Secure Analytics: Key Features and Functionalities

Cisco Secure Analytics collects and analyzes telemetry from all parts of the enterprise network to provide visibility, advanced threat detection, and network compliance. With this continuous monitoring, you are able to quickly respond to any threat that has managed to infiltrate the organization or might have originated within. Secure Analytics offers two deployment models: Secure Network Analytics is deployed on-premises with hardware appliances or virtual machines, whereas Secure Cloud Analytics is delivered as a SaaS solution.

Secure Analytics product suite

Secure Network Analytics
(Stealthwatch Enterprise)

Enterprise network monitoring

On-premises data storage, granular tuning, SecOps and NetOps use cases, air-gapped networks

Hardware or virtual appliance

Priced by FPS (flows per second)

Secure Cloud Analytics
(Stealthwatch Cloud)

Public cloud monitoring	Private network monitoring
Suitable for all organizations using public cloud infrastructure like AWS, Azure, GCP and serverless environments	Simple deployment, automated tuning, SecOps and light NetOps use cases
SaaS based	SaaS based network monitoring (including Meraki, container)
Usage-based pricing determined by volume of log data	Endpoint-based pricing

Secure Network Analytics and Secure Cloud Analytics Use Cases

The below table lists the use cases and functionalities that are available for both Secure Analytics' on-premises and SaaS offerings, with each category further broken out based on currently available features versus ones that are either in development or on the roadmap.

Use case/Functionality	Secure Network Analytics		Secure Cloud Analytics	
	Available today	Roadmap	Available today	Roadmap
Public cloud monitoring		✓	✓	
On-prem network monitoring	✓		✓	
Dynamic entity modeling	✓[1]	✓*	✓	
Host/Entity Groups	✓		✓	✓*
Threat detections	✓		✓	
Policy violations	✓		✓	✓*
Custom Security Events	✓		✓[2]	✓*
ISE user and device attribution	✓		✓[3]	✓*
ISE Remediation/Mitigation	✓			✓
ISE Network Segmentation	✓			✓
Extendable hot storage	✓		✓	
Extendable long-term cold storage		✓		✓
Response Management – Emails Syslog, APIs	✓		✓	
Cisco Threat Response	✓		✓	✓*
SecureX	✓		✓	
Alarm/Alert Customization	✓		✓[2]	✓*
NetOps Monitoring	✓		✓[2]	✓
Forensics	✓		✓	
Threat Intelligence	✓		✓	
Encrypted Traffic Analytics: Malware Detection	✓		✓	
Encrypted Traffic Analytics: Cryptographic Audit	✓		✓	
NAT/Load Balancer/Proxy support	✓			✓
Endpoint telemetry and alerting	✓			✓
Firewall log storage and alerting	✓	✓*	✓	

✓ [1] Based on IP only
[2] Limited
[3] User only

✓ * In current development

2111126 05/20 C1462798-0921