

The Demand For Proactive Endpoint Security: CA's Integrated Threat Management Vision

APRIL, 2007

Christopher Wraight

CA SECURITY MANAGEMENT

Table of Contents

Executive Summary

SECTION 1 2

The Rise of Electronic Threats

Types of Attacks

SECTION 2 4

Simplify Threat Protection With an Integrated Approach

So what is required for an effective threat management vision to become reality?

Simplified Threat Management —
The CA Vision and Approach

SECTION 3 8

Reduce Risks While Lowering Security Costs

SECTION 4 9

Conclusions

SECTION 5 9

About the Author

ABOUT CA Back Cover

Executive Summary

Challenge

Companies of all sizes want to improve and expand global information access while preventing exposure to threats from the gateway to the various endpoints. However, new, combined threat attacks are arriving daily in the form of spyware, malware (e.g., viruses, worms, Trojans, etc.). Left undetected, these threats can compromise a business' security, reduce productivity and compromise data integrity. All of these attacks can disrupt service continuity, result in damage to the company's reputation, affect the bottom line and possibly precipitate regulatory action.

Opportunity

To manage today's spyware and malware challenges efficiently and effectively, enterprises require a comprehensive threat management solution that assists with detection, thorough removal and streamlined management capabilities. Drawing upon more than 30 years' experience as the management software experts, CA has developed a comprehensive set of threat management solutions for both the endpoint systems (desktop, server, laptop and other network access point) and gateway (spam, HTTP, SMTP). In addition, these products seamlessly integrate and combine with CA's broader security and network management products, such as the CA Unicenter® technology, enabling network and security operations consolidation.

Benefits

RISK MITIGATION By providing zero-day threat protection and adopting a multilayered threat approach, enterprises greatly reduce the various threat attacks resulting in improved risk profile for the entire enterprise.

COST REDUCTION Mitigating successful threat attacks yields many financial benefits to an enterprise. With real-time alerts and automatic threat updates users become more productive while help desk costs are reduced dramatically.

ASSET PROTECTION The protection of critical corporate assets such as web applications, platforms, operating systems, critical system files and repositories are what the business operations depend on, and so must be protected from unauthorized access at all costs.

SERVICE CONTINUITY Proactive management of threats can reduce catastrophic effects on the availability of IT infrastructures which in-turn impacts an enterprise's bottom-line.

FACILITATE REGULATORY COMPLIANCE Extensive reporting and logging capabilities help an enterprise to identify and neutralize threats rapidly, and can be used to assist with investigations and regulatory compliance.

SECTION 1

The Rise of Electronic Threats

Virtually all computer users have experienced the results of the stunning increase in computer threats over the recent past. Attacks of all kinds have become much more sophisticated and harder to detect. These attacks also appear almost immediately as soon as news of a new vulnerability is made available. For businesses that must constantly battle these attacks, it has become imperative to prevent, as well as detect and remove them swiftly and completely. The life of the business can be at stake.

The nature of computer attacks has changed over the past few years. Unlike early viruses that were often created by hackers whose sole interest was in gaining visibility within the hacker community, the new attacks are much more sinister and have just the opposite visibility goals; they are usually motivated by the desire for money. The result is often fraud committed on thousands of unsuspecting users, commonly referred to as “crimeware”. For example, capturing personal or company information without the knowledge or consent of the owner of the computer system can lead to catastrophic results for individuals, as well as for businesses, government entities, medical/healthcare organizations and educational institutions. Even the innocent act of playing a music CD on a computer can leave it open to attack. Spyware can accompany the music when it is automatically downloaded onto the hard drive, rendering the computer vulnerable to attack.

A recent survey of IT executives at major corporations found that malware attacks increased by 48% in 2006. About 42% of the malware allowed outside access to the infected machine, 40% downloaded code from a website and 34% stole information. One-sixth of these attacks attempted to disable the machine’s anti-virus software. These statistics indicate the variety of attacks that have emerged, and the prevalence of attacks of all kinds that all PC users face.

Faced with constantly evolving threat and attack methodologies by well-funded and determined entities that want to “own” the behavior of large numbers of computer systems (including yours) and potentially steal or manipulate the data contained within them — computer security strategies must now adapt rapidly to counter new and more sinister threats. There have been cases of whole networks brought down by virus attacks, and millions of dollars lost when software was erased from poorly backed-up PCs. The great productivity windfall of the Internet is now giving way to the productivity loss of sophisticated and fraudulent “eBusiness”. Without adequate protection, computing infrastructures may very well become unusable and require complete re-building.

Let’s examine some of the ways that a computer can become infected or contaminated with malware, rootkits, spyware or other pests.

Types of Attacks

The most common attacks are no longer simple (or even complex) viruses. Many forms of malware and assorted other unwanted software programs are using complex combinations of attacks to spread — not simply relying on one method alone. And these combinations are time- and geographically-independent, sometimes spreading out over several weeks and several continents. The following are some of the major areas of vulnerability that could result in attacks:

- Operating system and software application vulnerabilities.
- Accepting downloads from unknown sources when visiting websites.
- Active-X, Java and scripts can either contain malicious code or download malicious code from various websites.
- Email file attachments.
- Shareware or freeware software that may have other unwanted software included as part of the installation process.
- Wireless access points (without strong security these are easy access points into your computer or enterprise network).
- Network shares (either sharing your computer resources or sharing other computing resources allows the possibility for malware to spread from computer to computer).

It should be clear that almost any activity that causes an interaction in any way whatsoever with the “outside world”, external to the PC, creates the potential for the PC to become infected.

The range of attack software waiting to exploit these seemingly innocuous user actions is very broad. It is important to note that many lines are being crossed, blended or blurred with newer malware, spyware, adware, rootkits and other unwanted software pests borrowing tricks and techniques from legitimate programming code, and even more so from each other. The distinction between one type of malware and another is becoming harder and harder to make as the threats borrow, combine and blend with each other.

Here are some of the most common types of unwanted software and pests:

- Adware
- Backdoors
- Browser Helper Objects (BHOs)
- Browser Hijackers
- Downloaders
- Droppers
- Keyloggers
- Password Crackers
- Remote Access Trojans (RATs)
- Rootkits
- Spyware
- Trojans
- Viruses
- Worms

The following matrix provides some insights into the nature of the more common forms of unwanted software. This matrix illustrates the “blurring of the lines” between the different forms of unwanted software. As is indicated within the matrix, there are very few attributes of these attacks that are unique to a given type of malware.

FIGURE A
Comparison of the most common forms of unwanted software

EVOLUTION OF THREATS

Evolution of Threats	Mid 1980's	1990's	Late 1990's	2000 Blended Threats	-2002 Spyware	-2002 Adware	~ 2003 Rootkits
Threat Categories	Viruses	Worms	Trojans	2000 Blended Threats	Spyware	Adware	Rootkits
Can Carry/Distribute Payloads	YES	YES	YES	YES	YES	YES	YES
Can Operate as a Defensive Mechanism	YES	YES	YES	YES	YES	YES	YES
Can be Destructive (Modify or Delete Data/Programs)	YES	YES	YES	YES	NO	NO	YES
Difficulty of Removal	LOW-HIGH	LOW-HIGH	LOW-HIGH	HIGH	MEDIUM	MEDIUM	HIGH
Rate of Infection	HIGH	HIGH	LOW	HIGH	LOW	LOW	LOW
Can Phone Home (Capture & Send Data/Retrieve Software)	YES	YES	YES	YES	YES	YES	YES
Can Self Propagate	YES	YES	NO	YES	NO	NO	NO
Stealth Mode/Obfuscation/Hiding	YES	YES	YES	YES	YES	NO	YES

SECTION 2

Simplify Threat Protection With an Integrated Approach

To deal effectively with the rapidly evolving threat landscape, a threat management solution should consist of tightly integrated components that provide comprehensive threat protection while forming a much broader security and enterprise IT management platform.

Comprehensive Threat Management

You need to take a concerted approach to security at all levels, using a flexible, well-rounded, and multilayered solution to protect endpoints both on and off the network. Malware and other threats can be managed much more efficiently and cost-effectively when you tackle them in a centralized and common manner.

Great efficiencies come with combining functions like anti-virus and anti-spyware into a single product under one web-based console with a common client agent and common logging facilities and updating tools. A common architecture allows the different solution components to complement and leverage one another, and centralized management enables easy installation, software updates, streamlined policy creation and deployment.

Tackling Unknown Threats

For protection against zero-day attacks and other unknown threats, you need to augment signature-based products with behavior-based technologies that can detect anomalies and prevent suspicious code from running. These solutions need to be flexible enough to adapt themselves to your business processes instead of the other way around, so you can protect systems without disrupting the user population. The best solutions blend personal firewall software with intrusion detection and intrusion prevention to create a powerful, centrally managed host-based tool that protects clients on and off the network. Enterprise-class products will also offer very granular options for policy creation and enforcement.

Managing the Threat Within

Stick to the same simplification theme and look for a secure content management solution designed to handle virtually every content security issue facing enterprises today. These include spam, phishing, malicious mobile code, peer-to-peer file sharing, misuse of confidential data, intellectual property theft and inappropriate Internet use.

The ideal content management solutions are highly customizable. Business-driven policy engines and centralized policy management will help you create your own rules for incoming and outgoing email and web access. By managing such a wide range of threats effectively through one integrated content management solution, you can protect your business while improving employee productivity, helping ensure regulatory compliance and optimizing the use of IT resources.

Highly Scalable and Across Diverse Client Populations

A comprehensive threat management solution must scale to meet the needs of the largest global enterprises, and support environments with diverse endpoint platforms and a mixture of user languages. The solution should protect your network both at the endpoint and the gateway, enabling you to safely manage and protect against a multitude of threats — known and unknown.

So what is required for an effective threat management vision to become reality?

Two fundamental elements: being Complete and being Integrated are required. Let's look in more detail at how each of these elements contributes to an effective threat management solution.

COMPLETE A complete solution is available across a broad range of platforms, to meet the needs of large, diverse corporations. It also provides comprehensive and proactive threat protection, to guard against the increasingly complex range of attacks. It should also include a world-class Security Management Research team so that future vulnerabilities, malware, spyware and threats can be quickly identified and defeated. The quick appearance of new threats makes this type of leading-edge threat research essential.

INTEGRATED An integrated threat management solution is based on a common, modular architecture. Services and capabilities are common across all the components of the solution. An integrated architecture of this kind has several very important benefits:

- **Centralized Management** of the entire threat environment, which makes management much simpler and less costly. Centralized threat management allows for easier product installation and software updates and streamlined, centralized policy creation and deployment.
- **Improved Service Availability** when anti-virus components are acquired and installed from different vendors, it often results in kernel-level conflicts of those components. Integrated components from a single vendor tend to work together much more effectively, without these types of algorithm clashes.
- **More Effective Threat Protection** from blended threats, attacks that combine several threat types into one. Blended attacks are more easily combated by a combined threat defense than if each anti-threat component were a stand-alone product.

Simplified Threat Management - The CA Vision and Approach

The purpose of IT is to support the business processes. These business processes are supported by IT services that are built on application environments which include the IT assets and the users associated with them. CA's vision is to enable IT to successfully deliver the services that the business demands. To make this a reality, all of IT must be managed and secured. Enterprise IT Management, or EITM, is CA's vision to unify, simplify and secure the management of enterprise-wide IT. CA has unique expertise in this area; CA has been a leader for many years in the management and security of large IT environments. CA has leveraged this expertise and broad customer experience to develop and deliver our integrated threat management vision and product suite.

CA has developed this comprehensive integrated threat management vision and product suite after consulting with customers, industry experts and analysts. CA believes that effective threat management solutions should have the following key characteristics and objectives:

- **Comprehensive Threat Protection** The best solution is one that fully addresses the scope of threats and pests that computer users face: viruses, worms, Trojans, malicious code, spyware, adware, spam, phishing scams and inappropriate web content. Fragmented, partial solutions are no longer effective.
- **Unified Management Structure** A single management infrastructure and standard web-based management console interface enables IT professionals to operate efficiently. System administrators can provide rapid response to security issues, deploy solutions and updates quickly, create and enforce policies, query endpoints and create needed management reports and charts with ease. A unified threat management console makes it easier to manage the security needs of a large network than is possible with disparate, stand-alone products.
- **Modularity** Enterprises want the flexibility of stand-alone modules that can be added easily with integrated components to create a single, seamless, comprehensive suite without possibility of operational conflicts.

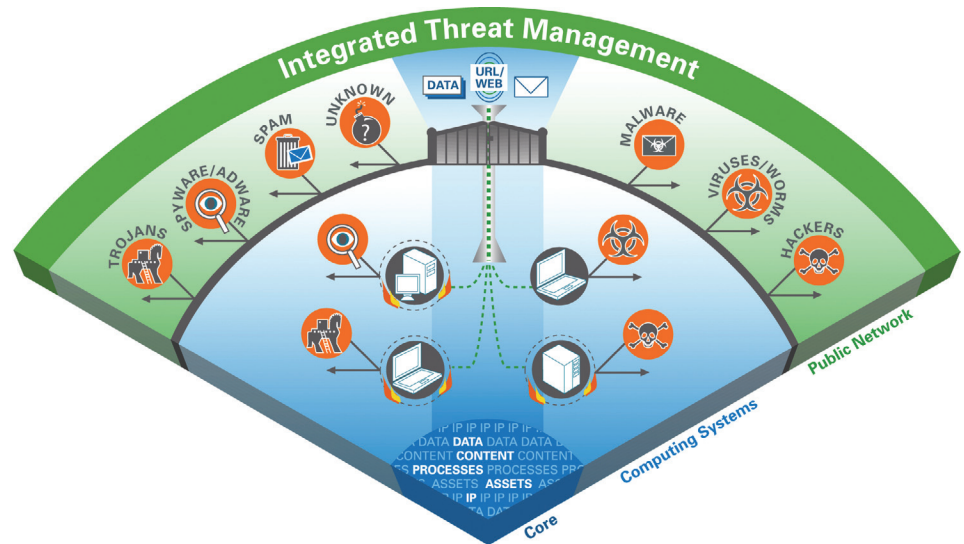
- **Cost Containment** A small footprint, transparent (and negligible) user impact, rapid implementation and streamlined management through a standard infrastructure and interface are just some of the ways an integrated threat management solution can reduce costs and accelerate payback/ROI.
- **Vendor Responsiveness** Given the ever-changing and complex nature of today's, and certainly tomorrow's threats, there is no substitute for a security management partner with a high-caliber, global research team that can respond and distribute threat remedies quickly.

True integrated threat management encompasses prevention, management and mitigation of current and future: threats, attacks, malware, spyware, adware, pests, spam, fraud (phishing and pharming) and content filtering (Web or URL) for office-based and remote/traveling endpoint systems (e.g., desktops, laptops, servers, etc.) and extends all the way to the gateway. CA's integrated threat management vision and solutions encompass a multilevel approach to security that begins with a common management platform, common agents, policy creation and enforcement, detailed reports and charts for the entire enterprise. Industry analysts have been very positive regarding the completeness of the CA integrated threat management vision. Figure B illustrates the CA vision of an effective threat management platform.

FIGURE B

The CA vision for integrated threat management defines solutions for both the endpoint and the gateway.

EFFECTIVE INTEGRATED THREAT MANAGEMENT IS MULTITIERED (ENDPOINT AND GATEWAY).



SECTION 3

Reduce Risks While Lowering Security Costs

With CA Threat Management solutions, you can address a wide range of computer threats, attacks and malicious code from the endpoint to the gateway, with one centrally managed solution that is cost-effective and efficient. Key benefits to be realized include:

RISK MITIGATION By reducing the threat of various attacks, you greatly improve the risk profile of your entire organization. Lowered IT risks translate to lowered corporate risks, which can have a significant impact on your company's overall market and financial position.

ASSET PROTECTION Your business operations depend upon computer and network systems, web applications and critical system files and repositories. These IT resources must be protected from unauthorized access and malware attacks since an attack on them is an attack on the business itself.

COST REDUCTION By greatly reducing the threat of successful attacks, you can reap significant financial benefits. Users and the IT staff become more productive because they spend less time dealing with attacks. Meanwhile security administration is much more efficient, because administrators and help desk personnel spend a lot less time in reactive mode, dealing with the aftermath of a successful attack.

SERVICE CONTINUITY Computer attacks can — and in fact often seek to — have a dramatic impact on the availability of critical enterprise IT services. The result can vary from an employee losing an hour of productivity while cleaning up an infected machine, to the catastrophic loss of a multimillion dollar financial transaction because a key application is shut down.

REGULATORY COMPLIANCE End-to-end security of the entire corporate IT infrastructure is a fundamental part of business regulations today. Auditors are looking for strong, effective IT controls that can detect, remediate and monitor the existence of software attacks of all kinds. Given the growing complexity of both the attacks and the IT environment, comprehensive and integrated threat management is essential for regulatory compliance.

Conclusions

In the past, threats have often been managed using separate threat management components, such as anti-virus, anti-spyware, etc. This “silo” approach leads to excessive administration costs, but more importantly, does not provide the effective and comprehensive threat management capability that is needed to combat these ever-increasing threats. This is because recent attacks have involved combinations of different kinds of malware, limiting the effectiveness of separate components designed to combat only a single type of attack. A more effective approach is an integrated threat management solution that provides centralized management of all anti-threat capabilities.

In the war against those who wish to control our computing resources, networks and even the Internet itself, it is important to have a flexible, adaptable, well-rounded, multilayered approach to threat defense. Such an approach should provide a centralized, scalable, policy-driven, command and control management center for dealing with threats, both now and in the future.

The ideal threat management solution should be Complete, Integrated and Open. CA’s integrated threat management vision, strategy and security solutions will provide you with the fully-integrated industry-leading threat management solutions that help you maximize your computing resources and shield you from the harmful effects of these insidious malware attacks. The result is significantly better security, as well as increased administrative efficiencies.

ABOUT THE AUTHOR



Christopher Wraight

Chris has over twenty years of Direct and Indirect Sales, Product Management, and Product Marketing experience in various enterprise and shrink-wrapped markets. Most recently, he was with Phase Forward, the leading provider of enterprise clinical trial and drug safety management solutions. Prior to that, he headed up the Americas marketing effort for Sophos where he helped double revenue two years in a row.

Chris lives in Southborough, Mass with his wife and three children and enjoys technology, photography, bicycling, kayaking and family time.

To learn more and see how CA software solutions enable organizations to unify and simplify IT management for better business results, visit ca.com/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.

WP05TMWP1E MP29314