WHITE PAPER

CDW PEOPLE WHO GET IT CANADA

DATA AND IDENTITY SECURITY

With daily reports of network breaches on the way up, now is the time to double down on solid network protection.

Table of Contents

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 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.

What's more, no longer does the IT department have a monopoly on computer sophistication. Many in the generation brought up on video games and computers now have sufficient technical know-how to take advantage of network weaknesses for purposes of espionage, revenge and plain-old making a buck.

To counter, most effective network security today is done in layers. The feeling is if an intrusion is missed at one level, it will be caught in subsequent layers. So whether you are shoring up security at the edge, the core or in between, a network secured in layers offers optimum protection.

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.

Earlier this year, the FBI and other authorities were alerted to initiate an investigation into what was called a "criminal cyber attack" on Sony's PlayStation Network. According to the report, the attack had compromised the personal data of some 70 million accounts on the online service. The information stolen included user names, addresses, log-in and password credentials, password security answers, e-mail addresses along with birth dates.

In addition, just in 2011, tens of millions of people have had personal information exposed or put at risk because of data breaches

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 serve as a wake-up call: no system will ever be perfectly secure.

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 – of ten through a web browser – are a threat to end-user workstations.

According to the *Symantec Global Internet Security Threat Report, Trends for 2010*, published in April 2011, "A growing proliferation of web-attack toolkits drove a 93 percent increase in the volume of web-based attacks in 2010 over the volume observed in 2009."

The same report notes that 260,000 is the number of identities exposed in each of the data breaches caused by hacking throughout 2010. It addition, more vulnerabilities were recorded last year than in any year since the report was started in 2002.

In reviewing 2010, the report goes on to note the following trends:

- **TARGETED ATTACKS** – While not new, targeted attacks gained notoriety from high-profile attacks against major organizations and significant targets.
- **SOCIAL NETWORKING** – The ability to research a target online has enabled hackers to create powerful social engineering attacks that easily fool even sophisticated users.
- **HIDE AND SEEK** (zero-day vulnerabilities and rootkits) – Targeted attacks depend on their ability to get inside an organization and stay hidden in plain sight. Zero-day vulnerabilities and rootkits have made this possible.

Data Breach Costs Rise – Fifth Year in a Row

According to the annual study *2010 U.S. Cost of a Data Breach*, conducted by Symantec and the Ponemon Institute and covering the breach experiences in 51 U.S.-based organizations in 15 industries, the average cost for a data breach increased to $7.2 million. This is up 7 percent from $6.8 million in 2009, while the per-compromised record cost increased to $214 in 2010 – up $10 or 5 percent from 2009.

Fallout from a security failure can take many forms. These include: disrupted business operations, damaged and lost relationships, diminished retail sales, penalties and fines, and a decline in stock price.

- **ATTACK KITS** – Innovations from targeted attacks will make their way into massive attacks, most likely via toolkits.
- **MOBILE THREATS** – All of these types of attacks are moving to mobile devices, limited only by attackers getting a return on their investment.

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 who capture passwords and other sensitive data
- Rootkits that hide 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

The *CSI Computer Crime and Security Survey 2010* found that half of the respondents (351 information security and IT professionals) experienced at least one security incident last year, and fully 45.6 percent of them reported that they'd been the subjects of at least one targeted attack. (A targeted threat includes 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.

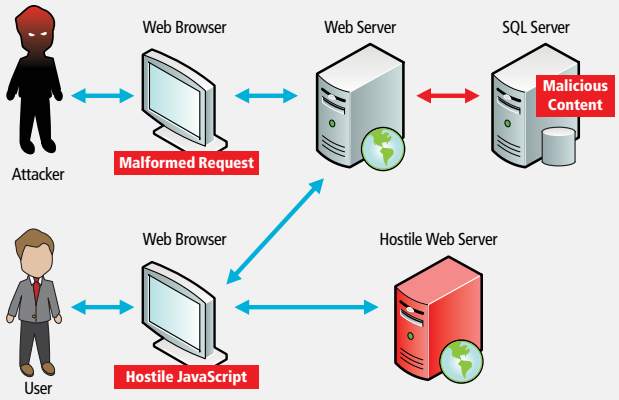
Once activated, computers infected with bot code register themselves on the network and begin wreaking havoc. When these massively parallel systems – sometimes into the millions of PCs – receive a command, they initiate an attack.

Social Network Safety

Microsoft has identified a steady rise in the number of attacks targeting social networks in 2010. According to the firm, this is fueled by a variety of phishing and social engineering tactics attempting to steal account credentials.

The *Microsoft Security Intelligence Report vol. 10*, covering the second half of 2010, found a steady increase in social network engineering attacks and an influx of rogue security software, designed to trick users into installing phony antivirus programs containing keyloggers, backdoors and other malware.

The report represents data pulled from Microsoft's customer base as well as partners and Internet service providers.



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.

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.

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 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 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.

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.

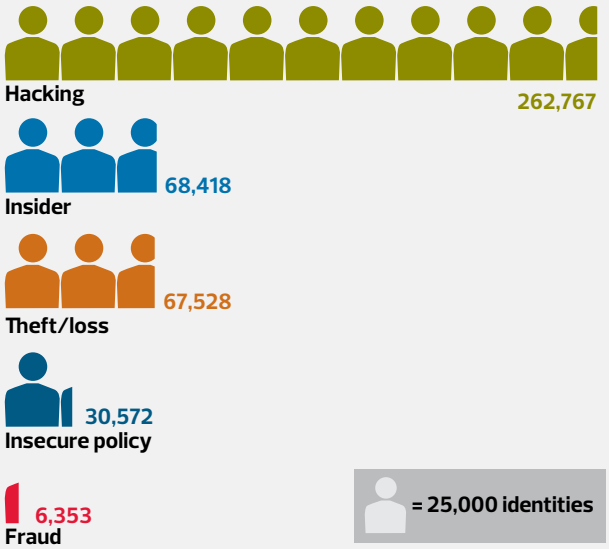
In fact, some argue that guarding the network perimeter is foolish. In previous years, IT administrators could build a strong exterior barrier designed to prevent intrusions. Consequently, one could trust that the network core was secure.

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.



Identities Exposed per Data Breach

In 2010, data breaches caused by hacking resulted in an average of over 260,000 identities exposed per breach. This is much more than any other cause. Breaches such as these can be especially damaging for the enterprise because they may contain sensitive data on customers as well as employees that even an average attacker can sell in the underground economy.

Source: Based on data provided by OSF DataLossDB

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 below.)

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 strategy 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.

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 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 graphical user interface (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 though 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 2010 Annual Study, *US Enterprise Encryption Trends,* remarkably found that 38 percent of respondents do not recognize encryption as "very important." In addition, nearly one-third of the firms surveyed had an overall encryption plan or strategy.

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 BitLocker To Go for USB 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, and social engineering techniques have become more prevalent and successful.

According to MarkMonitor, a San Francisco company that tracks domain-name abuse, more than 85,494 phishing attacks took place in the fourth quarter of 2010. 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 it enters 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 become 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 stand-alone 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, Trojan horses 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 a virtual private network. It's no newcomer to an effective risk prevention strategy, but the technology has become more sophisticated in recent years.

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.

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.

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 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 system 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 businesses 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 to threat management 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, companies 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 firm for greater business success.

CDW: A Security Partner That Gets IT

Threat prevention includes a series of strategies that build a multilayer security protection plan designed to prevent malicious attacks from entering your environment and corrupting systems and data.

CDW helps with security solutions that protect the five key network areas most susceptible to threats. These include: gateway and network, server security, client security, data loss prevention and application security.

Your CDW account manager and are ready to assist with every phase of choosing and leveraging the right threat prevention solution for your IT environment. Our approach includes:

- An initial discovery session to understand your goals, requirements and budget
- An assessment review of your existing environment and definition of project requirements
- Detailed manufacturer evaluations, recommendations, future environment design and proof of concept
- Procurement, configuration and deployment of the final solution
- 24x7 telephone support as well as ongoing product lifecycle support

To learn more about CDW's security solutions, contact your CDW account manager!

SONICWALL®

Extend your network, safely and securely. Increasingly, corporations are building their communications fabric over the public Internet for cost savings, flexibility and performance. With virtual private network (VPN) technologies, organizations now can transmit data securely to its destination without the risk of being corrupted or hijacked.

The broad range of SonicWALL VPN-based network security solutions facilitates both telecommuting and mobile computing. Whether you are a telecommuter seeking a secure alternative to the "un- trusted" home network or a road warrior connecting from a hotel room, SonicWALL has a solution designed to meet your specific business needs.

CDW.ca/sonicwall

Symantec™

Symantec is a global leader in providing security, storage and systems management solutions to help our customers — from consumers and small businesses to the largest global organizations — secure and manage their information against more risks at more points, more completely and efficiently, than any other company. Symantec's unique focus is to eliminate risks to information, technology and processes, independent of the device, platform, interaction or location.

CDW.ca/symatec

websense®

Websense offers a leading data loss prevention (DLP) solution designed to protect customer information, intellectual property, and enforce and report on regulatory compliance. Through a patented PreciseIDTM technology, Websense automatically discovers confidential data, monitors its use, and enables administrators to create and implement content enforcement policies.

CDW.ca/websense

CDW PEOPLE WHO GET IT™ CANADA