Cisco Threat Defense for Borderless Networks

Executive Summary

Traditional security techniques are unable to respond to threats that can arise from anywhere. To protect today's borderless networks, IT managers must adapt by implementing faster, smarter security measures that monitor the constantly changing global landscape.

This white paper, written for IT managers and executives, examines the security risks and needs of borderless networks, details a systematic plan of action, and describes how Cisco can help implement threat defenses that will serve you today and for years to come.

Today's Networks Are Borderless

In the not too distant past, data-center and branch-office networks were protected by perimeter firewalls backed by policy-based rule sets. The Internet world at large was kept outside the firewall perimeter, although VPNs and other technologies could grant controlled access to specified individuals, usually partners and customers. The perimeter was the borderline where all policies were set and policy enforcement systems were located. Although it could be complex to manage, the architecture was straightforward to understand and police.

Today, the way organizations conduct business and access information is radically different. Mobility, virtualization, cloud computing, and social networking applications are expanding what can be accomplished remotely, pushing productivity to new levels. These applications are also challenging security norms: The perimeter of the traditional enterprise network is dissolving, with data entering and exiting from many directions. Recognizable borders no longer exist.

The rise of the borderless enterprise is a call to action for IT managers, who must start thinking differently about their enterprise security strategies.

Today's Network Threats Are Shape-Shifters

Today's threats are increasingly complex—attacks come from all directions and at rapid speeds, and no two threats are the same. There are hundreds of application, operating system, driver, and firmware updates annually, each with possible undiscovered vulnerabilities, creating virtually unlimited network entry points.

Once those vulnerabilities are found, hackers move quickly to mount both day-zero and well-publicized threats faster than software and operating system vendors can develop patches and workarounds. In addition to broad-scale malware and virus outbreaks, hackers create network threats specifically designed to avoid detection and bypass traditional defenses. Often the exploits are so targeted that there are no signatures to stop them.

Internal and external threats can be characterized by the following "rap sheet":

- Threats are persistent, sophisticated, and constantly mutating
- Each attack instance is slightly different
- Content mutates and mimics legitimate traffic
- Domains are rotated in days, even hours
- The vast majority of bots use dynamic IP addresses

Where Network Threats Gain Access

There are three primary vectors for network attacks: communications applications, infected systems, and internal propagation.

Communications Applications

Email, websites, file transfers, instant messaging (IM), and social media all have the potential to introduce myriad threats to unsuspecting users. Unfortunately, many users assume these communications vehicles are secure, so they do not take extra measures to protect themselves.

Email and IM: Inbound spam can contain spoofed web links for phishing purposes or attachments infected with spyware, viruses, and other malware. Outbound email and IM create “holes” through which information can leak or be leaked, leading to user privacy concerns and the potential loss of intellectual property.

Websites: Spoofed and fraudulent websites with tiny bits of malicious code can be difficult to detect and monitor. Even worse, threats from legitimate domains are growing exponentially. No longer can you just block suspicious URLs; now, even the local bank website can be infected, and can unknowingly harbor and propagate malware. According to data collected from Cisco Security Intelligence Operations (SIO), one in every 600 PDFs downloaded from the web contains malicious software (Cisco Security Report 2009). Cisco SIO calculated that threats from legitimate domains grew 190 percent in 2008.

Application and operating system vulnerabilities: As previously noted, software and firmware updates create unlimited opportunities for trouble. Hackers simply exploit a weakness in an Internet browser or publishing application to bypass security defenses and infect computer systems.

Infected Systems

Mobile devices have the potential to pick up infections from various sources, and can introduce these infections into the corporate network. To add to the problem, personal devices such as iPhones and Androids, increasingly used by corporate users, are frequently unmanaged by the IT department, and therefore lack enterprise-grade security. External threats can also come from unauthorized users, or from someone using a lost or stolen mobile device to attempt to access a corporate network.

Internal Propagation

According to our own research, 80 percent of spam comes from infected clients—a startling statistic (Cisco Security Report 2009). Despite best efforts at preventing the infection of internal systems, malware still manages to bypass security controls, activate, and distribute copies of itself to other trusted systems.

Employees can also compromise a secure network by bringing in private, unauthorized wireless access points to gain access to network resources. Unauthorized users can also circumvent missing or incomplete switch or server authorization measures and access configuration data.

New Security Needs for IT

To manage and secure today’s borderless networks, IT managers need an adaptable threat defense with interacting components across all layers of the infrastructure. The defense requires tight linkages between the security intelligence elements and policy management to proactively defend against a wide array of threats and reduce the mean time to respond to and mitigate them.

Farsighted vigilance: New and zero-day threats are difficult to defend against because of the time it takes to develop signatures or knowledge to counteract them. IT departments need automatic processes and tools that can proactively stop attacks, regardless of origin, from circumventing security defenses.

360-degree threat visibility: IT managers need global visibility that spans the infrastructure and dives deep into system components. They need tools that operate in real time to detect policy violations, vulnerability exploits, and the kind of anomalous behavior that signals the suspicious presence of harmful traffic. The accuracy of these detection and prevention tools is important, because it reduces the amount of data IT staff must sift through and analyze before responding.

Unceasing protection: To make sure that new threats do not enter the network from otherwise trusted users and devices, IT managers need continuous endpoint security protection, posture checking, and validation. Authentication methods must accommodate bandwidth-intensive applications, filtering out threats without introducing latencies. Protection must extend to mobile and wireless devices, because they provide potential launching points for network attacks that are typically not handled by existing antivirus and antispyware software.

Simpler threat control management: IT departments are continually expanding their tool portfolios to combat threats, which generally results in more systems, more processes, more alarms—more complexity. IT managers need to bring these elements together under a cohesive architecture in a way that reduces day-to-day management and improves efficiency.

Fighting Back: A Systems Approach to Threat Defense

Your best defense is a strong offense. The best way to take control of network security risks and compliance requirements is through a systematic, architectural approach built on a standards-based network security infrastructure. A comprehensive, proactive security strategy is a constantly evolving process; identifying the crucial tasks is an important first step.

Security Evaluation and Rework Steps	Cisco Service Resources
Step 1: Review network security at the system component and network levels to determine your strengths and weaknesses. The assessment can help you address both immediate and long-term needs. Once you've created a baseline, you can add security technology in phases to meet your business requirements.	**Cisco Security Assessment Services** can identify gaps in your security infrastructure, evaluate regulatory compliance policies and procedures, and examine all or specific elements of your security operations. For information on these services, visit: http://www.cisco.com/go/securityconsulting
Step 2: Deploy new security elements based on a clear understanding of your overall security architecture. • Strengthen your perimeter security and ensure it does not introduce latencies • Secure major communications/content vehicles • Fortify the remote sites of your organization • Ensure security and policy is enforced throughout the network • Add wireless and mobile security and policies • Expand and increase the effectiveness of your compliance and policy management	**Cisco Security Design Services** can help you develop a strong threat defense plan. For information on these services, visit: http://www.cisco.com/go/securityconsulting
Step 3: Maximize the efficacy of your existing infrastructure: Can you add or repurpose components, adding security to data center switches and remote routers? Incremental changes to existing systems can dramatically improve the security posture of your organization and extend your network equipment ROI.	**Cisco Security Deployment Services** bring sound network integration expertise to accelerate successful implementation. For information on these services, visit: http://www.cisco.com/go/securityconsulting
Step 4: Consider services that can distill the numerous security advisories and focus them on the threats that are directly relevant to your organization or industry.	**Cisco IntelliShield Alert Service** can help minimize the time spent reviewing new threat alerts from groups such as CERT or SANS. For more information on this service, visit: http://www.cisco.com/go/intellishield

Cisco Threat Defense: Powerful Players on Your Team

Armed with your strategy, you can team up with Cisco to implement a threat defense that will serve you today and for years to come. We believe the most effective proactive threat control solution combines comprehensive policy control and timely threat correlation and alarm management systems, backed by a global security intelligence operation.

Cisco combines key threat defense strategy components to secure today's borderless networks.

- Firewalls and VPNs
- Intrusion detection and prevention
- Email and web security
- Endpoint security
- Compliance and policy management
- Real-time global security intelligence

Table 1: Cisco Threat Defense Product and Services Offerings summarizes the featured Cisco security products and the areas they protect.

Cisco offers integrated and standalone onsite modular, scalable platforms as well as in-the-cloud and hybrid offerings. Products such as Cisco® ASA 5500 Series Adaptive Security Appliances provide intelligent threat defense and highly secure communications services, integrating industry-leading firewalls, unified communications security, VPN technology, intrusion prevention, and content security in one unified platform. Other products include integrated hardware or software modules that add powerful security features to existing Cisco routers and switches, extending the value and lifetime of your network equipment.

You can deploy solutions independently to secure specific areas of your network infrastructure, or combine them for a layered, defense-in-depth approach.

Firewalls and VPNs

Firewalls have always been the starting point for threat prevention. They are the first and last lines of Internet defense and can provide invaluable information on the status of the network at any given time.

Cisco's flexible, integrated firewall solutions:

- Standalone Cisco ASA 5500 Series Adaptive Security Appliances offer a wealth of services, from advanced application-aware firewall, voice over IP (VoIP), and multimedia security, locating and stopping malware-infected endpoints from propagating threats, intrusion prevention using global threat correlation, to robust site-to-site and remote-access IP Security (IPsec) VPN connectivity.
- The Cisco Firewall Services Module (FWSM) for Cisco Catalyst® 6500 Series Switches and Cisco 7600 Series Routers is a good solution for enterprise and service provider data centers and campus distribution points.
- Cisco IOS® Firewall software runs on numerous branch office Cisco routers. This option lets you take advantage of other advanced routing capabilities.

Intrusion Detection and Prevention

Cisco intrusion prevention system (IPS) solutions protect against increasingly sophisticated attacks, including worms, botnets, malware, and application abuse. When implemented at all points of entry to the network, and at various internal demarcation points within a corporate Intranet, IPS tools can rapidly and accurately identify different types of global blended threats and exploit attempts, vulnerability signatures, the reputation of the perpetrator, and anomalous behavior—and stop attempts before they cause damage. Using global threat correlation, powered by Cisco Security Intelligence Operations, Cisco IPS solutions can automatically correlate multiple threat parameters, for a more effective and accurate IPS sensor.

Cisco's flexible, IPS options:

- Standalone IPS 4200 Series Appliances dedicated to preventing threats using Global Correlation
- Integrated IPS on the Cisco ASA 5500 Series Adaptive Security Appliances combine online prevention services with high-performance firewalls to provide solutions for small offices up to enterprise data centers.
- The Intrusion Detection System Module (IDSM-2) for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers inject intrusion prevention directly into the network infrastructure.
- Cisco IOS IPS software for Cisco Integrated Services Routers manage security for remote site and branch offices.
- The companion Cisco Services for IPS provides ongoing signature file updates, operating system and application software updates, and hardware and software support to assure maximum coverage and detection.

Email and Web Security

Cisco content security tools scrub email, IM, and web transmissions for malware, adware, and spyware, as well as phishing, spam and malicious content. Remote gateway content security and policy enforcement helps ensure that users are going to the correct websites, securing network endpoints and infrastructure, particularly on unmanaged devices or where users have turned off security controls.

Cisco's flexible email and web security options:

- Cisco IronPort® Email Security Appliances are easy-to-deploy solutions that block a wide variety of threats. Eight of the ten largest ISPs and more than 40 percent of the world's largest enterprises use IronPort products.
- Cisco IronPort Web Security Appliances integrate web usage controls, reputation filtering, malware filtering, and data security. The appliances use Cisco SIO and global threat correlation to optimize detection and mitigation.
- Cisco IronPort Hosted Email Security is a dedicated service residing in Cisco data centers. The service bundles software, hardware, and support together for optimum simplicity.
- The ScanSafe cloud-based security service scans all web content, extending real-time protection and policy enforcement to employees wherever and however they access the Internet.

Endpoint Security

Cisco endpoint security validates the security posture of endpoints, including wireless and mobile devices, before network access is granted, preventing inadvertent admission over trusted links. Implemented with consistent corporate policies, endpoint security can increase convenience and flexibility for all authorized users. Cisco endpoint protection also limits access to internal systems, networks, and applications to dramatically reduce the accidental or intentional introduction of threats to the infrastructure.

Cisco's featured flexible endpoint security options:

- Cisco Network Admission Control (NAC) Appliances enforce security policies, allowing access only to compliant and trusted devices.
- Cisco Secure Access Control System (ACS) Software controls network access based on dynamic conditions and attributes.
- Cisco TrustSec™ software on Cisco Catalyst switches examines endpoint devices before allowing access via wired, wireless, or VPN connections. It enforces security policies across the entire network, protecting network data confidentiality and integrity at the switch port level.
- Cisco ASA Botnet Traffic Filter (or Cisco Layer 4 Traffic Monitor) detects malware-infected endpoints and blocks them from sending "phone-home" traffic to command and control host machines.

Cisco's featured flexible wireless and mobile security options:

- Cisco Adaptive Wireless IPS software integrated into the network infrastructure automatically monitors wireless vulnerabilities and rogue access points, collaborating with Cisco products to create a layered security approach.
- The Cisco AnyConnect Secure Mobility solution secures the remote workforce using the AnyConnect client, Cisco IronPort Web Security Appliance, and Cisco ASA 5500 Series security appliance for context-aware, preemptive, continuous protection.
- The Cisco Virtual Office solution consists of Cisco integrated services routers and IP phones, VPN routers, and centralized policy management to extend secure remote network services outside the office environment.

Compliance and Policy Management

Security, network, and host devices often generate tremendous volumes of data during security events. Processing this information manually can overload IT groups, making standard tools ineffective and making it nearly impossible to find threats in real time.

Managing the volume of alarms and information and assuring minimal damage during an event is crucial. Cisco's coordinated policy management and event visibility tools can reduce response times by up to 90 percent by automatically looking for patterns, correlating events into risk categories, and determining a best course of mitigation. They also help assure conformance to governance policies and regulations.

Cisco's featured flexible security compliance and policy management solutions:

- Cisco Security Manager management software simplifies and consolidates configuration and management for Cisco firewalls, VPNs, IPS sensors, and integrated services routers. Cisco Security Manager is ideal for large, complex network deployments.
- Cisco Security Information and Event Management (SIEM) technology partners are authorized vendors backed by Cisco security devices. These partners provide long-term log archiving, forensics, and compliance reporting services for heterogeneous environments.
- Cisco IronPort Security Management Appliances centralize reporting, message tracking, spam quarantine, and management across IronPort email and web security products.
- Cisco Remote Management Services (RMS) for Security provides 24x7x365 protection against attacks, malware, and security vulnerabilities. The service is backed by a dedicated team of highly skilled experts acting as an extension of your IT organization.

Table 1: Cisco Threat Defense Product and Services Offerings

Cisco Products and Services	Firewall and VPN	Intrusion Detection and Prevention	Web Security	Email Security	Endpoint Security	Wireless Security	Compliance and Policy Management
Appliances							
Cisco ASA 5500 Series Adaptive Security Appliance	√	√	√		√ with ASA Botnet Traffic Filter	√ with Cisco AnyConnect Secure Mobility Solution	
Cisco IPS Sensor Appliance		√					
Cisco Network Admission Control (NAC) Appliance					√		
Cisco IronPort Web Security Appliance			√			√ with Cisco AnyConnect Secure Mobility Solution	
Cisco IronPort Email Security Appliance				√			
Cisco IronPort Security Management Appliance			√	√			√
Integrated Security							
Cisco Integrated Services Routers (ISRs)	√ with Cisco IOS Firewall software	√ with Cisco IOS IPS software				√ with Cisco Virtual Office solution	
Cisco Catalyst 6500 Series Switches	√ with Firewall Services Module	√ with IDSM-2			√ with TrustSec software		
Cisco Secure Access Control System (ACS) Software					√ on servers		
Cloud-Based Services							
ScanSafe Web Security			√				
Cisco IronPort Cloud Hybrid Email Security				√			

Management Software and Services							
Cisco Security Manager	√	√					√
Cisco SIEM Technology Partners	√	√	√	√			√
Cisco Remote Management Services (RMS) for Security	√	√	√	√			√
Cisco Security Intelligence Operations (SIO)	√	√	√	√	√	√	√

Cisco Security Intelligence Operations

Cisco Security Intelligence Operations is the back-end security ecosystem that powers Cisco Threat Defense components. The cloud-based service combines global threat information, reputation-based services, and sophisticated analysis to deliver stronger protection and faster response times.

Cisco Security Intelligence Operations (SIO) consists of three pillars:

- Cisco SensorBase, a global, real-time, and historical threat and vulnerability analysis and mitigation database, using more than 700,000 live threat feeds across email, web, firewall, and IPS systems.
- The Cisco Threat Operations Center, staffed by more than 500 security experts around the world who research vulnerabilities, as well as automated systems performing correlation and analysis using more than 200 parameters.
- Dynamic updates, every three to five minutes, automatically deliver the latest protection to Cisco devices and security best practices to Cisco customers to keep them informed and protected. Organizations can stay up to date with tools such as the Cisco IntelliShield Alert Manager or the Cisco SIO-to-Go iPhone application.

Summary

The threat landscape has changed. IT and security operations teams must combat an array of threats to the network infrastructure and simultaneously assure network access for all who need it. Many current and emerging threats take advantage of existing vulnerabilities, even though organizations can become distracted by emerging threats. It is important to focus time, energy, and resources on what is strategically, financially, and competitively most important to safeguard your organization and that means taking a close look at your entire security system.

Cisco provides robust, high-performance market-leading solutions to help organizations secure and manage their borderless networks, and backs them up with proactive intelligence from Cisco Security Intelligence Operations. To learn more about Cisco Threat Defense solutions, visit http://www.cisco.com/go/threatdefense or contact your local reseller. To find a reseller in your area, visit http://www.cisco.com/web/partners.

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 C11-609140-00 06/10