forfusion

cisco Partner
Advanced Security Architecture Specialized

Data Sheet

# Cisco Secure Cloud Analytics

(formerly Stealthwatch Cloud)

Secure Workplace

## Gain the visibility and continuous threat detection needed to secure your public cloud and hybrid environments.

As organisations move more IT resources to the public cloud, they need the visibility necessary to detect threat actors targeting their cloud assets. In addition, they need an easy-to-use, operationally efficient solution. Secure Cloud Analytics provides the visibility and threat detection capabilities you need to keep your workloads highly secure in all major cloud environments like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform.

Development teams are also continuously adopting new and more dynamic compute environments like serverless and containers such as AWS Lambda and Kubernetes. Secure Cloud Analytics provides visibility into these environments so that organisations don't have to compromise on security on their path to digital transformation.

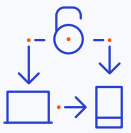
Secure Cloud Analytics provides comprehensive visibility and high-precision alerts with low noise, without the use of agents. Organisations can also monitor their cloud security posture to ensure configuration best practices and adherence to internal policies, thereby limiting potential risk and exposure of their cloud infrastructure. Secure Cloud Analytics is a cloud-based, Software-as-a-Service (SaaS)-delivered solution. It detects ransomware and other malware, data exfiltration, network vulnerabilities, system, event and configuration risk, and role changes that indicate compromise.

In addition to securing the cloud environment, Secure Cloud Analytics can also be extended to the private network with Cisco Secure Network Analytics SaaS (formerly Stealthwatch Cloud Private Network Monitoring) to provide hybrid environment visibility and threat detection using a single dashboard.

The number of connected devices on the private network is increasing dramatically. As a result, security personnel struggle to know what entities are operating in their environment, let alone whether they pose a threat to the organisation. So, with Secure Cloud Analytics, organisations 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.

And Secure Cloud Analytics also comes with Cisco SecureX, the broadest, most integrated security platform, to unify visibility, simplify threat response and enable automation across every threat vector and access point.

## New to Secure Cloud Analytics is a highly flexible event viewer that allows users to manage cloud posture with ease. Here's how it works:

| Feature | Initiative |
|---|---|
|  **Network and cloud analytics** | Provides fully automated, real-time analysis of device-level network traffic and patterns of communication for visibility across all devices and resources operating in the public cloud and on the private network. |
|  **High-fidelity security alerts** | Delivers actionable intelligence while reducing false positives, enabling smarter security actions. |
|  **Built-in SecureX platform** | Unify visibility, simplify threat response and enable automation with the industry's broadest, most integrated security platform. |
|  **Risk and posture Monitoring** | Quickly identify misconfigurations and changes that could introduce risk to the cloud environment, aligned with industry best practices or your internal policy. |
|  **SaaS** | Adds the ease of use, deployment, and flexibility that organisations need to deploy security at scale. |
|  **Entity modelling** | Provides a behavioural model of every device and entity on the network to automatically identify sudden changes in behaviour and malicious activity indicative of a threat. |
|  **Automatic role classification** | Identifies the role of each network device and cloud resource automatically based on its behaviour. |
|  **Agentless deployment** | Consumes native sources of telemetry and logs from the network and Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP) cloud instances, with no need for specialised hardware or software agents. |
|  **Monitoring private network/ hybrid environments** | Detects threats and anomalies in the private network as well as your public cloud resources using a single tool to streamline security operations and workflows. |

## Security for the modern network

Today's organisations are struggling with security "blind spots." There is an explosion of devices on the private network, and more workloads are being migrated to the public cloud. Meanwhile, security practitioners are inundated with security alerts to the point of unmanageability.

Only 51 % of security alerts are investigated, and more than half of those are not remediated, according to the Cisco 2019 CISO Benchmark Study.

Attackers are quick to take advantage of these developments to breach network defences and remain undetected. As a result, organisations need an easy way to see their network activity, understand "normal" entity behaviour, and identify the signs of threats. Secure Cloud Analytics accomplishes this by consuming sources of telemetry and logs from the public cloud and then modelling behaviour to identify threat activity.

### Visibility and analytics

This telemetry is processed in Secure Cloud Analytics to provide visibility of all active entities across your modern network, including the private network, branch, and public cloud. Through entity modelling, the solution can detect various threat activities with a high degree of accuracy. The high-fidelity security alerts support smarter security decisions, reduce the number of false alarms, and shorten the time spent conducting investigations.

### Flexibility and ease of use

Secure Cloud Analytics is delivered as SaaS, making it easy to try, easy to buy, and simple to use. There is no specialised hardware to purchase, no software agents to deploy, and no special expertise required. From the moment the solution begins receiving data, there is no additional configuration or device classification required. In addition, all the analytics are automated and as a result, it requires very little management or security expertise to operate.

### Cloud security posture management

Secure Cloud Analytics begins checking your cloud resources for risky configurations and changes upon deployment. You can also create your own watchlists to be alerted to activity of interest and to ensure cloud resources are adhering to your internal policy.

### Entity modelling for advanced threat detection

As telemetry is collected, Secure Cloud Analytics creates a model—a sort of simulation—of every active entity on the network or in the monitored public cloud. This use of modelling helps you rapidly identify early-stage and hidden indicators of compromise. There are no signature lists to update or software agents to deploy.adhering to your internal policy.

Each model consists of five key dimensions of entity behaviour:

- **Forecast:** Predicts entity behaviour based on past activities and assesses the observed behaviour against these predictions.
- **Group:** Assesses entities for consistency in behaviour by comparing them to similar entities.
- **Role:** Determines the role of an entity based on its behaviour, then detects activities inconsistent with that role.
- **Rule:** Detects when an entity violates organisational policies, including protocol and port use, device and resource profile characteristics, and block listed communications.
- **Consistency:** Recognises when a device has critically deviated from its past behaviour in data transmission and access characteristics.

Entity modelling allows the solution to detect a variety of behaviours associated with potential threats. For example, Secure Cloud Analytics auto-classifies a public cloud resource. This resource's behaviour will be compared to the behaviour of similar entities over time. These communication patterns build a baseline for 'normal' behaviour. Suppose there is traffic that deviates from this baseline. In that case, users can receive custom alerts via email, other Cisco apps and even remediate the threat through the Cisco SecureX platform or other third-party solutions. Secure Cloud Analytics can identify roles for all major public cloud providers. It will detect any new behaviour in near-real-time and generate an alert with details of the suspicious traffic.

DNS abuse, geographically unusual remote access, persistent remote-control connections, and potential database exfiltration are examples of Secure Cloud Analytics alerts. In addition, network reports for the top IPs, most used ports, active subnets with traffic statistics, and more are available.

## About Forfusion

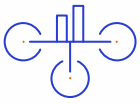
Forfusion specialises in supporting and delivering Cisco solutions into mid-market and enterprise. As an Advanced Security Architecture Specialized Partner we can help you manage your cloud threat protection and response posture with Secure Cloud Analytics.

We consistently deliver robust, dependable solutions into extremely secure and challenging environments, we can be relied on to innovate, and de-risk significant business investments for our clients. Challengers and problem-solvers, we uncover our customers' requirements and work with them in a long-term partnership.

Our straight-talking nature and painstaking attention to detail ensure that we deliver expert services without compromise. And because we are committed to conducting business with strong moral principles, our clients can count on us to do what is right for them every step of the way.

Empowering companies to mitigate risk, and plan for the future through innovation and adoption, as well as optimising business performance through digital transformation.

**Our Advanced Specializations are:**



Advanced Enterprise Networks Architecture

Advanced Collaboration Architecture

Advanced Security Architecture.

**Our engineering and support teams hold between them the following Cisco certifications:**

61x CCNA

7 x CCNP

4 x CCIE

forfusion

Discover how Cisco Secure Cloud Analytics can benefit your organisation.

Sign up for free trial →

Free on-demand webinar →

Transforming business, together.

**forfusion.com**