Secure Network Analytics

(formerly Stealthwatch Enterprise)

Cisco Partner
https://cs.co/1page

Cisco **Secure Network Analytics** collects and analyzes network data to automatically detect threats that manage to infiltrate the perimeter, even if originated from within. Secure Network Analytics can quickly, detect threats such as C&C attacks, ransomware, DDoS attacks, illicit Cryptomining, unknown malware, as well as insider threats.

Benefits:

- **Continuously monitor and detect** advanced threats that have either bypassed existing security controls or originate from within.
- **Focus on incidents, not noise**. Using the power of behavioral modeling, multilayered machine learning, and global threat intelligence, SNA reduces false positives and alarms on critical threats affecting your environment.
- **Respond quickly and effectively** with complete knowledge of threat activity, network audit trails for forensic investigations, and integrations with existing security controls.
- **Scale security with growing business needs** whether adding a new branch or a data center, moving workloads to the cloud, or adding more devices.
- **Ensure compliance** with policy violation alarms that can be tuned to the business logic.
- **Know every host**. See every conversation. Understand what is normal. Be alerted to change. Respond to threats quickly.
- **Respond quickly and effectively** with knowledge of threat activity, network audit trails for forensic investigations, and integrations with existing controls.
- **Leverage existing investments** into the IT infrastructure and use the rich network telemetry for better security.

Use Cases:

Visibility Everywhere: Analyze enterprise telemetry from any source, provide end to end visibility across extended network, cloud or with remote workers.

Unique Threat Detection: Combination of multi-layer machine learning and behavioral modeling provides ability to detect inside and outside threats.

Encrypted Traffic Analytics (ETA): Analyze encrypted traffic to detect malware and ensure policy compliance without decryption.

Smart Segmentation: Use logical functional business groups that, monitor the effectiveness of segmentation policies through contextual alarms.

Flexible deployment options for visibility everywhere:

Secure Network Analytics | Secure Network Analytics SaaS

Discovery Questions:

- Do you know what applications are used in the enterprise?
- Do you understand who/what is communicating with applications/data?
- Is communication with your current workload secure and trusted?
- Do you know what devices are active on your network?
- Can you detect activity such as unusual remote access or abnormal data transfers?
- Are you able to monitor lateral movement behind the network perimeter?
- Can you detect insider or targeted attacks that avoid signature-based detection?

Solution Components:

Manager [1] – The Management Console collects and analyzes network data to deliver comprehensive visibility for even the largest and most dynamic networks.

Flow Collector [1] - Leverage telemetry such as NetFlow, IPFIX, and other types of flow data from routers, switches, firewalls, endpoints, and other network devices.

Flow Rate License [1] - Required to collect, manage, and analyze flow telemetry aggregated at the Secure Network Analytics Manager.

Flow Sensor [2] - Produces telemetry of switching and routing infrastructure that can't generate NetFlow to identify applications and protocols on the network.

Endpoint License [2] - Allows you to conduct in-depth, context-rich investigations into endpoints that exhibit suspicious behavior.

Threat feed [2] - A global threat intelligence feed powered by Cisco Talos to provide an additional layer of protection against botnets and other sophisticated attacks.

UDP Director [2] - Central collector for flow data generated by flow-enabled devices.

Encrypted Traffic Analytics [2] - Analyze encrypted traffic data elements in enhanced NetFlow by applying machine learning and statistical modeling.

Telemetry Broker [3] - Provide increased visibility to hybrid cloud environments in on prem tools through AWS VPC Flow Log translation to IPFIX.

[1] Required | [2] Optional | [3] Optional or Stand Alone

Resources:

SalesResources | Ordering Guide | At-a-Glance | Data Sheets | Data Store Design Guide | Secure Analytics Training Center | Case Studies | YouTube Channel | Public page

Example SKU: ***ST-SEC-BUN***