The CA Threat Management Solutions
Table of Contents

Executive Summary

SECTION 1: CHALLENGE 2
The Security Threat Landscape
Security Threats
Productivity Threats

SECTION 2: OPPORTUNITY 4
Types of Malicious Software
Viral Threats
Spyware and Other Non-Viral Threats
Blended Threats

SECTION 3: BENEFITS 8
An Effective Threat Strategy Yields Multi-Fold Benefits
Business Benefits of the CA Threat Management Solutions

SECTION 4: CONCLUSIONS 12

SECTION 5: REFERENCES 12

ABOUT CA Back Cover
Executive Summary

Challenge

Businesses are critically dependent upon their IT systems and failure to counter threats to IT systems can not only result in damage to network, systems and data, but can also affect the reputation of your business. Threats to computer systems affect both system security and productivity. Viruses and spyware are the main threats to business IT systems, but blended threats, where different types of malicious software are used in combination, are now very common.

Opportunity

The sophistication of threats and the rate at which they are evolving dictates that a unified and integrated threat management solution is required. Few computer threats can be easily defined as a virus, or as spyware, particularly with the rise of blended threats. So an effective threat strategy must be designed to provide a complete set of protection technologies and comprehensive threat management tools, which protect against all types of threat that may be part of an attack.

Benefits

The CA Threat Management Solutions presents a complete set of protection technologies, including anti-virus, anti-spyware and desktop firewall that provides a complete suite of threat management tools. These tools have been designed to complement each other and all use centralized Web-based consoles. A single vendor is responsible for covering all of the threats, so the CA Threat Management Solutions helps you to make sure that there is protection against all types of malware and that nothing is overlooked. Blended attacks are countered by a combined single-vendor threat defense.
The Security Threat Landscape

A threat is any potential occurrence, malicious or otherwise, that might damage or compromise the assets that your business depends on. Assets typically include your network, systems, data and other less tangible items, such as, your corporate credibility and reputation within your industry. There are many types of threat to computer systems that can affect system security and productivity.

**Security Threats**

There are many threats to the confidentiality and integrity of the information that is held on your IT systems, including:

- **Stolen user ID and passwords** If attackers gain access to user IDs and passwords, you run the risk of losing data, either through theft or because your information is tampered with. Attackers can potentially use user IDs to access other networks, such as those of financial institutions, or associate companies.

- **Unauthorized access to confidential information** If attackers can gain access to your network resources, they may be able to view confidential information and use this information to damage your business, by selling secrets to competitors, for example.

- **Loss of intellectual property** For most businesses, the most valuable asset is intellectual property, such as research data, and product development information. If this is lost, the effect can be catastrophic.
Remote control of company PCs If attackers can take control of any of your computers, they can then use the computer as a platform for further attacks within your business, as well as to launch attacks against third-parties. Such attacks can damage your reputation with customers and suppliers, and can also lead to legal action.

Theft of customer data If attackers compromise or steal your customer information, your business will suffer because you rely on accurate information. You may lose crucial historical records or order details and, probably more importantly, you may also lose the confidence of your customers.

All of these threats may have regulatory or legal implications. It is not enough to protect only your own data, because if you allow customer or supplier information to be unprotected, this is also a serious issue for your customers.

Productivity Threats

As well as impacting on the availability of your IT systems, malicious software can adversely affect the productivity or your business. Productivity threats could reduce employee productivity directly, or reduce the productivity of IT personnel and help desk resources, which may indirectly affect your employees and your customers. For example, IDC study\(^1\) estimates that 40-50% of all help desk calls are spyware related. Microsoft\(^2\) reported that over 50% of the crash reports they get are related to spyware.

Typical threats to productivity include:

- **Negative impact on network systems** Spyware transmits and receives data across a network, so causes significant overhead and wastes available bandwidth.

- **Negative impact on Internet access** Spyware, such as browser hijackers, may change the default homepage or prohibit users from visiting certain websites. Hijackers can also change the results of Web searches. Adware can inundate computers with pop-up ads.

- **Decreased workstation performance** Spyware can significantly reduce the performance of computers. The computer may seem sluggish, take longer to start up, or take longer to retrieve Web pages. For example, a computer with as little as two adware applications could take more than 14 minutes to boot. In some cases, the decreased performance is due to conflicts between spyware applications.

- **Denial of Service** A Denial of Service (DoS) attack makes a high number of requests for a limited network resource, for example bandwidth, so that access is denied to legitimate users. DoS attacks can also take advantage of bugs in operating system networking code, so that specially created network packets cause instability in that code. This type of attack can slow down the computer, may effectively kill the network connection or prevent it from receiving new connections, or hang the operating system (OS).

---

Types of Malicious Software

Malicious software (or malware) is any program or file that is harmful to a computer user. Examples of malware include computer viruses, worms, Trojan horse programs and spyware that gather information about a computer user without permission from the user.

The two main categories of malware (spyware and viruses) differ in several significant ways:

- **Purpose**  Computer viruses are usually designed to cause harm but can also be intended to take control of a personal computer (PC). Spyware is designed to monitor what users are doing on their PCs. Spyware can range from annoying pests like adware, which displays unwanted advertising and tracks Web surfing habits, to sophisticated backdoor hacker tools, which can cause serious security problems. The result of spyware infection can be serious, particularly if a computer is running multiple types of spyware simultaneously. Even adware can slow your PC to a crawl by bombarding it with unwanted ads.

- **Visibility**  Malware creators used to seek notoriety, but are increasingly becoming involved with organized crime. Therefore, they increasingly seek anonymity, so they can steal information and money without detection. For many types of spyware the users of a computer may be completely unaware that spyware is running on their computer. Increasingly, professional companies develop spyware for the sole purpose of stealing valuable data and sensitive information as unobtrusively as possible. This new, more dangerous wave of spyware threats is sometimes called 'Crimeware'.

- **Vector**  Computer viruses spread from computer to computer, and they were so named because their method of infection is similar in many ways to biological viruses. Spyware does not usually spread in this way and most spyware comes from Web browsing, or through email attachments.

- **Definition**  It is usually straightforward to classify viral malware, but it can be difficult to classify a piece of software as spyware. Spyware companies often claim that their software provides a benefit in return for the information it collects, and will complain to anti-spyware vendors if their software is identified as “spyware”. For this reason the anti-spyware industry has developed standards and definitions for spyware. If all companies agree, it then becomes harder for spyware creators to claim legitimacy. CA is a member of the Anti-Spyware Coalition and has developed the CA Anti-Spyware Scorecard as an open and transparent set of definitions that are used to classify a piece of software as spyware.

- **Mutation rate**  Both spyware and other forms of malware now mutate very quickly, with the intention of fooling security tools into treating new mutations as legitimate software. Malware creators have a vested interest in getting high infection rates, so security tools must be able to protect against a rapidly changing threat profile.
Figure B shows the results from a recent IDC study\(^3\) which confirms that viruses remain the leading threat to businesses, but that spyware has now moved up to become the number two concern. The IDC study also shows unsolicited email, known as spam, in third place. Spam is an annoyance in itself, but is also a major distribution mechanism for spyware and viruses.

**Viral Threats**

Viral malware includes viruses and worms. Viruses and worms are both self-replicating, but differ in other respects:

- **Virus** A computer virus is a program that includes code so that it can replicate itself. A virus spreads by attaching itself to a host program, document or boot sector. When the host is executed or opened, the virus code also runs and starts the process of infecting new hosts. Some viruses include an additional payload, which can execute code and cause damage, such as deleting or renaming particular system files.

- **Worm** A computer worm is usually defined as self-replicating code that uses network connections to distribute itself. Because worms use network resources, they can be responsible for denial of service attacks. As with viruses, some worms include an additional payload.

---

Spyware and Other Non-Viral Threats

The term spyware refers to any non-viral software program that aids in gathering information about people or businesses without their knowledge, and can relay this information back to an unauthorized third party. These types of malware are unable to spread of their own accord. The main types of spyware or non-viral malware are:

- **Trojans**  A Trojan is a program that appears to be useful or harmless but contains hidden code that is designed to exploit or damage the system on which it is run. Trojans are typically distributed through email messages that misrepresent the program's purpose and function. Trojans deliver their malicious payloads or tasks when they are run. Trojans are now the dominant form of malware and some Trojans specifically target particular businesses or types of users (a trend that appears to be on the increase).

- **Polymorphic Trojans and Adware**  Polymorphism is a technique used to avoid detection, where a malicious encrypted application (traditionally a virus) mutates its decryptor on each replication to take a different form that is intended to evade an anti-virus signature detection. Polymorphism is not new, and was first noted as a concept in 1990. Polymorphism has been developed over time to include sophisticated and advanced techniques. Various polymorphic engines have been used by numerous viruses and even some worms over the last decade. However, as a detection-evasion technique it has been out of vogue until recently.

- **Remote Access Trojans (RATs)**  RATs are a specific type of Trojan that gives a hacker complete control over a PC, as if the hacker was at the keyboard.

- **Keyloggers**  Keyloggers can record every keystroke made on a PC and by doing so can steal passwords and confidential data.

- **Hacker tools**  Hacker tools are designed to penetrate remote computers to use them for other attacks (by using backdoors) or to download other malicious programs to victim computers. Hacker attacks may use a single specific exploit, several exploits at the same time, a mis-configuration in a system component or a backdoor from an earlier attack.

- **Distributed Denial-of-Service agents (DDoS)**  Attackers are unlikely to be able to mount effective bandwidth-consumption DoS attacks against large sites from a single attacking computer. Therefore, attackers usually use DDoS attacks in which a number of computers, called zombies, are coordinated so that each computer provides part of the network traffic that is necessary to produce the DoS attack. The DDoS components are typically distributed as Trojans.

- **Ransomware**  Ransomware is a particular type of spyware which encrypts user data and then displays a ransom demand for the data to be restored. The victim is led to believe that after the ransom has been paid, the attacker will send the decryption key, so that the kidnapped files can be decrypted. Such malware extortion attacks (that encrypt or delete data) are becoming more common.

- **Rootkits**  A rootkit is a type of malware that is installed below the level of the OS. Rootkits communicate directly to the computer hardware and send misleading information to the OS, in an attempt to be undetectable. However, for most rootkits, the delivery mechanism (such as a Trojan) and the installation mechanism can be successfully detected by good anti-spyware tools.
• **Browser Hijackers**  Browser Hijackers can reset the default homepage and search results. Some may prevent users from changing their browser homepages back to the original default or visiting a particular site.

• **Browser Helper Objects (BHOs)**  BHOs can search all of the pages viewed in Internet Explorer and replace banner advertisements with targeted advertisements, monitor and report on user actions, and change a user’s homepage.

• **Vulnerability Exploits**  There has been a dramatic decrease in the time between the discovery of vulnerability in an operating system or other software and its exploitation by the creators of viruses and spyware. The most vivid example of this occurred at the very end of 2005 with the Microsoft Windows Meta File processing vulnerability. Within a day of the vulnerability being announced it was being used actively in the wild by several Trojan families. A couple of days later it was being exploited by a worm that was spread by using Windows Messenger and it continues to be exploited by Trojans and malicious web pages.

Some of the effects of spyware can be indirect. The spyware components installed on a computer may not in themselves cause harm, but can open your business to other types of exploitation, including:

• **Social Engineering Attacks**  Social Engineering is the practice of obtaining confidential information by using manipulation. Examples include the spam used for phishing attacks, banner and search engine ads that falsely lure users in to a malware site, and SMS text messages on mobile phones and Personal Digital Assistants (PDAs) that direct users to go to a malware site by using their PCs.

• **Phishing**  Phishing is defined as fraudulently acquiring information, such as usernames and passwords. Typically it is a mechanism for identity theft. The most common examples are emails claiming to be from a financial institution, which either directs the user to a Web site to capture identity information, or includes an attachment that installs spyware, such as a keylogger or remote control tool. Phishing is now a problem for business users as well as for home users.

• **Direct Port Attacks**  A direct port attack installs malware on an unprotected port. Examples of malware that is often installed include botnet software and remote control tools. If an unprotected laptop is used on public hotspots, malware is installed, which then becomes a threat when the laptop is plugged into the business network.

You also need to prevent spyware from using any one of your computers as part of its distribution system. Although these distribution components may not directly affect a specific computer, it is important that you do not allow your computers to become a channel for infection across your network. Such components include:

• **Spam relays**  A spam relay sends mail to a destination through a third-party mail server or proxy server in order to hide the address of the source of the mail. Most email servers (SMTP servers) are now locked down and require some form of authentication, so spam relay is typically provided by proxy servers and botnets.

• **Botnets**  A botnet is a network of distributed computers, typically made up of compromised computers that can be used without the owner’s knowledge. The typical uses of these networks are as spam relays, adware servers, to launch DoS attacks or as remote disk storage for pornography sites.
**Blended Threats**

A blended threat is one where different types of malware are used in combination, so that there are multiple attack vectors. Blended threats can spread rapidly and are now very common. Examples of blended threats include the following:

- Phishing attacks that combine spam and spyware as an attachment.
- Mytob and other worms that install spyware, including botnet software, on the infected computer.
- Sony rootkit, in which the copy protection software was automatically installed from audio CDs and created vulnerabilities in the operating system, which were rapidly exploited by other spyware.

Effective threat management must include protection against blended threats.

**An Effective Threat Strategy Yields Multi-Fold Benefits**

Few computer threats can be easily defined as a simple virus, or as non-viral spyware, and the attack vectors can be complex when part of a blended threat. So an effective threat strategy must be designed to provide a complete set of protection technologies. Tools that are designed to remove viruses cannot protect against spyware. Perimeter and endpoint firewalls cannot stop all malware from reaching desktop computers and servers, because many types of spyware can spoof the network traffic it generates so that it appears to the firewall to be legitimate.

Although all businesses must have effective perimeter firewalls, it is important to know that a perimeter firewall cannot, on its own, protect your workstations and servers from all threats:

- A perimeter solution cannot clean a system that was already infected before the solution was installed.
- A perimeter solution cannot protect mobile systems, when the mobile systems are outside the corporate network.
- A gateway is not always the best place to detect spyware, because the spyware may be designed to get past the firewall without detection. Many types of spyware are distributed as small innocuous components that only get assembled when they reach the desktop.

For these reasons you need a range of tools to counter the various threats and the range of attack vectors. The minimum protection package must include:

- **Anti-virus**  To detect and remove viral malware threats that evades detection by firewalls or filters.
- **Anti-spyware**  To detect and remove non-viral malware threats that evades detection by firewalls or filters.
- **Endpoint firewall**  To minimise the risk of malware components reaching the desktop through the network.
For most businesses you should also add the following to this minimum list:

- **Anti-spam**  To minimise the risk of malware components reaching the desktop through email.

- **Web and email content filtering**  To minimise the risk of malware components reaching the desktop through email or Web traffic.

For effective protection against blended threats you must use comprehensive threat management solutions that protect against all the types of threat that may be part of the attack. Although it appears easy to make a distinction between viral and non-viral malware, this is not always the case. For example, the line between Trojan and worm (as between virtually all malicious applications) is becoming blurred, because bots and agents that are unable to spread on their own are evolving into self-propagating, self-updating packages when they are combined with additional components from their controllers.

Figure C shows the range of threat management solutions that should be part of an integrated threat management implementation, and how these solutions are used on both endpoint and gateway computers within and outside the network.
Business Benefits of the CA Threat Management Solutions

The CA Threat Management Solutions are designed to counter security and productivity threats, by protecting computers against all forms of malicious software and malware. The CA Threat Management Solutions provide a complete suite of threat management tools. These tools have been designed to complement each other, and use common or similar Web consoles. You can also integrate the threat products with other third-party solutions if necessary.

- **CA Threat Manager**  CA Threat Manager combines CA Anti-Spyware with CA Anti-Virus and extends the functionality of both products with a central, Web-based management console. CA Threat Manager uses a common agent, logging facilities and updating tools, and is compatible with and complementary to other CA security products, including CA Host-Based Intrusion Prevention System (CA HIPS), and CA Secure Content Manager (CA SCM). For more information about “CA Threat Manager”, see “Technology Brief – Protecting Endpoint Systems Using Threat Management Solutions”.

- **CA Anti-Spyware**  CA Anti-Spyware detects and removes spyware and non-viral malware. For more information about CA Anti-Spyware, see “Technology Brief – Protecting Endpoint Systems against Spyware”.

- **CA Anti-Virus**  CA Anti-Virus detects and removes viruses from business PCs, servers and PDAs. For more information about CA Anti-Virus, see “Technology Brief – Protecting Endpoint Systems against Viral Malware”.

- **CA Host-Based Intrusion Prevention System (CA HIPS)**  CA Host-Based Intrusion Prevention System is a stand-alone firewall, intrusion detection system, and intrusion prevention system. It provides endpoint protection for desktops and laptops, which is administered through a central management console. For more information about CA Host-Based Intrusion Prevention System, see “Technology Brief – Protecting Endpoint Systems Using Host-Based Intrusion Prevention”.

- **CA Secure Content Manager (CA SCM)**  CA Secure Content Manager provides gateway protection, by using SMTP and HTTP filtering to safeguard businesses from incoming Web and messaging threats or spam, and from data confidentiality breaches through outgoing email traffic. CA Secure Content Manager includes anti-virus protection for the gateway; CA Secure Content Manager Suite also has CA Anti-Virus for desktop anti-virus protection. All CA SCM installations can be administered through a central management console.
Table A shows the threats countered by each product in the CA Threat Management Solutions and the key methodology used by each product.

**TABLE A: THE CA THREAT MANAGEMENT SOLUTIONS: THREATS AND METHODOLOGIES**

<table>
<thead>
<tr>
<th>PRODUCT</th>
<th>THREATS ENCOUNTERED</th>
<th>KEY METHODOLOGY</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA Threat Manager</td>
<td>Spyware, non-viral and viral malware</td>
<td>Uses anti-spyware and anti-virus engines to prevent spyware and other non-viral and viral malware from executing on the computer.</td>
</tr>
<tr>
<td>CA Anti-Spyware</td>
<td>Spyware, non-viral malware</td>
<td>Uses anti-spyware engine to prevent spyware and other non-viral malware from executing on the computer.</td>
</tr>
<tr>
<td>CA Anti-Virus</td>
<td>Viral malware</td>
<td>Uses anti-virus engine to prevent viral malware from executing on the computer.</td>
</tr>
<tr>
<td>CA Host-Based Intrusion Prevention System</td>
<td>Spyware, non-viral and viral malware, adware and other rogue software</td>
<td>Uses firewall and intrusion detection methods to prevent malicious software from reaching the network.</td>
</tr>
<tr>
<td>CA Secure Content Manager</td>
<td>Spyware, non-viral and viral malware, adware and other rogue software</td>
<td>Uses anti-virus engine to prevent viral malware from entering the network through email or Web traffic. Uses Web security and URL filtering on HTTP and FTP traffic. Uses email filtering and anti-spam content filtering on SMTP traffic.</td>
</tr>
</tbody>
</table>

The principal benefit of the CA integrated approach is that the CA Threat products are designed to work together by using common or similar management and reporting tools that work together with your whole threat management toolkit. CA Threat Manager and the CA Protection Suites, for example, share common deployment technologies for anti-virus and anti-spyware. The CA integrated threat management approach provides centralized management of all anti-threat capabilities. The result is significantly better security, as well as increased administrative efficiencies.

Another key benefit of using CA technology is that there is a single vendor responsible for dealing with all of the threats:

- This ensures that there is protection against all types of malware and that nothing is overlooked due to different vendor definitions of “viruses”, and “spyware”.
- Blended attacks are more easily countered by a combined single-vendor threat defense.
- Kernel-level conflicts between your threat management applications are avoided. Integrated components from a single vendor tend to work together much more effectively, without these types of algorithm clashes.
CA is also developing a Single Threat Engine Strategy. The aim of this strategy is for all threats to be countered by using a single threat engine together with one set of updates and reduced network bandwidth requirements to maintain this single engine. There is also reduced computer system overhead when using a single engine. The first result of this strategy is that CA Anti-Virus now uses a single anti-virus engine. The second phase will feature a single threat engine for both CA Anti-Virus and CA Anti-Spyware.

CA Threat Management Solutions are supported by the CA Security Advisor team, who have been providing security information to governments, businesses, educational institutions and non-profit organizations since 1987. CA researchers continuously monitor new security threats, develop mitigation procedures, and aggregate security data from over 400 sources by using a patent pending process for the research, testing and validation of threats.

SECTION 4: CONCLUSIONS

Threats to business computer systems affect system security and productivity. Viruses and spyware are the main threats to these systems, but complex blended threats are an increasingly significant problem. An effective threat strategy must provide a complete set of protection technologies to protect against all types of threat. The CA Threat Management Solutions provides an integrated and comprehensive set of applications to protect all business computers and ensures that there is protection against all types of malware.

SECTION 5: REFERENCES

“Anti-Spyware Coalition”: http://www.antispywarecoalition.org/

“Center for Democracy and Technology”: http://www.cdt.org/


To learn more about the CA Threat Management architecture and technical approach, visit CA Threat Management Solutions
CA, one of the world’s largest information technology (IT) management software companies, unifies and simplifies complex IT management across the enterprise for greater business results. With our Enterprise IT Management vision, solutions and expertise, we help customers effectively govern, manage and secure IT.

Learn more about how CA can help you transform your business at ca.com