White Paper

Double Your Defenses with Cisco Enterprise Network Security Solutions

5 Steps to Help Defend Your Network

Your Network Holds the Key to Defending Your Business

Which do you want first, the good news or the bad news?

The bad news: you are likely already infected. In an analysis of major multinational enterprises, Cisco® Security Services teams examined how many had malicious traffic visible in their networks. The result? As reported in the Cisco 2014 Annual Security Report, 100 percent of the business networks analyzed by Cisco teams have traffic going to websites that host malware. The enterprise attack surface is increasing due to mobility, the cloud, and the Internet of Things (IoT). At the same time, the industrialization of hacking is spawning sophisticated and hard-to-detect threats. And many enterprises are still relying on slow and complex mitigation processes. The combination of these factors is creating a big problem for enterprises.

The good news: you can do something about it. A powerful arsenal of network defenses is available that can help you safeguard points of infiltration on your network, protect against even the most advanced threats, and radically accelerate your ability to detect and mitigate them. And the **really** good news? Many of those defenses are already at your fingertips in the Cisco network you already have deployed. So you can protect your intellectual property, your customer and financial data, and your reputation, while reducing the complexity and time to defend your business.

Ready to learn more? Keep reading.

The Growing Threat

Security analysts used to say it's not a question of if you'll be attacked but when. Today, the facts are even more alarming: we no longer need to wonder when your network will be targeted. Your business is under attack right now. According to the Cisco 2014 Annual Security Report, threat alerts grew 14 percent in 2013 from the previous year, most of which were new threats, not updates. And despite companies' best efforts, millions of records are stolen from the largest business and public sector networks each year.

Cisco Security Services teams have worked with hundreds of enterprises in the last year, including dozens of Fortune 500 companies. These are among the largest multinational companies in the world that invest millions of dollars and countless hours to protect their networks. Every day, Cisco Security Services blocks 80 million web requests to malicious sites and detects 50,000 network intrusions.

A Growing Enterprise Attack Surface

As fast as malicious threats are growing, the number of potential points of infiltration into your business is growing even faster. There are now many more endpoints and inroads into your network than a decade ago and so much data that's not under enterprise control.

According to Cisco analysts, nearly 80 percent of U.S. white-collar workers now use a mobile device for work purposes, and more than half of IP traffic worldwide will be mobile by 2017. Every new device, especially those over which you don't have total control, is a potential target for attack.

The same is true for your data and applications, more and more of which are now hosted in the cloud. The Cisco Global Cloud Index forecasts that the amount of cloud traffic worldwide will triple by 2017, and businesses will experience a 44 percent increase in cloud workloads annually.

Things will only grow more complicated with the rise of the IoT. Cisco forecasts 50 billion smart objects connecting to the world's networks by 2020, any number of which can serve as a target to be compromised or a potential launch pad for further attacks.

More Sophisticated and Hard-to-Detect Threats

As adversaries have grown more sophisticated and better funded, the threats have become far more dangerous. If you follow the evolution of attacks, you'll see how threats have changed from relatively easy-to-contain viruses to more advanced worms and rootkits to sophisticated spyware, and now, to advanced persistent threats (APTs).

Today, cybercrime is a major global business. What started as not very sophisticated phishing attempts now includes Attack-as-a-Service offerings from billion-dollar criminal syndicates. These cybercriminals build highly-targeted malware that produce attacks that are customized to target your specific vulnerabilities based on extensive surveillance of your networks and business practices by criminals who often know more about your network than you do. They include APTs that can remain on your network for months as they gather data about your network, devices, and users to launch attacks from elsewhere in your environment.

Slow and Complex Mitigation Processes

The growing complexity of your network and application environment also applies to security. You're dealing with many more network endpoints, applications communicating inside and outside your enterprise, and security systems from multiple vendors that often don't talk to each other and require separate management and mitigation processes. The result is that even as you add more defenses to try to keep pace with the bad guys, your threat response gets slower and more complicated.

The 2014 Data Breach Investigations Report from Verizon found that nearly 90 percent of malicious breaches take only minutes to compromise an asset. According to the Ponemon Institute, attacks take an average of 80 days to discover and 123 days to resolve.

These threats are not just hypothetical, they're already happening. In just the last few years, there have been nearly 3000 major enterprise breaches with confirmed data loss, including:

- More than 100 million credit card and personal information records stolen through attacks on retail point-of-sale (POS) systems
- Tens of millions of e-commerce user accounts hacked
- Millions of customer email records stolen through phishing attacks as well as against cloud and application service providers

How confident are you that your business is safe?

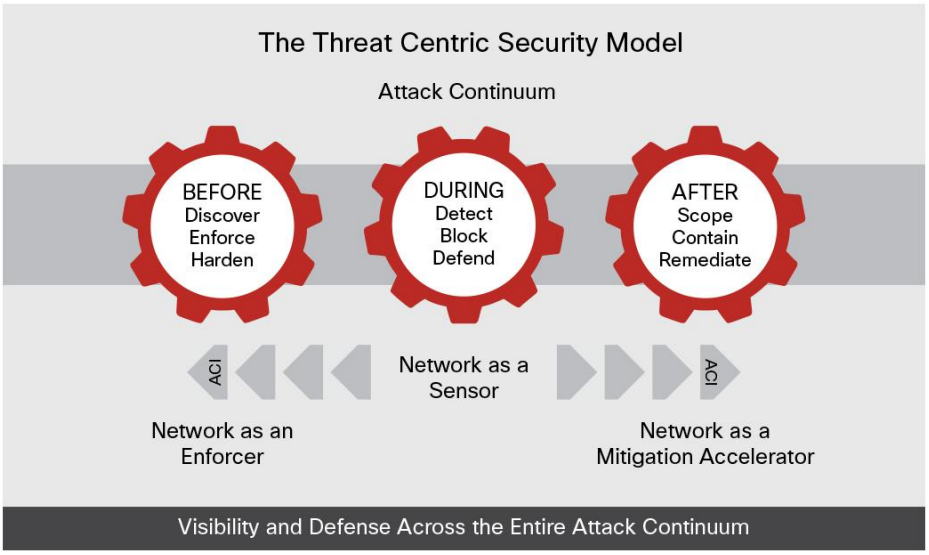
Taking a Network Approach to Information Security

Despite the diversity of malicious threats, security systems, and devices that present a potential entry point into your business, there is one thing they all have in common: they all operate and communicate over your network. That common thread is why the enterprise infrastructure is the best platform for monitoring and protecting your business. The network doesn't replace your various security systems, such as malware protection, perimeter security, and secure policies and procedures, but it can complement and empower them to further safeguard your customers and data.

Cisco provides a broad portfolio of capabilities to improve your defenses across the entire attack continuum (Figure 1):

- **Before an attack:** Use the network as a sensor and inspector to achieve broader and deeper visibility into your environment to detect the undetected and know your normal
- **During an attack:** Use the network as a sensor and as an enforcer to contain the attack and help to prevent access to sensitive resources
- **After an attack:** Use the network as a sensor and enforcer through new software-defined networking (SDN) capabilities to automate your threat response and achieve near real-time infrastructure updates across large enterprise networks, accelerating threat defense and mitigation

Figure 1. Capitalizing on the Network for Threat Defense



Translating Security Intent into Network Action with Cisco ACI

Further complicating an enterprise's ability to enforce security and quickly respond to threats is the state of modern enterprise security policy. Historically, policy has been based on infrastructure, that is, defining and enforcing rules for which users and devices can connect with which assets, IP addresses, and network segments. But explosive growth in virtual resources, cloud applications, and employee devices has made enterprise networks much more complex. For security to keep pace with these changes, enterprise policy frameworks must become smarter and faster.

Cisco Application-Centric Infrastructure (ACI) is a new policy paradigm for the modern enterprise. It provides a common, centralized policy-based operational model that extends from the data center throughout the enterprise network. You can use Cisco ACI to define and enforce security policy much faster and more efficiently.

Cisco ACI centralizes and automates policy based on application profiles. You can define security policy based on applications and users independent of specific network segments, IP addresses, or connectivity methods. Using new network programmability capabilities provided through the Cisco Application Policy Infrastructure Controller (APIC) Enterprise Module, you can use Cisco ACI to make security configuration changes and threat response actions once, centrally. The Cisco APIC Enterprise Module then propagates them throughout the network and automatically enforces them everywhere. In this way, Cisco ACI can help you align your security policy with the complex real-world network environment in which your business operates and dramatically accelerate your ability to mitigate threats.

Cisco provides a broad portfolio of the latest security capabilities to protect your business before, during, and after an attack. By tapping these capabilities, you can use your network as:

- **A sensor:** Identify the malicious traffic flows, policy violations, and compromised devices that otherwise might go undetected, detect the undetected and know your normal.
- **An enforcer:** Segment the network to contain attacks and limit the attack surface; encrypt your sensitive traffic and secure your branch locations.
- **A mitigation accelerator:** Automate threat mitigation and remediation response across the network.

Let's take a closer look at what your Cisco network can do to protect your business before, during, and after an attack.

The Network as a Sensor

You can't protect what you can't see. But in a world where your data travels among tens of thousands of devices and people inside and outside your enterprise, how can you know what's happening out there? Cisco provides the tools you need to detect suspicious traffic flows, policy violations, and compromised devices anywhere in your environment. Many of those tools are already in your network, ready to be activated.

NetFlow at the Heart of the Network as a Sensor

Cisco IOS Flexible NetFlow is a powerful information source for every network conversation. It captures each and every network conversation over an extended period of time. It is able to characterize IP traffic and identify its source, traffic destination, timing, and application information providing information much like that contained in a telephone bill, that is, who was called, when, and for how long.

Cisco IOS Flexible NetFlow can be used as a critical tool to identify a security breach. It helps to identify anomalous activities, provide forensic evidence to reconstruct sequence of events, and be leveraged for regulatory compliance. Cisco IOS Flexible NetFlow data can drive security alerting and network automation, and can be stored for future forensic analysis.

An important distinction should be drawn between Cisco IOS Flexible NetFlow and a “lite” or other sample-based approach to NetFlow. Security requires a complete Cisco IOS Flexible NetFlow approach, because you want to be able to identify all flows to detect malicious traffic, rather than a small percentage that can drop critical information.

Exploit the Power of Your Cisco Network to Detect Threats

Your network is the playing field on which every device, traffic flow, application, user, and malware attack operates. If it happens in your business, it happens on your network, which means you can see it if you know how to look. Cisco infrastructure and security solutions give you a powerful platform to gain visibility, control, context, and analytics across the following.

- **Devices:**
  - Detect rogue access points with the Cisco Aironet® Access Point Module for Wireless Security for Cisco Aironet access points.
  - Detect compromised or noncompliant devices with the Device Sensor capabilities embedded in Cisco Catalyst® switches and the Cisco Identity Services Engine (ISE), which provides a central point of contextual identity and policy control across Cisco wired, wireless, and VPN infrastructures.
  - See when the reputation of any internal or external device changes with Cisco IOS Flexible NetFlow data and analytics intelligence with Lancope StealthWatch System capabilities. The Lancope StealthWatch System provides a powerful interactive interface for analyzing network data, while optimizing that data, so you can store more of it for longer.
- **Traffic:**
  - Detect suspicious traffic pattern anomalies, malware command and control traffic, and APTs by analyzing contextual traffic flow data using Cisco IOS Flexible NetFlow, Lancope StealthWatch, and Cisco ISE.
  - Defend against network denial of service (DoS) attacks with the Cisco IOS Software Control Plane Policing features in Cisco infrastructure devices and the Cisco CleanAir® technology in Cisco wireless access points and wireless LAN controllers.
- **Applications:**
  - Recognize a wide variety of applications and detect application behavior anomalies with Cisco IOS Flexible NetFlow and Next Generation Network Based Application Recognition (NBAR2).
- **Users:**
  - Identify users attempting to violate access policy with complete contextual user and device information provided by Cisco ISE and by the Cisco TrustSec® Security Group Tag (SGT) capabilities in the Cisco routers, switches, and access points you have deployed right now.

- **Malware:**
  - Detect malicious email and web traffic across your distributed enterprise with the Cisco ScanSafe security features embedded in Cisco branch routers and Cisco Cloud Web Security.
  - Identify a broad range of malware attacks, intrusions, botnets, SQL injection, and more, with Cisco Intrusion Prevention System (IPS) modules for Cisco routers, switches, and security appliances, and Cisco Adaptive Wireless IPS Software in Cisco wireless infrastructure.
  - Detect sophisticated APTs using the Cisco Advanced Malware Protection for Networks capabilities, which are integrated with Cisco web and email security appliances and Cisco Cloud Web Security services.
  - Detect quickly internal malware propagation and data exfiltration with the Cisco IOS Flexible NetFlow and Lancope StealthWatch System traffic-analysis intelligence integrated with Cisco infrastructure and security solutions.
  - Get early warning intelligence to detect new emerging threats from Cisco Security intelligence operations.

No other vendor can deliver the scope of network infrastructure security visibility and threat detection capabilities that Cisco can provide, nor products that capitalize on the enterprise network investment you've already made that Cisco solutions can.

The Network as an Enforcer

Your network is not only well positioned to detect sophisticated threats but as the infrastructure connecting every user and device to every piece of information in your business, it's also a good place to enforce your security policy, control access, and block and isolate threats.

Your Cisco enterprise network provides the critical capabilities you need to:

- Contain attacks, block potential points of infiltration, and prevent threats that get through to your network from causing widespread damage
- Encrypt communications where appropriate to protect data from malicious actors capitalizing on your sensitive traffic
- Provide secure, scalable direct Internet access with comprehensive threat defense at distributed branches

Containing the Attack

A longstanding practice of successful military campaigns is divide and defend, that is, press a strategic advantage by dividing territory into smaller, contained areas that are more easily protected. The same principle holds true on your network.

Instead of having a large open network environment where everything can freely access everything else, you can contain attacks by segmenting the network. In this way, you can tightly control who and what can access various resources. And even if your network is hit with a zero-day attack, APT, distributed DoS (DDoS), or infected device, you can limit it from having a widespread impact. You can contain attacks by the following.

- **Segmenting the network:**
  - Use the Cisco TrustSec solution with Cisco ISE to segment your network and enforce role-based, topology-independent, and access-independent access control. With Cisco TrustSec technology, you can block access to network segments and resources by context and user, device, and location according to your security policy. For example, you can set a policy that only traffic with a SGT from an authorized Finance Department user can access Finance resources. With SGTs, a user with maintenance contractor credentials is blocked from accessing Finance data, regardless of network topology or whether this contractor was using wired or wireless access to the network. (You can immediately detect that user with the wrong job descriptions are attempting to access a resource for which they not authorized).
  - Simplify regulatory compliance efforts using network segmentation capabilities. For example, by segregating the parts of the network that process financial or health information data from the rest of the environment, a company can reduce the scope, cost, and complexity of the Payment Card Industry Data Security Standard (PCI DSS) and Health Insurance Portability and Accountability Act of 1996 (HIPAA) network compliance audits.
- **Applying granular and consistent access control:**
  - The Cisco Unified Access™ network platform provides a framework for applying consistent policies and a consistent user experience across your wired and wireless domains. Combined with Cisco ISE, and the capabilities embedded in your Cisco infrastructure, you can control access based on user, device, location, time of day, connection type, and more, and apply a uniform access control policy across all access methods: wired, wireless, and VPN.
  - Cisco ISE automates and simplifies network access control, which is especially important for companies that launch bring-your-own-device (BYOD) initiatives. For example, you can allow executives to access certain sensitive resources when they're logged on to a corporate PC at the office, but not from their smartphones or home computers.

Encrypt Traffic to Protect Your Data in Motion and Prevent Prying Eyes

Your Cisco network is your best defense against prying eyes. It gives you the tools to do the following.

- **Encrypt data in motion where appropriate:**
  - Cisco network routers, switches, security platforms, and wireless infrastructure provide built-in capabilities to encrypt traffic across wired (MACsec), wireless (Datagram Transport Layer Security [DTLS]), and WAN (IPSec, SSL) connections.
  - Cisco ISE also supports mobile traffic encryption as part of Cisco Mobile Device Management (MDM) partner integration capabilities.
- **Prevent spoofing:**
  - Cisco Catalyst integrated security feature set (Port Security, DHCP Snooping, IP Source Guard, Dynamic ARP Inspection), and the Cisco IPv6 First Hop Security (FHS) features embedded in Cisco routers, switches, and wireless LAN controllers protect against spoofing.
  - Cisco CleanAir technology protects against rogue access points and wireless spectrum attacks.

Secure Communications at the Branch

Branch offices present attractive targets for cybercriminals, because their smaller size and distance from the main corporate security infrastructure too often translate to a weak spot in an enterprise's defenses. Using advanced Cisco security solutions combined with the security features embedded in the Cisco branch routers you already deployed, you can wall off malicious Internet traffic before it can infiltrate the rest of your network.

Your Cisco network can provide:

- **A secure branch edge** with Cisco Integrated Services Routers (ISRs) that support strong local firewalling, intrusion prevention systems, and VPN connectivity to block external threats
- **Secure traffic segmentation** that uses Cisco Intelligent WAN capabilities in Cisco branch routers to securely offload traffic from the WAN with rich application and security services
- **Protection against malicious websites** through real-time web filtering enabled by Cisco Application Visibility and Control (AVC) features in Cisco ISRs, and advanced malware protection and threat analytics from Cisco Cloud Web Security

You've already invested in a Cisco network. Take advantage of the full potential of that investment to protect your business during an attack by activating the network segmentation, encryption, and distributed branch security capabilities it can provide.

The Network as a Mitigation Accelerator

Your Cisco network provides a broad range of capabilities to help you detect suspicious behavior and enforce your security policy. But your adversaries are intelligent, well-funded, and relentless in their attempts to infiltrate your business. How quickly can you respond when you discover a breach?

New Cisco security solutions exploit the power of SDN and network programmability, combined with Cisco Prime® Infrastructure management and the capabilities embedded in your Cisco network infrastructure and security solutions, to radically accelerate your threat response.

Accelerate and Automate Mitigation

The heart of advanced mitigation capabilities is the Cisco Application Policy Infrastructure Controller (APIC) Enterprise Module. Cisco APIC Enterprise Module extends the Cisco ACI vision from the data center to the enterprise network. With it, you can create application profiles based on policy, so you can create a programmable network environment you can use to take action for threat detection, mitigation, and access control list (ACL) management centrally, and automatically propagate them across the network.

This automated network programmability is particularly crucial for network changes affecting security. Consider two examples:

- **Threat detection and response:** Imagine the threat intelligence technology integrated in your Cisco infrastructure detects a threat in a device in one building on your main campus. To block the threat you may need to make an ACL change. In the past, you would have to manually provision that change across every infrastructure device in your environment, a process that takes days, or more likely, weeks. But with Cisco APIC Enterprise Module, you need to make the ACL change only once. Cisco APIC Enterprise Module then automatically provisions it across the entire global enterprise network, every campus, every branch within hours.

- **Proactive ACL management and error correction:** A typical enterprise has thousands of lines of ACL code on every switch and router. A single misconfiguration anywhere in your enterprise network can leave you vulnerable to an attack or compliance failure and requires many hours to detect and fix using traditional manual processes. In the same way that Cisco APIC Enterprise Module propagates an ACL change when responding to a threat, it can also monitor the network to assure that all devices have the correct ACLs and identify and help fix those that don't. With Cisco ACI you can have a single consistent security compliance policy that is checked periodically from data center to WAN and access to your network to ensure that no changes are violating your overall security policy.

These capabilities save you countless hours and resources with your network security management and in your operations. But even more important, they empower you to respond to malicious threats anywhere and everywhere in your business in a fraction of the time it takes today.

Five Steps to Help Defend Your Network

The threat to your business from malware and cybercriminals is significant and growing. Fortunately, so are the defensive capabilities of your Cisco network. To protect your data, your customers, and your reputation, take full advantage of your Cisco network investment by following these five steps:

1. **Enable** Cisco IOS Flexible NetFlow to understand your baseline for normal traffic and proactively identify suspicious behavior.
2. Deploy Cisco TrustSec network segmentation **technology** to contain attacks and shrink the attack surface with contextual, role-based topology and access independent control.
3. **Encrypt links** and use Cisco Catalyst integrated security features to protect your data in motion.
4. **Deploy** Cisco Intelligent WAN to secure branch offices with direct Internet access.
5. **Deploy** Cisco APIC Enterprise Module to accelerate security configuration and threat mitigation.

For More Information

To learn more about how you can harness the power of your Cisco network to defend your business, visit http://www.cisco.com/go/en.

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 C11-733382-00 12/14