securonix

aws

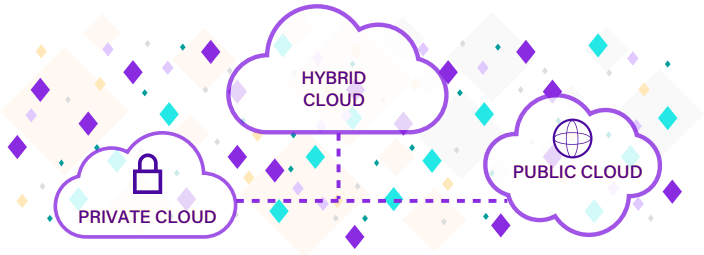
SOLUTION BRIEF

Amazon Web Services (AWS) Cloud Security Monitoring

Expand Detection and Response to Cloud Threats

Remove Cloud Security Blind Spots

Amazon Web Services (AWS) provides services to detect traditional cybersecurity attacks. However, AWS is vulnerable to insider threats such as credential compromise and data exfiltration due to the complexity of hybrid cloud environments. AWS security monitoring services are fragmented, making it difficult to get a holistic view of AWS for cloud monitoring detection and response.



Our Approach

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 a bi-directional integration with AWS components to analyze possible security events and provide end-to-end security monitoring. By collecting all threat information into a single source of truth, you gain the ability to detect advanced threats, retain your data in a centralized place, and automate incident response.

Detect and Respond to Cloud Threats in AWS

Gain 360 Visibility

Correlate cloud security events with on-premises network data. Now, your security team has a holistic security picture across their ecosystem.

Detect Threats Faster

Decrease your mean-time-to-detect with context-rich data insights and advanced threat chain analytics.

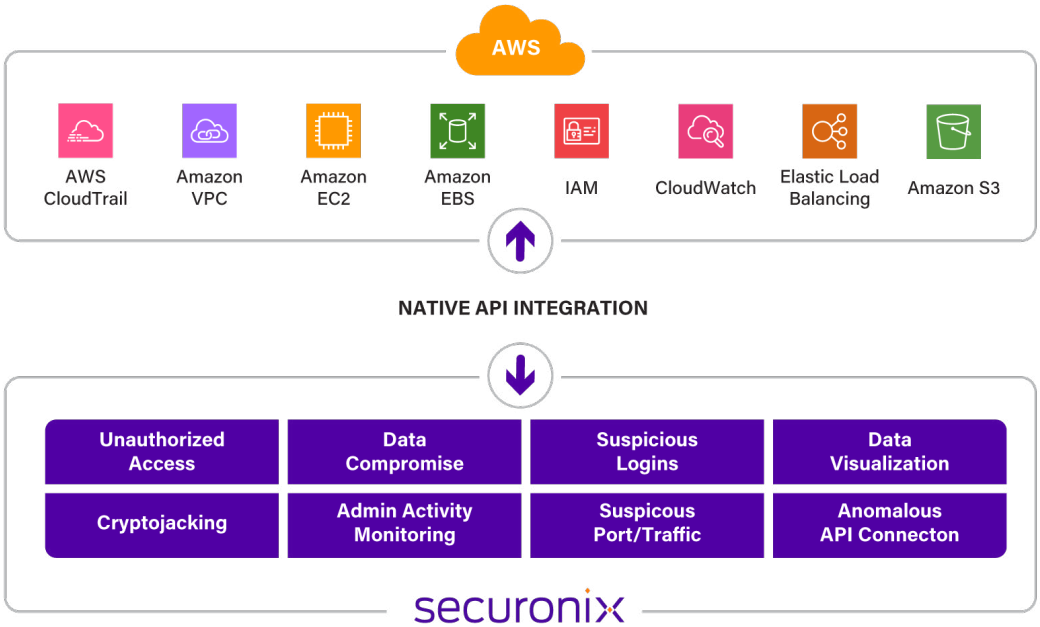
Unlock Data Insights

Visualize security events and changes in your AWS environment with out-of-the-box and custom dashboards and reports.

How it Works

Securonix has a direct API integration with AWS, allowing Securonix to collect and analyze logs across various AWS products. Then, Securonix enriches this data with additional context to quickly detect AWS-linked security events including data compromise, unauthorized access attempts, suspicious traffic, and more. 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.



AWS Validated Security Competency

aws partner network
Advanced
Technology
Partner
Security Competency

Securonix is an Amazon Web Services (AWS) Security Competency Partner. This designation recognizes that Securonix demonstrates 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. Securonix offers specialized software designed to help organizations adopt, develop, and deploy complex security projects on AWS. To receive this designation, APN partners must possess deep AWS expertise and deliver solutions seamlessly on AWS.

Key Use Cases for AWS Cloud Monitoring

- **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.

For more information about Securonix, schedule a demo at: www.securonix.com/request-a-demo

awsmarketplace

Visit Securonix in AWS Marketplace

About Securonix

Securonix is redefining SIEM for today's hybrid cloud, data-driven enterprise. Built on big data architecture, Securonix delivers SIEM, UEBA, XDR, SOAR, Security Data Lake, NDR and vertical-specific applications as a pure SaaS solution with unlimited scalability and no infrastructure cost. Securonix reduces noise and prioritizes high fidelity alerts with behavioral analytics technology that pioneered the UEBA category. For more information visit securonix.com