Cisco Cyber Threat Defense Solution: Delivering Visibility into Stealthy, Advanced Network Threats

What You Will Learn

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. These threats infiltrate the interior of the network - the core, the distribution layer, and the user access edge - where threat defense and visibility is minimal. From there they quietly target specific assets, and even specific people, within an organization. The goal of these advanced cyber threats is not notoriety and fame, or even setting up a for-profit botnet; it's to gather and exfiltrate intellectual property or state/trade secrets for competitive advantage in industry, economy, and sociopolitical ends.

This document explains:

- What's at stake and key challenges in gaining visibility to customized threats
- Cisco® Cyber Threat Defense Solution, which provides greater visibility into these threats by identifying suspicious network traffic patterns within the network interior thus giving security analysts the contextual information necessary to discern the level of threat these suspicious patterns represent

Business Challenge

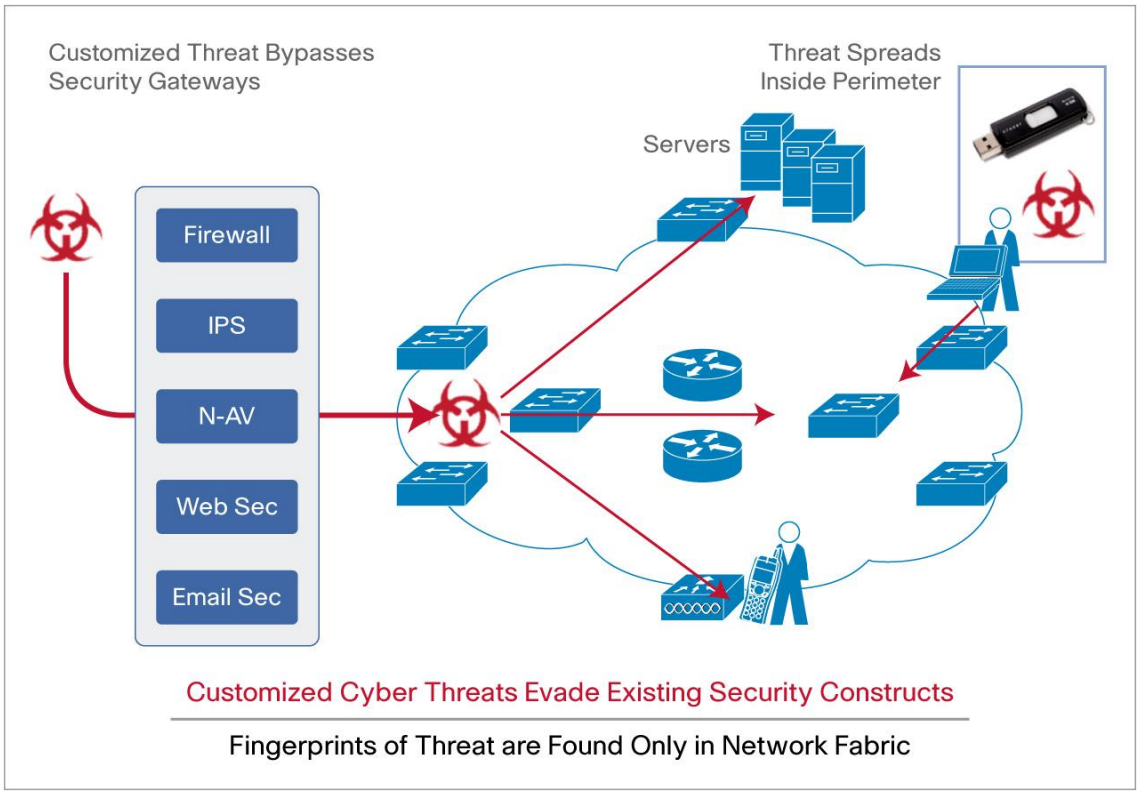
Well-understood and known security threats are effectively combated by a well-designed and mature security infrastructure that includes components like intrusion prevention, antivirus, content security and firewall. But custom-written threats designed for specific targets with specific intent represent a tougher challenge. Customized threats are designed based on specific knowledge of a target, often based on reconnaissance of the network or people at the organization, or both. Once the custom threat has breached the perimeter defenses of the network, they typically spread laterally in the interior of the network where threat defense devices are not generally pervasively deployed. By remaining quiet and hidden in the noise of normal network traffic the threats can spread under the radar among specific targets. Perimeter defenses do not have visibility into these threats. Many times these threats are actually introduced inside the perimeter via social engineering, spear phishing, or external media like USB drives. And while prevention is important, even the most diligent patching will not completely guard against these threats.

Quantification of the risk and damage caused by advanced cyber threats varies by source. Victims of these types of security breaches are not motivated to disclose their impacts, but primary research into advanced cyber threats indicates that this is a quickly growing problem with significant impact. Some key statistics to consider:

- 63% of threats are customized for their target environment - a three-fold increase since 2006[1]
- A five-fold increase in attacks against the U.S. government from 2006 to 2009[2]
- 59% of organizations in the United States believe they have been targets of cyber threats[3]

Once these threats have penetrated the network perimeter, the only place left to identify these threats is where they live - the network interior. One must look for “fingerprints” of the threat by analyzing traffic patterns across the switches and routers that comprise the network interior. From this analysis one can gain insight into patterns that are indicative of advanced cyber threat traffic. Whether it is an internal client trying to set up peer-to-peer connections with other clients on its subnet or clients communicating with unusual regions of the world, analyzing traffic patterns provide visibility into potential cyber threats.

Figure 1. Advanced Cyber Threats Evade Perimeters, Must Be Detected in the Network Interior



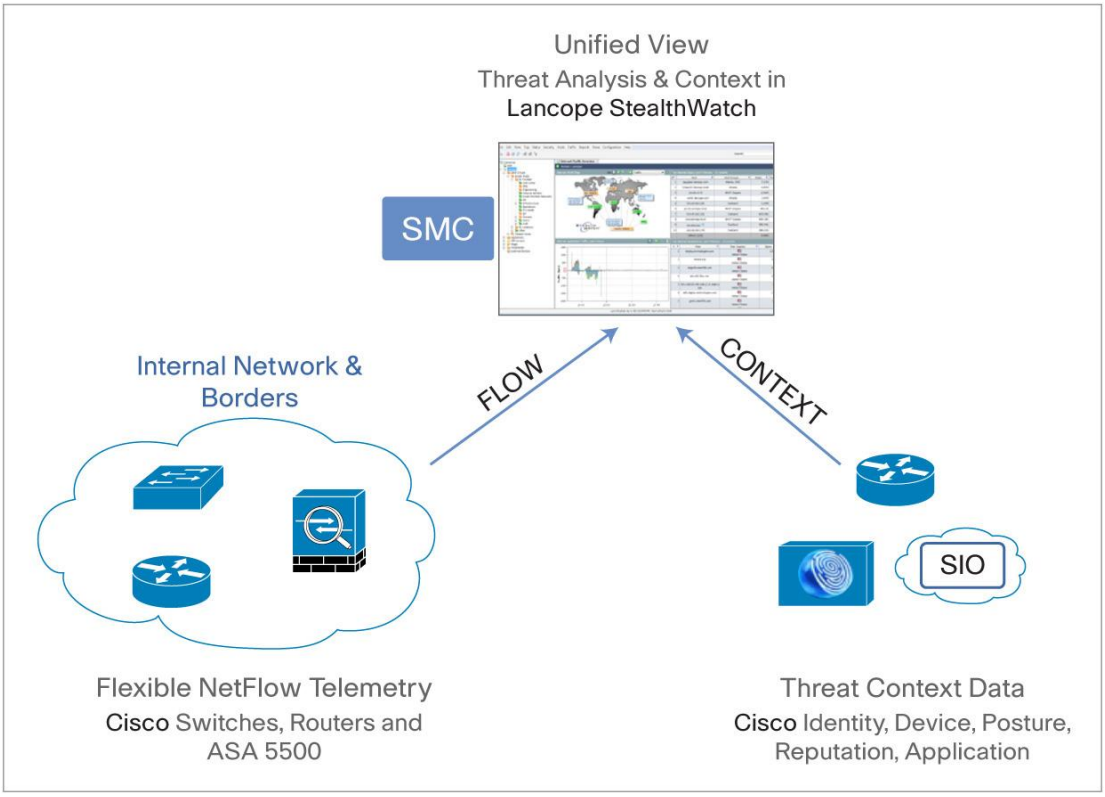
Overview of the Cisco Cyber Threat Defense Solution

The Cisco Cyber Threat Defense Solution combines the following elements to provide visibility into the most evasive and dangerous cyber threats:

- Unique interior network traffic telemetry utilizing scalable unsampled NetFlow capabilities of Cisco Catalyst® switches, Cisco routers, and Cisco ASA 5500 Series Adaptive Security Appliances.
- Network traffic analysis capabilities provided by the Lancope StealthWatch System. Cisco has partnered with Lancope to jointly develop and offer the Cisco Cyber Threat Defense Solution.

- Identity, reputation, and application-type contextual information for discerning the nature and severity of a threat. These context points are delivered by the Cisco Identity Services Engine, Cisco Security Intelligence Operations (SIO), and Cisco routers, respectively.

Figure 2. Components of the Cisco Cyber Threat Defense Solution



Using this telemetry and contextual information a network security analyst can, from a single pane of glass, identify suspicious activity, gather pertinent user information, identify the application, and lookup the host's reputation. This enables assessment of the nature and the potential danger of the suspicious activity. With this information, the analyst can decipher the correct next steps for advanced cyber threats such as:

- Network reconnaissance - The act of probing the network looking for attack vectors that can be utilized by custom-crafted cyber threats
- Network interior malware propagation - Spreading malware across hosts for the purpose of gathering security reconnaissance data, exfiltrating data, or creating back doors to the network
- Command and control traffic - Communications between the attacker and the compromised internal hosts
- Data theft - Exporting sensitive information back to the attacker, generally via command and control communications

Benefits of the Cisco Cyber Threat Defense Solution

The Cisco Cyber Threat Defense Solution 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 their context to decipher their potential damage.

Key benefits of the Cisco Cyber Threat Defense Solution:

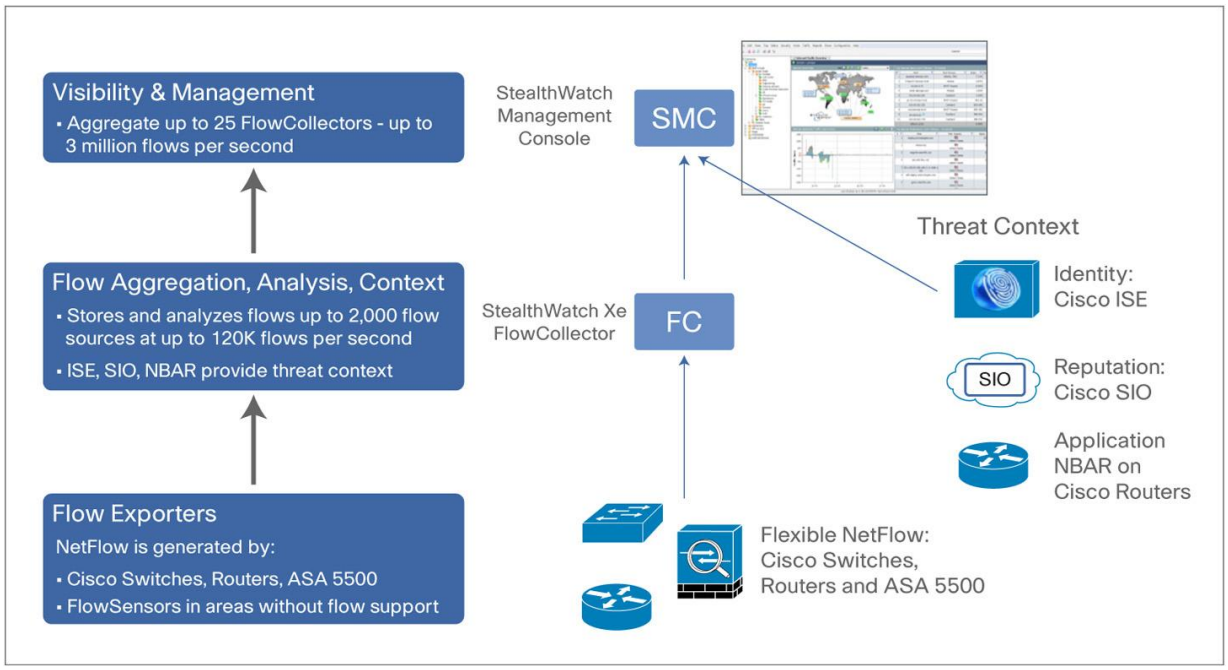
- Provides threat defense in the network interior, where the most elusive and dangerous threats target
- Detects threat closer to the source to minimize damage and propagation
- Enables scalable, ubiquitous, and cost-effective security telemetry throughout the network
- Simplifies manual, error-prone, and expensive threat investigation processes
- Uses the Cisco switching, routing, and ASA 5500 network footprint

Solution Components

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

- Generating network-wide security telemetry - NetFlow export from Cisco switches, routers, and Cisco ASA 5500
- Aggregating, normalizing, and analyzing NetFlow telemetry data to detect threats and suspicious behavior - Lancope StealthWatch System
- Providing contextual information to decipher nature and severity of threat - User identity, endpoint device profiling, and posture information from the Cisco Identity Services Engine

Figure 3. Products that Comprise the Cisco Cyber Threat Defense Solution



Full Security Telemetry from the Network Interior: Cisco Network Infrastructure

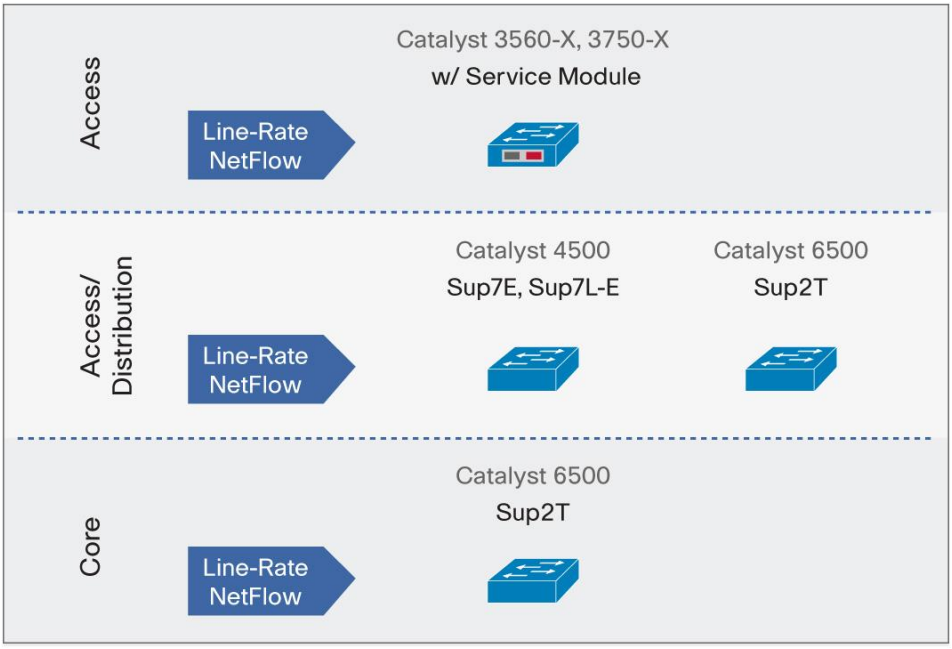
Recent advances in Cisco Catalyst switches enable the industry's first pervasive network traffic telemetry - from the user access edge to distribution to the core of the switching network. The line-rate, non-performance-impacting NetFlow telemetry capabilities of the Cisco Catalyst 3560-X, 3750-X, 4500, and 6500 Series provide insight into traffic patterns that indicate threats have bypassed the security perimeter and are attempting to remain below the detection radar. Key to delivering this visibility is Cisco's ability to generate unsampled NetFlow data in scale from these platforms.

NetFlow telemetry comes in two forms:

- Sampled - A small subset of traffic, usually less than 5%, is sampled and used to generate NetFlow telemetry data. This gives a “snapshot” view into network activity, like reading a book by skimming every 100th page.
- Unsampled - All traffic is used to generate NetFlow telemetry, providing a comprehensive view into all activity on the network. Using the book analogy, this is reading every word in the book.

The customized, stealthy nature of advanced cyber threats requires full visibility into network traffic patterns if they are to be detected. This can only be achieved using full, unsampled NetFlow telemetry. Only a Cisco Catalyst switch can deliver this unsampled NetFlow data at line rate without any impact to network performance.

Figure 4. Catalyst Switches Capable of Line-Rate NetFlow



Detecting Threats and Suspicious Activity: Lancope StealthWatch System

With the Cisco network infrastructure delivering ubiquitous NetFlow telemetry, the next step is to collect and analyze that data. The Lancope StealthWatch System, available from Cisco, is purpose-built to aggregate and normalize massive amounts of NetFlow data, then apply security analytics to detect malicious and suspicious network traffic patterns as presented through the StealthWatch Management Console.

The primary components of the Lancope StealthWatch System are:

- FlowCollector - A physical or virtual appliance that aggregates and normalizes NetFlow and application-type data collected from up to 2,000 Cisco Catalyst switches, Cisco integrated services routers, or Cisco ASA 5500 adaptive security appliances per FlowCollector.
- StealthWatch Management Console - A physical or virtual appliance that aggregates, organizes, and presents analysis from FlowCollectors, the Cisco Identity Services Engine via graphical representations of network traffic, user identity information, customized summary reports, and integrated security and network intelligence for drill-down analysis.

The optional components of the Lancope StealthWatch System are:

- FlowSensor - A physical appliance that provides an overlay solution for generating NetFlow data for legacy Cisco network infrastructures not capable of producing line-rate, unsampled NetFlow data. Also for environments where IT security prefers a dedicated overlay architecture separate from the network infrastructure.
- FlowSensorVE - A virtual appliance that provides the same function as the FlowSensor, but for virtual machine environments.
- FlowReplicator - A physical appliance that provides a single point for forwarding NetFlow data as a single data stream to other consumption devices.

In addition to real-time cyber threat detection and analysis, Lancope StealthWatch stores NetFlow data to provide a forensics capability for ongoing and historical incident investigation.

Threat Context: Cisco Identity Services Engine, Cisco SIO for Reputation, and Application Recognition

Identifying suspicious traffic patterns is key to threat detection and visibility, but deciphering the danger associated with those threats requires relevant contextual information. The Cisco Cyber Threat Defense Solution presents a unified view of the traffic pattern analysis via NetFlow and relevant contextual information regarding that traffic, such as user identity, user policy, device type, external host reputation, and application information.

Key to establishing the potential threat of suspicious traffic is contextual information regarding the user associated with that traffic. Utilizing the Cisco Identity Services Engine, Cisco's flagship network policy engine, user identity, device and posture information can be bound to NetFlow data in the StealthWatch Management Console, thus providing a unified view of suspicious traffic patterns and the user information relevant to establishing if those patterns are malicious. Using the Cisco Identity Services Engine as part of the Cyber Threat Defense Solution provides insight into:

- Who is being targeted? - Associating suspicious traffic flows with users
- Is the user a critical target? - User title and role in the organization (per Active Directory/LDAP)
- What information does the user have access to? - Network authorization group the user belongs to
- What device is the traffic coming from? - Laptop, smartphone, etc.
- Has the user had security posture failures recently? - Quarantine and posture event status
- Are there other relevant user session events? - Access to all AAA events associated with the user
- How best to execute user-based remediation? - Comprehensive event and status visibility of the user affected by the threat needed to determine and execute the right next steps for remediation.

Additionally, the application associated with the suspicious traffic is key to deciphering the nature and severity of the threat. Application information can be discerned utilizing network-based application recognition (NBAR) information collected from Cisco routers. This information is also collected and reported to the Lancope StealthWatch Management Console.

Finally, the reputation of external hosts associated with suspicious traffic may be looked up from Cisco SIO (via the Cisco IronPort® SenderBase Network) from the traffic analysis screen within the Lancope StealthWatch Management Console. Understanding the reputation of the external host associated with a suspicious flow is critical to establishing the nature and severity of the threat.

Using these points of context a security analyst can, from a single pane of glass, identify suspicious activity, gather pertinent user information, identify the application and spawn a web lookup to Cisco SenderBase for host reputation, and can then assess the potential danger of the suspicious activity. Utilizing the comprehensive user visibility capabilities of the Cisco Identity Services Engine, the analyst can formulate and execute remediation for affected users. Cisco Identity Services Engine provides complete insight to the history and status of the user, policy, posture and device as well as quarantine or network disconnect remediation functions. Collectively these context and remediation capabilities enable the analyst to decipher the correct next steps to take concerning the threat in a timely, efficient, and cost-effective manner.

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 reputation context, Cisco delivers:

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

For More Information

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

Citations

[1] Data Breach Investigations Report, Verizon & U.S. Secret Service; April 2011

[2] U.S. Federal Cybersecurity Market Forecast 2010-2015, Market Research Media; December 2010

[3] U.S. Advanced Persistent Threat Analysis, Enterprise Strategy Group; October 2011

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 www.cisco.com/go/offices.

Printed in USA C22-700869-00 02/12