Cisco Cyber Threat Defense Solution

Overview

The network security threat landscape is ever evolving. But always at the cutting edge are custom-written, stealthy threats that evade traditional security perimeter defenses. The Cisco® Cyber Threat Defense Solution provides greater visibility into these threats by identifying suspicious network traffic patterns within the network interior. These suspicious patterns are then supplemented with contextual information necessary to discern the level of threat associated with the activity.

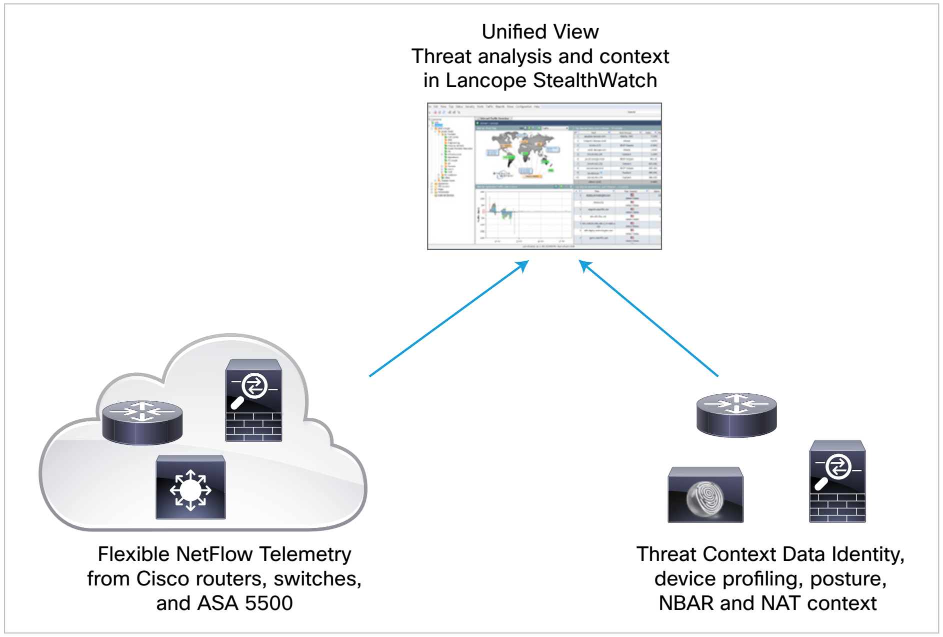
Solution Highlights

Cisco Cyber Threat Defense focuses on the most complex and dangerous information security threats–threats that lurk in networks for months or years at a time stealing vital information and disrupting operations. Cisco provides visibility into these threats and context to decipher their targets and potential damage. Security analysts gain visibility into advanced cyber threats such as:

- Network reconnaissance
- Network interior malware proliferation
- Command and control traffic
- Data exfiltration

The Cisco Cyber Threat Defense Solution is built upon the following components:

- Unique interior network traffic telemetry capabilities of Cisco Catalyst® switches, Cisco routers and Cisco ASA 5500.
- Network traffic analysis capabilities provided by the StealthWatch System from Lancope, Cisco's cyber threat solution partner. Cisco offers the StealthWatch System via its development partnership with Lancope.
- Identity, security, and application-type contextual information for discerning the target and severity of the threat. These context points are delivered by the Cisco Identity Services Engine, NAT correlation on ASR 1000 routers and ASA 5500 appliances, and Network-Based Application Recognition (NBAR) on Cisco routers, and are presented in a unified view via the StealthWatch Management Console.



Unified View
Threat analysis and context
in Lancope StealthWatch

Flexible NetFlow Telemetry
from Cisco routers, switches,
and ASA 5500

Threat Context Data Identity,
device profiling, posture,
NBAR and NAT context

Benefits

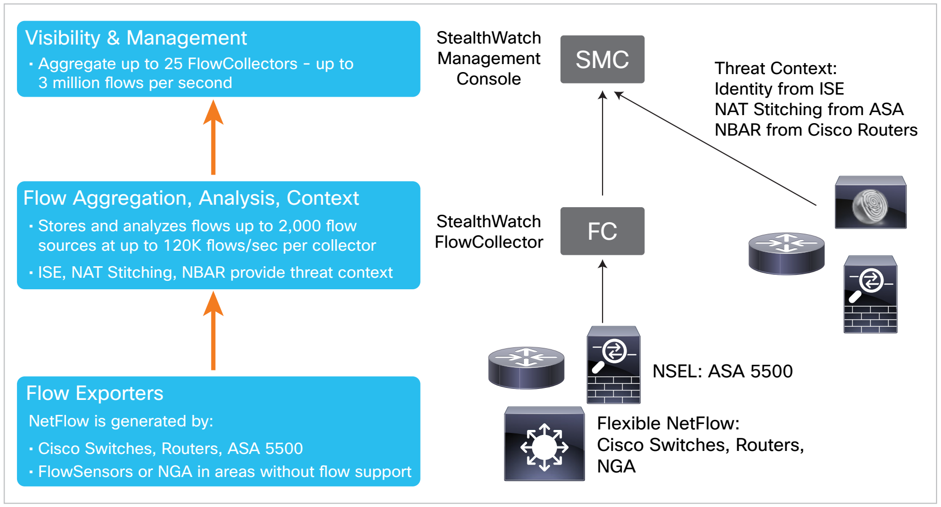
The Cisco Cyber Threat Defense Solution:

- Provides threat defense in the network interior, where the most elusive and dangerous threats are
- Enables scalable, ubiquitous, and cost-effective security telemetry throughout the network using NetFlow data from the Cisco network infrastructure
- Simplifies error-prone and expensive manual threat investigation processes
- Uses existing Cisco switch, router, and ASA 5500 network footprint

Solution Components

There are three functional components of the Cisco Cyber Threat Defense Solution:

- Generating network-wide security telemetry – NetFlow export from Cisco Catalyst switches, Cisco ISR, and Cisco ASA 5500. Overlay StealthWatch FlowSensors may be deployed in networks without NetFlow scale or support.
- Aggregating, normalizing, and analyzing NetFlow data to detect threats and suspicious behavior – Lancope StealthWatch FlowCollectors and Management Console
- Providing threat context – User identity, endpoint device profiling, and posture information from the Cisco Identity Services Engine, and application type from NBAR on Cisco routers.



Visibility & Management
- Aggregate up to 25 FlowCollectors - up to 3 million flows per second

Flow Aggregation, Analysis, Context
- Stores and analyzes flows up to 2,000 flow sources at up to 120K flows/sec per collector
- ISE, NAT Stitching, NBAR provide threat context

Flow Exporters

NetFlow is generated by:
- Cisco Switches, Routers, ASA 5500
- FlowSensors or NGA in areas without flow support

Why Cisco?

The Cisco Cyber Threat Defense Solution delivers broad visibility into the most dangerous and stealthy network threats by providing ubiquitous threat detection within the interior of the network. By combining traffic analysis with user, application, and firewall context, Cisco delivers:

- Ubiquitous interior network visibility where little exists today
- A cost-effective approach for ubiquitous visibility
- Full, unsampled data security telemetry via line-rate NetFlow
- Relevant contextual information for deciphering the intent and severity of the threat via the Cisco Identity Services Engine, NAT stitching, and application recognition
- Proven scalability for the most demanding environments
- Network architecture design and deployment support

Ordering Information

Lancope StealthWatch FlowCollectors – Aggregates NetFlow and NBAR from Cisco infrastructure.

SKU	Model	Maximum Flows Per Second	Maximum NetFlow Exporters (e.g., Switches, Routers)	Maximum Hosts Monitored (IP Addresses)	Flow Storage Capacity
L-LC-SMC-NF-VE-K9	FlowCollector VE	30,000*	1000	500,000	1 TB
LC-FC-NF-1000-K9	FlowCollector 1000	30,000	500	250,000	1 TB
LC-FC-NF-2000-K9	FlowCollector 2000	60,000	1000	500,000	2 TB
LC-COLLECT-4000	FlowCollector 4000	120,000	2000	1,000,000	4 TB

* Dependent on virtual machine resources.

Lancope StealthWatch Management Console – Aggregates, organizes, and presents analysis from FlowCollectors, Cisco Identity Services Engine, and other sources.

SKU	Model	Maximum FlowCollectors Supported	Flow Storage Capacity
L-LC-SMC-VE-K9	SMC VE	5*	1 TB
LC-SMC-1K-K9	SMC 1000	5	1 TB
LC-SMC-2K-K9	SMC 2000	25	2 TB

* Dependent on virtual machine resources.

Lancope StealthWatch FlowSensors – Optional component that produces NetFlow data for infrastructures that do not support NetFlow.

SKU	Model	Traffic Capacity
L-LC-FSVE-VMW-K9	FlowSensor VE	1 per ESXi server
LC-FS250-2C-K9	FlowSensor 250	100 Mbps
LC-FS1K-3C-K9	FlowSensor 1000	1 Gbps
LC-FS2K-SC-K9	FlowSensor 2000 with 5 copper interfaces	2.5 Gbps
LC-FS2K3C-2F-K9	FlowSensor 2000 with 2 fiber ad 3 copper interfaces	2.5 Gbps
LC-FS3K-2F-K9	FlowSensor 3000	5 Gbps

NB: FlowSensor traffic does not count against Flow license capacities.

Lancope StealthWatch Flow Licenses – Required to aggregate flows at the StealthWatch Management Console. Flow licenses define the volume of flows that may be collected. Licenses may be combined in any permutation to achieve the desired level of flow capacity.

SKU	License Type
L-LC-FPS-1K=	Flow Collection License – 1000 Flows
L-LC-FPS-10K=	Flow Collection License – 10,000 Flows
L-LC-FPS-25K=	Flow Collection License – 25,000 Flows
L-LC-FPS-50K=	Flow Collection License – 50,000 Flows
L-LC-FPS-100K=	Flow Collection License – 100,000 Flows

NB: FlowSensor traffic does not count against Flow license capacities.

Cisco NetFlow-Enabled Infrastructure – Generates the flow telemetry collected for analysis by StealthWatch.

Model	Hardware Required	Recommended Software Version
Cisco Catalyst 3560-X Series	Cisco Service Module	Cisco IOS® Software Release 15.0(1) SE3
Cisco Catalyst 3750-X Series	Cisco Service Module	Cisco IOS® Software Release 15.0(1) SE3
Cisco Catalyst 4500 Series	Supervisor Engine 7-E or 7L-E	Cisco IOS Software Release 15.0.(2)X0
Cisco Catalyst 6500 Series	Supervisor Engine 2T	Cisco IOS Software Release 15.0(1)SY2
Cisco Integrated Services Routers	–	Cisco IOS Software Release 15.2(4)M2
Cisco Aggregated Service Router (ASR) 1000 Series	–	Cisco IOS Software Release 15.2(1)S or Cisco IOS XE 3.5
Cisco ASA 5500 Series	–	Cisco ASA Software Release 8.4(4)1
Cisco NetFlow Generation Appliance		Cisco NGA Software Version 1.0

Cisco Threat Context Platforms – generates the contextual information to integrate with flow analysis in StealthWatch

Platform	Context Generated	Recommended Software Version
Cisco Identity Services Engine	User identity, posture, endpoint type, authorization level	Cisco ISE Software 1.1
Cisco Network-Based Application Recognition (NBAR)	Application type	Generated by Cisco Integrated Services Routers and included in StealthWatch analysis

For More Information

For more information about the Cisco Cyber Threat Defense Solution, visit: http://www.cisco.com/go/threatdefense