

Protecting Endpoint Systems Against Viral Malware

Table of Contents

Executive Summary

SECTION 1: CHALLENGE **2**
Issues Surrounding Viral Threats

SECTION 2: OPPORTUNITY **2**
Requirements for Effective Virus Protection

What Is CA Anti-Virus?

Client-Server Mode

Client-Only Mode

The Anti-Virus Client

Alerts

Quarantine

Signature and Rules Updates

Network Protection Support

How Is CA Anti-Virus Deployed?

How Is CA Anti-Virus Managed?

Reporting

SECTION 3: BENEFITS **11**
Business Benefits of CA Anti-Virus

Certification

Platform Support

Business Benefits of Anti-Virus Protection in an Integrated Solution

SECTION 4: CONCLUSIONS **14**

SECTION 5: REFERENCES **14**

ABOUT CA **Back Cover**

Executive Summary

Challenge

The top computer threats are viruses and worms. Both these types of viral malware replicate themselves and can rapidly spread unless there is good anti-virus protection. For this reason, traditional anti-virus tools are fundamental to enterprise threat defense. Good anti-virus applications must be able to protect computers against all types of viral threats and also be able to rapidly respond to new and emerging viral malware.

Opportunity

An effective anti-virus application must have a reliable scanning engine that can remove viral threats rapidly. There are several internationally recognized anti-virus certifications that can be used to verify the effectiveness of anti-virus software.

Anti-virus applications must be regularly updated when new virus signatures are developed. Administrators can configure and manage anti-virus clients from a central location by using policies. Policies are an important tool that should be used, together with other simple deployment tools, so that anti-virus protection can be deployed automatically to clients across the network.

Benefits

CA Anti-Virus protects computers by using signature-based techniques to identify viral threats. These techniques complement the approach used by anti-spyware applications and the behavioral techniques used by intrusion prevention applications, such as CA Host-Based Intrusion Prevention System (CA HIPS). CA Anti-Virus works with these other CA Threat Management Solutions providing a complete suite of threat management tools.

SECTION 1: CHALLENGE

For more information about types of malware, see “Technology Brief — The CA Threat Management Solutions”.

Issues Surrounding Viral Threats

A recent IDC study¹ found that the top computer threats are viruses, then spyware and then unsolicited email, or spam. For this reason, traditional anti-virus protection is fundamental to enterprise threat defense.

A computer virus is a program that includes code so that it can replicate itself. Viruses spread by attaching themselves to a host program, document or boot sector. When the host program is executed or opened, the virus code also runs and starts the process of infecting new hosts. The other common type of viral malware is a worm. Worms are similar to viruses, but use network connections as the distribution vector. Some viruses and worms can execute code and cause additional damage, such as deleting or renaming particular system files. Viruses can also use a technique called polymorphism to attempt to avoid detection. A polymorphic virus changes its filename, and aspects of its code, after each replication. Polymorphism is not new — it was first recorded in a ‘proof of concept’ virus in 1990 and, since then, has been developed to include sophisticated and advanced techniques. Various polymorphic engines have been used by numerous viruses, and even some worms, over the last decade.

Malware developers create viruses and worms to try and exploit gaps in existing viral protection. The challenge for anti-virus applications is to protect computers against existing threats and minimise the opportunity for new viral threats to infect computers before their anti-virus protection can be updated. This is particularly challenging for polymorphic viruses, which replicate to take a different form that the malware developer hopes will evade anti-virus detection.

SECTION 2: OPPORTUNITY

An “in-the-wild” virus is one which is currently circulating between the computers of unsuspecting users.

Requirements for Effective Virus Protection

Effective anti-virus applications should include the following components:

- **Reliable and comprehensive scanning engine** It is essential that anti-virus applications are able to remove viral threats rapidly and effectively. To help assess the effectiveness of anti-virus products, there are several internationally recognized detection and removal certifications. ICSA Labs issues certifications for anti-virus products that can detect and clean 100% of “in-the-wild” viruses. West Coast Labs certifications include specific Checkmarks for different types of malware detection and removal, such as Anti-Virus Level 1, Anti-Virus Level 2 and Trojan. Virus Bulletin has the “100% Award” for anti-virus products that remove all viruses during test. You can also carry out your own tests; for example, the European Expert Group for IT-Security, also known as Eicar, provides a downloadable anti-malware test file that you can use to test anti-virus software.
- **Regular signature and software updates** All anti-virus applications must be able to be updated quickly when new virus signatures are developed. Signature updates must be packaged so that updates can be rapidly deployed across all computers in an enterprise. The anti-virus software itself must also be able to be updated to meet new types of viral threats.

1 Source: IDC, “Worldwide Secure Content Management 2006-2010 Forecast Update and 2005 Vendor Shares: “The Convergence of Secure Content and Threat Management,” #203550, September, 2006

- **Policy-based Management** Policies are an important tool that administrators can use to configure and manage anti-virus clients from a central location. Policies can be used to schedule updates and virus scans, manage alerts and set the level of protection required. The ability to use policy-based management is important for most enterprises, because all users and computers do not require the same settings for anti-virus protection.
- **Simple Deployment Tools** If multiple computers are installed across several physical locations, it is important to be able to rapidly deploy anti-virus protection by using automated methods. It must also be simple to deploy software updates across the network and to identify any computers that have not been updated.

For more information about the server components, see “Technology Brief — Protecting Endpoint Systems Using Threat Management Solutions.”

What Is CA Anti-Virus?

CA Anti-Virus protects computers against viral malware; viruses and worms. CA Anti-Virus provides anti-virus security for business PCs, servers and Personal Digital Assistants (PDAs). CA Anti-Virus is a client (endpoint) protection tool, which can be installed as an Agent Only Install for isolated clients, such as home office computers, or can be configured and managed from a central management server.

You can use CA Anti-Virus on its own, as “standalone” threat protection, or as part of CA Threat Manager or a CA Protection Suite. In either case, CA Anti-Virus can be installed in one of two modes: client-server mode or client-only mode.

Client-Server Mode

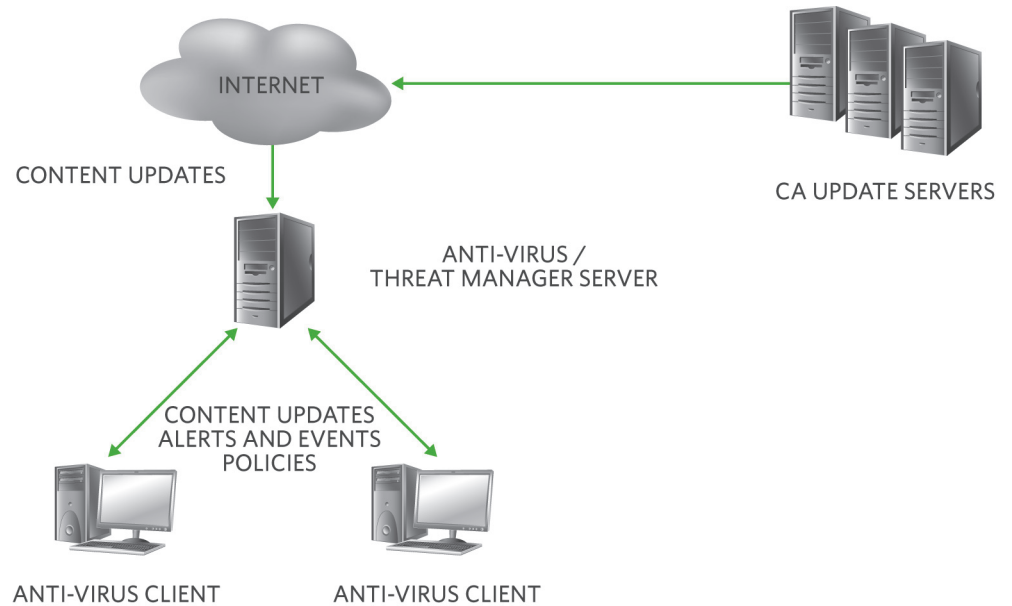
For most enterprises, client-server mode is the best way to use CA Anti-Virus, so that a central server manages the anti-virus protection on all the client computers. In this mode, CA Anti-Virus has these components:

- **Server components** The main server component is the management server, which includes the web-based management console and Alert Manager. Policies are managed from the server and stored in a database, before they are deployed to client computers. There is also an option to install additional redistribution servers, to help distribute anti-virus updates to client computers. Another optional server component is the Remote Install Utility, which is used to deploy CA Anti-Virus to Windows client computers.
- **Client components** The main client component is the anti-virus agent, which includes a Web interface and the shell scanner. The client components are described in more detail later in this brief.

FIGURE A

CA Anti-Virus is generally used in client-server mode.

CA ANTI-VIRUS CLIENT-SERVER MODE



For information about the discovery process, see “Technology Brief — Protecting Endpoint Systems Using Threat Management Solutions.”

When the anti-virus agent is running on the client computer, the agent initiates communications between itself and the web-based management console. To reduce bandwidth requirements, the frequency that the agent “phones home” to the management console to report its status and obtain new policy configurations is a separate configuration option to the frequency that clients poll for signature updates. The defaults for these two settings are every two days for “phone home” and every hour for signature updates.

A different process is used if a scheduled job, such as a hard disk scan, is defined as a policy on the server. In this case, at the time specified for the job, the server pushes the job details to all the clients that are affected by the policy. The client does not store the details of this policy. This means that administrators can easily create new scheduled jobs, and have them run at any time, without having to wait for the clients to first contact the server to get updated information.

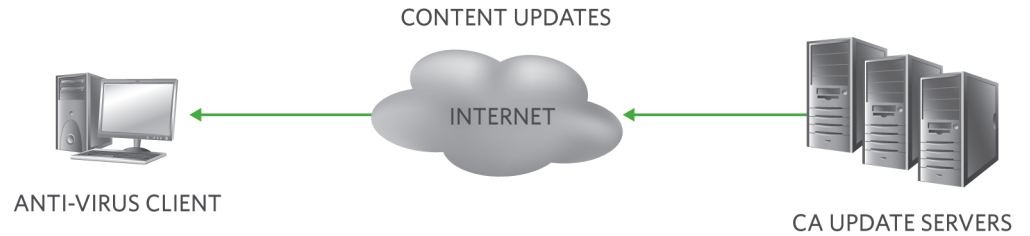
Client-Only Mode

If necessary, you can use CA Anti-Virus in client-only mode. This mode can be useful in situations where it is not possible to use centralized management. Computers used by home office workers, or laptops used out of the office, may be suitable for this mode. In client-only mode CA Anti-Virus is installed directly to each client, and each client makes an independent connection to the CA Content Update servers to download updated virus signatures and rules. In client-only mode there is no central management function, but you can easily migrate standalone clients to client-server operation by using discovery.

FIGURE B

CA Anti-Virus can be installed in client-only mode.

CA ANTI-VIRUS CLIENT-ONLY MODE



The CA Anti-Virus Client

The anti-virus client works in the same way, whether used in client-server or client-only mode. CA Anti-Virus provides comprehensive scanning of:

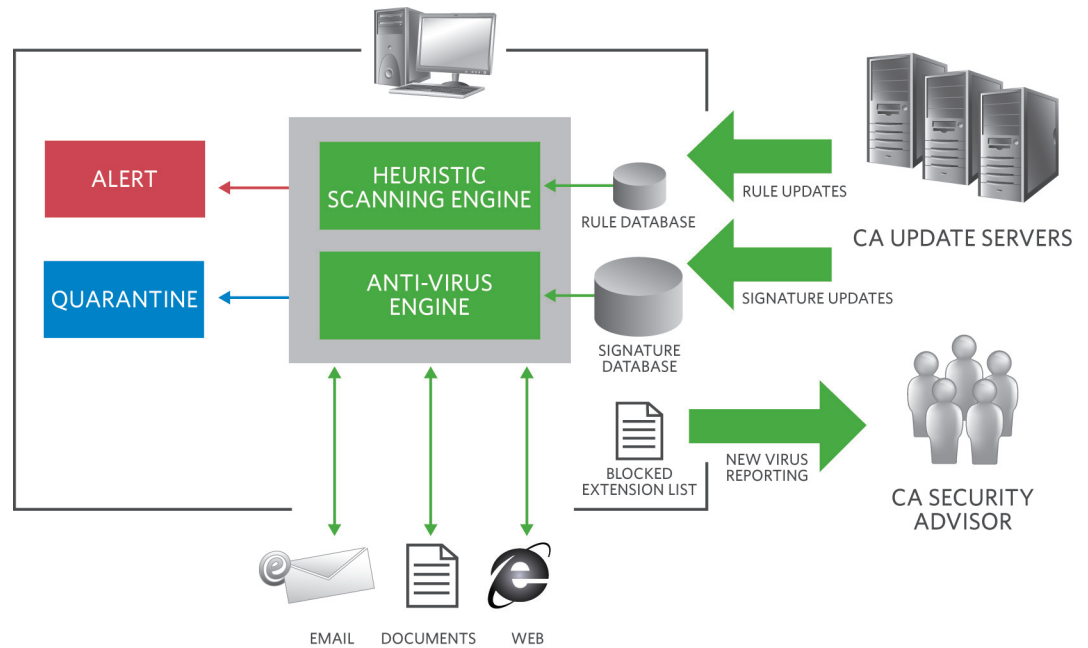
- **Boot sectors** Boot sector viruses infect the first sector of a hard drive and can have a serious effect on disk operation if they change information, such as boot records. CA Anti-Virus automatically scans for boot sector viruses.
- **Files** CA Anti-Virus can be configured to protect both local and network drives. Any files that are created or modified are automatically scanned, including temporary files that are created by web browsers when web pages are being viewed.

CA Anti-Virus not only removes malicious content from data that is being processed, but also restores an infected system to a safe and secure state, so it offers comprehensive virus scanning, detection and removal capabilities.

FIGURE C

CA Anti-Virus uses several components as part of the virus protection process.

CA ANTI-VIRUS CLIENT COMPONENTS



The main components of the CA Anti-Virus client are:

- **Anti-Virus Engine** This engine is responsible for the real-time and scheduled scanning of boot sectors, files and emails. This engine uses the signature database during the scanning process, to compare the items it is scanning with virus records in the database. If a piece of code in the item matches any virus identified in the database, the anti-virus engine refers to its configuration options to determine what action to take, such as using quarantine or sending an alert.
- **Heuristic Scanning Engine** This engine provides a protection mechanism against zero-day attacks. Heuristic scans do not use virus signatures, but instead look for particular instructions or commands within program code that are not usually found in legitimate application software. This engine can, therefore, detect potentially malicious functionality in previously unexamined viral malware.

The heuristic scanning engine in CA Anti-Virus uses rules to determine whether the program code in the file that is being examined is statistically likely to be a virus. Because heuristic scanning uses probability, there is always the possibility that legitimate code may be flagged as viral (false positives). Heuristic scanning also requires more computer resources and may affect computer performance, so the default setting for the heuristic scanning option in CA Anti-Virus is “not enabled”.

A zero-day attack is an exploit that is released before, or on the same day, that an operating system or application vulnerability is identified, and sometimes before a fix has been released.

CA Host-Based Intrusion Prevention System (CA HIPS) uses sophisticated behavior-based scanning to identify anomalous and potentially malicious code and help protect against zero-day attacks. For more information about CA HIPS, see “Technology Brief – Protecting Endpoint Systems Using Host-Based Intrusion Prevention” in this series.

- **NTFS alternate data streams** In NTFS, a file consists of different data streams. One stream holds standard file information and a second stream holds security information, such as the access control list. However, there may be alternate data streams (ADS), which are hidden from Windows Explorer and other normal file and directory tools. CA Anti-Virus provides a “scan alternate data streams” option, which scans ADS. Scanning of NTFS ADS is set to “off” by default, because it makes scanning slower.
- **Blocked Extension List** CA Anti-Virus offers a one-step virus block feature, which helps to rapidly isolate networks that may be experiencing a new virus outbreak. If a file extension is added to the Blocked Extension List, users cannot access any file that has that extension. This provides another strategy to use in situations where new or potential viruses are detected and associated with a particular extension. After signature updates that include protection against the new threat have been distributed, you may be able to remove the file extension from the blocked list.

Alerts

You can configure CA Anti-Virus to generate an alert when a virus is detected. These alerts can be sent to:

- **The local Alert Manager** The Alert Manager utility is a Windows-only application and is usually run on the anti-virus server. Alert Manager is used to collect alerts and forward them to system administrators by using email, SMS messages, pager or enterprise management applications, such as CA Unicenter®.
- **Event logs** On Windows computers, alerts can be sent to the application Event Log and on UNIX/Linux computers, alerts can be sent to the System Log.
- **Another computer** Alerts can be forwarded to another computer, so that information from across the enterprise can be collected and processed centrally. In a typical configuration, client computers forward alerts to an anti-virus or threat manager server. The server also forwards its own alerts to itself, so that all alerts (including its own) are collected. The server is also configured to send alerts to its own local Alert Manager, so that administrators receive immediate notification of priority alerts.

Quarantine

When managing malware threats, the term quarantine refers to the isolation of infected or potentially damaging files. In CA Anti-Virus there are two related quarantine processes:

- The quarantine folder is a secure folder for infected files, so that users can decide whether to restore, cure or delete the affected file.
- The quarantine option is used to prevent an infection spreading across the network. If the quarantine option is enabled on the anti-virus client, when a user tries to access an infected file from a server, or copy an infected file to or from a server, the user is blocked from accessing the server for a specified length of time. This option is only available for Windows NT, Windows 2000, Windows XP and Windows Server 2003 computers.

For more information about content update servers, see “Technology Brief — Protecting Endpoint Systems Using Threat Management Solutions.”

Signature and Rules Updates

The virus signature and rules updates for CA Anti-Virus use MicroDAT technology to ensure that content updates are less than 100 KB in size. This helps to ensure up-to-the-minute virus protection, because the small size of the updates means distribution has minimal impact on network traffic. If a distribution server is unavailable, because the server is offline or a mobile user is using a laptop from a public network, anti-virus clients automatically look for and acquire the latest signature from the next available designated distribution server.

Network Protection Support

CA Anti-Virus supports network protection technologies from Cisco and Microsoft. These technologies are designed to ensure that endpoint computers are compliant with network health policies, such as up-to-date anti-virus software, or personal firewall applications. If a computer has all the software required by the health policy, and the software is correctly configured, the computer is considered compliant and is granted the appropriate access to the network.

Cisco Network Admission Control (NAC) uses the network infrastructure to enforce security policy compliance. Cisco Trust Agent (CTA) agent software runs on endpoint devices, such as PCs, servers, and PDAs, and sends reports to a Cisco Access Control Server (ACS). The ACS compares the data in the report with a set of policies that were previously defined by a network administrator. Based on the results of the comparison, the end-point device may either be granted full primary network access or placed into a separate virtual network, where the device can go through a remediation process before it is allowed to connect to the primary network. The CA Posture Plug-in for Cisco NAC discovers the configuration and status for CA Anti-Virus on an end-point device, and reports these attributes to the CTA that is running on the end-point device.

Microsoft Network Access Protection (NAP) is a similar policy enforcement platform that is built into Microsoft Windows Vista and the next release of Windows Server (code name "Longhorn"). The CA System Health Agent for Microsoft NAP integrates with NAP to ensure that clients that connect to the network use the correct version of anti-virus software and that the virus signature files are up-to-date. The agent also ensures that clients meet required configuration standards and have all appropriate patches and updates installed.

If you administer CA Anti-Virus users on networks that are protected by Cisco NAC and Microsoft NAP, these tools help to ensure that client protection is up-to-date, and cannot be bypassed, either deliberately or accidentally.

How Is CA Anti-Virus Deployed?

There are several ways to deploy CA Anti-Virus across an enterprise. If you have a small number of client computers you can use the CA Anti-Virus CD-ROM and run setup on each computer. However, for most enterprises some form of automated deployment is required and CA Anti-Virus can be deployed by using several deployment tools:

- **Remote Installation Utility** This utility can be installed on the anti-virus server and is used to configure client installation options. These options are saved in an Installation Control File (ICF). This utility can then push client installations to computers on the network.

The same deployment tools that are used to deploy CA Anti-Virus are used to deploy CA Anti-Spyware; for more information about the deployment options, see “Technology Brief — Protecting Endpoint Systems Using Threat Management Solutions.”

- **Command-line installation** You can use the ICF with a command-line installation tool to install CA Anti-Virus from a network share point. If required, you can configure the installation to be silent, so that users are unaware that CA Anti-Virus is being installed on their computer.
- **Software delivery** You can use an automated software delivery tool, such as CA Unicenter® Software Delivery or Microsoft SMS, to deliver CA Anti-Virus application packages to client computers. CA Unicenter Software Delivery can be used to deliver CA Anti-Virus to all supported client platforms. Microsoft SMS can only be used to deliver CA Anti-Virus to Windows clients.
- **Login Scripts** You can use a login script together with any of the silent installation command-lines, to deliver silent installations across the network.

How Is CA Anti-Virus Managed?

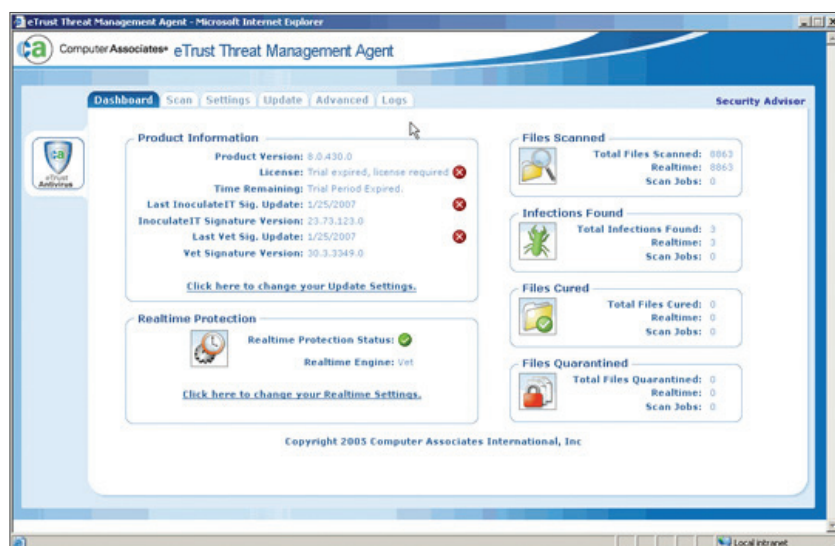
CA Anti-Virus uses a multi-tiered architecture, with a hierarchical organization structure, so that users and computers can be defined in relation to the business unit, location or other criteria. After you have defined your users and computers, you can apply anti-virus policies to different parts of your enterprise by using your organization structure. Management tools are available on both the anti-virus client and the management server.

Client user interface. The anti-virus client can be installed without a user interface by using an option in the ICF. If the user interface is enabled, the interface displays status information and includes several configuration options. However, even if the user interface is available, you can use policy options to prevent users from changing some of the settings.

FIGURE D

The anti-virus client can be installed so that there is a user interface.

CA ANTI-VIRUS CLIENT USER INTERFACE



For more information on the server components, see “Technology Brief — Protecting Endpoint Systems Using Threat Management Solutions.”

On Windows computers, the client user interface is the same whether CA Anti-Virus is installed on its own, with CA Anti-Spyware, or as part of CA Threat Manager (CA Anti-Spyware is not available for non-Windows platforms). If CA Anti-Spyware is also installed, the interface includes an Anti-Spyware tab. The user interface is divided into several tabs:

- The Dashboard tab provides the user with a summary of the current status of the anti-virus client, including signature and engine versions and anti-virus activity.
- The Scan tab enables the user to set up and configure scans of local disks.
- The Settings tab enables the user to configure options such as alerts and logging.
- The Update tab enables the user to specify signature update frequency and which servers should be contacted for updates.
- The Advanced tab enables the user to manage quarantine activity and inspect the job queue, such as pending scanning or update jobs.
- The Logs tab enables the user view activity logs.

SERVER TOOLS When you install the server components you get these tools:

- **Server console** This provides information about the server, software versions and the clients that are managed from the server. The console is also the tool you use to manage clients and client policies, and receive reports about threat activity. The console provides a complete view of the anti-virus situation in your enterprise.
- **Alert manager** This enables you to configure how alerts are sent to people or devices in your organization, so you can quickly respond to alerts. For example, alerts can be sent to an email Inbox, a pager, an NT event log, an SNMP trap, CA Audit®, or CA Unicenter. The Alert Manager runs on Windows only.
- **Redistribution server** This can also be installed on its own, for a computer that only acts as a redistribution server. When this is installed, in addition to the standard agent components and UI, there is an extra item on the Update tab that enables you to configure the redistribution.

Reporting

When installed in client-server mode, you can configure the anti-virus client to send status and event information to the central server. You can configure severity levels for the different types of information sent, so that critical messages are forwarded to the server Alert Manager for immediate attention. The server stores all the event information it collects from anti-virus clients and periodically processes this information into reports, by default every 24 hours. All CA Anti-Virus reports are generated on the server by using the web console.

The reporting engine in CA Anti-Virus provides 75 different types of graphical and detailed reports, including:

- **Top ten viruses** This report gives a summary of the most prevalent viruses across your network.
- **Top ten computers** This report gives a summary of the computers that have reported the most virus-related events across your network.
- **Top ten users** This report gives a summary of the user accounts that have reported the most virus-related events across your network.

All the top ten reports can be formatted for hourly, daily, weekly, monthly and quarterly reports.

- **Signature exception lists** This report shows the clients that have not received the latest signature updates, which can be a useful indicator of network problems or mis-configured clients.

By default, every 2 days, the reporting engine also runs a discovery process across the network and collects information about all the Windows computers, by domain or workgroup, and whether they are running CA Anti-Virus or other CA threat Management Solutions. These sets of reports also show the computers that do not have anti-virus installed and provide an up-to-date list of the systems that represent potential risks because they are not protected.

SECTION 3: BENEFITS

Business Benefits of CA Anti-Virus

CA Anti-Virus includes a range of features that are designed to protect client computers from viral threats and include:

- **Comprehensive Scanning** Comprehensive virus scanning, detection and removal capabilities mean that enterprises can use CA Anti-Virus as their primary defense against viral threats.
- **Central Web-based Management** A single web-based management console for managing any size of diverse environment is important, because:
 - It provides a complete view of the anti-virus situation within your enterprise.
 - You can use Windows, UNIX, Linux and Macintosh platforms as the core platforms for managing all anti-virus clients.
- **Bandwidth Savings for Signature Updates** MicroDAT signature updates (less than 100KB) help to ensure up-to-the-minute virus protection, because their small size speeds distribution with minimal impact on network traffic.

Certification

CA Anti-Virus is certified by industry experts and has received detection and removal certifications from ICSA Labs, West Coast Labs and Virus Bulletin. CA Anti-Virus consistently receives the "100% Award" from Virus Bulletin. CA has also received Checkmark certifications from West Coast Labs for malware detection and removal (Antivirus Level 1, Anti-virus Level 2 and Trojan). CA Anti-Virus is ICSA Labs certified for detecting and cleaning 100% of "in-the-wild" viruses.

These certifications provide enterprises with independent verification that CA Anti-Virus is effective in protecting their computers against current viral threats.

Platform Support

CA Anti-Virus has multi-language support, and can be run on a wide range of computer platforms:

- **Language Support** Depending on the operating system, CA Anti-Virus supports English, French, Italian, German, Spanish, Japanese, Brazilian Portuguese, Traditional Chinese and Simplified Chinese. If your enterprise is multi-lingual or global, you can select the best language for your users.

- **Supported environments** CA Anti-Virus is available for a range of operating system and application environments. Wide platform support means you can use one product across your whole network. The following lists show the environments that are supported by CA Anti-Virus r8.1, but legacy clients, such as Windows 9.x computers, can still use CA Anti-Virus r7, and the management tools support environments if both these versions are in use.

On Windows computers, CA Anti-Virus r8.1 supports the following Windows versions for the client:

- Windows NT 4.0 SP6a
- Windows 2000 Workstation and Windows 2000 Server
- Windows XP (32/64-bit)
- Windows Server 2003 (32/64-bit)
- Windows Vista (32-bit)

The following non-Windows operating systems are supported for the client:

- Linux (32-bit): Red Hat Enterprise Linux 3 and greater, SuSE Linux Enterprise Server 8 and greater, SuSE 9.0 and greater
- UNIX: Sun Solaris 8 and greater; HP-UX 11.0 and 11.11
- Apple: Macintosh OS X 10.3 and greater for Power PC; Macintosh OS X 10.4 and greater for Intel
- Novell: NetWare 5.1 and greater

CA Anti-Virus r8.1 also protects PDAs. The following platforms are supported for the PDA client:

- Palm
- Microsoft Windows Mobile 2002/2003/2005
- Microsoft Smartphone 2005
- Pocket PC 2003

There are versions of CA Anti-Virus which protect application platforms and network appliances. The following platforms are supported:

- Microsoft Exchange 2000 and 2003
- Lotus Notes/Domino 4.6.2 and greater
- Citrix Presentation Server 4 for Windows
- NetApp Filer NAS Appliance

The anti-virus management server can be installed on Windows or other operating systems. The following operating systems are supported for the management server component:

- Windows: Windows NT 4.0 Server (SP6a or later), Windows 2000 Server and Windows Server 2003
- Linux (32-bit): Red Hat Enterprise Linux 3 and greater, SuSE Linux Enterprise Server 8 and greater, SuSE 9.0 and greater
- UNIX: Sun Solaris 8 and greater
- Apple: Macintosh OS X 10.3 and greater for Power PC; Macintosh OS X 10.4 and greater for Intel

The anti-virus server is managed by using a web console and can be accessed from any platform that supports any of the following browsers:

- Internet Explorer 6 SP1 and above
- Mozilla Firefox 1.5 and above
- Safari 1.2 and above

Business Benefits of Anti-Virus Protection in an Integrated Solution

How CA Anti-Virus Works with Other CA Threat Management Solutions

One product or technique cannot protect against every possible threat. Multiple layers of defense are required, which are provided by different products for different threats. A combination of products that work together is needed to protect network-enabled workstations and mobile devices from network-based attacks. CA Anti-Virus has been designed to integrate with CA Anti-Spyware, to provide protection against both viral and non-viral threats.

When used together, CA Anti-Virus and CA Anti-Spyware are managed from the same web-based administration console that runs on an integrated threat management server, and both client applications are deployed as a single agent. This integration works in the same way whether you buy CA Anti-Virus and CA Anti-Spyware as separate products, or buy them bundled as CA Threat Manager.

CA ANTI-VIRUS is a core product within the CA Threat Management Solutions, which includes solutions for both endpoint systems (desktop, server, laptop, and other network access points) and gateways:

- **CA Anti-Spyware** Standalone anti-spyware protection for endpoint systems.
- **CA Threat Manager** Integrated anti-virus and anti-spyware protection for endpoint systems.
- **CA HIPS** Personal firewall, intrusion detection system and intrusion prevention system for endpoint systems.
- **CA Protection Suites** Integrated anti-virus and anti-spyware protection for endpoint systems, together with data backup and optional endpoint anti-spam.
- **CA Secure Content Manager** Anti-virus protection for the gateway, SMTP and HTTP filtering for incoming Web and messaging threats or spam, and content filtering of outgoing email traffic.

CA Anti-Virus is designed to work with other products in the CA Threat Management Solutions, to provide comprehensive endpoint threat protection:

- CA Anti-Virus is designed to detect and remove viral threats. When used with CA Anti-Spyware, either standalone or as part of CA Threat Manager or the CA Product Suites, CA Anti-Virus detects and removes malware threats that evade detection or that previously infected the endpoint.
- CA HIPS helps to prevent known and unknown threats, such as malware, spyware, adware and rogue software, from penetrating the network. CA HIPS provides proactive, host-based security against zero-day attacks. System administrators can use the key functionality in CA HIPS to learn system behavior and then create or edit existing policies to detect anomalies.
- CA Secure Content Manager monitors, filters and blocks potential threats from messaging, such as malware in spam and infected Web traffic.

SECTION 4: CONCLUSIONS

Anti-virus tools are fundamental to enterprise threat defense. CA Anti-Virus works with other CA Threat Management Solutions to help provide a complete suite of threat management tools. CA Anti-Virus signature-based techniques identify viral threats, and these techniques complement the approach that is used by anti-spyware applications and the behavioral techniques that are used by intrusion prevention applications, such as CA HIPS.

SECTION 5: REFERENCES

“CA Security Advisor”:
<http://www3.ca.com/securityadvisor>

“European Expert Group for IT-Security”:
<http://www.eicar.org>

“ICSA Labs”:
<http://www.icsalabs.com>

“Virus Bulletin”:
<http://www.virusbtn.com>

“West Coast Labs”:
<http://www.westcoastlabs.org>

To learn more about the CA Anti-Virus architecture and technical approach, visit [CA Anti-Virus Product Page](#)

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.

TB05AVPES01E MP317610607

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

