Securonix

Next-Generation SIEM

Key benefits

- Gain complete visibility into AWS data, including Amazon Virtual Private Cloud (VPC), Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), login, and application programming interface (API) events.
- Fast detection and response using streamlined, out of the box API integration with Amazon Web Services, including Amazon Simple Storage Service (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 partner network

Advanced Technology Partner

Security Competency

Product overview

Built on an open big data platform, Securonix Next-Gen security information and event management (SIEM) provides unlimited scalability and log management, behavior analytics-based advanced threat detection, and automated incident response on a single platform. Customers use it to address their insider threat, cyber threat, cloud security, and application security monitoring requirements.

Product features

Unlimited scale

The Securonix platform delivers unlimited scale, powered by first-rate behavior analytics, machine-learning-based advanced threat detection and modeling, and automated incident response. Securonix can scale beyond 500,000 events per second (EPS).

Lower meant time to repair (MTTR)

Lower your mean time to detect, respond, and stop threats with SIEM-as-a-service. No need to re-architect your security as you scale. No limits on the number of concurrent use cases. Text-based threat hunting with near real time response.

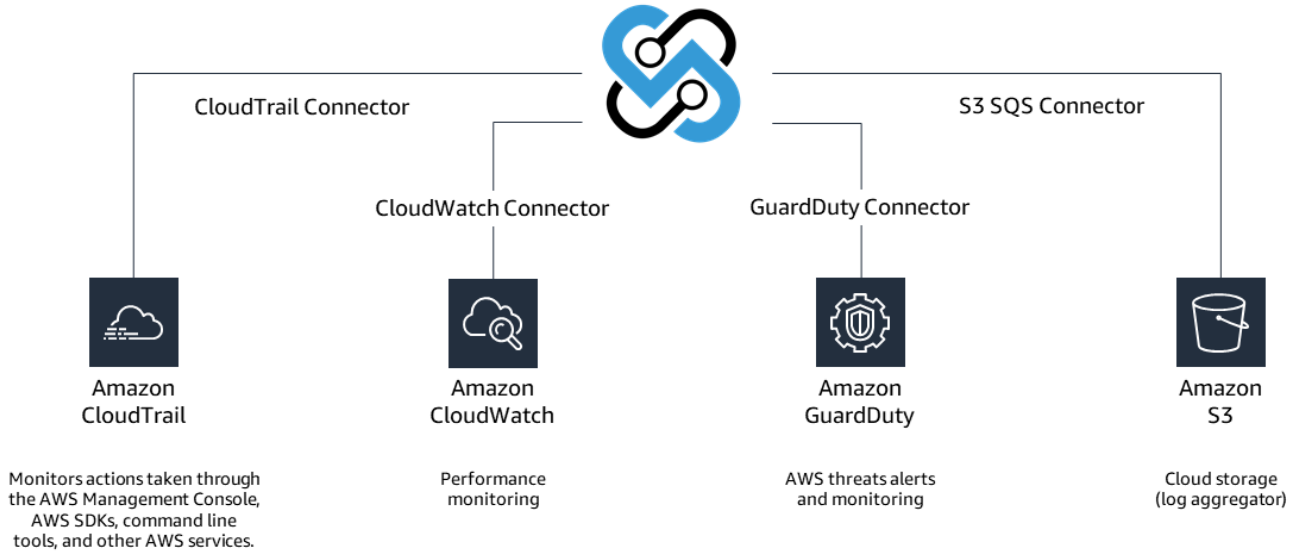
Immediate value

The software as a service (SaaS) platform leverages cloud-native, big data, and artificial intelligence (AI) to deliver immediate value. No hardware cost and operational overhead. With native support for thousands of third-party solutions, it easily scales from startups to global enterprises.

How it works

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.



Differentiators

Securonix integrates with:

- **Amazon CloudTrail**: Monitors API calls to the AWS platform from around 154 different services.
- **Amazon CloudWatch**: Provides performance monitoring, such as central processing unit (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), ELB, and CrowdStrike.
- **Amazon GuardDuty**: Organizes monitoring and alert generation.

Solution available in [AWS Marketplace]