Cisco Secure Network Analytics (formerly Stealthwatch)

January 2024

Contents

Cisco Secure Network Analytics

This document describes the information for Cisco Secure Network Analytics (formerly Stealthwatch Enterprise). The Cisco Secure Cloud Analytics (formerly Stealthwatch Cloud) datasheet can be reviewed here.

For more detailed information, go to https://cs.co/sna.

Solution overview

Cisco Secure Network Analytics provides enterprise-wide network visibility to detect and respond to threats in real- time. The solution continuously analyzes network activities to create a baseline of normal network behavior. It then uses this baseline, along with non-signature-based advanced analytics that include behavioral modeling and machine learning algorithms, as well as global threat intelligence to identify anomalies and detect and respond to threats in real- time. Secure Network Analytics can quickly and with high confidence detect threats such as Command-and-Control (C&C) attacks, ransomware, Distributed-Denial-of-Service (DDoS) attacks, illicit cryptomining, unknown malware, and insider threats. With an agentless solution, you get comprehensive threat monitoring across the entire network traffic, even if it's encrypted.

Organizations have already invested a lot into their IT infrastructure and security. Yet, threats continue to find ways to get through. Moreover, it often takes months or even years to detect breaches. This lack of visibility is a function of continuously growing network complexity and constantly evolving threats. Security teams with limited resources and disjointed tools can only do so much. Practically all organizations have security solutions, such as firewalls, but how do they know whether these tools are working, managed, and configured correctly? How do they know that these tools are doing the job that they need them to do?

We decided to turn the problem on its head—why not enlist your existing investment, the network, to secure your organization? The network telemetry is a rich data source that can provide valuable insights about who is connecting to the organization and what they are up to. Everything touches the network, so this visibility extends from the HQ to the branch, data center, roaming users, smart devices extending to private and public clouds. Analyzing this data can help detect threats that may have found a way to bypass your existing controls before they are able to have a major impact.

The solution is Secure Network Analytics, which enlists the network to provide end-to-end visibility of traffic, on- premises as well as in private and public clouds. This visibility includes knowing every host and seeing who is accessing which information at any given point. From there, it's important to understand what is normal behavior for a particular user or "host" and establish a baseline from which you can be alerted to any change in the user's behavior the instant it happens.

Secure Network Analytics offers two different deployment models — on-premises as a hardware appliance or as a virtual machine. Secure Cloud Analytics (formerly Stealthwatch Cloud) is the Software-as-a-Service (SaaS) version of Secure Network Analytics. In addition to monitoring the private network, Secure Cloud Analytics can also be deployed to detect threats and configuration issues in the public cloud.

Primary use cases

Real-time threat detection

Simply put, by providing the most comprehensive and context-rich network visibility, paired with time-tested and industry-leading security analytics, Secure Network Analytics delivers the broadest and most high-fidelity behavioral- based threat detection capabilities to dramatically improve:

- Unknown threat detection: Identify suspicious behavioral-based network activity that traditional signature- based tools miss, such as communications and malicious domains.
- Insider threat detection: Get alarmed on data hoarding, data exfiltration, and suspicious lateral movements.
- Encrypted malware detection: Leverage multilayered machine learning and extend visibility into encrypted web traffic without decryption.
- Policy violations: Ensure that security and compliance policies set in other tools are enforced.
- Incident response and forensics: Respond quickly and effectively with complete knowledge of threat activity, network audit trails for forensics, and integrations with SecureX and other Cisco Secure solutions.

Remote worker monitoring

Secure Network Analytics has made endpoint record telemetry data from the AnyConnect Network Visibility Module (NVM) a primary telemetry source. This enables users to capture a wide range of additional granular, endpoint-specific user and device context to effectively provide organizations with complete and continuous visibility into mobile remote worker endpoint activity, regardless of whether a user is using a single VPN session to work, optimizing their remote work experience using split tunneling or if they are disconnected from VPN entirely. This bolsters organizations' security postures through visibility into activities that they were previously blind to, such as employees running older operating system versions with vulnerabilities that need patching, employees engaged in data hoarding or data exfiltration, and more.

Group-based policy reporting

Users can leverage Cisco Secure Network Analytics' integration with Cisco Identity Services Engine to accelerate their group-based policy adoption efforts by generating group-based policy reports that provide new ways to visualize group communications. Group-based policy reports enable users to effortlessly visualize, analyze, and drill down into any inter-group communication, validate the efficacy of policies, adopt the right policies based on their environment's needs, and streamline their policy violation investigations via insights into relevant flows and associated IPs. To learn more, reference the At-a-Glance.

Encrypted traffic analytics

The rapid rise in encrypted traffic is changing the threat landscape. While encryption is excellent for data privacy and security, it has also become an opportunity for cybercriminals to conceal malware and evade detection. Today, roughly 95% of all web traffic is encrypted, and over 70% of attacks are expected to use encryption. Traditional threat inspection with bulk decryption, analysis, and re-encryption is not always practical or feasible for performance and resource reasons. Also, it compromises privacy and data integrity. With its expertise in the network infrastructure market, Cisco has introduced a revolutionary technology to analyze encrypted traffic without any decryption. This allows organizations to 1) detect threats in encrypted traffic and 2) ensure cryptographic compliance. To learn more, go to https://www.cisco.com/go/eta.

Key benefits

- **No more blind spots:** Secure Network Analytics is the only security analytics solution that can provide comprehensive visibility across the private network and into the public cloud without deploying sensors everywhere. It is also the first solution to detect malware in encrypted traffic without any decryption.
- **Focus on incidents, not noise:** By using the power of behavioral modeling, multilayered machine learning, and global threat intelligence, Secure Network Analytics significantly reduces false positives and alarms on critical threats affecting your environment.
- **Catch them in the act:** Secure Network Analytics constantly monitors the network to detect advanced threats in real-time. Stealthy attacks are commonly preceded by activities such as port scanning, constant pinging, and reconnaissance tactics. The solution recognizes these early warning signs and alarms on them to stop attackers early on. Once threats are identified, users can also conduct forensic investigations to pinpoint their source and determine where else it may have propagated.
- **Make the most of your investment:** With an agentless solution, you are using the rich telemetry generated by your existing network infrastructure to improve your security posture.
- **Scale security with business growth:** Now there's no need to compromise on security as the business needs to change. Whether you are adding a new branch or a data center, moving workloads to the cloud, or simply adding more devices, any Secure Network Analytics deployment can easily provide coverage by scaling to the needs of your network. It can be deployed on-premises or in the cloud, can be consumed as a SaaS-based or license-based solution, and provides automatic role classification capabilities to automatically classify new devices as they are added to the network.
- **Integrate your security ecosystem with SecureX:** The solution comes with the SecureX platform built-in to offer extended threat investigation and response capabilities. Secure Network Analytics integrates with SecureX to unify visibility, simplify threat response and enable automation across every threat vector and access point.

Solution components

At the core of Secure Network Analytics are the required components: the Manager, Flow Collector, and Flow Rate License. In addition, we offer optional components like the Flow Sensor, the Cisco Telemetry Broker and the Data Store, which are also available to provide a flexible and robust architecture.

Required components of the system

Manager

The Secure Network Analytics Manager aggregates, organizes, and presents analyses from up to 25 Flow Collectors, Cisco Secure Network Access (formerly Cisco Identity Services Engine), and other sources. It uses graphical representations of network traffic, identity information, customized summary reports, and integrated security and network intelligence for comprehensive analysis.

The capacity of the manager determines the volume of telemetry data that can be analyzed and presented, as well as the number of Flow Collectors that are deployed. The manager is available as a hardware appliance or a virtual machine. Table 1 lists the benefits of the manager.

Table 1. Major benefits of the Manager

Benefit	Description
Real-time, up-to-the- minute data	Delivers data flow for monitoring traffic across hundreds of network segments simultaneously so that you can spot suspicious network behavior. This capability is especially valuable at the enterprise level.
Capability to detect and prioritize security threats	Rapidly detects and prioritizes security threats, pinpoints network misuse and suboptimal performance, and manages event response across the enterprise, all from a single control center.
Management of appliances	Configures, coordinates, and manages Cisco Network Analytics appliances, including the Flow Collector, Flow Sensor, and UDP Director.
Use of multiple types of flow data	Consumes multiple types of flow data, including NetFlow, IPFIX, and sFlow. The result: cost-effective, behavior-based network protection.
Scalability	Supports even the largest of network demands. Performs well in extremely high-speed environments and can protect every part of the network that is IP reachable, regardless of size.
Audit trails for network transactions	Provides a complete audit trail of all network transactions for more effective forensic investigations.
Real-time, customizable relational flow maps	Provides graphical views of the current state of the organization's traffic. Administrators can easily construct maps of their network based on any criteria, such as location, function, or virtual environment. By creating a connection between two groups of hosts, operators can quickly analyze the traffic traveling between them. Then, simply by selecting a data point in question, they can gain even deeper insight into what is happening at any point in time.
Flexible delivery options	You can order the Physical Appliance, a scalable device suitable for any size organization. Or you can order the Virtual Edition, designed to perform the same functions as the appliance edition, but in a VMware or KVM Hypervisor environment.

Manager specifications

- Secure Network Analytics Manager 2210 — Part number: ST-SMC2210-K9
- Secure Network Analytics Manager 2300 — Part number: ST-SMC2300-K9
- Secure Network Analytics Manager Virtual Edition — Part number: L-ST-SMC-VE-K9

Flow Collector

The Flow Collector collects and stores enterprise telemetry types such as NetFlow, IPFIX (Internet Protocol Flow Information Export), NVM, and SYSLOG from existing infrastructure such as routers, switches, firewalls, endpoints, and other network infrastructure devices. The Flow Collector can also collect telemetry from proxy data sources, which can be analyzed by the cloud-based machine learning engine (global threat alerts).

The telemetry data is analyzed to provide a complete picture of network activity. Months or even years of data can be stored, creating an audit trail that can be used to improve forensic investigations and compliance initiatives. The volume of telemetry that can be collected from the network is determined by the total combined capacity of the deployed Flow Collectors. Multiple Flow Collectors can be installed. Flow Collectors are available as hardware appliances or as virtual machines. Table 2 outlines Flow Collector's benefits.

Table 2. Major benefits of the Flow Collector

Benefit	Description
Threat detection	Ingests proxy records and associates them with flow records to deliver the user application and URL information for each flow to increase contextual awareness. This process enhances your organization's ability to pinpoint threats and shortens your Mean Time to Know (MTTK).
Flow traffic monitoring	Monitors flow traffic across hundreds of network segments simultaneously so that you can spot suspicious network behavior. This capability is especially valuable at the enterprise level.
Extended data retention	Allows organizations and agencies to retain large amounts of data for long periods.
Scalability	Performs well in extremely high-speed environments and can protect every part of the network that is IP reachable, regardless of size.
Deduplication and stitching	Performs deduplication so that any flows that might have traversed more than one router are counted only once. It then stitches the flow information together for complete visibility of a network transaction.
Choice of delivery methods	You can order the Appliance Edition, a scalable device suitable for any size organization. Or you can order the Virtual Edition, designed to perform the same functions as the appliance edition, but in a VMware or KVM Hypervisor environment. This solution scales dynamically according to the resources allocated to it.

Flow Collector specifications

- Secure Network Analytics Flow Collector 4210 — Part number: ST-FC4210-K9
- Secure Network Analytics Flow Collector 5210 — Part number: ST-FC5210-K9
- Secure Network Analytics Flow Collector 4300 — Part number: ST-FC4300-K9
- Secure Network Analytics Flow Collector Virtual Edition — Part number: L-ST-FC-VE-K9

Data Store

The Data Store provides a solution for environments requiring high data ingest capacity levels or long-term retention times that exceed the capacity of one or more Flow Collectors. The Data Store cluster can be added between the Secure Network Analytics Manager and Flow Collectors. For these larger and more extensive networks, one or more Flow Collectors ingest and de-duplicate flow data, perform analyses, and then send the flow data and its results directly to the Data Store. This flow data is then distributed equally across a Data Store, which is comprised of a minimum of three Data Node appliances. The Data Store facilitates flow data storage and keeps all your network telemetry in one centralized location, as opposed to having it spread across multiple Flow Collectors in a distributed model. This new centralized model offers greater storage capacity, flow rate ingestion, and increased resiliency versus the distributed model.

Table 3. Major benefits of the Data Store

Benefit	Description
Increases data ingest capacity	Data Stores can be combined to create a single cluster of data nodes capable of monitoring over 3 million Flows Per Second (FPS) to aid in relieving ingestion bandwidth challenges for organizations with high flow volumes.
Enterprise-class data resiliency	Telemetry data is stored redundantly across nodes to allow for seamless data availability during single node failures, helping to ensure against the loss of telemetry data. Deployments with two Data Stores or more can support up to 50% of data node loss and continue to operate.* The Data Store also supports redundant interconnection switches to remain fully operational during network upgrades and unplanned outages. *Depending on your hardware configuration and installation.
Significant query and reporting response time improvements	The Data Store provides drastically improved query performance and reporting response times that are at least 10x faster than those offered by other standard deployment models. It can also perform an increased number of concurrent queries, whether through APIs or the Secure Network Analytics Manager web UI. These query improvements stand to deliver substantial operational efficiency gains. Through the ability to run reports and get answers more quickly, the Data Store enables practitioners to pinpoint and respond to threats more quickly to expedite triage, investigation, and remediation workflows.
Storage scalability	The Data Store offers organizations with growing networks enhanced flexibility around data storage scalability through the ability to add additional database clusters.
Long-term data retention	Scalable and long-term telemetry storage capabilities enable long-term flow retention of up to 1 to 2 years' worth of data with no need to add additional Flow Collectors. This aids in satisfying regulatory requirements and reducing costs and complexity associated with purchasing and integrating third-party storage solutions or extra Flow Collectors.

Data Store specifications

- Cisco Secure Network Analytics Data Store 6200 – Part number: ST-DS6200-K9
- Cisco Secure Network Analytics Data Store 6300 – Part number: ST-DN6300-K9
- Cisco Secure Network Analytics Virtual Data Store – Part number: L-ST-DS-VE-K9

To learn more, reference the Secure Network Analytics Data Store Solution Overview.

Flow Rate License

The Flow Rate License is required to collect, manage, and analyze flow telemetry aggregated at the Secure Network Analytics Manager. The Flow Rate License defines the volume of flows that may be collected and is licensed based on Flows Per Second (FPS). Licenses may be combined in any permutation to achieve the desired level of flow capacity.

- Cisco Secure Network Analytics Flow Rate License – 100 Pack – Part number: ST-FR-100-LIC
  - Orderable through the Secure Network Analytics XaaS subscription – Part number: ST-SEC-SUB

Optional components of the system

Flow Sensor

The Flow Sensor is an optional component and produces telemetry for segments of the switching and routing infrastructure that can't generate NetFlow natively. It also provides visibility into the application layer data. In addition to all the telemetry collected by Secure Network Analytics, the Flow Sensor provides additional security context to enhance the security analytics. And starting with Secure Network Analytics Software Release 7.1, the Flow Sensor can also generate enhanced encrypted traffic analytics telemetry to be able to analyze encrypted traffic. Advanced behavioral modeling and cloud-based, multilayered machine learning is applied to this dataset to detect advanced threats and perform faster investigations.

The Flow Sensor is installed on a mirroring port or network tap and generates telemetry based on the observed traffic. The volume of telemetry generated from the network is determined by the capacity of the deployed Flow Sensors. Multiple Flow Sensors may be installed. Flow Sensors are available as hardware appliances or as virtual appliances to monitor virtual machine environments. It also works in environments where an overlay monitoring solution requiring additional security context better fits the operations model of the IT organization.

Table 4. Major benefits of the Flow Sensor

Benefit	Description
Layer 7 application visibility	Provides true Layer 7 application visibility by gathering application information. This includes data features like RTT (Round Trip Time), SRT (Server Response Time), and Retransmissions.
Packet-level performance and analysis	Provides true Layer 7 application visibility by gathering application information. This includes data features like RTT, SRT, and Retransmissions.
Alerts on network anomalies	Additional telemetry from the Flow Sensor, such as URL information for web traffic and TCP flag detail, helps generate alarms with contextual intelligence so that security personnel can take quick action and mitigate damage.
Lower costs	Enhances operational efficiency and reduces costs by identifying and isolating the root cause of an issue or incident within seconds.

Benefit	Description
Choice of delivery methods	You can order the Appliance Edition, a scalable device suitable for any size organization. Or you can order the Virtual Edition, designed to perform the same function as the appliance edition, but in a VMware or KVM Hypervisor environment.

Flow Sensor specifications

- Secure Network Analytics Flow Sensor 1210 — Part number: ST-FS1210-K9
- Secure Network Analytics Flow Sensor 3210 — Part number: ST-FS3210-K9
- Secure Network Analytics Flow Sensor 4210 — Part number: ST-FS4210-K9
- Secure Network Analytics Flow Sensor 4240 — Part number: ST-FS4240-K9
- Secure Network Analytics Flow Sensor 1300 — Part number: ST-FS1300-K9
- Secure Network Analytics Flow Sensor 3300 — Part number: ST-FS3300-K9
- Secure Network Analytics Flow Sensor 4300 — Part number: ST-FS4300-K9
- Secure Network Analytics Flow Sensor Virtual Edition — Part number: L-ST-FS-VE-K9

Cisco Telemetry Broker

The Cisco Telemetry Broker is capable of ingesting network telemetry from a variety of telemetry sources, transforming their data formats, and then forwarding that telemetry to one or multiple destinations. For example, it can ingest any of the following:

- On-premises network telemetry, including NetFlow, SYSLOG, and IPFIX
- Cloud-based telemetry sources, such as AWS VPC flow logs and Azure NSG flow logs

And it can forward that telemetry to any or all of the following example destinations:

- Cisco SNA, Cisco XDR
- Analytics platforms, such as Hadoop
- Network management and automation platforms, such as Cisco DNA Center and Cisco Nexus Dashboard Insights
- Security Information and Event Management (SIEM) platforms
- Storage/smart capture, such as Cisco Security Analytics and Logging (On-premises)

The Telemetry Broker can ingest not only on-premises network telemetry, including NetFlow, Syslog, and IPFIX, but also other nontraditional telemetry sources, such as cloud-based AWS VPC flow logs and Azure NSG flow logs, and then transform them into IPFIX records or other data formats compatible with Secure Network Analytics. This further expands Secure Network Analytics' data collection capabilities through the ability to ingest and analyze network telemetry from nonstandard sources.

Table 5. Major benefits of the Cisco Telemetry Broker

Benefit	Description
Brokering data	The ability to route and replicate telemetry data from a source location to multiple destination consumers to facilitate quick onboarding of new telemetry-based tools.
Filtering data	The ability to filter data that is being replicated to consumers for fine-grain control over what consumers can see and analyze. This can also help users save money by removing the need to send data to expensive tools.
Transforming data	The ability to transform data protocols from the exporter to the consumer's protocol of choice. This enables Secure Network Analytics and other tools to consume multiple and prior, noncompatible data formats.

Cisco Telemetry Broker specifications

- Cisco Telemetry Broker Appliance – Part number : ST-TB2300-K9
- Cisco Telemetry Broker 100GB/day license – Part number: TB-ESS-100GB
- Orderable through the Cisco Telemetry Broker Subscription – Part number: TB-SEC-SUB

To learn more, reference the Cisco Telemetry Broker Data Sheet

Additional licensing

The following are other optional licenses available for added functionality:

Cisco Secure Network Analytics Endpoint License: Available as a license add-on to extend visibility to end-user devices. The Endpoint License helps organizations secure remote workforces by providing complete and continuous visibility into mobile remote worker endpoint activity. (Requires Cisco AnyConnect® Network Visibility Module [NVM] to be purchased separately.)

- Cisco Secure Network Analytics Endpoint License – Part number: ST-EP-LIC
- Orderable through the Secure Network Analytics XaaS subscription – Part number: ST-SEC-SUB

To learn more, reference the Cisco Secure Network Analytics Endpoint License At-a-Glance.

Cisco Secure Network Analytics Threat Feed: A global threat intelligence feed powered by the industry-leading threat intelligence group, Cisco Talos®, provides an additional layer of protection against botnets and other sophisticated attacks. It correlates suspicious activity in the local network environment with data on thousands of known command-and-control servers and campaigns to provide high-fidelity detections and faster threat response. Cisco Talos sees 1.5 million unique malware samples and blocks 20 billion threats per day.

A Threat Feed License is required for each Flow Collector in the deployment. Below are the Threat Feed Product IDs for each Flow Collector model:

- Cisco Secure Network Analytics Threat Feed for FC1K License – Part number: L-LC-TI-FC1K=
- Cisco Secure Network Analytics Threat Feed for FC2K License – Part number: L-LC-TI-FC2K=
- Cisco Secure Network Analytics Threat Feed for FC4K License – Part number: L-LC-TI-FC4K=
- Cisco Secure Network Analytics Threat Feed for FC5K License – Part number: L-LC-TI-FC5K=

To learn more, reference the Cisco Secure Network Threat Feed License At-a-Glance.

Security Analytics and Logging On-premises: Security Analytics and Logging (SAL) On-premises provides enterprise-class central log management and storage for large-scale firewall deployments. It can support firewall logging at a sustained rate of 100,000 Events Per Second (EPS) with an average retention period of 30 days. Moreover, the service connects this extensive data set to the Cisco Firewall Management Console (FMC) via APIs, effectively enhancing FMC's data storage capacity by 300X (or 30,000%).

Security Analytics and Logging (SAL) On-premises is delivered via a freely downloadable application that can be installed on Secure Networks Analytics release versions 7.3.1 and later. To run the service, users must purchase a volume-based license, which is available as follows:

- A la carte license – Part number: SAL-OP-LT-1GB
- Orderable through the parent Product ID – Part number: SAL-SUB
- Bundled license attached to a firewall subscription – Part number: SEC-LOG-OP
- Orderable through the parent Product ID – Part number: FPR1150-NGFW-K9

SAL On-premises can be hosted on either of the following two deployment architectures (HW or Virtual):

- Single-Node: Scale 20,000 firewall eps OR Multi-Node: Scale 100,000 firewall eps
  - Cisco Secure Network Analytics Manager – Part number: SMC-2210-K9 or SMC-2300-K9
  - Secure Network Analytics Flow Collector 4210 – Part number: ST-FC4210-K9 or ST-FC4300-K9
  - Cisco Secure Network Analytics Data Store 6200 – Part number: ST-DS6200-K9 or ST-DN6300-K9. For more information please refer to Data Store Solution Overview.

To learn more, reference the Ordering Guide, Getting Started Guide or visit cisco.com/go/sal.

Field Replaceable Units (FRU) for M6 Hardware Appliances

Table 6 lists the Cisco Secure Network Analytics component spares that can be used as Field Replaceable Units (FRUs) for M6 hardware.

Table 6. M6 Hardware – Spare components for the Cisco Secure Network Analytics

Part Number	Applicable Product	Description
UCS-HD600G10K12N=	FS3300 and FS4300	600GB 12G SAS 10K RPM SFF HDD
UCS-HD12TB10K12N=	SMC2300 and FC4300	1.2 TB 12G SAS 10K RPM SFF HDD
UCS-HD18TB10K4KN=	DN6300	1.8TB 12G SAS 10K RPM SFF HDD (4K)
UCSC-PSU1-1050W=	FS3300,FS4300,SMC2300, FC4300,DN6300	Cisco UCS 1050W AC Power Supply for Rack Server Platinum

Ordering information

Secure Network Analytics is available as a one-, three-, and five-year term subscription.

For Secure Network Analytics SaaS and Secure Cloud Analytics, 1-, 12-, 24-, 36-and 60-month terms subscriptions are available. There's also an option provided for 1-and 12-month auto-renewals. After selecting the term options, you can add the Public Cloud Monitoring and Private Network Monitoring offers.

To place an order, contact your account representative.

Table 7 lists the Cisco Secure Network Analytics component spares that can be used as Field Replaceable Units (FRUs) for M5 hardware.

Table 7. M5 Hardware – Spare components for the Cisco Secure Network Analytics

Part Number	Applicable Product	Description
ST-M5-HDD-600GB=	FS1210, FS3210, FS4210, FS4240, UDP2210, FC5210-E	Cisco Stealthwatch 600 GB 12G SAS 10K RPM SFF HDD
ST-M5-HDD-1.2TB=	SMC2210, FC4210, FC5210-D, DS6200	Cisco Stealthwatch 1.2 TB 12G SAS 10K RPM SFF HDD
ST-M5-PWR-AC-770W=	FS1210, FS3210, FS4210, FS4240, SMC2210, FC4210, FC5210-E, FC5210-D, DS6200, UDP2210	Cisco Stealthwatch AC Power Supply 770W
ST-M5-PWR-AC-1050=	FS1210, FS3210, FS4210, FS4240, SMC2210, FC4210, FC5210-E, FC5210-D, DS6200, UDP2210	Cisco Stealthwatch AC Power Supply 770W
UCSC-RAILB-M4=	FS1210, FS3210, FS4210, FS4240, SMC2210, FC4210, FC5210-E, FC5210-D, DS6200, UDP2210	Ball Bearing Rail Kit for C220 and C240 M4 and M5 rack servers

Cisco environmental sustainability

Information about Cisco's environmental sustainability policies and initiatives for our products, solutions, operations, and extended operations or supply chain is provided in the "Environment Sustainability" section of Cisco's Corporate Social Responsibility (CSR) Report.

Reference links to information about key environmental sustainability topics (mentioned in the "Environment Sustainability" section of the CSR Report) are provided in the following table:

Sustainability topic	Reference
Information on product material content laws and regulations	Materials
Information on electronic waste laws and regulations, including products, batteries, and packaging	WEEE compliance

Cisco makes the packaging data available for informational purposes only. It may not reflect the most current legal developments, and Cisco does not represent, warrant, or guarantee that it is complete, accurate, or up to date. This information is subject to change without notice.

Service and support

Several service programs are available for Secure Network Analytics. These services help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Professional Services, see the Technical Support homepage

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital® makes it easier to get the right technology to achieve your objectives, enable business transformation, and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can allow you to acquire hardware, software, services, and complementary third-party equipment in easy, predictable payments. Learn more.

For more information

For more information about Secure Network Analytics, visit https://www.cisco.com/go/secure-network-analytics or contact your Cisco security account representative to learn how your organization can gain visibility across your extended network by participating in a complimentary Secure Network Analytics visibility assessment.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C78-739398-10 01/24