Cisco Stealthwatch Cloud

Secure your private network, public cloud, and hybrid environment

Only 56 percent of security alerts are investigated, and more than half of those are not remediated, according to the Cisco 2017 Annual Cybersecurity Report. Responding to these alerts is an overwhelming job, and most organizations do not have the security staff to keep up. Companies of all sizes face the challenge of securing their public cloud environments as well as their on-premises infrastructure.

Adding effective security measures for public cloud 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 infrastructure. A public cloud offers fewer network monitoring capabilities even as it undergoes a very high change rate in assets. To provide effective security while reducing the number of false positives, a new approach is necessary.

Imagine that 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® Stealthwatch Cloud provides the actionable security intelligence and visibility necessary to identify these kinds of malicious activities in real time. You can quickly respond before a security incident becomes a devastating breach.

With Stealthwatch Cloud, you can detect external and internal threats across your environment, from the private network to the branch office to the public cloud. Stealthwatch Cloud is a Software-as-a-Service (SaaS) solution delivered from the cloud. It is easy to try, easy to buy, and simple to operate and maintain. When data is received, it requires very little additional configuration or device classification. All the analysis is automated.

Benefits

- **Gain actionable intelligence** through visibility of your environment, from the private network to the public cloud
- **Rapidly detect** advanced threats and indicators of compromise
- **Grow your security with your business** while lowering operational overhead
- **Greatly reduce false positives** with higher-fidelity alerts supported by underlying observations
- **Attain a stronger security posture** across the enterprise, including the public cloud

“We were looking for a better way to monitor our network security. This service gives us much better visibility into all of the devices in our VPC and their network activity. If one ever behaves in a suspicious or abnormal fashion, we can take fast action to resolve possible issues.”

– Taylor Higley, Director,
American Federation of Government Employees

Secure your environment with entity modeling

Threats are constantly evolving. To detect tomorrow’s attacks, you need security that keeps ahead of them. Stealthwatch Cloud 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. Stealthwatch Cloud detects this behavior in real time and alerts you to it.

Using dynamic learning, Stealthwatch Cloud creates a model—a kind of simulation—for each device and network entity. This model is able to:

- 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

With these capabilities, Stealthwatch Cloud allows your staff to spend more time remediating issues instead of wasting time manually analyzing log data to determine their cause.

Detect threats in your public cloud

As organizations 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. Stealthwatch Cloud’s 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. Stealthwatch Cloud can be deployed in these environments in a matter of minutes with no disruption to service availability.

Stealthwatch Cloud uses this data to model the behavior of each cloud resource, a method called entity modeling. It is then able to detect sudden changes in behavior, malicious activity, and signs of compromise.

Protect your environment today

Try Stealthwatch Cloud today with a free no-risk trial. To learn more, go to https://www.cisco.com/go/stealthwatch-cloud or contact your local Cisco account representative.

Secure your private network too

Network visibility and threat detection are no longer just for large enterprises. According to a survey conducted by Ponemon Institute for businesses with fewer than 1000 employees, 55 percent experienced a cyber attack in the past year, and almost one-third couldn't determine the root cause of a breach. Stealthwatch Cloud's Private Network Monitoring can deliver the visibility necessary to detect threats on the network in real time, without the need for expensive equipment, IT resources, or extensive security staff time.

Stealthwatch Cloud receives a wide variety of network telemetry and logs. It uses entity modeling to determine each network entity's role and what the entity's normal behavior is. If an entity exhibits new, abnormal behavior or signs of malicious activity, an alert is generated, so security professionals can quickly investigate and respond.

C45-739611-00 09/17