



Data and Identity Security

Rock-solid protection needed as changing business models provide greater network access to sensitive data, intellectual property and trade secrets.

TABLE OF CONTENTS	1 Executive Summary
	2 A Changing Security Landscape
	2 Different Brands of Breach
	4 Strategic Security Approaches
	5 Putting Security to Work
	7 Beyond Technology

Executive Summary

Keeping data safe and thwarting attackers is something no business can ignore. The loss or exposure of customer records, trade secrets or intellectual property can cause irreparable damage and wreak havoc with a company's reputation and revenues. A lack of accountability and compliance can also lead to government sanctions and fines.

And the situation isn't getting any easier. Risks constantly evolve. Staying current with the state of security — and related technology — is exceedingly difficult. Moreover, enterprise information technology is changing rapidly, as a decentralized infrastructure and mobile devices become commonplace.

As organizations find themselves under constant assault, business and IT executives must recognize that a comprehensive approach to security is not a luxury. It's essential to focus on a variety of strategies and technologies offering a multilayered approach that identifies, locates, isolates and stops attacks before they cause serious damage.

A Changing Security Landscape

There's no question that the Internet has ushered in an era of unsurpassed opportunity. But the same systems and tools that enhance productivity and boost efficiency create new risks.

Several years ago, much of the data theft activity was conducted by individuals or small groups. Today's landscape includes more highly organized and sophisticated organizations that can enlist and train best-in-class perpetrators.

In addition, the cost of network breaches has risen significantly. Threats now spread across the globe in real time. And the failure of one system can ripple out to business partners, employees, contract workers and customers. Many of these breaches take place in corporate and government environments.

Recently, three people were indicted for a sophisticated hacking pursuit that yielded more than 130 million credit and debit card numbers from several stores in New Jersey. U.S. authorities noted the intrusion to be the largest hacking and identity theft to date.

Organizations as diverse as TJX Companies, Citibank, Radisson Hotels and Resorts, and the United States Department of Veterans Affairs have found themselves the target of cybercriminals.

Threat Environment

For better or worse, the security field changes rapidly. It differs from other IT work in that predicting the next challenge generally proves quite difficult. Threats appear to come out of nowhere, and incidents seem to strike at random.

On the other hand, like all other areas of IT, security as a discipline constantly builds on itself and rarely takes a step backward. Over the last year, attacks have been used in new and complex combinations, and the sophistication of online criminal activities has grown.

These developments have either overwhelmed traditional security measures or made them only marginally effective. As a result, organizations have had to change their tactics in order to cope. This should provide a wake-up call to the fact that all of our systems will never be perfectly secure.

Cost of Compromised Records

Make no mistake: a data breach has a substantial cost. Research conducted by the Ponemon Institute indicates that every record compromised costs an enterprise somewhere between \$90 and \$305. Consequently, a breach of 1,000 records could result in a direct loss as great as \$305,000.

Worse, the cost of discovery, notification and response averages \$50 per record; lost employee productivity leads to another \$30 per record; and regulatory fines sometimes reach into the millions of dollars. Opportunity costs and indirect costs, including restitution and additional security and audit requirements, also figure into the total cost.

The good news is that IT security experts have remained equally dedicated and creative in finding ways to address developing threats.

Source of Trouble

Security problems, breakdowns and challenges arise from an array of sources. One of the most problematic areas is malicious software, generally known as malware. It has proliferated and become far more sophisticated in recent years.

Viruses often attack via hostile attachments to e-mail. SQL injection attacks, cross-site scripting flaws and other methods that surreptitiously download malware — oftentimes through a web browser — are a threat to end-user workstations.

According to the Symantec Global Internet Security Threat Report, "Trends for 2008," published in April 2009, "Malicious activity has increasingly become web-based with attackers targeting end users instead of computers."

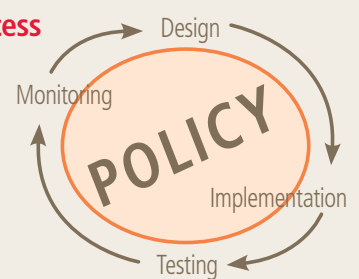
Interestingly, attacks on websites have grown more robust despite the fact that they don't involve new exploitation techniques. Instead, attackers are now combining older, well-known methods in new combinations.

In many instances, thieves use social engineering techniques, including so-called phishing and pharming. The idea is to lure unsuspecting recipients into opening an attachment or clicking a link to a fraudulent but realistic looking website.

In fact, phishing — directing a user to a realistic looking but fraudulent website — has become a huge danger. The Anti-Phishing Working Group (APWG), an organization dedicated to raising awareness about the problem and stamping it out, reports that the number of detected rogue animalware programs, fake security software and other malicious code grew by 585 percent from January to June 2009.

Security As a Process

Network security should be approached as a never-ending process or a series of steps or phases. This process consists of four phases: design, implementation, testing and monitoring.



Different Brands of Breach

Malware Menace

Malware is designed to infiltrate a computer without the owner's consent. It can unleash a spate of problems.

These include:

- Keyloggers that capture passwords and other sensitive data

- Rootkits that hide the fact that a system has been compromised and facilitate the replacement of vital system executables and control key functions
- An array of other viruses, worms and Trojan horses

A recent CSI Computer Crime and Security study found that 27 percent of respondents had experienced a “targeted” attack. (A targeted attack involves sending a class of malware directly to a specific organization or industry.) What’s more, these breaches are becoming stealthier all the time.

In some cases, malware attacks rely on sophisticated botnets to take control of systems — including enterprise computers — so that thieves can hijack or control the machines in order to perform malicious tasks. Such tasks include password and identity theft, keystroke logging, spamming, adware production and the generation of Distributed Denial of Service (DDoS) attacks.

Computers that fall prey to bots are referred to as “Zombie” systems. They typically lie in a dormant state until the perpetrator unleashes them. All the while they surreptitiously spread and infect other systems.

Once activated, computers infected with bot code register themselves on the network and begin wreaking havoc. When these massively parallel systems — sometimes into the millions of PCs — receive a command, they initiate an attack.

Attacks On Web Browsers/Hostile E-mail Attachments

Web browsers and e-mail have become the backbone of enterprise communication and collaboration. But their widespread use also makes them a convenient target for thieves. In fact, they are often the way in which attackers gain a foothold into an organization.

In some cases, thieves use pop-up ads to indicate that a system is infected with malware. They then convince the user to download a program supposedly designed to fix the problem.

Instead, it actually contains malicious code. Social networking sites, such as Facebook, MySpace and Twitter, have increasingly become the source of such attacks.

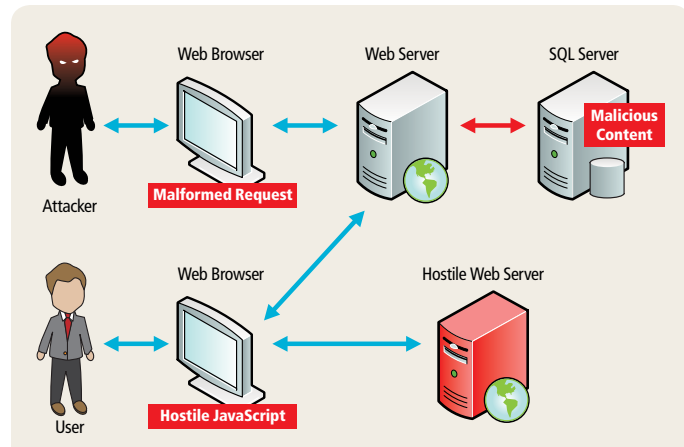
Spam has also become a huge problem, one that extends beyond being a mere productivity drain. Several billion spam messages circulate daily. And many include files that look legitimate but unleash a deadly payload.

Organizations have increasingly turned to spam filters to ferret out potentially dangerous messages. Combined with an antivirus application that scans messages, it’s possible to intercept problem files before they’re opened.

SQL Injection Attack

This type of attack has emerged as a common website attack method over the last several years.

With SQL injection, an attacker’s malicious input corrupts the application layer of the website. The resulting persistent cross-site scripting flaws affect the SQL commands issued to the database, thereby compromising end-user workstations.



SQL Injection/Cross-Site Scripting Example

An attacker constructs a request designed to tamper with the SQL composed by the .ASP application. The application submits altered SQL to the database, inserting malicious content. A user makes a standard website request and the .ASP application issues normal SQL to the database — of which the contents have already been altered. The malicious content is then returned.

The malicious code is inserted into strings that are passed to a SQL server. The script allows hackers and thieves to vandalize and replace web pages, steal credit card and other private data, and manipulate databases. Such attacks have the potential to compromise thousands of records.

Preventing such attacks requires improved programming — including avoidance of dynamically generated SQL code. Scanning for attempted breaches can also be helpful.

Configuration Management/PC Lockdown

Configuration management and the lockdown of client PCs represent another weak point within many companies. Too often, employees and independent contractors use weak passwords.

Assorted systems and applications create additional vulnerabilities and failure points. These areas of weakness include software and data residing on notebook PCs and portable storage devices.

Unfortunately, internal risk is often overlooked. It’s not uncommon for employees, contract workers, consultants and others to have access to systems they’re not entitled to use. What’s more, disgruntled employees and others on the inside of a business often find gaps or breakdowns to exploit.

Still another problem is that many companies lack coherent exit policies. Employees retain access to systems for days or weeks after they’ve left the organization.

Finally, rogue business processes frequently go unnoticed. Such processes include employees sharing e-mail messages and files with others that aren’t authorized to view the information.

Password Issues

A number of potential problems exist with passwords. Each can lead to a significant level of network compromise.

First, employees may write passwords on sticky notes that can be found and exploited. Or they may recite them out loud when they're recovering a lost password from the IT help desk. In addition, employees may use weak passwords that are easily cracked, including their name or a common word.

Some applications can generate strong random passwords. However, employees must also understand their role in generating and protecting them. A strong password consists of a combination of letters, numbers and symbols and is at least seven characters long.

Many organizations have moved past separate passwords for separate systems and have embraced a single log-on structure. Companies are also turning to multifactor authentication using a combination of authentication methods. These can include such things as a USB token and a password or a biometric scan and password to authenticate the user.

This type of authentication technology also offers the advantage of knowing who is logged into the system.

Wireless Security

The challenge of protecting an enterprise is magnified by the pervasive use of mobile technology. The use of mobile smartphones, notebooks and netbooks has companies expanding into different ways of connecting to the network. This makes the network and its data more exposed, offering new opportunities to hackers.

Forrester Research reports that 73 percent of global enterprise workforces will be mobile by 2012. Already, it's estimated that 70 percent or more of enterprise data resides in some form on mobile devices.

However, wireless security must extend beyond the actual devices. If employees and contract workers use an unsecured Wi-Fi connection, it's possible for thieves to capture data over the air.

Wireless technology is also being used in new and different ways. Consider retail operations where wireless networks connect cash registers and barcode scanners with store computers. These networks can be vulnerable to breaches and can provide a "treasure-trove" of data to unscrupulous cyberthieves.

Even secure systems can be continually monitored for the slightest hint of weakness. A wireless technique known as "wardriving" or "warwalking" consists of an individual in a car or walking using a portable PC to identify unprotected wireless networks.

Once found, perpetrators can set up wireless LANs outside of a business and use them to hack into systems. According to published reports, this was the case regarding the network breach at TJX Companies several years ago.

Loss of Mobile Devices

Despite their enormous value, mobile devices create a huge security risk. The reason: They allow employees and others to carry highly sensitive data outside an organization's boundaries.

LAX Laptop Loss

According to a study conducted by the Ponemon Institute, approximately 1,200 notebook PCs are lost weekly at the Los Angeles International Airport. The five airports with the highest number of lost, missing or stolen notebooks include LAX, Miami International, Kennedy International and Chicago O'Hare.

Airport Insecurity: The Case of Missing and Lost Laptops, Ponemon Institute, June 30, 2008

Unfortunately, about 10 percent of notebooks and other mobile devices wind up lost or stolen. And over 95 percent are never recovered. Airports, offices and an array of other locations present genuine risk.

Unfortunately, many firms lack the ability to track and lock devices, encrypt data and use a remote wipe feature to clear a lost or stolen computer or smartphone. At the heart of the problem: Employees who are left to the task of following rules, policies and procedures often willfully or inadvertently fail to do so.

Consequently, use of software to provision and manage devices — along with tools to encrypt data — goes a long way toward achieving protection and ensuring adequate security. Likewise, blocking specific features and locking down specific components, such as camera phones, further reduces security risks.

Strategic Security Approaches

Beyond Basic Protection

Shared systems and cloud computing have evolved from niche ideas into mainstream business practices. IT decision makers understand that the concept of data ownership has blurred. The network perimeter is all but gone.

In fact, some argue that guarding the network perimeter is foolish. In previous years, IT administrators could build a strong exterior barrier designed to prevent intrusions. Consequently, one could trust that the network core was secure.

This mentality worked adequately when a firm's workforce was static. However, the enterprise has become highly mobile over the last few years. What's more, partners, customers and even prospects often require at least some access to internal resources.

Today, Cisco refers to this computing model as "borderless networks." RSA uses the term "hyper-extended enterprise." Regardless of the moniker, the situation is the same. As apps and infrastructure move into the cloud, the requirement to harden every piece of infrastructure is paramount.

Security Travels with Data

Today, security must travel with data as it flows between IT systems operated by partners, customers and service providers. Security is now part of the data itself rather than relying solely on security where the information resides.

The ability to encrypt hard drives on mobile devices and use token-based authentication on various systems ratchets up protection. And centralized policy management makes it far more difficult for an employee to accidentally or purposely breach security.

(Note: Data Loss Prevention, or DLP, takes this concept to a higher level. It can analyze data in a more sophisticated way and track how and where it is moving. See right for details.)

The benefits of this approach extend beyond stronger security. It also leads to more efficient spending on infrastructure security. Infrastructure systems will strongly authenticate users and devices, and grant access to only needed resources.

This approach also marks a shift away from concentrating on firewalls, antivirus and Intrusion Prevention Systems (IPS). They will now be considered the last line of defense.

Inside-Out Security Model

If history is any indication, hackers and crime syndicates will always find new ways to penetrate networks — often at the worst possible moment. Factor in challenging economic times and it's clear that businesses are looking to optimize resources while approaching network security in a more comprehensive way.

Such thinking has progressive IT administrators looking to adopt an inside-out approach to network security. Such a strategy aims to maintain business functions and operations during any cyber attack or other security threat.

An inside-out security approach attempts to take control of the network via two elements: secure design and threat protection.

Secure design builds policy enforcement into the fabric of the infrastructure to ensure that only trusted people and devices participate in the network. The secure design toolbox includes authentication technologies, Virtual Private Networks (VPNs) and network quarantining systems.

Threat protection incorporates multilayer network security as a way to minimize inside and outside risks. Here, effective security strategies include the use of Intrusion Detection Systems (IDS), Public Key Infrastructure (PKI) access control and DLP tools.

Trusted Security Measures

The continued use of niche security tools — firewalls, antivirus, IPS and similar systems — is still vital. In addition, firms must adopt solutions that function effectively across a supply chain, authenticate users and devices, encrypt sensitive data and grant access to resources only as its needed.

The end goal is to achieve a high level of interoperability. IT leaders also want to improve data management from creation to its logical endpoint.

Putting Security to Work

Data Loss Prevention (DLP)

One of the most significant advances in data security is data loss prevention. It protects data in motion as well as at rest.

Because it is content-aware, DLP monitors data flow and identifies unauthorized data sharing and other potential breaches. It also tightens controls and, as a result, improves the odds of keeping enterprise assets secure.

Using content discovery, file system protection, network protection and GUI/kernel protection, DLP offers a comprehensive defense. In addition, central policy management and reporting tools, built into DLP solutions, vastly improve the ability of IT and security managers to track data flow.

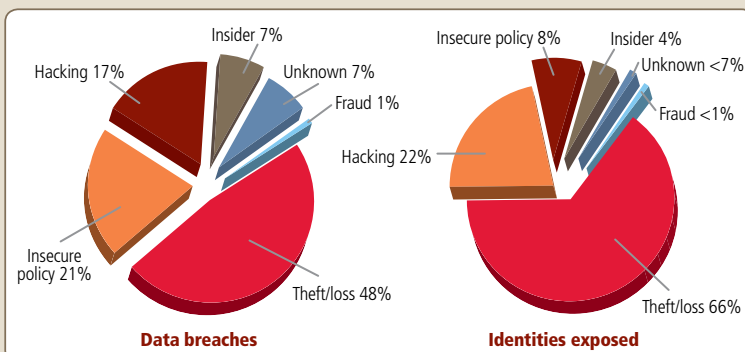
Among other things, DLP can block the transfer of content from one application to another. It can thwart the use of encryption when it is not appropriate. And it can also limit cutting and pasting, screen captures, page printing and transferring data across media.

By combining multiple layers of security and taking the focus off individual computers, servers and devices, DLP slices through complexity. The technology provides a unified way to oversee policies, workflow and data motion.

Encryption

Another key security component is encryption. The ability to lock and scramble documents — e-mail messages, text files, spreadsheets and more — and to keep databases and other information under lock and key goes a long way toward constructing a secure enterprise environment.

PGP's 2009 Annual Study, "U.S. Enterprise Encryption Trends," remarkably found that 41 percent of respondents do not recognize encryption as



Causes of Breaches That Could Lead to Data and Identity Theft

In 2008, the primary cause of data breaches that could facilitate identity theft was the theft or loss of a computer or other medium on which data is stored or transmitted, such as a USB key or a backup medium. Based on data provided by OSF DataLoss DB.

Source: Symantec Global Internet Security Threat Report, "Trends for 2008," published April 2009

“very important.” In addition, nearly one-third of the firms surveyed haven’t yet launched any type of encryption initiative.

Encryption is mostly used to prevent data breaches and comply with privacy and data protection regulations. Still, PGP reports that businesses are increasingly tapping it with the aim of preserving their brand and reputation.

Over the last few years, full-disk encryption (also known as whole-disk encryption) has garnered a good deal of attention. It offers nonstop disk protection for multiple platforms, including Microsoft and Apple OS X and across desktop PCs, notebooks and removable media.

An effective encryption tool built directly into Ultimate and Enterprise editions of Windows Vista and Windows 7 is BitLocker, which provides on-the-fly whole-disk encryption for documents and folders. The latest version of BitLocker, found in Windows 7 and Windows Server 2008 R2, offers the added feature of flash-drive encryption.

E-mail

It’s no secret that e-mail remains one of the weakest links in the enterprise security chain. Every day, thousands — in some cases hundreds of thousands — of messages flow in and out of enterprise computers and smartphones.

As these messages cross the corporate firewall and land in employees’ inboxes, the potential for abuse is significant. Viruses and other malware have indeed grown more sophisticated, but social engineering techniques have become more prevalent and successful.

According to MarkMonitor, a San Francisco company that tracks domain-name abuse, more than 150,000 phishing attacks took place in the second quarter of 2009. In some cases, cybercrooks are using a more focused approach.

Incidents of Spear Phishing, which targets a very narrow group of recipients or even an individual, are also on the rise. Once an individual clicks a link or opens an executable file, a malicious application installs on the computer and, in many cases, it spreads rapidly across the network.

Client- and network-based malware applications intercept viruses, spam and spyware as they enter the enterprise through e-mail or instant messaging. Furthermore, these applications now block phishing sites — including those accessed via e-mail — and stop spam and fraudulent messages. Some also update virus definitions as often as every five to 15 minutes.

In this way, a new virus appearing in the wild can be detected and eradicated before it causes damage. Some of these applications also incorporate encryption and protections for web browsers.

Finally, there’s the use of e-mail encryption. It ensures that information flowing in and out of an enterprise is protected.

Web Content Filtering

The ability to connect to a seemingly endless array of websites is both a boon and a curse for businesses. On one hand, it allows workers to tap into a vast reservoir of knowledge and uncover information quickly. On the other hand, questionable and sometimes dangerous sites are only a click away. Here, identity and data theft became very real possibilities.

Content filtering uses a blacklist to block access to undesirable or dangerous websites. Some also rely on algorithms to detect suspicious patterns.

Although these applications don’t stop hacks or an array of other attacks, they do prevent employees from downloading malicious code from websites. They’re able to sniff out malicious code because they inspect every packet passing through a firewall, caching device or proxy server.

It’s possible to implement content filtering through software or a hardware appliance. Content filtering tools usually provide a web-based console for configuring computers and other systems.

These tools can be set up to function in a standalone mode or incorporated into a firewall or proxy server. Software products often provide greater power and flexibility, but appliances are simple to set up and manage.

Server Security

Most organizations host vital data and applications at the server level. Threats in this area can compromise the company as a whole. Tools for effective server security include Network Access Control (NAC), clear and comprehensive security policies, and patch management policies that safeguard the integrity of the network at all times.

NAC can provide an identity-based approach to securing endpoint devices such as notebook PCs, netbooks and smartphones along with the data they hold. It allows a firm to unify endpoint security and create a common interface for managing a disparate array of systems across a network.

Moreover, today’s NAC solutions provide a high level of flexibility. If a security policy changes, an organization introduces a new application, or the need for guest access occurs, it’s possible to make changes and have them take effect instantly.

These applications also allow organizations to adapt policies to specific risk levels and integrate network access controls with identity services and other remediation controls. In most instances, NAC serves as an additional protection against viruses, worms, Trojans and other malware that spreads easily across a network.

Yet protecting servers requires more than NAC and antivirus software. An organization must have clearly defined security policies and a strategy for managing patches and essential updates.

The former requires collaboration and discussion among business leaders, security experts and IT. The latter course requires IT to apply security patches and updates in a consistent and regular manner in order to address

security flaws, bugs and vulnerabilities. Larger patches, or “service packs,” address a number of issues simultaneously and play a key role in reducing risk.

Virtual Private Networking

Another essential security feature is virtual private networking. It’s no newcomer to an effective risk prevention strategy, but the technology has become more sophisticated in recent years.

In fact, some organizations are migrating from older Internet Protocol Security (IPSec) VPNs to more advanced Secure Sockets Layer (SSL) VPN solutions. These provide more robust security and more granular policy and access controls.

A VPN creates an encrypted tunnel between devices or systems. Once a user logs in, a private connection is created. VPNs are particularly valuable for organizations with widely distributed offices and facilities.

VPNs offer a way — using the existing public telecommunications infrastructure — to create a secure connection to virtually any user in any part of the world without incurring the expense of establishing and managing a WAN.

In recent years, VPN technology has become more scalable and flexible, particularly SSL VPNs. It also has gained capabilities such as clientless remote access and support, integration with mobile and wireless devices, and the ability to establish granular policies based on users and devices.

Client-Level Security

Although DLP, content filtering, VPNs and other tools drastically reduce the risk of lost data, it’s also essential to install antivirus software, a local firewall and other protection at the client level. Moreover, an enterprise must know which applications reside on computers and other endpoint devices.

Some client security solutions now address the spate of challenges head on. They provide Active Directory support which can control client access, remote access and other functions that aren’t specific to the client platform. These can include password managers that autofill a browser and other forms, policy management tools, along with full-disk encryption and integrated fingerprint readers.

In some cases, users can also set up personal questions for retrieving forgotten passwords. They can also use enhanced spyware and fraud detection systems.

In addition, many IT and security officers are also taking a closer look at client security due to mobility. This is leading organizations to embrace full-disk encryption built into notebook PCs. Firms are also turning to software-based solutions such as Microsoft’s BitLocker, which is built into Windows Vista and Windows 7.

Beyond Technology

A successful security strategy is more than the sum of the technology. An often overlooked aspect to data protection is ensuring that employees and others working with various systems understand how to minimize risk through their actions and behavior.

Although DLP solutions, VPNs and other security tools enforce rules at the enterprise level, there’s still no way to eradicate human error and workarounds. As a result, education and training are vital components that every enterprise must address.

Among other things, users must understand what constitutes a strong password. They must know how to avoid practices that increase the odds of a stolen password or an intruder breaking into a system.

Users must also be aware of what’s necessary to keep personally owned computers and smartphones (that connect to an enterprise network) updated, patched and free of malware. Helping employees understand how social engineering methods work and how they might inadvertently spread a virus by opening an e-mail attachment or clicking to a malicious website is also critical.

No less important is the ability to integrate systems and tie them directly to business processes. Developing a flexible and agile framework helps an organization avoid costly dead ends and vulnerabilities.

Establishing multilayer protection and involving various internal groups and stakeholders in design and management goes a long way toward building a best-practice security model. Ultimately, the most successful organizations view security as a platform for business enablement rather than as a group of discreet tools and technologies designed to foil intrusions, hacks or outright theft.

Developing an effective strategy may also mean turning to outside expertise for an objective, third-party analysis. Here, you can find a full lifecycle of security services, including assessment, implementation, monitoring and management.

A holistic approach addresses everything from vulnerabilities to costs for gateway and network security, remote access security, mobility, and compliance and policy management. This multitiered approach maximizes ROI while minimizing Total Cost of Ownership (TCO).

Fast-Changing Landscape

The security challenges facing an enterprise grow more difficult by the day. As organizations interconnect systems, embrace mobility, and reach out to customers and business partners via the web and e-mail, the risk of a system breach and data theft increases dramatically.

Today’s fast-changing security landscape demands a comprehensive approach that addresses the full spectrum of issues. It’s no longer effective to respond to threats by tossing spot solutions at vulnerabilities and hoping for positive results.

As corporate assets appear in the crosshairs of hackers and online criminals — and the risk of data theft grows — organizations must take steps to reduce direct and collateral damage, including lost productivity, the cost of litigation, fines and reduced public trust. In the end, an integrated and holistic security approach pays dividends and positions a company for greater business success.

Security Spending Increases

In spite of a slow economy, both large and small enterprises are stating that they spent a higher percentage of IT budgets on security in 2009.

In a study recently released by Forrester Research, the pressure to scale back IT spending is not slowing the trend toward increased spend on network security.

According to the research, firms were planning to devote 12.6 percent of IT budget to security in 2009 versus 11.7 percent in 2008 and 7.2 percent in 2007.

Security Partner

CDW's Technology Services team specializes in providing comprehensive security assessments. The process involves careful analysis to identify, quantify and prioritize network risk.

Designed to focus on different parts of the infrastructure, the vulnerability assessment provides a detailed analysis of potential security flaws. It helps to identify high-risk scenarios, network threats and the advancement of effective risk reduction.

The assessments allow a firm to take immediate corrective action.

The results can also be used as a stepping stone to future security planning. CDW offers consultation that not only protects networks from harm, but also helps organize and streamline security efforts, lowers network cost of ownership and enables greater productivity.

Providing professional security assessments for all types of organizations, CDW was the first Cisco partner worldwide to earn a Master Security Specialization. This accolade is awarded to only those partners with the highest level of expertise.

CDW security assessments are custom-tailored to reflect individual business needs. Each security report highlights individual concerns and goals. CDW security assessments include analysis of any or all of the following:

- Internet Security
- Internal Network Security
- Partner/Extranet Security
- Dial-Access Security
- Wireless Network Security

When you partner with CDW, you partner with the best in the business:



CDW holds the status of National Channel Partner (NCP) at Trend Micro. CDW has two dedicated Trend Micro account managers, an onsite CDW Trend Pre-Sales System Engineer and a team of trained Security Specialists to assist with any business solution needs.

By working closely with customers and strategic partners to create the next generation of integrated threat management, Trend Micro is incorporating security into the fabric of the corporate network and the web.

Trend Micro's ability to successfully identify and develop solutions to emerging threats is reflected in their long history of innovations and industry firsts.

CDW.com/trendmicro »



CDW is a Platinum Channel Connect Partner at Websense.

With five dedicated members from Websense, an onsite CDW Websense Pre-Sales System Engineer and a team of trained Security Specialists to assist with any business solution need, CDW is poised to help your organization put a security plan into place.

Websense technology helps companies protect against today's Internet threats. 90 percent of malware comes from users visiting infected websites, and over 70 percent of those sites are the top 100 most frequently visited sites on the Internet. Websense categorizes and scans over 1 billion websites per day and is the only vendor that provides real-time security for Internet-based threats while allowing access to Web 2.0 sites.

CDW.com/websense »



WatchGuard builds affordable, all-in-one network and content security solutions to provide defense in depth for corporate content, networks and the businesses they power. WatchGuard's Extensible Threat Management (XTM) network security solutions combine firewall, VPN and security services to protect networks from spam, viruses, malware and intrusions.

The new Extensible Content Security (XCS) appliances offer content security across e-mail and web combined with data loss prevention for complete content protection. WatchGuard extensible solutions scale to offer right-sized security for small businesses up to enterprises with 10,000+ employees.

CDW.com/watchguard »



CDW is a Cisco Gold Certified Partner and holds specializations in Advanced Routing and Switching, Advanced Data Center Storage Networking and Advanced Wireless. CDW also holds Master Specializations in Security and Unified Communications.

CDW and Cisco work together to help your company succeed by providing a professional services organization with numerous Cisco certifications, over 50 cross-vendor certifications and regional sales coordination. Together, we're positioned to bring a wealth of knowledge to our customers.

CDW.com/cisco »