Cloud-native Security for Microsoft Azure

There are numerous benefits to adopting cloud infrastructure. It helps improve your business agility, time to market, and availability, all while reducing costs. Cisco Secure Cloud Analytics helps organizations preserve these benefits while providing behavioral security analytics, comprehensive visibility, and effective threat detection.

Cisco Secure Cloud Analytics (formerly Stealthwatch Cloud) can be deployed in Microsoft Azure environments in as little as 10 minutes without the need for agents. It works by consuming Azure Network Security Group (NSG) flow logs[1], which provides information on north-south and east-west traffic within an Azure virtual network.

[1] Secure Cloud Analytics relies on NSG Flow Logs version 2, which will initially be available in the Azure West Central US region. Support will be rolled out across all Azure regions globally by early 2019.

Cisco Secure Cloud Analytics for Microsoft Azure provides:

- Comprehensive and agentless visibility
- Effective threat detection
- Low-noise, high-fidelity alerts
- Compliance verification
- Easy-to-deploy and easy to-manage security

Flow log pricing model

Cisco Secure Cloud Analytics has a simple and intuitive pricing model based on usage. It is priced based on the amount of flow log information that you send to us. In addition—and to your benefit—Cisco Secure Cloud Analytics optimizes the flow log data to reduce your costs. This usage- based metric is called “Effective Mega Flows.”

For a better idea of what your costs could be, please sign up for a 60-day trial of entity modeling. This no-obligation trial is completely free and helps you see your exact costs based on actual VPC data usage.

High-fidelity threat detection with Azure NSG flow logs

Alert fatigue is a major security challenge. According to the Cisco 2018 Annual Cybersecurity Report, only 56 percent of security alerts are investigated, and of those, only 34 percent are legitimate alerts. Cisco Secure Cloud Analytics was built with a laser-focus on creating a low-noise, high-value security solution. Ninety-four percent of Cisco Secure Cloud Analytics alerts are rated “helpful” by customers. We accomplish this through a combination of good data and behavioral security analytics.

For Microsoft Azure environments, Cisco Secure Cloud Analytics’s primary data input is NSG flow logs. NSG flow logs is a form of traffic metadata, similar to NetFlow in on-premises networks. Whenever a communication happens within an Azure virtual network, or between an internal and external host, NSG flow logs record basic information.

NSG flow logs record:

Source and destination IP addresses

Source and destination port

Protocol

Time

Cisco Secure Cloud Analytics analyzes NSG flow logs using entity modeling to identify suspicious and malicious activity.

For every active entity on the network, Cisco Secure Cloud Analytics builds a behavioral model – a simulation of sorts – to understand what the entity's role is, how it normally behaves, and what resources it normally communicates with. Then it uses this model to identify changes in behavior consistent with misuse, malware, compromise, or other threats.

For instance, if an Azure resource normally only communicates with internal hosts, but suddenly it begins sending large amounts of data to an unknown external server, it could be a sign of data exfiltration. Cisco Secure Cloud Analytics would detect this behavior in real-time and alert your security team.

Try today!

Interested in Cisco Secure Cloud Analytics?
You can try it today with our no-risk, 60-day free trial.
To sign up, click here.