Advanced Threat Detection: Gain Network Visibility and Stop Malware

What You Will Learn

The Cisco® Cyber Threat Defense (CTD) solution brings visibility to all the points of your extended network, allowing you to detect threats that have infiltrated it. It shines a spotlight on even the darkest areas of the network where advanced threats may hide.

Five dark areas that the Cisco CTD solution illuminates are:

- User-to-user activity
- Specialized networked devices
- Encrypted traffic
- Remote networks
- Inside the data center

Operating in the Dark

Stealthy threats and dynamically changing IT environments make it difficult to detect malicious network traffic. According to the Ponemon Institute, malicious attacks take an average of 80 days to discover and 123 days to resolve. Most organizations don’t have the visibility they need to identify advanced attack campaigns that remain in networks for long periods of time, all the while stealing valuable data or disrupting operations. Nor do they have the ability to continuously monitor modern extended networks and their evolving components that spawn new attack vectors.

Vulnerable network components can include mobile devices, web-enabled and mobile applications, hypervisors, social media, web browsers, home computers, and even vehicles. The single network perimeter has been replaced by a constantly morphing set of users, locations, applications, access methods, and devices. Despite their best efforts, organizations are challenged to keep up. In fact, according to the Cisco 2014 Annual Security Report, 100 percent of companies analyzed have connections to domains that are known malware threat sites.

Advanced attacks routinely evade traditional point-in-time technologies that scan only once. They infiltrate the network where they are difficult to locate, let alone eradicate. Adding further complexity to security analysts’ tasks, many organizations deploy dozens of disparate products that don’t—and can’t—work together. The result? Security analysts are left operating in the dark.

The Cisco CTD solution helps you overcome these challenges by bringing visibility to all the points of your extended network, allowing you to detect threats that have infiltrated it. Cisco CTD provides a Cisco validated framework of best-in-class tools that accelerate your implementation of an advanced threat detection and response system for network and endpoint security. These tools include Cisco Adaptive Security Appliance (ASA) firewalls, intrusion prevention systems, advanced malware protection, email and web security appliances, cloud web security, and the Cisco Identity Services Engine (ISE), along with Cisco network infrastructure components such as routers, switches, and servers.
Because you can’t protect what you can’t see, the Cisco CTD solution includes two additional components aimed at enhancing visibility: Cisco NetFlow and the Lancope StealthWatch System. Together, they bridge the gap between the network and security infrastructure to help you identify suspicious network traffic patterns as they emerge, and then take action.

Let’s take a closer look at how Cisco Cyber Threat Defense helps organizations put a spotlight on potential threats already inside the network.

**Exposing Advanced Threats**

The threat landscape is ever evolving and always advancing with custom-written, stealthy threats that evade traditional security perimeter defenses. The Cisco CTD solution gives greater visibility to these threats by identifying suspicious network traffic patterns within the network interior. These suspicious patterns are then supplemented with the contextual information necessary to discern the level of threat associated with the activity.

NetFlow, a type of telemetry data generated by Cisco network and security devices, sheds light on every network conversation. It captures each and every network communication, or traffic flow, over an extended period of time. It represents traffic in metadata form by capturing the source and destination, timing, and amount of information transferred, providing information much like that contained in a telephone bill: who was called, when, and for how long. Historically used for billing and accounting, network capacity planning, and availability monitoring, NetFlow has tremendous security value as well. It helps you to identify anomalous activities, and it provides forensic evidence to reconstruct the sequence of events. It can also be used for regulatory compliance. NetFlow data can support security alerting and network automation, and it can be efficiently stored for future forensic investigations.

An important distinction should be drawn between Flexible NetFlow and a “NetFlow lite” or other sample-based approach to NetFlow. Cisco CTD requires an unsampled approach, because you want to be able to identify all data flows, rather than a small percentage of them, which could miss critical information. This is particularly important for identifying advanced malware that spreads laterally through the internal network to reach its target. Visibility across the entire network and as close to the source of the traffic as possible increases the chances of detecting unusual behavior that would otherwise go unnoticed.

**Knowing More About Your Network**

Cisco partners with Lancope to jointly offer the Lancope StealthWatch System as part of the Cyber Threat Defense solution. The Lancope StealthWatch System is a leading solution for flow-based security monitoring and performs NetFlow collection and analysis in the Cisco CTD solution.

The StealthWatch System consists of two main components: First, the Lancope StealthWatch FlowCollector appliance provides NetFlow collection services and performs analysis of the records to detect suspicious traffic pattern anomalies, malware command-and-control traffic, and advanced persistent threats. Monitoring, prioritizing, and analyzing network traffic, it creates comprehensive security intelligence for better protection. Second, the StealthWatch Management Console provides centralized management for all StealthWatch appliances and provides real-time data correlation, visualization, and reporting of NetFlow data. It also integrates with Cisco ISE so that you can associate user and device identity with network traffic to understand the full “who, what, when, where, and how” of communications over the network.
Correlating and analyzing vast amounts of network traffic data, the Lancope StealthWatch System illuminates potential threats that could previously hide in the dark recesses of the network. With comprehensive information, analysis, and reporting you can gain faster, more precise incident response. You will have greater confidence in your response—be it a restriction on network access for compromised devices, dynamic inline blocking, or endpoint-based remediation. Using automation to present the data in real time has the added benefit of freeing up highly skilled cybersecurity professionals to focus on attacks and events that are truly critical to the security of your organization.

Further, NetFlow and Lancope StealthWatch are just as relentless as the attackers targeting your digital assets. The solutions remain ever vigilant, continuously monitoring network traffic, collecting and storing data over long periods of time, and performing context-aware security analytics against current and historical information to identify emerging threats so you can take action quickly. The StealthWatch System is able to quickly analyze large volumes of data spanning extended periods of time, detecting breach activity carried out in a “low and slow” manner to prevent detection. Moreover, it preserves an audit trail that provides a powerful resource to aid forensic investigations.

Shedding light more broadly and deeply across the network, NetFlow and Lancope StealthWatch help security professionals gain visibility into even the darkest areas of the network where advanced threats often hide.

**Getting Visibility into Five Dark Areas of the Network**

**User-to-User Activity**

Although full-packet inspection devices are a critical part of the security infrastructure, they are not designed to monitor all traffic between all hosts communicating within the network interior. The volume generated by copying every packet on the network to an aggregation point for inspection would cripple the efficiency and capacity of the network as it grows. This situation forces a network security architect to limit the depth of visibility within the network interior, creating dark areas along the access layer. Some user-generated traffic, like traffic destined for the Internet, will pass through an inspection point. User-to-user traffic visibility, however, is commonly limited. Although host-based sensors can fill the gap created in this area, host-based solutions fall short if a truly network-based approach is desired.

![Figure 1. User-to-user malware activity at the access layer](image)

NetFlow can bring visibility to user-to-user activity along the access layer without hampering network performance. Since NetFlow data makes up a small fraction of a given flow, there is much less overhead in routing it to a collection point for analysis.
Gaining user-to-user visibility is particularly important to understanding how malware is propagating through your network. Behavior-based analysis, like that provided by the Lancope StealthWatch System, is particularly useful for detecting traffic patterns associated with malware. With StealthWatch you can visualize a malware outbreak and gain valuable forensic information for a better understanding of the initial infector and the sequence of all subsequent infections.

Specialized Networked Devices

Endpoint security agents are available for many popular desktop and server operating systems. Specialized devices, however, like multifunction printers, point-of-sale (POS) terminals, automated teller machines (ATMs), and other Internet of Things (IoT) devices, rarely accommodate endpoint security agents. Yet these devices sport all the vulnerabilities of the underlying operating system. Moreover, embedded systems commonly include vulnerable server software, like web servers, and represent a weak link in your network’s security. So without endpoint security agents, the networks of these devices become another dark area for the security team. As a result, hackers view these devices as easy targets for infiltration into an organization.

Figure 2. Specialized devices for Industrial Control Systems, Point-of-Sale, and other Internet-of-Things applications

NetFlow-based analysis can be effectively used to bring threat visibility to specialized networked devices without interrupting the devices’ primary, and often critical, functions. The other common trait of these types of devices is that they usually follow a predictable pattern of communication. So it’s no surprise that products like Lancope StealthWatch are ideally suited to detecting anomalous traffic within this class of devices.
Encrypted Traffic

Encrypted communications can create another dark area within the network with respect to threat visibility. Increasingly, command-and-control traffic between a malicious server and a compromised endpoint is encrypted to avoid detection. The challenge becomes, How do you detect threats within encrypted traffic without knowing the contents?

Using the phone-bill analogy introduced earlier, it’s not always necessary to know what was said to determine that malicious activity is taking place. By collecting the source, destination, time stamp, amount of data transferred, and other data points provided by NetFlow, it’s possible to identify threats without knowing exactly what was communicated.

To illustrate this concept, consider a common military situation: One group is using encryption to prevent its adversary from knowing its next moves. The adversary is presented with two options for determining what’s happening: (1) attempting to break the cryptography so that the contents will be known or (2) analyzing the communications and extrapolating a probable next step based on the pattern of the activity. Behavioral analysis follows the second approach, detecting threats based on the characteristics of communications rather than the contents.

Now consider another example that applies such behavioral analysis to a real-world setting. Within a typical network, data exfiltration can be exposed with a behavioral anomaly detection system. Commonly, an internal host is baselined as usually communicating only with internal servers, but it suddenly begins communicating with an external server and transferring large amounts of data. The risk associated with this host increases dramatically, and it immediately becomes a concern that warrants further investigation.
Remote Networks

Security-related costs increase as the number of inter-networked locations increases. You must either backhaul traffic for inspection, increasing WAN costs, or you must implement a local inspection device at the perimeter. Even with perimeter inspection at a remote location, you may still face limited visibility among user-to-user activity, as outlined earlier.

Figure 4. (a) Distributed security controls at each remote network, (b) Backhaul of traffic to central point for security inspection, (c) Backhaul of netflow only optimizes cost and bandwidth

NetFlow technology was invented in the 1990s, when a T1 data circuit was considered a high-speed WAN link. Efficiency of transport was a top concern then, leading to the development of NetFlow as a lightweight source of telemetry.

The use of NetFlow, backhauled over the WAN link to a central collection point, can remove yet another dark area of the network. For example, a printer with fax capabilities may become compromised through its telephone link. In this example, the printer is at a distributed location. Once attackers have infiltrated the network, they may begin to compromise hosts on the local segment of the network. Without NetFlow visibility, it’s possible for the security administrator to miss this activity altogether.
Inside the Data Center
The speed of traffic traveling east to west within the data center can quickly overcome most deep-packet inspection devices today. To overcome this hurdle, security architects commonly place deep-packet inspection at the perimeter of the data center. This type of traffic is commonly referred to as north-south traffic. Further compounding the visibility problem within the data center, gaining visibility between two virtual machines on a single host can be difficult.

![Data Center Network Diagram](Image)

**Figure 5.** Netflow restores visibility of east-west traffic within the Data Center

NetFlow allows east-west traffic to be efficiently monitored with little impact to the network’s capacity. NetFlow can also help with the virtual machine visibility problem. Most modern hypervisors support the export of NetFlow telemetry and the latest Cisco Unified Computing System™ (Cisco UCS®) platforms can even generate and export NetFlow without affecting the host’s CPU performance by using specialized hardware acceleration.

Finally, the data center can demonstrate a high level of diversity in operating systems. As explained above, this presents a challenge that endpoint software simply fails to meet completely, resulting in a loss of visibility. Since NetFlow operates at the network level, it represents an ideal way to gain visibility over host types where an endpoint agent is not available.

**Conclusion**

The Cisco Cyber Threat Defense solution helps security professionals move toward security systems built on a foundation of broad-based visibility and extensive data retention. They can see more, learn through correlation and context, and then take action against advanced threats. Cisco NetFlow and the Lancope StealthWatch System play an essential role in enabling this transition. The combined solution exposes advanced threats hidden in the recesses of the network by bringing visibility and insights into:

- **User-to-user activity** along the access layer, without hampering network performance
- **Specialized networked devices**, without interrupting the devices’ primary, and often critical, functions
- **Encrypted communications** based on characteristics of the communications rather than the contents
- **Remote networks**, by backhauling NetFlow telemetry over the WAN link to a central collection point
- **The data center and between virtual machines** without affecting network capacity
For More Information

To learn more about how you can gain visibility into five dark areas of your network and the Cisco Cyber Threat Defense solution visit: Cisco Cyber Threat Defense.