



Why Threat Control and Containment?

Network security threats have the potential to significantly impede productivity, disrupt business and operations, and result in loss of information—which can lead to financial losses and noncompliance. Hackers continue to develop new techniques to gain access to information, for their own financial gain, and these techniques are harder than ever to detect. Businesses need comprehensive solutions that are highly manageable and operational to proactively address these threats.

What Problems Need to Be Solved?

Businesses are faced with myriad security problems, such as:

- Employee and IT productivity during a virus or worm outbreak
- Security of confidential information
- Protection of company reputation and brand
- Communications disruptions and impacts to daily business
- Continuity of e-business applications

Examples of Real Threats Affecting Real Networks

- *Zotob virus for credit card forgeries*—The Zotob worm infected organizations including CNN, ABC News, the New York Times, Boeing, and the United States Department of Homeland Security in an effort to facilitate credit card forgeries. FBI investigators believe that the creator of Zotob may have been paid to create more than 20 other viruses.
- *"rxbot" trojan horse for financial gain*—The so-called rxbot trojan horse infected 400,000 computers with adware programs that netted its creator more than \$60,000 from pay-per-click advertising software makers. The alleged perpetrator was arrested in November 2005 on suspicion of compromising thousands of machines, including computers at the Weapons Division of the U.S. Naval Air Warfare

Center and those belonging to the U.S. Department of Defense's Defense Information Systems Agency.

- *Custom-based trojan for corporate intelligence gain*—Designers of a custom-based trojan horse are alleged to have created and distributed spyware aimed at corporate intelligence gathering and marketed the program to three private investigation firms. These firms then allegedly used the spyware to steal data from their clients' competitors. According to police, the program exploited operating system vulnerabilities using standard data capture methods, including keystroke logging, screen capture, and file transmissions. Police said this Trojan was planted via e-mail or a promotional computer disk supposedly sent to target companies by a well-known and reliable business contact, according to reports. Dozens of companies, including possible U.S. and European firms, may have been victimized.

Threat Control and Containment Solution

The Cisco Threat Control and Containment solution offers customers a comprehensive approach to controlling and containing threats, providing unparalleled protection from Internet-based and targeted attacks and intrusions for organizations of all sizes.

- *360° Visibility and Protection: Delivering comprehensive and proactive network defense*
 - Infrastructure-wide threat intelligence is delivered cost-effectively across a variety of systems and devices
 - Multivector threat identification captures policy violations, vulnerability exploits, and anomalous behavior
- *Simplified Control: Streamlining policy and management across the network*
 - Standardized policy management across multiple network components

- Infrastructure-wide implementation across a variety of systems and devices
- *Business Continuity: Ensuring the enterprise's operations*
 - Unparalleled collaboration and correlation across systems, endpoints, and management
 - Enables adaptive response to real-time threats
 - Core element of the Cisco Self-Defending Network strategy

Core Elements of the Threat Control and Containment Solution

- *Cisco ASA 5500 Series Adaptive Security Appliances*—Modular platform that provides the next generation of security and VPN services for environments ranging from small offices to large enterprises. <http://www.cisco.com/go/asa>
- *Cisco ASA 5500 Anti-X Edition*—Combats Internet threats at the gateway, including spyware, spam, viruses, and other threats associated with Internet content. <http://www.cisco.com/go/asa>
- *Cisco Security MARS*—Provides the security threat management interface that translates raw network and security data into actionable intelligence. <http://www.cisco.com/go/mars>
- *Cisco Intrusion Prevention System (IPS) solutions*—Protects servers, applications, and other critical assets from network and application attacks and worms, at the gateway, branch, data center, and throughout the LAN. <http://www.cisco.com/go/ips>
- *Cisco Security Agent*—Defends servers and desktops against targeted attacks, spyware, root kits, and day-zero attacks. <http://www.cisco.com/go/csa>
- *Cisco Network Admission Control (NAC)*—Validates user and system security credentials to protect the network and infrastructure from infection. <http://www.cisco.com/go/nac>

The Cisco Security Center web portal provides a single, integrated source of guidance on current security events including applied intelligence on how Cisco products and services can be used to mitigate new threats.

Lifecycle Security Services for Threat Control and Containment Solutions

- The Cisco Security Center portal provides a single, integrated source of guidance on current security events, including intelligence on how Cisco products and services can be used to mitigate threats.
- Cisco IPS Signature Subscription customers have access to the Cisco Security IntelliShield Alert Manager database, which provides comprehensive intelligence on IPS events and can correlate IPS signatures to IntelliShield alerts to speed remediation of potential attacks.

- Cisco IPS, Cisco Security MARS, Cisco NAC, and Cisco Security Agent deployment consulting services simplify the deployment of new solutions by Cisco experts using sound security design principles and network integration expertise.
- The Cisco IPS Remote Update and Tuning Service simplifies the day-to-day operations of IPS devices by deploying and tuning signature updates as they become available.

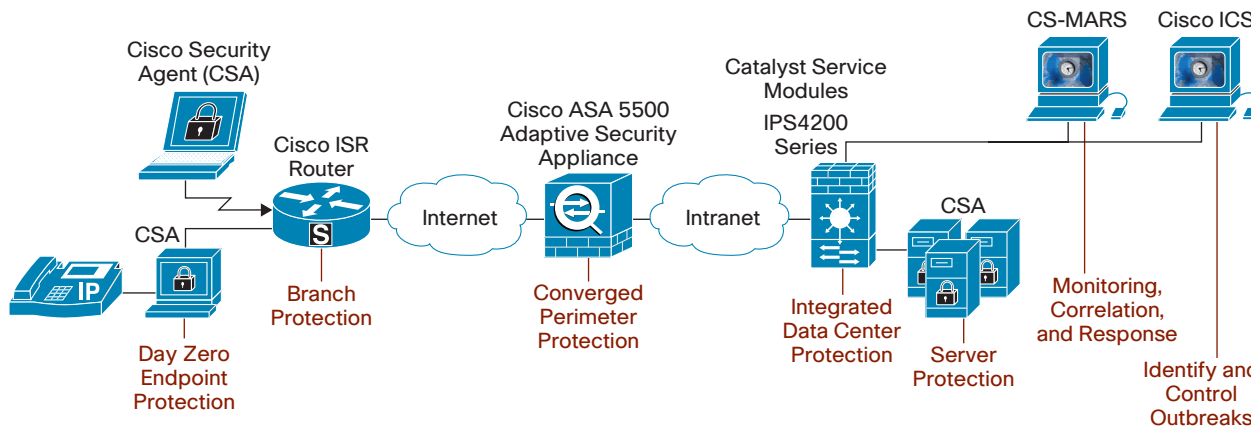
Where Do I Start?

Most organizations have tools in place that can be used as a starting point to comprehensive a robust threat prevention architecture. Technology can be introduced in phases as the security strategy for the company is revised. Security processes should be periodically reviewed to assure the organization is adopting best practices. A comprehensive, proactive security strategy

is a constantly evolving process; identifying the crucial points is an important first step. Refer to the Cisco Threat Control and Containment white paper, available from your Cisco **account representative**, for more details on how you can start your next phase of the security solution.

Why Cisco?

Cisco is the world leader in network security solutions. Cisco offers the broadest ability to combat threats across the entire IT infrastructure, from endpoint to network to management layer. Cisco's integrated, collaborative, and adaptive security solution comprehensively addresses the threats that face organizations today, helping to ensure IT and employee productivity and protection of an organization's most critical information assets. From Internet threats to targeted attacks and intrusions, Cisco solutions offer IT and security administrators the tools they need to defend their organizations in an era of increasingly complex, difficult to combat information security threats.



1 Source: <http://www.securityfocus.com/news/11297>

2 Source: <http://www.techweb.com/wire/security/177103378>

3 Source: TechWeb <http://www.techweb.com/article/showArticle.jhtml;jsessionid=U45GMNUB4Y4V0QSNLPSKH0CJUNN2JVN?articleId=181501294&pgno=2>