Monitor and Protect Google Cloud Platform Environments Using Native Telemetry

Organizations use the public cloud infrastructure to improve their business agility, responsiveness, and availability while reducing costs. Cisco® Stealthwatch Cloud protects these benefits by providing visibility and effective, low-noise threat detection in your public cloud without inhibiting innovation. In as little as 10 minutes, you can deploy Stealthwatch Cloud and see security value in your Google Cloud Platform (GCP) environments.

Google VPC Flow Logs, which offers detailed flow-level metadata down to an individual virtual interface, is a powerful source of security insight. By itself, VPC Flow Logs provides transparency into all IP flows in a virtual private cloud network. However, VPC Flow Logs is also useful for flow analysis, such as entity modeling provided by Stealthwatch Cloud. By using this data source, Stealthwatch Cloud can easily instrument GCP environments, without customers deploying agents or software sensors, and provide high-fidelity threat detection.

VPC Flow Logs are similar to Cisco IOS NetFlow, but with additional features. VPC Flow Logs can track:

- Internal virtual port channel (VPC) traffic
- Flows between your VPC and on-premises deployments over both VPNs and Google Cloud Interconnects
- Flows between your VPC resources, such as servers and virtual appliances, and any Internet endpoint
- Flows between your VPC resources and any Google services

Flow log pricing model

Stealthwatch Cloud 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—Stealthwatch Cloud 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.

Please register for your free 60-day trial now by visiting http://cisco.com/go/stealthwatch-cloud.

Entity modeling with Google VPC Flow Logs

Stealthwatch Cloud uses entity modeling to help companies gain actionable security insight from flow metadata. Entity modeling uses flow data much in the same way a credit card company uses transaction data. The technology builds a model of normal activity from observed device behavior and uses this model to spot changes in behavior that may be due to misuse, malware, or compromise.

Instead of detecting threats based on signatures, Stealthwatch Cloud detects suspicious and malicious behavior. Ultimately, this allows you to focus your security resources on a very small number of deviations from normal patterns and activities identified by entity modeling. And it is available as a subscription service, so you don't have to worry about capital expenditures and long-term financial commitments.

With Google VPC Flow Logs, gaining the security benefits of Stealthwatch Cloud in GCP environments has never been easier or quicker. Simply subscribe to our service and configure access to your VPC Flow Logs from within the Stealthwatch Cloud customer portal. It's fast and easy. And after that initial setup, entity modeling will help you gain security awareness and stay ahead of potential adversaries.

Consider this example: A customer's Google VPC is usually only accessed remotely from locations within the United States, but a user logs in from Europe. This is highly unusual and could represent a security risk. Stealthwatch Cloud would automatically alert the customer to this activity in near real time, allowing them to assess and respond to the threat before any significant damage is done.

Try today!

To sign up for a free, 60-day trial visit
https://cisco.com/go/stealthwatch-cloud