CISCO
SECURE

Cisco Secure Cloud Analytics and Catalyst 9000 Direct-to-Cloud Solution

Protecting your organization from attacks is a difficult job that is even harder to do when you lack visibility into your network. How can you effectively discover threats in your network if you don't know where they are or what they're doing? As a result, visibility is an important first step to detecting and responding to threats that might be lurking within your network at any point in time.

Getting this visibility isn't easy either because the modern network is hybrid, spanning the enterprise, branch, campus, data center, remote offices and into the cloud. Obtaining deep knowledge of your traffic by deploying a sensor or probe at each location isn't always possible. This lack of visibility is often a barrier to shining a light on what threats are lurking within.

Benefits

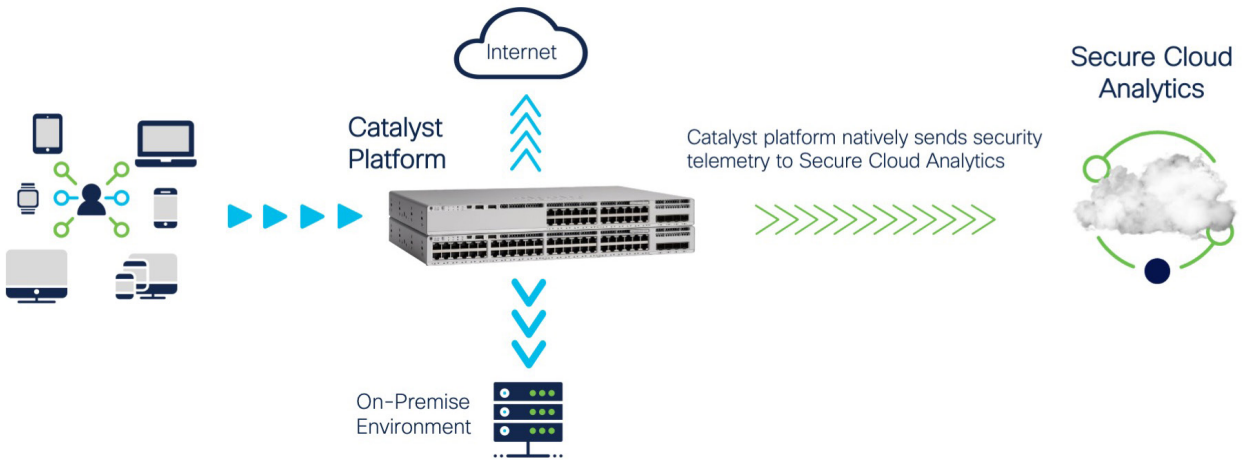
- Gain comprehensive security visibility into your distributed network
- Rapidly detect advanced threats, indicators of compromise, and anomalies
- Automate response with extended threat detection and response
- Simplify networking and security with no additional hardware or sensors
- Achieve quick time to value with an easy, lightweight solution

Networking and security made simple

As the recognized leader in networking and the world's largest cybersecurity vendor, we offer a simple solution that provides comprehensive visibility into threats across your network through integration between Cisco® Secure Cloud Analytics (formerly Stealthwatch Cloud) and products in the Catalyst 9000 family. This integration supports Catalyst family products such as the Catalyst 9200 and 9300 Series Switches and the Catalyst 9800 Series Wireless Controllers.

Our solution allows you to easily send telemetry from branches and your access layer using native IOS XE functionality built into the Catalyst platform to your Secure Cloud Analytics portal. Secure Cloud Analytics then collects and analyzes this data to detect malicious threats or anomalous behavior in your network. All of this is done without deploying any additional hardware or sensors into your environment.

Integration between Cisco Secure Cloud Analytics the Catalyst 9000 family



Easy direct-to-cloud integration

Secure Cloud Analytics is a software-as-a-service (SaaS) solution delivered from the cloud. It is a lightweight solution that is easy to try, simple to configure, and easy to manage. Thus, customers have reported quick time to value, with deployments up and running under 30 minutes.

We know that adding hardware or sensors into your environment to collect and transmit security analytics can be painful and time-consuming. As a result, we've designed this integration to be as simple to deploy as possible via a direct-to-cloud solution. Sending branch, access, and wireless telemetry from your Catalyst platform to Secure Cloud Analytics doesn't require any additional hardware, sensors, or complex deployments. It is a native function of IOS XE, which means it is simple to set up and is just waiting to be turned on.

Once turned on, you will get comprehensive visibility into your branch or access traffic that is streamed to you Secure Cloud Analytics portal. The Catalyst direct-to-cloud solution allows you to easily obtain visibility into your hybrid network, which includes your on-premises environment and public cloud resources. This enables Secure Cloud Analytics to detect and respond to threats, anomalies, and other suspicious behavior seen in your network.

The Secure Cloud Analytics integration works with Catalyst 9200 Series Switches, Catalyst 9300 Series Switches, and Catalyst 9800 Series Wireless Controllers starting with IOS XE 17.5.1. Since this integration is built into the Catalyst platform, you only need a Secure Cloud Analytics subscription and IOS XE version 17.5.1 on your Catalyst devices to benefit from the solution.

Explore security outcomes with Secure Cloud Analytics and SecureX

Learn more about how SecureX automates response with our security outcome videos, which give you an overview of different use cases for the Secure Cloud Analytics integration with SecureX.

Next steps

Try Secure Cloud Analytics today with a free 60-day trial.

Contact your local Cisco account representative.

Unified threat detection across the hybrid network

Secure Cloud Analytics protects your network by giving you visibility, detecting threats, and responding to attacks across your complete hybrid environment. This includes on-premises infrastructure and public cloud environments such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

It consumes telemetry from all of these different sources and then models devices and entities on the network to establish a baseline of normal behavior. Secure Cloud Analytics then watches your network for any changes in behavior and alerts you in case of malicious activity, signs of compromise, or potential anomalies.

This behavioral modeling is enhanced by machine learning that turns large amounts of security telemetry into high-fidelity threat alerts, which allows your security team to focus on investigating the most critical threats to your organization. In addition, Secure Cloud Analytics is powered by Cisco Talos®, the largest nongovernmental threat intelligence team in the world, which offers supervised detections and immediate alerts based on global threat intelligence.

You can also confidently move into automated response and remediation through Cisco SecureX™ integration built into Secure Cloud Analytics, which provides extended threat detection and response (XDR) capabilities. SecureX unifies visibility from multiple security products in a single, centralized console, simplifies threat response by providing additional context on security incidents and integrated controls, and enables automated response with prebuilt and custom workflows.

Learn more: cisco.com/go/secure-cloud-analytics