SECURONIX™

SOLUTION BRIEF

Securonix Security Monitoring for Amazon Web Services (AWS)

Enterprises worldwide use the AWS platform to enable their IT infrastructure, host sensitive applications and data, as well as enable critical enterprise functions. As a result, the security of the AWS platform is a key concern.

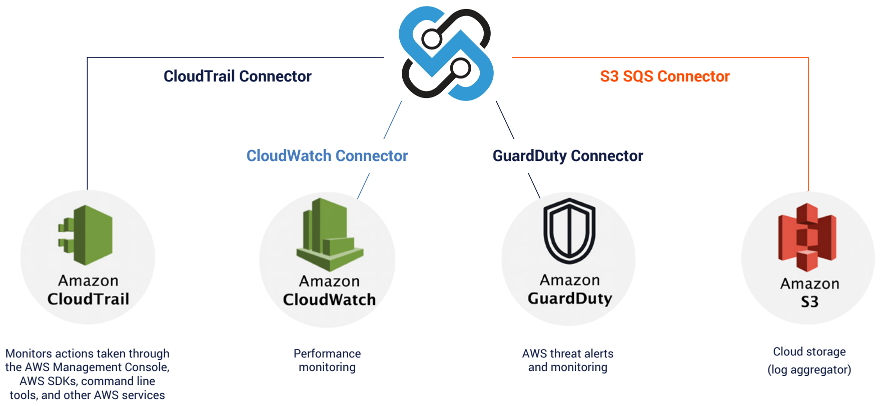
Securonix uses bi-directional integration with AWS components to provide end-to-end security monitoring, advanced threat detection, data retention, and automated incident response capabilities.

In order to enable quick access to AWS-linked security events, Securonix has direct API integration with AWS, allowing Securonix to collect and analyze logs across various AWS products. The Securonix platform integrates with multiple AWS security touchpoints, combining information and context in order to show you the security status of your AWS environment at a single glance.

The Securonix platform integrates with:

- **Amazon CloudTrail:** Monitors API calls to the AWS platform from around 154 different services.
- **Amazon CloudWatch:** Performance monitoring, such as CPU and disk usage, as well as other log types.
- **Amazon Simple Storage Service (S3):** Log storage from multiple sources, such as CloudFront, web application firewall (WAF), Elastic Load Balancer (ELB), and CrowdStrike.
- **Amazon GuardDuty:** Monitoring and alert generation.

This information is processed by Securonix in order to identify tangible threats, including data compromise, unauthorized access attempts, suspicious traffic, and several others.

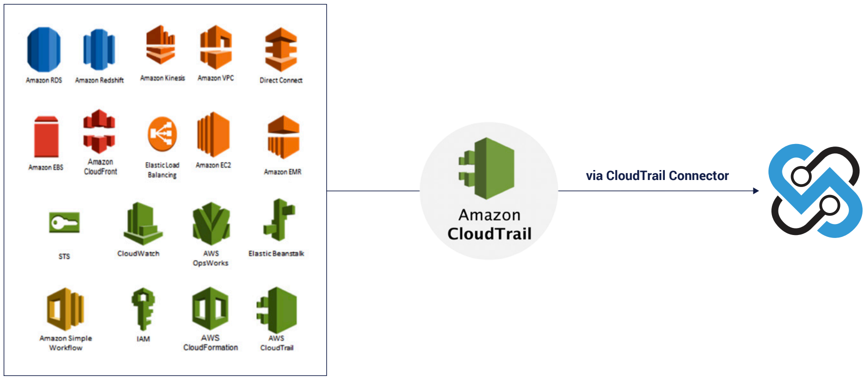

CloudTrail Connector
S3 SQS Connector
CloudWatch Connector
GuardDuty Connector
Amazon CloudTrail
Amazon CloudWatch
Amazon GuardDuty
Amazon S3
Monitors actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services
Performance monitoring
AWS threat alerts and monitoring
Cloud storage (log aggregator)

Solution Benefits

- Streamlined, direct API integration enables fast event gathering.
- Complete AWS log coverage, including Amazon Virtual Private Cloud (VPC), Amazon Elastic Compute Cloud (EC2), ELB, login, and API events.
- Enrichment of data with additional context for threat modeling.
- Out-of-the-box bi-directional integrations for Amazon S3, Amazon CloudWatch, and Amazon GuardDuty.
- Data Insights: Securonix for AWS enables you to visualize activities and changes in your AWS infrastructure with out-of-the-box dashboards and reports that can be easily customized.

AWS CloudTrail Integration

AWS CloudTrail monitors actions taken within multiple AWS services by logging API calls from them. Securonix integrates with AWS CloudTrail in order to pull these logs for processing.



AWS CloudWatch Integration

AWS CloudWatch aggregates logs from Windows/Linux servers, Amazon VPC, Amazon Relational Database Service (RDS), and Amazon Elastic Kubernetes Service (EKS) for performance monitoring. Securonix integrates with the Amazon CloudWatch connector, pulling performance information to correlate with events and identifying threats that may cause performance problems or resource misuse.

Amazon S3 Integration

Amazon S3 acts as a log aggregator, combining logs from various source such as ELB, Amazon CloudFront, CrowdStrike, and WAF (through Amazon Kinesis Firehose). Securonix integrates with Amazon S3 and uses this logging information for security monitoring and additional security context. Securonix is also able to write data back into Amazon S3, or retrieve it in real time through Amazon Athena for searching and threat hunting.

Sample Use Case: Threat Modeling by Correlating Alerts

Securonix threat models stitch together indicators of compromise (IOC) across data sources in order to detect targeted attacks. For example, in order to detect a cryptojacking attack, some of the IOCs are:

- A suspicious console login found in the AWS console logs.
- A related permission elevation found in the AWS Identity and Access Management (IAM) logs.
- A spike in start instances in AWS or rare start instances found in the Amazon EC2 configuration logs.
- AWS CloudTrail logging being disabled according to the AWS IAM logs.

AWS Validated Security Competency

Securonix has achieved Amazon Web Services (AWS) Security Competency status. This designation recognizes that Securonix has demonstrated technical proficiency and proven customer success in delivering SIEM as a service on the AWS platform.

Achieving AWS Security Competency differentiates Securonix as an AWS Partner Network (APN) member that offers specialized software designed to help organizations adopt, develop, and deploy complex security projects on AWS. To receive the designation, APN partners must possess deep AWS expertise and deliver solutions seamlessly on AWS.

Key Use Cases

- Unauthorized access such as a login from a rare IP or geolocation, a spike in failed logins, a land speed anomaly, or a malicious IP.
- Amazon EC2 configuration anomalies such as a spike in instance creation or deletion, suspicious admin activities, or a rare instance.
- Suspicious AWS IAM activity such as suspicious user creation, admin privilege changes, password policy changes, or rare privileged activity.
- Anomalous API connections including from a rare IP or geolocation, or a malicious IP address.
- Suspicious Amazon VPC traffic including port scans or connections on anomalous ports.

aws partner network

Advanced
Technology
Partner

Security Competency

About Securonix

The Securonix platform delivers positive security outcomes with zero infrastructure to manage. It provides analytics-driven next-generation SIEM, UEBA, and security data lake capabilities as a pure cloud solution, without needing to compromise. For more information visit www.securonix.com.

SECURONIX™

LEARN MORE
www.securonix.com

LET’S TALK
+1 (310) 641-1000