WHITE PAPER

MANAGED SECURITY SERVICES FOR IP COMMUNICATIONS: BUSINESS ADVANTAGES FOR THE ENTERPRISE

To enjoy the benefits of IP Communications for productivity, flexibility, and cost reduction, companies need to protect the network from viruses, worms, and intruders. Proven security solutions from Cisco Systems help protect the availability of the IP Communications network and the privacy of traffic traveling over the network.

OUT-TASKING SECURITY TO A MANAGED SERVICE PROVIDER IS A COST-EFFECTIVE WAY TO PROTECT THE IP COMMUNICATIONS NETWORK, APPLICATIONS, AND TRAFFIC.

EXECUTIVE SUMMARY

As companies increasingly rely on IP networks for communications among employees, customers, and partners, the importance of security soars. Without effective network security, threats such as viruses, worms, and hacker attacks can disrupt the business to cause a loss of productivity, customer confidence, and revenues. Preventing security breaches also avoids costly remediation efforts. The impact of network security threats experienced by businesses in the 2005 CSI/FBI Computer Crime and Security Survey were reported to exceed US$130 billion. Effective network security is also essential to ensure the privacy of confidential communications pertaining to financial information or strategic planning, for example.

To protect their IP Communications networks and ensure business continuance, companies need a comprehensive security strategy. Components of the strategy include securing the network from the desktop to the data center, designing solutions that can scale readily with business growth, and proactively protecting against rapidly spreading attacks with automated, regular virus updates.

Most companies lack the in-house security expertise to design and implement security solutions and then to monitor and effectively respond to network threats 24 hours a day. Often the most cost-effective option is to out-task security services to a managed security service provider (MSSP). Not only does out-tasking IP Communications network security give a company access to in-depth expertise and 24-hour monitoring and response, it frees internal resources to focus on strategic core activities.

Cisco Systems® has designed a suite of IP Communications security services that companies can acquire through MSSPs. This white paper describes the security challenges for businesses with IP Communications networks, explains proven ways to address the challenges, and provides a short overview of Cisco® managed security services available from MSSPs. The white paper concludes with descriptions of actual service offerings from MSSPs that belong to the Cisco Powered Network Program.

SECURITY CHALLENGES FOR IP COMMUNICATIONS

Network security threats have become more frequent, faster moving, and more damaging. In the 1980s, the most common threats were boot viruses that infected individual computers and took weeks to spread. In the 1990s, threats expanded to include macro viruses, e-mail viruses, denial-of-service (DoS) attacks, and limited hacking. This second generation of threats affected networks as well as individual computers, and in days rather than weeks. Today, companies must protect their business against a barrage of sophisticated threats including network DoS; blended threats combining worms, viruses, and Trojans; turbo worms; and widespread system hacking. Regional networks can be affected in just minutes. Looming on the horizon are new forms of infrastructure hacking, flash threats, massive worms, and damaging payload viruses with the potential to bring down global infrastructures in seconds.

Viruses, worms, and DoS attacks affect the availability of IP Communications applications. Companies also need security measures to prevent threats to information privacy and integrity. IP Communications are subject to the same threats as IP networks in general, which include:

- *Eavesdropping,* in which criminals try to listen in on or snoop a phone conversation. A security solution prevents unintended disclosure of information such as confidential financial data and strategic plans.
- *Impersonation*, when someone diverts calls intended for one person's IP phone or softphone to their own to receive calls intended for the other person.
- *Loss of integrity* that can result when the network lacks quality of service (QoS) or security. If someone reads a series of digits and the network has poor QoS, one zero might not be heard, transforming $100,000 into $10,000.
- *DoS attacks directed at voice servers and gateways.* These attacks can affect voice quality or even lead to loss of dial tone.

HOW TO SECURE THE IP COMMUNICATIONS NETWORK

Provide Privacy, Protection, and Control

Successful security solutions provide three essential components: privacy, protection, and control (Table 1). Only Cisco Systems provides all three components, integrating the technologies deep into the fabric of the network.

Table 1. Cisco Solutions for Privacy, Protection, and Control

Business Need	Cisco Security Solution	How it Works
Privacy—Intruders cannot listen to voice conversations or messages or view video traveling over the LAN or WAN	Secure connectivity	Encrypt communications for transmission over a secure VPN
Protection—Intruders cannot access the network to compromise devices, applications, or data	Threat defense systems	Block internal and external threats using firewalls and intrusion-prevention systems
Control—Only authorized people can access certain information, and at the allowed times	Trust and identity systems	Provide selective access to applications and data using access-control technology

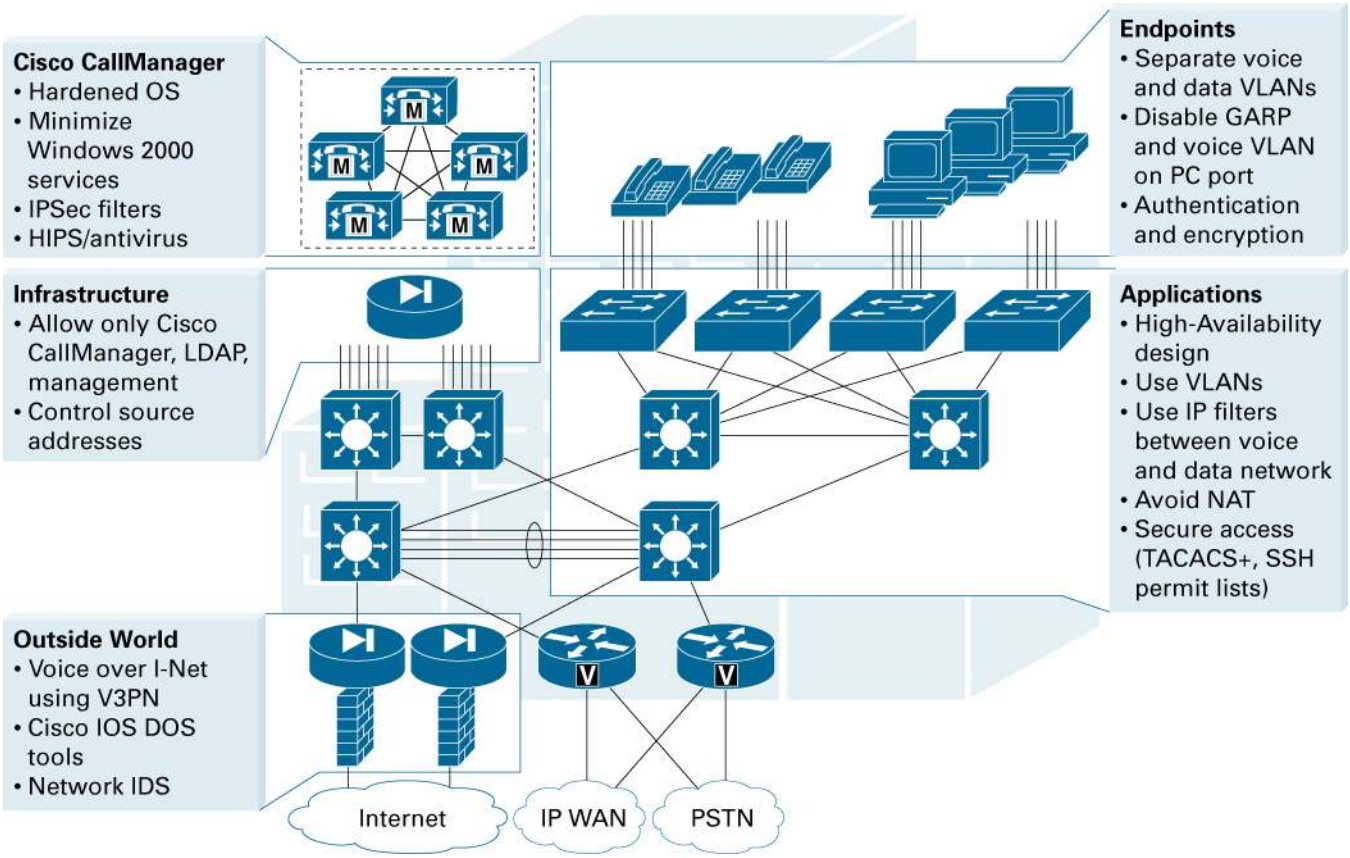
Protect All Levels of the Network

Companies need to protect all levels of their IP Communications networks, including the infrastructure, endpoints, call control, and the IP Communications applications themselves (Figure 1). Table 2 summarizes Cisco security technologies that protect each network layer.

Table 2. Cisco Security Technologies for Each Network Layer

Network Layer	How Cisco Secures the Layer
Infrastructure—Cisco routers and switches that connect phones, video terminals, and other delivery devices on the campus network	A Cisco IP phone automatically sets up a VLAN for voice communications whenever it is plugged into the network. Any signals across this link can be encrypted using Secure Real Time Protocol, rendering them unintelligible to hackers.
Call control—Provided by Cisco CallManager servers	Cisco CallManager protects against viruses, worms, and hacker attacks with Cisco Security Agent, which detects anomalous behavior. In addition, Secure Sockets Layer (SSL) VPN connections to corporate directories and digital certificates prevent rogue IP phones from being connected to the network.
End points—Cisco IP phones, video terminals, and other delivery devices	Cisco IP phones use digital certificates plus voice and media signaling encryption, so that hackers can neither listen in on conversations nor record the digits being dialed on the phone.
Applications—Call forwarding, interactive voice response (IVR), Cisco MeetingPlace®, and Cisco Unity® Unified Messaging	Systems used for contact centers and Web collaboration, such as Cisco IP Contact Center (IPCC) and Cisco MeetingPlace, come with integrated security features such as secure operating systems, Cisco Security Agent, and antivirus software.

Figure 1
Layered Approach to IP Telephony Security



ADVANTAGES OF OUT-TASKING BUSINESS VOICE SECURITY TO A MANAGED SERVICE PROVIDER

To gain privacy, protection, and control at all levels of their IP Communications networks, companies can either design, deploy, or manage a solution with in-house resources that provide 24-hour monitoring and response, or else out-task security to a MSSP. Managed security services from MSSPs range from basic firewall solutions for small companies to comprehensive security lifecycle management for global enterprises. Many MSSPs tailor solutions to their customers' business needs by combining services for firewall management, VPNs, intrusion detection solutions, virus scanning, Website security assessments, 24-hour monitoring, applet scanning, content inspection, and URL blocking.

Out-tasking managed security services for IP Communications provides measurable return on investment (ROI), a result of the following factors:

- *Business continuity*—Companies protect employee productivity and customer satisfaction when they prevent network downtime with proactive monitoring and regular security updates. Effective security services help protect customer service, product development, and other day-to-day activities.
- *Reduced costs of virus remediation*—Proactive security measures prevent costly recovery efforts after network security breaches.

- *Minimal upfront and ongoing costs*—MSSPs provide 24-hour network monitoring for all aspects of a network at a fixed monthly cost, so companies can transform a variable cost to a predictable cost. The service-level agreement (SLA) includes new security technology, so the company does not need to spend more to protect against new types of threats.
- *Ability for IT to focus on core business*—When IT can focus on strategic initiatives instead of routine security monitoring and maintenance, companies gain a competitive edge.

MANAGED SECURITY SERVICES FROM CISCO SYSTEMS

Companies that use Cisco IP Communications solutions can protect their networks with a comprehensive suite of managed security solutions, including firewalls, intrusion detection systems, virus scanning, encryption, authentication, and vulnerability assessment. Unlike point security solutions, Cisco Integrated Security solutions are built into Cisco network devices, for greater effectiveness and lower cost. For example, Cisco Secure Integrated Software on IOS adds firewall functions to Cisco routers to authenticate users, generate real-time alerts, defend against network attacks, and control access.

Cisco provides a wide range of security services to managed security service providers (MSSPs). These service providers, in turn, offer the services to their business customers.

Managed Firewall

The Cisco Managed Firewall service protects a company's IP Communications network from unauthorized access. Authorized employees receive secure access to the Internet, while incoming and some outgoing traffic is restricted based on factors such as the sender's address. As part of the service, the MSSP provides a firewall at the customer premises or a hosting center and also provides provisioning, staging, installation, and configuration. The MSSP remotely manages the firewall to ensure optimal performance, and provides regular traffic analysis reports for the company's review. The MSSP is also responsible for managing security-policy change management and for facilitating regular vulnerability scans.

ROI: Cisco compared monthly costs of a do-it-yourself firewall approach and managed firewall approach, assuming a nine-site enterprise with 2500 users. With the managed firewall approach, monthly recurring management costs dropped by 65 percent. Furthermore, the company gained greater network reliability because of 24-hour monitoring, lower implementation, and training costs; and the flexibility to reallocate IT staff to strategic core projects.

Managed Intrusion Detection System

The Cisco Managed Intrusion Detection System (IDS) service detects and responds to inappropriate attempts to access the network, systems, services, applications, or data. The MSSP installs IDS appliances on the customer premises, continuously monitors traffic, then classifies and responds to each event in real time based on the customer's security policy. Companies that subscribe to the service receive comprehensive reporting, system maintenance, identification of new threats, and application of new patches and virus signatures.

ROI: Cisco compared monthly costs of a do-it-yourself IDS approach and managed IDS approach, assuming the company had four IDS sensors. With the managed IDS service, monthly recurring management costs dropped by 75 percent. As with the Cisco Managed Firewall solution, the company gained greater network reliability because of 24-hour monitoring, lower implementation, and training costs; and the flexibility to reallocate IT staff to strategic core-business projects.

Managed Antivirus Protection

The Cisco Managed Antivirus Protection service checks for viruses at the gateway or firewall, in e-mails, e-mail attachments, and file transfers. It also scans all e-mail traffic, blocks downloads of infected Websites, and continuously protects against destructive programs such as viruses and worms, spam, and Web page content. The MSSP installs and configures server and management software at the customer premises or hosting center and manages it remotely. The service can include automatic updates.

Managed Authentication

The Cisco Managed Authentication service monitors and directs processes and technologies to verify the identities of users who attempt to access systems, services, or applications. The MSSP applies best practices for controlling access to corporate resources, intellectual property, and mission-critical business applications. Comprehensive authentication methods, including username/password and user-token systems are also used. The MSSP designs, provisions, installs, and configures authentication servers, analysis software, and other equipment either on the customer premises or at a hosting facility. The MSSP manages the entire system and administers user information, passwords, audit logs, reporting, and system maintenance.

MSSP PROFILES

Leading MSSPs around the globe already offer Cisco managed security services to their customers with IP Communications networks.

Equant

Equant offers out-tasked IP Communications services to its business customers over one of the largest end-to-end Cisco networks in the world. Equant is a member of the Cisco Powered Network Program. In conjunction with its IP Communications offering, Equant offers a portfolio of managed security services ranging from initial assessment to 24-hour global monitoring and support. The Managed-Intrusion Detection System (M-IDS) service protects corporate networks both from internal and external attacks with constant surveillance and defense by highly skilled experts. To ensure that its service remains available 24 hours a day, Equant maintains resilient, redundant security operation centers in various locations worldwide. “There is a level of trust with Cisco,” says Peter Glock, Equant’s head of security products. “Equant extends that level of trust with their managed security offering.”

AT&T

AT&T offers a comprehensive portfolio of security services to protect its business customers’ IP Communications services, including AT&T Internet Protect, AT&T Managed Authentication, AT&T Managed Firewall, and AT&T Managed Intrusion Detection. All services are offered over an end-to-end Cisco network. AT&T and Cisco together have deployed security services at General Motors, Ford Reserve, and other companies of varying sizes.

With AT&T's Managed Intrusion Detection Services, customers receive 24-hour surveillance and the simplicity of a fully managed solution spanning installation, maintenance, monitoring, and management of all associated hardware and software. The AT&T Managed Firewall Services provide another essential layer of network security, protecting the business infrastructure with fully managed firewall solutions that include all hardware and software components, day-to-day management and maintenance, as well as expert support and proactive 24-hour security monitoring and management. In addition to managing the firewall, AT&T also provides industry and manufacturer updates after appropriate testing so that business customers always have the latest security technology.

SBC

The largest reseller of Cisco IP telephony equipment, SBC also offers high-end security services over its end-to-end network. Its Security Consulting Services provide security policy design, security network design, and forensic analysis if a company experiences a security breach. Management services include firewall administration, managed VPN services, perimeter scans, intrusion detection services, and managed content filtering and virus scanning services. In contrast to a universal approach, SBC PremierSERV Security Services offer businesses the flexibility to design a security system tailored for their business needs.

FOR MORE INFORMATION

To learn more about Cisco managed security solutions, take the managed services e-tour at: http://www.cisco.com/go/managedservices.

To learn more about Cisco IP Communications solutions, go to: http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/networking_solutions_packages_list.html.

To learn more about Cisco Integrated Security, go to: http://www.cisco.com/en/US/netsol/ns643/networking_solutions_packages_list.html.

To learn more about Cisco Managed Security Service Providers, go to: http://www.cisco.com/cpn.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

DM/LW8123 03/05

Printed in the USA