrastructure IT.

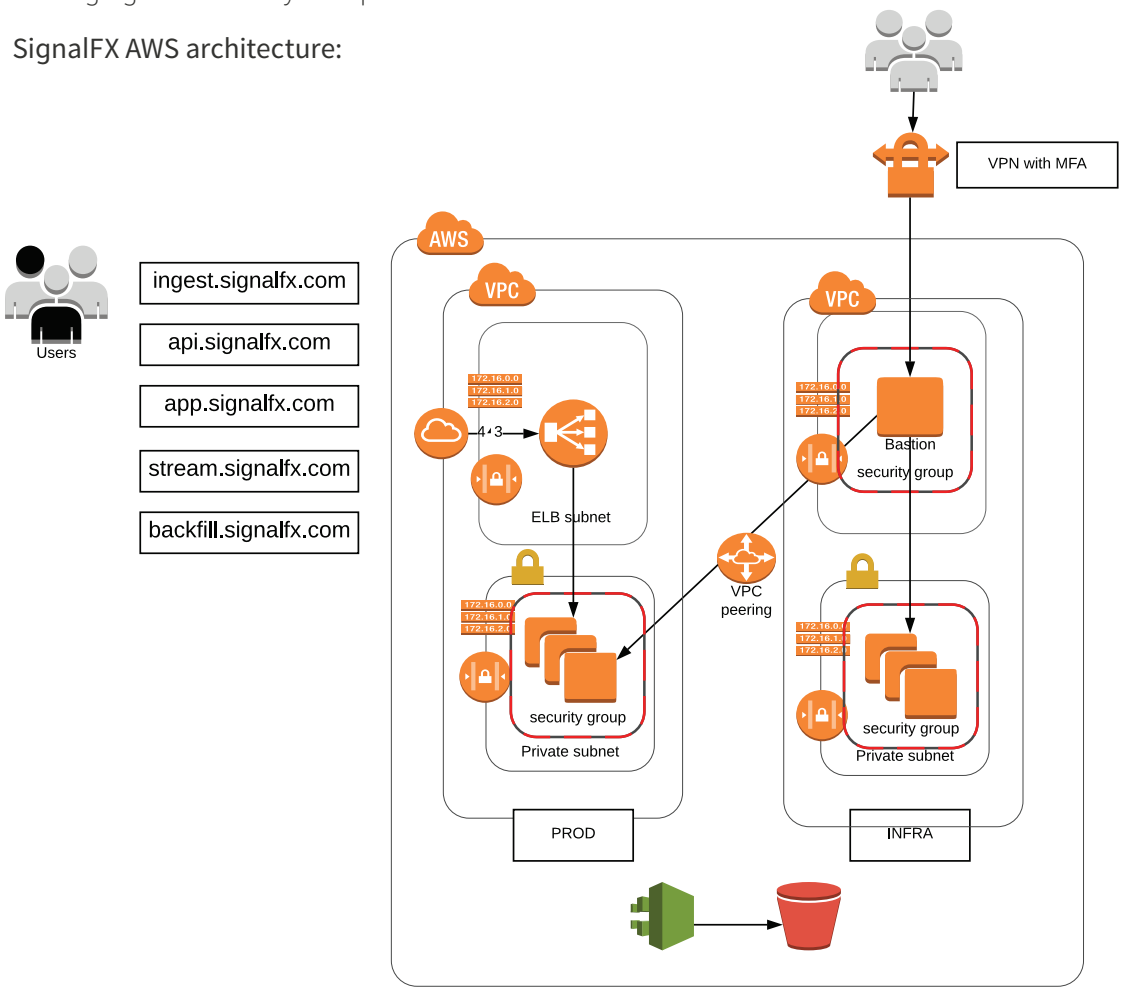
In SignalFx, organizing users into teams lets you create links between content (dashboard groups and detectors) and teams. Linked content is used to create a team landing page, which lets team members quickly view relevant content on a single page. Dashboards and detectors for a given team can be modified only by members of that team.

Customers are responsible for managing their own accounts, including provisioning and de-provisioning their own users.

Infrastructure security

SignalFx designed its AWS architecture in accordance with the AWS Shared Responsibility model, leveraging AWS security best practices.

SignalFX AWS architecture:



SignalFx is deployed on AWS inside a PROD VPC. ELBs are deployed in a public subnet and all production instances are deployed in a private subnet. Each subnet is associated with a routing table controlling subnet communication with external networks and with a network access control list (NACL) controlling traffic in and out of a subnet.

User traffic coming to the internet gateway is routed to a public subnet with ELBs configured to listen on port 443.

All production instances are deployed in a private subnet, have no publicly facing IP addresses, and can receive connections via ELBs. The private subnet is associated with a private routing table and a NACL. Additionally, each instance in the private subnet is associated with security groups controlling inbound and outbound instance connections.

A restricted group of SignalFx engineers can access PROD VPC in order to troubleshoot. To gain access an engineer has to first connect via VPN with MFA and then through a VPC peering connection to the instances in VPC PROD. All connections as well as executed commands are logged and monitored.

AWS ACCOUNT MANAGEMENT

SignalFx leverages IAM users, groups, and roles to manage access to our AWS account. AWS groups are created based on job functions. Permissions are managed through AWS managed policies and assigned to individual users via group membership.

SignalFx follows the "least privileged" access principle. Users are allowed to manage their own credentials and have limited access to list and describe AWS resources. Administrator access is restricted to a small group of SignalFx engineers and reviewed periodically.

All AWS access keys are rotated every six months.

SignalFx requires all IAM users to have multifactor authentication activated for their individual accounts for console and command line (CLI) access.

Use of the root account is restricted to four senior engineers (red group). Access to the root account requires an MFA code generated from a Gemalto hard-token. The token is locked in a safe and access to the safe is restricted to three senior employees (blue group). SignalFx implemented dual control over access to the root account via segregation of the root password and physical access to the Gemalto hard-token.

LOGGING AND MONITORING

SignalFx logs and monitors all AWS API calls. CloudTrail is enabled in all regions and CloudTrail logs are sent to a secure S3 bucket. To ensure that CloudTrail logs are not tampered with, SignalFx enabled CloudTrail validation, encrypted CloudTrail S3 buckets, and requires MFA to delete CloudTrail S3 buckets.

SignalFx proactively monitors AWS API calls for high risk activity.

AWS VULNERABILITY SCANNING

SignalFx performs a weekly scan of its AWS account against the Center for Internet Security (CIS) Benchmark. The scan checks for insecure configurations on AWS resources and provides recommended remediation steps. All findings are reviewed, validated, and remediated as needed.

Host security

SignalFx leverages AWS security groups to secure its hosts. Each host is associated with security groups controlling inbound and outbound connections. Security groups are protected from unauthorized modifications and scanned for misconfigurations weekly.

SignalFx uses Qualys to scan all EC2 instances monthly for vulnerabilities. All findings are reviewed, validated, and remediated as needed.

Every instance runs Salt to monitor changes to selected directories and files.

Conclusion

Data protection is critical to every activity, product, and service that SignalFx provides. Our strategic security and privacy protocols have proven to be effective and reliable. As our technology environment evolves to facilitate new products, services, and features we will continue to have security at the forefront of everything we do. The clearest manifestation of this commitment is the addition of the Chief Information Security Officer to our executive leadership team.

If you have questions or suggestions for how we can improve, please don't hesitate to contact us at security@signalfx.com.

SignalFx

SignalFx is a real-time operational intelligence platform for data-driven DevOps. The service discovers and collects streaming metrics across every component in the cloud, replacing traditional point tools and providing real-time visibility into today's dynamic cloud and container environments. The massive scalability of the service is optimized for container, microservices, and function based architectures and provides powerful visualization, proactive alerting, and collaborative triage capabilities for organizations at any stages of their cloud transition.