

AWS VPC Flow Logs

A New Tool for Your Security Arsenal

Amazon Web Services (AWS) Virtual Private Cloud (VPC) Flow Logs containing network flow metadata offer a powerful resource for security. Not only can you log all IP flows in a VPC network with help from flow logs, but you can also use this data to perform various types of flow analysis. That brings security and network processes practiced in AWS environments closer to those practiced for conventional IT. Importantly, as you will see here, flow logs help enable a very specific security technology called entity modeling, which can significantly improve your network security and overall AWS server understanding.

Since its inception, Cisco Secure Cloud Analytics, formerly Cisco Stealthwatch Cloud, has been transforming the way companies get value from flow metadata with our entity modeling solution. 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.

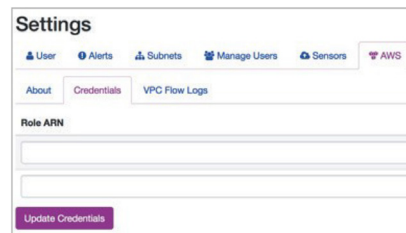


To put it another way, Secure Cloud Analytics helps you stop chasing cybercriminals and their never-ending myriad of exploits, malware, and other threats by trying to keep up with their signatures. Instead, you can focus your security efforts on the very small number of significant and automatically detected deviations from established patterns and activities, as identified by entity modeling. And the best thing about our technology: it's available as a subscription service, so you don't have to worry about capital expenditures and long-term financial commitments.

Entity modeling in AWS VPC environments

Our VPC Flow Log collector now makes it extremely easy to add entity modeling to your AWS VPC environments. Simply subscribe to our service, and configure access to your VPC Flow Logs from within the Secure Cloud Analytics customer portal. It's fast and easy. And after that initial set-up, entity modeling will help you press your advantage over potential adversaries using exact knowledge of your endpoint devices at all times.

Configuring access to your VPC Flow Logs from within the Secure Cloud Analytics customer portal is fast and easy and gives you exact knowledge on your endpoint devices at all times.



Increased visibility leads to improved security

To learn how Secure Cloud Analytics can help you perform entity modeling in AWS VPC environments, please visit <https://www.cisco.com/go/secure-cloud-analytics> today.

Flow log pricing model

We offer a simple and intuitive pricing model based on usage. We charge based on the amount of flow log information that you send to us. In addition—and to your benefit—we use optimization techniques to decrease the flow log data to reduce your costs. We call this usage-based metric “Effective Mega Flows” (EMFs).

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 <https://www.cisco.com/c/en/us/products/security/stealthwatch/stealthwatch-cloud-free-offer.html>.