Cisco Secure Cloud Analytics

Secure your private network, public cloud, and hybrid environment

Comprehensive analytics for any environment

Adding effective security measures for public and private cloud and hybrid workloads—with solutions that can reduce the number of false positives—is a critical task. However, the public cloud infrastructure differs from an on-premises or hybrid infrastructure. Regardless of the environment, it merely provides fewer network monitoring capabilities despite a very high asset change rate. To provide effective security while reducing the number of false positives, a new approach is necessary.

Imagine if an employee's cloud credentials are compromised, through phishing or another method, can you tell if that employee begins logging in from another country? Cisco Secure Cloud Analytics provides the actionable security intelligence and visibility necessary to identify malicious activities in real time. You can quickly respond before a security incident becomes a devastating breach.

Secure Cloud Analytics is a Software-as-a-Service (SaaS) product that you can use to identify internal and external threats in on-premise, public, and hybrid cloud environments. It is simple to use, simple to buy, and simple to maintain. When data is received, little additional configuration or device categorization is needed. The analysis is entirely automated, and the workflow between the Cisco XDR platform and Secure Cloud Analytics to deliver Extended Detection and Response (XDR) capabilities is seamless.

Benefits of an analytics solution

Complete your digital transformation by updating your security operations. Secure Cloud Analytics was built in the cloud to provide Network Detection and Response (NDR) use cases for the modern network. Comprehensive visibility across environments detects advanced threats faster, reduces false positives, and assists in establishing a better security posture, allowing security teams to improve detection and response capabilities and businesses to decrease operational overhead.

- **Gain** actionable intelligence by monitoring your whole environment, from the private network to the public cloud.
- **Detect** advanced attacks and indicators of compromise rapidly by using the formidable behavioral analytics to detect unknown, sophisticated, or ignored threats to radically cut the mean time to detect and respond.
- **Boost** your security while minimizing the operational costs to third-party vendors, support management, ease of integrations + compatibility among the tools they do use.
- **Reduce** false positives significantly with higher-fidelity, detailed, and actionable alerts supported by real-world observations.
- **Attain** a higher level of security across the company, including the public, private cloud, and hybrid environments.

Complete and comprehensive analytics

Cisco Secure Cloud Analytics brings together your existing network and cloud to provide comprehensive analytics of traffic.

- As part of our extended detection and response solution, Secure Cloud Analytics provides automatic or manual response capabilities in response to the detection of suspicious network traffic with Cisco SecureX.
- Secure Cloud Analytics analyzes network flows and/or traffic telemetry (for example, NetFlow records) in real time or near real time.
- Secure Cloud Analytics monitors and analyzes north/south traffic (as it crosses the perimeter) as well as east/west traffic (as it moves laterally throughout the network).
- Secure Cloud Analytics provide high-fidelity, fully contextualized threat detection that can be quickly assessed by a SOC analyst, reducing time to detect and time to respond to actual threats and attacks.
- Secure Cloud Analytics models and tracks entity behavior over time, allowing it to detect malicious patterns aligned with MITRE ATT&CK rather than just network anomalies within session activity —modeling normal network traffic and flaging suspicious traffic that deviates from the norm.

Behavioral detection techniques (non-signature-based detection), such as statistical outliers and advanced analytics can help you detect evolving threats. Secure Cloud Analytics uses a behavior-modeling approach that detects a threat based on how it acts on the network. For example, if a domain controller begins to transfer data using the File Transfer Protocol (FTP), that is likely to be the first sign of a compromise. Secure Cloud Analytics detects this behavior in real time and alerts you to it.

Using dynamic learning, Secure Cloud Analytics creates a model—a kind of simulation—for each device and network entity. This model can:

- Link alerts to MITRE Tactics and Techniques to provide a standard industry framework for responding and acting on findings.
- Dynamically determine the role of an entity based on its behavior and then detect activities inconsistent with that role.
- Identify anomalies and sudden changes in behavior, both in data transmission and in access characteristics.
- Detect when an entity acts differently than similar devices do.
- Identify when an entity violates organizational policies, including protocol and port use, device and resource profile characteristics, and blacklisted communications.
- Predict host or device behavior based on past activities and assess observed behavior against those predictions.

Enhanced Analytics, Greater Outcomes with Cisco XDR

Secure Cloud Analytics and Cisco XDR are coming together to elevate security operations capabilities. By consolidating, correlating, and analyzing security events in real time, Cisco XDR enhances Secure Cloud Analytics outcomes, empowering security teams to promptly detect and respond to threats with increased efficiency. One of the key benefits is the ability to prioritize incidents based on business impact and asset value, enabling more targeted actions. Moreover, the integration harnesses intelligence from multiple sources, providing security practitioners with informed insights and improved threat detection. For comprehensive threat hunting, security teams gain access to extensive telemetry analysis, ensuring more effective investigations. The combination of inventory data with security insights creates a holistic asset context, facilitating better threat correlation. Additionally, the integration offers swift and precise automated response recommendations, upleveling the abilities of your security analysts to take confident actions, leading to reduced response time and enhanced overall effectiveness in managing security incidents.

Thanks to these capabilities, more time can be spent on remediating issues instead of manually analyzing data.

Detect threats in your public cloud

Secure Cloud Analytics' public cloud monitoring provides the visibility and threat detection capabilities you need to keep your workloads highly secure in Amazon Web Services (AWS) and Microsoft Azure environments.

It consumes all sources of telemetry native to AWS, including Amazon Virtual Private Cloud (VPC) flow logs, to monitor all activity in the cloud without the need for software agents, and can be deployed in a matter of minutes with no disruption to service availability. This data is used to model how each cloud resource is used. It can then detect sudden changes in behavior, malicious activity, and signs of compromise.

Secure your private network too

Secure Cloud Analytics' private network monitoring can be extended to the private network to provide hybrid environment visibility and threat detection using a single dashboard. As the number of connected devices on the private network increases, security personnel struggle to identify the various entities in their network and determine whether they pose a threat. With Secure Cloud Analytics, organizations can accurately detect threats in real time, regardless of whether an attack is taking place on the network, in the cloud, or across both environments.

Protect your environment today

Try Secure Cloud Analytics today with a free no risk trial.

To learn more, go to:
cisco.com/go/securecloudanalytics
or contact your local Cisco account representative.