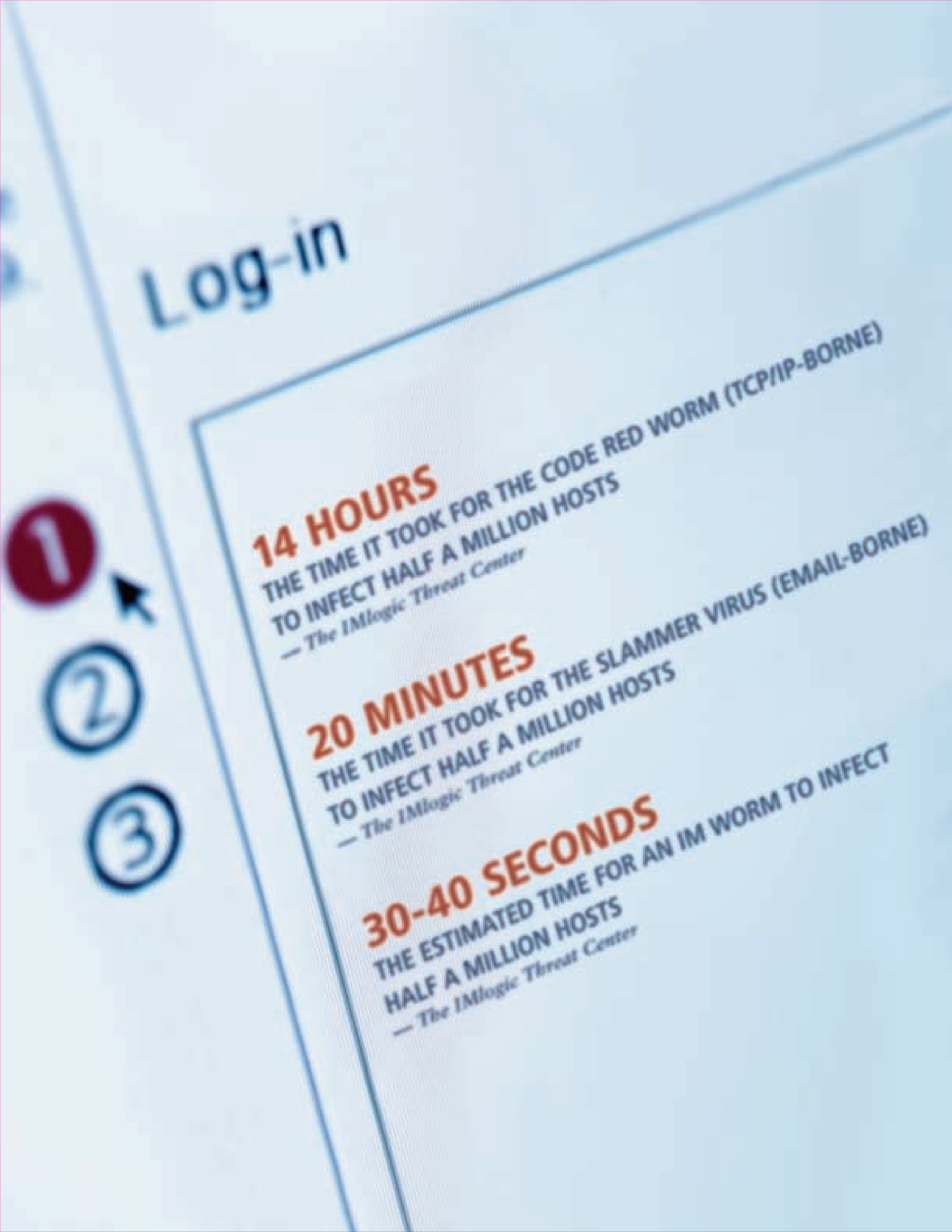
Issue 4 | Volume 1

TREND ADVISORY

SECURE PRODUCTIVITY

Achieving server security while supporting collaborative platforms



Log-in

14 HOURS
THE TIME IT TOOK FOR THE CODE RED WORM (TCP/IP-BORNE) TO INFECT HALF A MILLION HOSTS
— The IMlogic Threat Center

20 MINUTES
THE TIME IT TOOK FOR THE SLAMMER VIRUS (EMAIL-BORNE) TO INFECT HALF A MILLION HOSTS
— The IMlogic Threat Center

30-40 SECONDS
THE ESTIMATED TIME FOR AN IM WORM TO INFECT HALF A MILLION HOSTS
— The IMlogic Threat Center

SECURING YOUR BUSINESS DOESN'T MEAN ISOLATING IT

Today — when Internet access is tantamount to delivering consistent customer service, shopping easily for supplies and communicating efficiently with partners — businesses cannot choose to mitigate risk by disconnecting from the Internet and, therefore, the rest of the world.

The Internet can be a hazardous place for businesses. The malware and thieves that hide in the vast data streams of cyberspace pose constant threats to computer networks. E-mail and instant messaging (IM) afford quick communication and collaboration by taking advantage of the Internet's omnipresent qualities, but they require networks to allow a certain amount of traffic through in order for these applications to function. IT administrators must keep their businesses connected, yet safe, by enacting measures that allow them to monitor what comes in and goes out via Internet protocol (IP) traffic, so they can detect threats before malicious code can take root in the network.

OPEN CHANNELS AND UNSUSPECTING USERS

Because e-mail and IM applications are operated by individual users who often make unfortunate judgments on which files are safe to open, certain network defenses can be circumvented. Viruses sent via e-mail can spread very quickly, overcoming workers' computers and creating unplanned reparation workloads for IT departments.

As quickly as e-mail viruses spread, IM worms spread even faster. Although an e-mail virus can send itself to entire address books, host after host, the method requires some action by the user before the malware is presented for activation. IM applications, however, are ever-open channels, and a tainted link or file pops right into someone's IM from a friend or colleague, so it's quite natural that users click and immediately execute the bad program. In this way, these packets of malicious code can propagate to 500,000 hosts in less than a minute. That means security measures for IM applications must employ real-time analysis and blocking to keep a corporate network from an infection that can spread in the blink of an eye.

200 million employees worldwide use IM applications.

— "Secure IM Boosts Worker Productivity," SearchVOIP.com

INTEGRATE SECURITY TO STAY SAFE AND KEEP IN TOUCH

The business world is entrenched in the use of e-mail. And, more and more, businesses rely on IM in their internal and external communication strategies. These platforms are not going away anytime soon. So, to take advantage of them and stay connected, spam filters and antiviral measures that scan incoming and outgoing e-mails address part of the security risk. Add IM management software and integration with firewall, secure remote connectivity, intrusion detection and prevention, and you're well on your way to a productive, safe network for your business.

SECURE THE NETWORK
BY THE ZONE

There are two basic kinds of threats to your network:

INBOUND: Attacks from outside of the corporate network (e.g., hacking, worms, viruses, spyware and phishing)

OUTBOUND: Intentional or unintentional attacks from within the corporate network (e.g., an employee device unwittingly propagating a worm or virus; users who respond to phishing by entering their data on a bogus site; spyware sitting on a machine; and data sabotage or theft)

To deal with the wide range of inbound and outbound attacks, we're seeing smart companies take an integrated approach to server security. This provides IT with a practical way to achieve server security because, if one zone is breached, the next will stop the attack or mitigate the damage that may occur.

ZONE 1: NETWORK PERIMETER

HOW? Firewall, antivirus, antispam, antispyware and Web filtering

WHY? Evolved and blended attacks make it necessary to deploy multiple methodologies to ensure that the wrong things aren't getting into — and out of — your network.

ZONE 2: SERVER SECURITY

HOW? Encryption, firewall, IPS, intrusion detection system (IDS), URL, content and Web filtering

WHY? Web servers and data centers — they're the beating hearts of business continuity, so you want to know you can protect them if other measures have been circumvented.

ZONE 3: PROTECTION OF CLIENTS AND END POINTS

HOW? Antivirus, antispam, antispyware, personal firewall, host intrusion-prevention system (HIPS), Web filtering, encryption, port control, data leakage prevention and policy

WHY? They're your users. And sometimes they'll use the network in ways that can expose your business to malicious e-mails and instant messages (IMs) unless you have the right defenses in place.

ZONE 4: SECURE REMOTE ACCESS

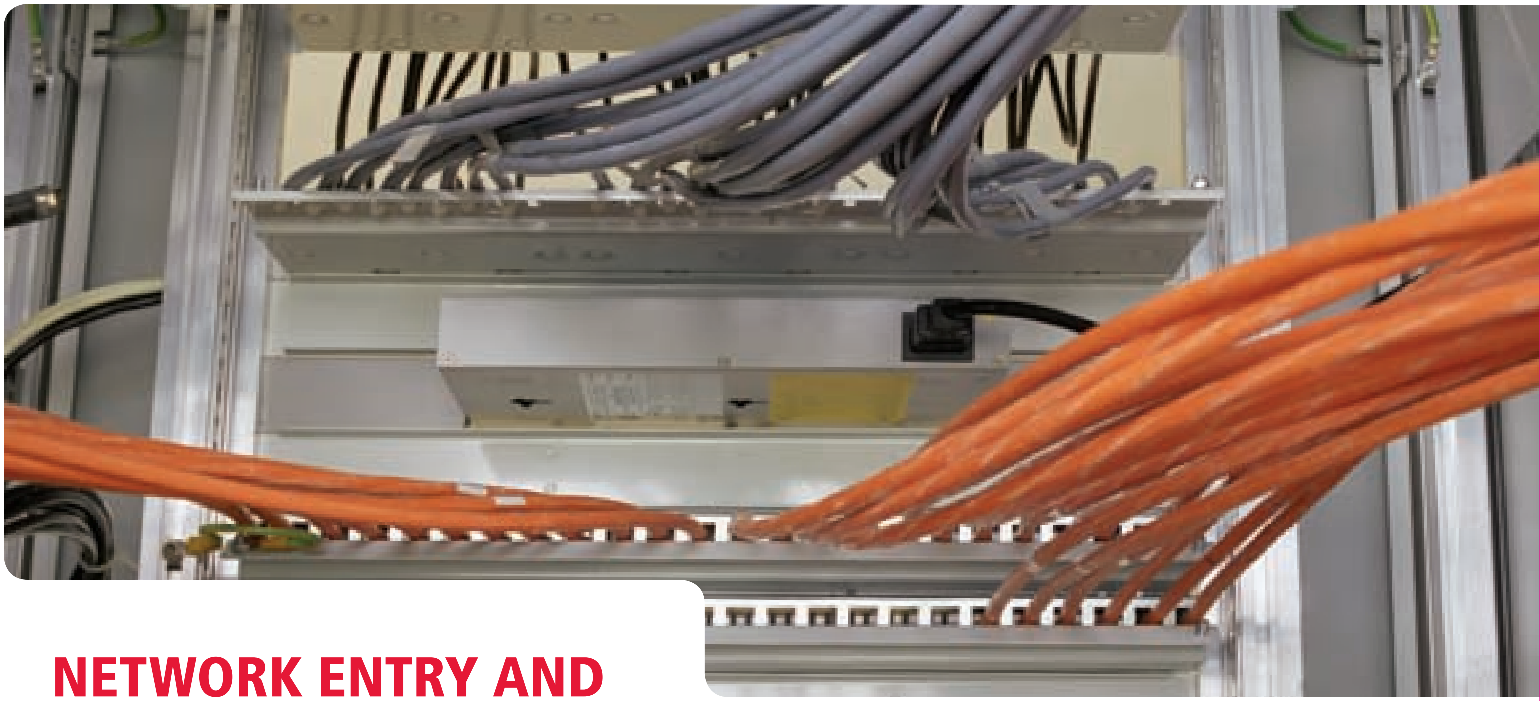
HOW? NAC, VPN, secure wireless access, user authentication and access control

WHY? Mobile workers are conducting business outside of your secure network on notebooks, handheld devices and smart phones. Protect them; protect your network.

ZONE 5: PREVENTION OF PHYSICAL THREATS

HOW? IP surveillance, security card access, biometric devices and encrypted USB thumb drives

WHY? With all the security you're building into your network, you'd hate to have someone literally walk off with it.



NETWORK ENTRY AND CLIENT END-POINTS

Keep up with the speed of business while you protect your network. Review your server security at the network entry and at client end-points (also known as Zones 2 and 3) to protect yourself from the threats associated with collaborative online applications.

ZONE 2: SERVER SECURITY

The most important zone of defense is the entry to your server from the network. Because, if all other measures have failed, it's really your last line of defense.

TACTICS: Firewalls, internal VPNs and IPS

- Protect business-critical resources by preventing unauthorized access
- Contain internal attacks launched by ill-meaning employees
- Protect against application-level attacks and worms

ZONE 3: PROTECTION OF CLIENTS AND END-POINTS

Your network supports your business users. And they generate both inbound and outbound traffic. Sometimes, users unwittingly expose the network in ways that can subject your business to malicious e-mails and instant messages, unless you have the right defenses in place. And remember: never underestimate the power of user education and enforceable policies.

TACTICS: Antivirus, antispam, antispyware, personal firewall, HIPS, Web filtering, policy management and IPS and IDS

- Block IM threats such as worms, viruses and spim (instant messaging spam)
- Enable a security-rich, collaborative computing environment
- Reduce administrative and help desk efforts due to infected client machines
- Involve your workforce in security policy

BEST-OF-BREED PRODUCTS MEET BEST-OF-BREED THINKING

▶ Every CDW account manager is backed by a team of dedicated security specialists. These specialists hold industry-standard certifications, including CCIE and CISSP (the "Ph.D." of security). They also receive rigorous training from CDW and security vendors such as CA, Check Point, Cisco, CompTIA, IBM, Microsoft, Novell, Sun and Symantec. Our single-source, vendor-neutral approach means you get the right mix of hardware, software and services, mapped to your exact business requirements.

Every CDW solution includes security assessment and design, hardware and software configuration, integration and on-site installation as needed. We help you identify the most vulnerable points in your network and focus your technology investments wisely, starting with an assessment that can take place on site or over the phone. After evaluating the computing needs of your workforce, we show you how to leverage your current technology assets. And when you need assistance getting your organization on board with your solution, we help you calculate cost savings and analyze return on investment (ROI).

When you're ready to launch your solution, we can configure, test and install it. And we offer continuous support, so we're there to follow up on the results you're getting from your solution and to help you guide it in the future as your business grows and your needs evolve.

BEST PRACTICES

A checklist to help you ward off messaging threats

□ Implement clear, comprehensive security policies that address employee use of both corporate and public messaging services

□ Enforce patch-management policies and solutions that safeguard the integrity of your network at all times

□ Engage solid NAC services to inspect any connecting computer and determine if the computer has been compromised with malware

□ Install a firewall in addition to your router to protect your network from unwarranted intrusion

□ Look closely at your method for authorizing only valid users to access the system

□ Ensure that all computers and notebooks are kept up to date with the latest patches and updates

Open communication and collaboration on a secure network. It's good for business.

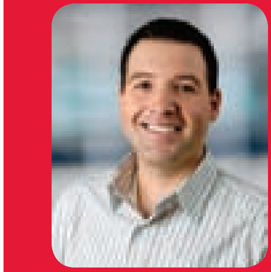
Think about the speed of business. Click, click, submit. And you've just purchased thousands of dollars of product. Click, click, send. And you've just assured another customer of your commitment to good service and quick response times. In the same blink of an eye, the fast and open channels of communication can allow unwelcome influences into your network unless you have multiple defenses to keep them out. Over the years, we have worked closely with our customers to understand their companies' security profiles and business needs, so we can help them keep their networks as responsive as they are secure.

KYLE MCGRANE

CISCO CSE, ADVANCE SECURITY, LIFECYCLE SERVICES, COMPTIA NETWORK+®, JUNIPER JNSA-S, SONICWALL CSSA, WEBSENSE CWSE

Multiple threats mean that no single protective measure can ever be 100 percent secure. So the key lies in having a layered approach. I work to understand what my customers consider to be their most important assets and then put together the best solution to prioritize the protection of those assets — all while striving to minimize the impact on my customers' ease of doing business. Beyond the technology my customers employ, education is the most important element of a security solution. What you teach your end users about safe use of the network can be your best weapon against attacks.

In the end, there are so many different security solutions out there. And almost all of them are the right choice. For someone. You need a partner who can listen to your business needs — as you define them — and help you find the best solution to meet them.



JEFFREY FALCON

CISSP (ISC)2, COMPTIA SECURITY+™

Each of my customers has a business to run. In some ways, I have several. My core competency isn't running a bank, a store, or a hospital, but it is making sure companies in all kinds of industries can run secure, responsive networks, so they can do what they do best.

At CDW, our ability to design multitiered network security solutions that meet your technical and business needs is a key differentiator. The education that we offer our customers on emerging security products is another. I want to teach my customers what I know after eight years of building secure solutions. But, more than anything, I want to understand my customers' unique business drivers, so I can play a role in meeting their organizations' objectives. Building the right security solution is a process that is just as much about the people as it is about the product.

YOUR SECURITY TEAM

▸ TAKE STOCK OF YOUR SECURITY NEEDS

Check out CDW's free security profiler at **CDWassessments.com/security**

CDW SELECTS

Solutions from CDW are made of hardware, software and experience. Our security specialists work closely with you and your account manager to assess your business needs and provide a practical, reliable approach to solving your current and future server security challenges.

NORTEL SECURE ROUTER 3120

Secure end-to-end converged solution

- Powerful modular system that converges routing, security and multimedia traffic-forwarding in a single platform for large networks
- Delivers fast, secure, reliable and scalable wide area network (WAN) access
- Features robust routing — low-latency, high-packet throughput for VoIP and multimedia transport, and integrated security with stateful packet-inspection firewall
- Supports QoS with multilevel, priority-based queuing to optimize voice, video and data

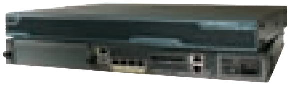
CDW 961547

CISCO® ASA 5510 SERIES ADAPTIVE SECURITY APPLIANCE

1U rack-mountable security appliance with Security Plus upgrade

- Offers organizations a comprehensive portfolio of services that are customized through product editions tailored for firewall, VPN and optional intrusion prevention, Anti-X capabilities
- Provides a high-performance firewall, three integrated Fast Ethernet interfaces and optional high-performance intrusion prevention and Anti-X services via a Security Services Module
- Scales to a higher interface density and integrates into switched network environments through VLAN support by installing a Security Plus upgrade license

CDW 792590



JUNIPER® NETWORKS SECURE SERVICES GATEWAY (SSG) 140

- Purpose-built security appliances that deliver a perfect mix of high performance, security and LAN/WAN connectivity for regional and branch office deployments
- Dedicated, security specific processing hardware and a complete set of Unified Threat Management (UTM) security features including Stateful firewall, IPSec VPN, IPS, Antivirus, Antispam, & Web Filtering
- Extensible I/O architecture delivers LAN and WAN connectivity options on top of unmatched security to reduce costs and extend investment protection

CDW 1065105

CA THREAT MANAGER[1]

- Combines best-of-breed CA Anti-Spyware r8.1 and CA Anti Virus r8.1 with an integrated management console
- Increases efficiency through a common agent, logging facility and updating tools
- Warns, detects, analyzes and provides remediation from attacks to minimize risks, system downtime and lost productivity resulting in enhanced service continuity

100-249 user competitive upgrade license[2]

CDW 1251863

100-249 user license[2]

CDW 1251963

Contact your account manager today at 800.800.4239 for product pricing or to discuss a custom security solution designed for your business.

[1] CA Threat Manager was formerly known as CA Integrated Threat Manager; only the product name has changed; this name change does not materially affect the functionality of the product

[2] Includes one-year Enterprise Maintenance (24 x 7 technical phone support and upgrade protection)