

# Protection Methodology for Malware Variant Attacks

---

# Table of Contents

---

## Executive Summary

---

SECTION 1: CHALLENGE 2

### **Protection Against the Latest Malware Variant Threat**

No One Can Guarantee Protection Against a Variant Release Inside a Corporate Network

---

SECTION 2: OPPORTUNITY 3

### **Recommendations for Security Posture Improvements**

---

SECTION 3: BENEFITS 6

### **Benefits of Malware Attack Protection Are Recognized**

---

SECTION 4: CONCLUSIONS 7

---

ABOUT CA **Back Cover**

# Executive Summary

## Challenge

---

Information Security involves more than just anti-virus, user account management or even network access controls. The technical sophistication of today's malware is unlike anything ever experienced in the past. Just one lapse in an overall, best practices information security posture can result in massive downtime and/or system outages that can affect employees, partners and especially customers. No matter how well a company may "believe" they are doing at protecting the network, systems and data; once customers learn that a company has been hit by a malware attack all confidence in the protection of information will erode overnight. For that reason, it is vitally important that everyone involved in information security have a complete understanding of the recent advances in the creation of malware variants and take a proactive stance to protect their IT environments from attack and eventual compromise.

## Opportunity

---

There are many companies that can be used as an example of major corporations that haven't been affected by even the last year's malware variant attacks because they have a mature and comprehensive information security program in place. It's not enough to be doing a fantastic job in several areas of security if a company lacks complete coverage across "all" areas. With today's new malware variant attacks, it only takes one computer, in some unmanaged group, in some out of the way location to bring down an entire, worldwide corporate IT network. Reviewing IT and security procedures after an incident is the wrong time to really decide if the company can afford a prolonged outage. In most cases, a review of just the basic areas of information security will reveal opportunities for improvement to take the proactive approach to guarding the corporate network from abuse and attack.

## Benefits

---

Along with the obvious benefits of not having a long and costly system or network outage, the outlined security improvements can actually improve the overall security posture of the company, systems, computers and network infrastructure. There are good reasons why these best practices are part of an overall information security audit program at most every major corporation in the world today. Most large corporations are looking for smarter ways to protect themselves such as the recently announced CA Host-Based Intrusion Prevention System (CA HIPS) which takes a leap forward in another example of proactive security protection. Taken out of the context of improving security posture, many of these outlined areas can also result in substantial cost savings if properly executed.

## Protection Against the Latest Malware Variant Threat

The malware industry isn't new; it's been around for about 20 years. Over the past year however, we've witnessed a massive increase in the technical sophistication of malware unlike anything we've seen in the past. This new breed of malware includes a strain that is primarily designed to evade detection and gain initial entry. We haven't seen a case of mass-transmitting malware in more than a year as malware authors have figured out that a new and better method is much more effective.

Computer malware writers continue to learn by trial-and-error and through the sharing of techniques. The "sharing" can be formal, through web groups, chat groups, IRC sessions, emails and web forums designed and run by malware authors. The sharing can also be informal, by a less-educated malware author dissecting a new piece of malware to learn how it works and applying their own enhancements to add or change the performance capabilities.

The latest strain of malware is designed to evade initial detection by infecting a vulnerable computer, then connecting to the "malware distribution server", to download new, unique malware generated automatically which can then spread rapidly through even the most secure network environment. Once inside, malware spreads to other computers on the network using tried and true methods such as spreading via file sharing access to administrative shares (admin\$) and through brute force dictionary attacks against the network account passwords.

These new malware writing techniques further enforce the fact that the only way to completely protect your computers on a network is through a defense in depth methodology. Defense in depth doesn't rely on just one method, system or application, but builds in multiple layers of protection. The use of anti-virus, anti-spyware or even a single engine anti-malware solution alone will not be able to completely prevent such outbreaks.

Most anti-malware products primarily rely on signatures that are based on a sample to create the detection. Some security products use "heuristics", which will improve the detection rate by looking at closely matching signatures or behaviors. Without the sample, most anti-malware products cannot detect the malware. Some of the latest, like CA HIPS use "whitelisting" and allow only known, good programs to run.

### **No One Can Guarantee Protection Against a Variant Release Inside a Corporate Network**

In this new breed of malware, once the vulnerable computer has been compromised, it acts as a direct pipeline to bring brand new, NEVER-before-seen malware directly inside the target company, bypassing all of the security mechanisms implemented to stop this very attack. The malware is generated automatically and has never before been seen "in-the-wild", so in most instances anti-malware solutions may not have the signatures to detect the initial or subsequent follow-up pieces of malware.

The use of anti-malware, firewalls, content inspection, web blocking or even intrusion prevention is incapable of complete protection if just one computer is successfully penetrated inside the network.

For this reason, it becomes even more imperative that companies proactively take steps to improve their overall security posture.

*"There is no guaranteed protection from an unknown malware variant released inside a corporate network."*

## Recommendations for Security Posture Improvements

The recommendations for security posture improvements can be categorized into the following areas; anti-malware, network/host-based intrusion prevention, patch management, vulnerability remediation and network access management.

If these security improvements areas are implemented properly, it will drastically reduce the risk of a security breach compared to an unimproved infrastructure.

### Anti-Malware (Includes Anti-Virus and Anti-Spyware)

The category of Anti-Malware denotes four major solutions that need to be in place. Whether they are part of a integrated solution or a stand-alone, they must all be properly implemented to be effective. The four solutions are Anti-Virus, Anti-Spyware, Anti-Spam and a HIPS component that includes a Personal Firewall.

For each of the four solutions, it is absolutely critical that each is fully implemented, managed and administered. Any lack of management may, and probably will, result in a full breach of security.

The following are the primary areas to verify the continued administration and management:

- Policies
  - Force anti-malware solutions to be resident and active on all computers
  - Lock down anti-malware policies so users can't disable them or stop scans and updates
  - Verify that all computers are part of a managed group and will receive all product updates and signatures regardless of whether they are located in the office or on the road
  - Push signature updates out to all workstations and servers at least daily
  - Enable incoming and outgoing protection on all computers
  - Block all non-essential ports from both incoming and outgoing connections at the workstation/server
  - Set up group blocking of spam at the gateway and allow for individual blocking at the mailbox
- Scans
  - Set up regular, daily and weekly scans for anti-virus and anti-spyware applications

### Content Inspection and URL Blocking

As with anti-malware, the two previously separate areas of content inspection and URL blocking have merged in recent years to where most solution providers now do both. Content inspection involves a gateway solution that inspects all incoming attachments and can block malicious or unwanted contents based on the type of file, size, kind of attachment or even by key words. URL blocking will deny access by either the contents of the site (for example, adult, games or non-business appropriate) or through an inspection of possible dangerous conditions to unsuspecting visitors. Many URL blocking systems today can also deny access to websites that are known to infect visitors.

*"It only takes one crack in a dam to allow the floodwaters to be released."*

*“HIPS offers an additional layer of threat protection to complement your traditional, signature-based threat prevention products and provide real-time protection from both known and unknown (zero-day) threat attacks.”*

### Network/Host-Based Intrusion Prevention

The first generation of intrusion prevention solutions to hit the market were placed on the network and looked at all traffic conditions to build patterns of normal versus abnormal or malicious traffic. If abnormal traffic was detected, it could be blocked. Most companies found Network-based Intrusion Prevention Systems (NIPS) to be difficult to manage due to the effort required to accurately differentiate “normal” from abnormal. When NIPS systems started blocking business traffic, they were doomed to failure.

Host-Based Intrusion Prevention Systems (HIPS) work at the host, or individual computer level. They look at incoming network traffic as well as local logon to the machine to determine if the connections should be allowed. Because HIPS systems can be implemented locally and managed as groups, they’ve become a much easier and faster solution to block both known as well as suspected malicious activity. HIPS solutions such as CA HIPS can also extend the layer of protection that you normally expect within the corporate environment to the road warriors who are required to connect their laptops to networks from some of the most hostile environments, such as hotel broadband connections.

HIPS technology allows companies to:

- add a layer of protection to computer users inside or outside the corporate network by blocking malicious activities, downloads or installation of non-approved software
- provide remote and traveling users with a managed personal firewall while connected to unprotected networks such as those in hotels
- provide remote and traveling users who are connecting into the corporate network from outside the corporate perimeter firewall with a managed personal firewall

### Patch Management

Keeping a corporate computer updated with the latest operating system security updates, application patches and browser patches is a difficult proposition for most companies considering that most don’t have the luxury of a homogeneous IT environment of just one type of computer with just one OS level. Most deal with literally hundreds of combinations of computer hardware, OS, applications and versions, as well as configurations. If this wasn’t an almost impossible task for most businesses, then we throw in the telecommuting worker or the traveling employee who must have their system up-to-date or risk the security and operations of the entire IT environment.

Even a basic level of control over patch management requires a COMPLETE inventory of all systems up-to-the-minute with the ability to receive immediate notification if an unknown system shows up on the managed network. Part of this situation can be eliminated by the use of Network Access Control (NAC), which will be discussed further in this paper.

*“Just one infected computer can communicate with a malware downloader site to bring in hundreds of never-before-seen malware variants in the first hour”*

If you have a complete asset inventory, here are the elements that must be included in an overall patch management strategy:

- Workstation/Server OS updates:
  - Prioritize on security updates, but ALL systems must be current with ALL published and applicable updates.
- Workstation/Server applications:
  - Build a list of “approved” corporate applications that are maintained through the corporate patch management system.
    - If Microsoft Office applications are used, these MUST be included in the patch management updates.
  - Investigate “denying” the use of unapproved applications that can risk system integrity or security (such as media players, browser plug-ins, games, stock trading, music sharing, etc.).
- Browser updates:
  - If you use Microsoft Internet Explorer, then updates are included in the Microsoft patches.
  - If you use another browser such as Firefox or Mozilla, then include browser patches.

### **Vulnerability Remediation**

Some software application vulnerabilities cannot be remediated simply through the application of a software patch. A large number of vulnerabilities in older versions of software, such as browsers, can't be patched due to the incompatibilities in the application. In many instances, the only way to completely resolve a vulnerability is to make changes in the settings of the application or through other remediation measures such as isolating the system on the network.

Vulnerability management systems and services are available today to reduce or eliminate this gap in the security defense. These systems scan the network, workstations, servers and network-attached hardware to search a massive catalog to verify that all systems are up-to-date with patches and have the correct configuration for compliance with that specific company's IT policies. Most of these systems can be configured to alert administrators when they have located systems that are out of corporate compliance.

Vulnerability Management systems can also be proactive in locating possible conditions that may become evident when a policy is instituted or changed. Think of this as running a “what if” scenario on all network connected systems for compliance changes.

### **Network Access Control**

Network Access Control (NAC), also called Network Admission Control, is a fairly recent development in the protection of IT through the regulation of connections from end user systems. NAC is a method of increasing network security for a closed IT environment by requiring authentication, authorization and security compliance before allowing a connection on the corporate network. NAC can also control or restrict what a user can do once they are on the network.

The typical NAC scenario is to check the authentication of a user, verify the system is up-to-date with all operating systems, browser and application patches, as well as anti-virus and anti-spyware updates, before allowing a controlled connection on the IT network.

Included in the requirements to manage every corporate computer, companies must also look at the other systems that must be managed for a complete, holistic approach to security including computers coming into the corporate network from outside by:

- partners
- customers
- telecommunicating employees
- traveling employees (i.e., sales, etc.)

For companies that aren't yet ready to dive into the full NAC solution, there are alternatives in use by many companies today that "mimic" the NAC methodology. Set up a system to query and verify that computers coming into the corporate network (by outside partners, customers, traveling employees, telecommuters, etc.) are protected before being granted any access to the network. At a minimum, protection should include anti-virus and anti-spyware software with the current signature updates installed. While you can't verify OS patches without Admin rights (in most cases), the verifications above provide an increased level of security.

---

### SECTION 3: **BENEFITS**

## Benefits of Malware Attack Protection are Recognized

Most companies aren't in the business of security and only implement security solutions as a means to properly protect their assets. Assets such as intellectual property, design, manufacturing and customer sales can be dramatically impacted by a lack of a comprehensive information security strategy.

As many Chief Information Security Officers have discovered, secure today doesn't mean they are still secure tomorrow. As has been quoted by many security professionals, "security is a journey, not a destination." To be secure means a constant vigilance of the latest attack methods and more importantly, the latest proactive protections.

Taken out of the context of improving security posture, many of the outlined areas can also result in substantial cost savings if properly executed. For example; many companies have been able to prove cost benefit from the implementation of a patch management solution such as CA's Unicenter® Patch Management over their previous manual process or even competitive software that hasn't delivered on it's promises. The latest laws and regulations on compliance require many of these security safeguards be in place, but the savings or reductions to the bottom line for many companies is an ancillary benefit.

---

## SECTION 4: CONCLUSIONS

*“CA Threat Manager 8.1 is a powerful, scalable solution that enables us to centrally manage anti-virus and anti-spyware security measures across our entire 15,000-node network,... Its real-time scanning features are particularly attractive to us as we cope with constantly evolving malware threats.”*

---

### **Bruce Wignall**

Chief Information Security Officer  
Teleperformance, a global leader in  
contact center management.

Many of the best IT operations in the world lack the resources, the skills or the time to dedicate personnel to many of the tasks required to maintain vigilance against the constant threat of malware infections.

CA offers a comprehensive array of support, education and service solutions to assist our customers in many ways that aren't associated with just the implementation of CA software solutions. CA also provides expert resources around-the-clock from CA Security Advisor to deliver comprehensive answers and advice to the most important security issues of today.

### **CA Technical Support**

CA offers online technical support which includes documentation, bulletins, support forums and other online resources to address your technical issues along with current information on CA products.

If someone in your company should find malware that isn't detected by your current anti-virus or anti-spyware solution, you should send it to CA for analysis.

If you are not yet a CA customer, send any suspected malware to CA by password-protected zip file emailed to [virus@ca.com](mailto:virus@ca.com) with the password of "virus".

If you are currently a CA customer, you can continue to send samples to [virus@ca.com](mailto:virus@ca.com) (with the same zip file password of "virus") and then contact your Level 1 Support team for immediate assistance.

For online technical assistance and a complete list of locations, primary service hours and telephone numbers, contact Technical Support at; <http://ca.com/support>.

### **CA Technology Services**

CA offers a variety of education and service solutions to assist our customers. CA Technology Services applies recognized best practices to deliver custom solutions that can unify and simplify the way your enterprise functions and performs.

For example consider paid services from CA such as training for the help desk in threat response and best practices for anti-virus or anti-spyware client policies. Training could include a plan to implement appropriate policies for systems that leave or operate outside the corporate perimeter. Such training could also include methods of using CA HIPS to lock down infected or suspect systems while those systems are being investigated.

For more information on CA Technology Services, visit the CA Technology Services website at; [www.ca.com/services/](http://www.ca.com/services/).

### **CA Security Advisor**

The CA Security Advisor delivers around-the-clock, dependable security expertise that has provided trusted security solutions to the world for 20 years. Providing a complete threat management resource, CA's Security Advisor is staffed by industry-leading researchers and skilled support professionals delivering the knowledge to secure.

*“After evaluating all the big players, CA Threat Manager has the most efficient centralized management as well as the smallest footprint on the end-users’ desktop. Once deployed and set up properly, it doesn’t require a full-time IT person to ensure that the product is functioning properly. Since we started using CA products for our customers, virus and spyware issues have been greatly reduced. In fact, we very seldom get malware calls.”*

---

**Daniel Root**

President and CEO, Technify, a cost-effective and reliable IT outsource.

CA Security Advisor is a complete threat management resource that computer users can depend on. It is comprised of a network of rapid response centers that vigilantly monitor threats around-the-clock. New security threats may include malicious code, software and hardware vulnerabilities and network attacks. Upon the discovery of a new security threat, the CA Security Advisor responds with solutions to detect and protect against a malicious attack. In addition, the CA Security Advisor provides information and assistance for combating the outbreak, including expert advice and descriptions of threats including risks, impacts, affected versions, distribution methods, detection signature files, validated recommendations and instructions for fixing the problem and clean-up utilities.

The CA Security Advisor helps ensure CA's award-winning Threat Management Solutions — CA Threat Manager, CA Anti-Virus, CA Anti-Spyware, CA Host-Based Intrusion Prevention System, CA Secure Content Manager, CA Policy Compliance, CA Vulnerability Manager and on the consumer side CA Internet Security Suite 2008, CA Anti-Virus 2007, CA Anti-Spyware 2007, CA Personal Firewall and CA Anti-Spam 2007 — are always ready to address tomorrow's security threats today. Additionally, the security expertise and resources of the CA Security Advisor provide benefits to help your organization:

- Effectively manage business risk. With the comprehensive security information, tools, and support available from the CA Security Advisor, enterprises are empowered to manage risks and business impact proactively — rather than simply react to security threats.
- Protect critical computing assets. IT security personnel stay updated on the latest security threats, enabling the correct protection to proactively secure an organization's critical computing infrastructure, and consequently reduce the risk of information compromise or costly downtime.
- Respond faster to security threats. The vigilant monitoring by CA's global network of CA Security Advisor Rapid Response Centers allows for the immediate discovery and notification of new security threats — no matter when or where they may surface — so enterprises can rapidly respond to an attack.

### **Independent Certifications**

CA Threat Manager and CA Anti-Virus are certified by ICSA LABs and West Coast Labs, and consistently receives the “VB 100%” awards from Virus Bulletin for detecting 100% of “in-the-wild” viruses. CA Anti-Spyware is also certified by West Coast Labs.

---

To learn more about security for your business visit CA Security Advisor at: [www.ca.com/securityadvisor](http://www.ca.com/securityadvisor)

To learn more about security for your home computers or home office visit CA Consumer Solutions at: [shop.ca.com](http://shop.ca.com)

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.

TB05THMGMT01E MP315400407

---

Learn more about how CA can help you transform your business at [ca.com](https://www.ca.com)

