cisco SECURE

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)		Secure Cloud Analytics (Stealthwatch Cloud)	
Enterprise network monitoring	Public cloud monitoring	Private network monitoring	
On-premises data storage, granular tuning, SecOps and NetOps use cases, air-gapped networks	Suitable for all organizations using public cloud infra- structure like AWS, Azure, GCP and serverless environments	Simple deployment, automated tuning, SecOps and light NetOps use cases	
Hardware or virtual appliance	SaaS based	SaaS based network monitoring (including Meraki, container)	
Priced by FPS (flows per second)	Usage-based pricing deter- mined by volume of log data	Endpoint-based pricing	

cisco SECURE

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		 Image: A second s	✓	
On-prem network monitoring	 Image: A second s		 Image: A second s	
Dynamic entity modeling	🗸 1	✓*	 Image: A set of the set of the	
Host/Entity Groups	✓		✓	✓*
Threat detections	 Image: A set of the set of the		 Image: A set of the set of the	
Policy violations	✓		✓	✓*
Custom Security Events	 Image: A second s		✓ ²	*
ISE user and device attribution	✓		3	✓*
ISE Remediation/Mitigation	 Image: A set of the set of the			 Image: A second s
ISE Network Segmentation	 Image: A second s			 Image: A second s
Extendable hot storage	 Image: A set of the set of the		 Image: A second s	
Extendable long-term cold storage		 Image: A second s		 Image: A second s
Response Management - Emails Syslog, APIs	 Image: A second s		 Image: A second s	
Cisco Threat Response	 Image: A set of the set of the		 Image: A second s	*
SecureX	 Image: A second s		 Image: A second s	
Alarm/Alert Customization	 Image: A second s		✓ ²	*
NetOps Monitoring	 Image: A second s		✓ ²	 Image: A second s
Forensics	 Image: A second s		 Image: A second s	
Threat Intelligence	 Image: A second s		 Image: A second s	
Encrypted Traffic Analytics: Malware Detection	 Image: A second s		 Image: A second s	
Encrypted Traffic Analytics: Cryptographic Audit	 Image: A second s		 Image: A second s	
NAT/Load Balancer/Proxy support	 Image: A second s			 Image: A second s
Endpoint telemetry and alerting	 Image: A second s			 V
Firewall log storage and alerting	 V 	✓*		

² Limited ³ User only

Connection[®] we solve IT[®]

Contact an Account Manager for more information. 1.800.800.0014 ■ www.connection.com/Cisco

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R) 2111126 05/20 CI462798-0921