forfusion

cisco Partner
Advanced Security Architecture Specialized

White Paper

Cisco Secure Cloud Analytics at a glance

Secure Workplace

Key challenges your business faces as it grows in the cloud

The transition to the cloud is complicated. In their quest to remain agile, businesses have flocked to the public cloud, a place where they can migrate workloads into managed, serverless and containerised environments that offer faster and more flexible deployments, higher efficiency and more scalable ways to grow their operations.

According to the Cisco Annual Internet Report, Cloud data centers will process nearly 95% of workloads in 2021. And while your organisation and cloud footprint continue to grow, so do your compliance concerns and your attack surface. 94% of cybersecurity professionals report that they are at least moderately concerned about public cloud security[1].

> 68% of organisations believe that misconfiguration of their cloud platforms is the biggest threat facing their cloud environments[1]

As their cloud footprint expands, businesses are increasingly more worried about ensuring compliance and the risk of threats, which is why maintaining proper cloud security posture is critical. Over the past 5 years, some big-name companies have fallen victim to attacks that stem from improper cloud management and resource configuration. With sensitive workloads and data up in the cloud, it is critical that you have the proper tools in place to monitor and protect this information.

It doesn't help that most IT tasks are divided into various functions. Your SecOps organisation is responsible for threat hunting and monitoring the network for attacks and malicious behavior, while your DevOps team is responsible for rapidly building and deploying applications in the cloud. These groups are separately trying to tackle a wide variety of challenges in the public cloud, and often don't work together as closely as they should. As organisations mature, they often pursue a strategy that enables close collaborations between SecOps and DevOps teams.

Monitor and protect your public cloud resources

With Cisco Secure Cloud Analytics, security teams can confidently monitor and protect their cloud workloads and perform quick security posture assessments of their cloud environments using a cloud-native, API driven solution that works the way a DevOps team would expect. With just one intuitive solution, both SecOps and DevOps can share information on cloud workloads and resolve compliance or configuration issues before an attack takes place.

Benefits:

- Rapidly detect advanced threats that may be taking advantage of misconfigured assets in the cloud
- Strengthen and maintain your cloud security posture through live event viewing
- Gain comprehensive visibility of activity occurring within your cloud resources
- Enable quick corrective action on security policies and configurations through seamless communication across your SecOps and DevOps teams

1. 2020 Cloud Security Report, Cybersecurity Insiders.

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:

Encourage better collaboration between SecOps and DevOps

Secure Cloud Analytics enables simple collaboration between the two groups who are most involved with cloud posture management, SecOps and DevOps. The SecOps team is responsible for monitoring the network for alerts and identifying holes, addressing alarms and responding to threats found within their cloud environments, while the DevOps team is responsible for actually configuring these environments and maintaining a solid structure and build in the cloud.

Secure Cloud Analytics brings synergy to these groups through automated detections and the ability to drill down into past events with a variety of filters that make it easy for SecOps to identify gaps in their cloud configurations. It also offers numerous integrations through webhooks and third party platforms as well as other Cisco technologies that allow SecOps to easily communicate its findings to the DevOps organisation. DevOps is responsible for remediating cloud infrastructure issues to ensure that all resources are configured properly and securely. The wide variety of auto- remediation options, webhooks and other integrations help customers keep these teams up-to-date on all cloud security posture concerns.

Maintain compliance to meet industry standards, internal rules and more

Secure Cloud Analytics now offers an event viewer to monitor cloud security posture. It allows the user to investigate accounts and individual resources for compliance with industry best practices and custom policies. Users can also pivot into query mode to perform more in-depth searches. Many organisations have numerous accounts and cloud service providers, which often makes visibility and consistency difficult, but with this view, SecOps gains instant access into all cloud accounts and can query by specific resource, rule and more over custom timeframes to hone in on misconfigurations or other compliance issues.

Seamlessly monitor and protect all your public cloud resources

Secure Cloud Analytics goes far beyond basic configuration and compliance rules, with automated high-fidelity alerts that identify malicious activity and behavioral anomalies which may be indicative of threats. It uses a process called dynamic entity modeling, which can determine the role of an entity based on its behavior and then alert on activity that deviates from the behavioral norm.

There's a saying that goes, "You can't secure what you can't see" visibility is critical. Secure Cloud Analytics is agentless and supports multi-cloud environments with the ability to monitor major cloud platforms like Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform. It automatically places all of your EC2 instances, AWS load balancers, S3 buckets, NAT Gateways (GCP) and more into roles and will use cloud-native telemetry like Virtual Private Cloud (VPC) and Network security group (NSG) flow logs to detect potentially malicious or harmful activity.

The new alerts tab provides mapping to the MITRE ATT&CK framework which adds additional context to each alert. This has information on the type of threat, what methods attackers may be using and what the best course of action to remediate should be. There are also detections that are unique to the behavior of cloud usage such as Geographically Unusual API Usage and AWS Lambda Invocation Spike, that are built specifically to alert on malicious activity in the cloud.

With the built-in Cisco SecureX platform, users can easily pivot into other applications like Umbrella and Talos to investigate further or block out threats for good.

About Forfusion

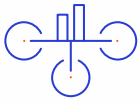
Forfusion specialises in supporting and delivering Cisco solutions into mid-market and enterprise. As an Advanced Security Architecture Specialized Partner we can help you manage your cloud threat protection and response posture with Secure Cloud Analytics.

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 →

Transforming business, together.

forfusion.com