SECURONIX™

SOLUTION BRIEF

Amazon Web Services (AWS) Security Monitoring

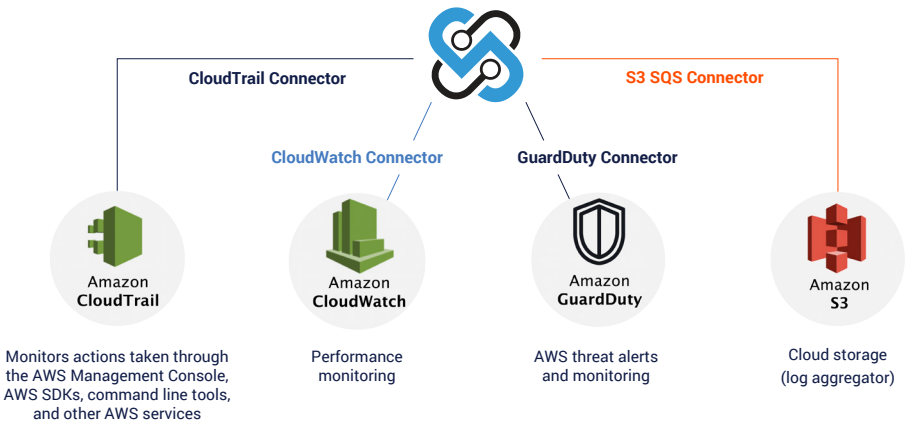
Organizations large and small use the AWS platform to enable their IT infrastructure, host sensitive applications and data, as well as enable critical enterprise functions. But as usage grows, so does the potential for attack. As with most public clouds, Amazon Web Services provides services to detect traditional cybersecurity attacks. However, AWS is vulnerable to insider threats such as credential compromise and data exfiltration. Additionally, AWS security monitoring services are fragmented and complex, so it's hard to get a holistic view of AWS cloud monitoring detection and response.

To help organizations gain visibility into their AWS infrastructure, and detect advanced cybersecurity attacks, Securonix offers customers a tightly integrated security monitoring solution. 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.

For quick access, Securonix has a direct API integration with AWS, allowing Securonix to collect and analyze logs across various AWS products. Securonix then combines this information with additional context in order to quickly detect AWS-linked security events including data compromise, unauthorized access attempts, suspicious traffic, and many others. This gives you complete visibility into your AWS environment in a single glance.

Securonix integrates with:

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



Solution Benefits

- Gain complete visibility into AWS data, including Amazon Virtual Private Cloud (VPC), Amazon Elastic Compute Cloud (EC2), ELB, login, and API events.
- Fast detection and response using streamlined, out of the box API integration with Amazon Web Services including Amazon S3, Amazon CloudWatch, and Amazon GuardDuty.
- Decrease mean time to respond by using enriched data combined with additional context for accurate threat modeling.
- Visualize activities and changes in your AWS data using out of the box dashboards and reports that can be 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 in order to detect and respond to possible security threats or performance issues such as 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.

Use Case: Threat Modeling by Correlating Alerts

Securonix threat models stitch together indicators of compromise (IOC) across data sources in order to detect advanced attacks. For example, in order to detect a cryptojacking attack, Securonix would stitch together the IOCs below to demonstrate an attack progression that needs investigation.

- 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 is an Amazon Web Services (AWS) Security Competency Partner. This designation recognizes that Securonix has demonstrated technical proficiency and proven customer success in delivering next-generation 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

Securonix transforms enterprise security with actionable intelligence. Using a purpose-built security analytics platform Securonix quickly and accurately detects high-risk threats to your organization. For more information visit www.securonix.com.

Visit Securonix in AWS Marketplace

aws marketplace

SECURONIX™

LEARN MORE
www.securonix.com

LET'S TALK
+1 (310) 641-1000
info@securonix.com