



Computer Associates®

eTrust™ Antivirus v7 Frequently Asked Questions

eTrust™ Antivirus v7 Frequently Asked Questions

Q. What is a virus?

A. A computer virus is a piece of programming code designed and written to make additional copies of itself and spread from location to location, typically without user knowledge or permission. A virus does not have to be destructive.

Q. How do viruses spread?

A. Viruses can spread by diskette, network, email or Internet downloads. Occasionally, they are accidentally spread within packaged software products. Viruses cannot spread on their own and must be executed by someone to cause damage. Boot sector viruses spread when a user inadvertently boots his/her workstation from an infected floppy disk. Macro viruses spread by the simple opening of an infected document. Mass mailing viruses use email to rapidly propagate, usually employing deceptive tactics to persuade the recipient to open the infected message.

Q. What kind of damage can viruses cause?

A. Once a virus is executed it can impact memory, affect performance, modify data or delete files. Some viruses wipe out hard disks or make them inaccessible. When a user has to fix the problem, viruses cause costly downtime and waste resources.

Q. How serious is the virus problem?

A. A survey of large organizations conducted by ICSA Labs reported that 99% have experienced a computer virus. The increasing use of the Internet and other online services has helped spread viruses.

Q. Does an independent third-party test antivirus software?

A. Yes. ICSA Labs tests and certifies antivirus software. To be certified, the software must detect 100% of "in-the-wild" viruses (in general distribution) and 90% of more than 6,000 test viruses. All versions of eTrust Antivirus are ICSA Labs-certified. The results can be viewed on the Web at icsalabs.com. The ability to detect all "in-the-wild" viruses is the real test of antivirus software.

Q. Why do I need antivirus software for my server?

A. As the central point in a network, a server can easily pass along a virus introduced from a client PC not running antivirus software. Running real-time antivirus software on the server will prevent this from happening. In addition, antivirus software can prevent viruses from spreading during server backups.

Q. Why do I need antivirus software for client PCs?

A. Client PCs are on the front line in the battle against viruses. Many documents flow into a PC and flow back out to customers, allowing for the transmission of viruses without ever reaching a file server. Running real-time antivirus software on the PC can prevent this from happening.

eTrust Antivirus v7 Frequently Asked Questions (cont'd)

Q. What features are important in choosing antivirus software?

A. Typically, the most important features to consider relate to virus detection, management, performance and ease of use. Other important factors include ease of maintenance and automated signature distribution.



eTrust™ Antivirus v7 Frequently Asked Questions

Q. What does eTrust Antivirus do?

A. eTrust Antivirus is an award-winning antivirus solution from CA that protects the entire enterprise against potentially damaging and costly virus attacks. Its features allow for easy configuration and management of multiple servers and clients. eTrust Antivirus provides all the tools a network administrator needs to manage antivirus efforts across the entire network.

Q. Can eTrust Antivirus protect servers and client PCs?

A. Yes. eTrust Antivirus is available for all versions of Windows, as well as for UNIX, Linux and NetWare servers, and Macintosh.

Q. How does eTrust Antivirus manage client installations?

A. Antivirus client nodes are managed through the multi-tiered, hierarchical management architecture of eTrust Antivirus. The eTrust Antivirus Admin Server tracks all instances of antivirus software discovered through an innovative, low-overhead process. Client configurations, including signature deployment policies, are easily maintained and deployed through the admin interface. To ensure that settings are not altered or virus protection is not disabled, client configurations can be "locked-down," safeguarding the network from dangerous gaps in protection.

Q. How does eTrust Antivirus detect viruses?

A. eTrust Antivirus scans files for known virus signatures or fingerprints. Once detected, a virus can typically be removed or cured. eTrust Antivirus also detects polymorphic and stealth viruses, which modify their signatures in attempts to avoid detection. In addition, eTrust Antivirus checks the boot sector and memory during virus scans.

Q. When will eTrust Antivirus check for viruses?

A. The eTrust™ Antivirus Realtime Monitor runs in the background, scanning files as they are executed and/or written to and read from a disk. Virus scans can be manually run or automatically scheduled to analyze all or selected files. eTrust Antivirus detects viruses in files downloaded from the Internet, online services and email systems, including compressed file archives.

Q. How can I get protection from the latest viruses?

A. Keeping antivirus software up to date is critical. CA's eTrust TARGET delivers the dependable, around-the-clock security expertise that has made it a trusted security advisor to the world for more than 15 years. eTrust TARGET provides virus signature file updates that can be automatically downloaded from CA's FTP site and distributed to all eTrust Antivirus client nodes.

eTrust Antivirus v7 Frequently Asked Questions (cont'd)

Q. What happened to InocuLAN®, Unicenter TNG® Advanced AntiVirus Option, Inoculate/IT® Personal Edition and eTrust™ Inoculate/IT®?

A. CA entered the antivirus business with the acquisition of Cheyenne Software and its InocuLAN product in 1996. With the 4.53 release of the product in 1998, InocuLAN was renamed Inoculate/IT® for inclusion in the IT product line. Inoculate/IT became eTrust™ Inoculate/IT in August 2001 with the 6.0 release and was rebranded as eTrust™ Antivirus with the v7 release.

Unicenter TNG Advanced AntiVirus Option was marketed as one of the many add-on components to Unicenter TNG®. Unicenter TNG Advanced AntiVirus Option and Inoculate/IT® Enterprise Edition (a stand-alone version of Unicenter TNG Advanced AntiVirus Option often labeled eTrust Antivirus) were both sold by the direct Enterprise Management sales force to



Computer Associates®

eTrust™ Antivirus v7 Frequently Asked Questions

large-scale enterprises. With CA's rebranding of products and the 6.0 releases of CA's antivirus solution line, eTrust Antivirus was launched as a single direct offering. eTrust™ Antivirus v7 can serve as a stand-alone solution or as an integrated component to Unicenter®.

Following the acquisition of Cybec Pty Ltd's product Vet® Anti-Virus in 1999, CA created the highly successful Inoculate/IT Personal Edition promotional program. Repackaging the Vet® application as a zero-cost antivirus solution for personal use yielded more than three million downloads in little more than a year and a half. Based on this success, CA launched my-eTrust.com™ and the eTrust™ EZ Armor™ suite. The Inoculate/IT Personal Edition promotional program ended on June 7, 2001.

Q. Where do my-eTrust.com™ and eTrust EZ™ Antivirus fit in?

A. Serving the home/consumer PC user, my-eTrust.com markets eTrust EZ Antivirus — an easy-to-use solution that delivers industrial-strength protection. As part of the eTrust EZ Armor suite, eTrust EZ Antivirus is sold and supported through the my-eTrust.com web storefront and through OEM agreements.

Q. How can I protect my network at the gateway?

A. eTrust Antivirus defends your network against incoming viruses and malicious mobile code (Java Applets and ActiveX) on SMTP, FTP and HTTP protocols before it can enter your network, reducing damage and costly downtime. Additionally, it verifies the digital signatures of signed objects, authenticates the Certificate Authority that issued the digital certificates and analyzes each Java executable object to be downloaded.

Q. Why does my organization need perimeter protection?

A. With an increasing number of companies relying on the Internet for information and services, malicious code attacks are a frequent occurrence. Companies need to protect their networks against today's threats. With eTrust Antivirus, you can rely on real-time attack intervention — automatic detection as well as blocking and notification of potentially malicious content, such as viruses, Java, ActiveX, VBScript and improperly signed/digitally signed objects. eTrust Antivirus provides immediate protection through out-of-the-box, predefined policies for a wide range of situations.

eTrust Antivirus v7 Frequently Asked Questions (cont'd)

Q. How does eTrust Antivirus defend clients against infected email?

A. While eTrust Antivirus analyzes the content of all inbound objects at the gateway, the antivirus engine scans objects for viruses — based on the scanning level defined by the administrator, specified keywords and email attachments used to identify potential viruses in email attachments. (This technology is not included in the Microsoft Proxy Server and Apache Linux Server editions.)

Q. With which proxy servers/firewalls will eTrust Antivirus work?

A. When used for perimeter protection, eTrust Antivirus can be plugged into the following proxy servers:

- **Microsoft Proxy Server**
- **Microsoft ISA Server**
- **Apache Linux Server**

eTrust Antivirus allows each proxy server to deliver the Internet objects for inspection. They are analyzed and compared to the enterprise's security plan, as set up in eTrust Antivirus. If the object is then allowed to enter the network, it will be sent to the client workstation via the proxy server; otherwise, notification will be sent to inform the user that the object was blocked.

- **eTrust Antivirus CVP Edition works with Check Point Firewall-1**



Computer Associates®

eTrust™ Antivirus v7 Frequently Asked Questions

- A rule needs to be added to Check Point Firewall-1's rule-base so that every executable entering the enterprise network is sent to eTrust Antivirus, where it is analyzed and evaluated against the enterprise security plan. Once the executable is approved by eTrust Antivirus to enter the network, it will be sent to the client workstation via Firewall-1.

Q. What tools does eTrust Antivirus provide to help enterprises set up security plans?

A. eTrust Antivirus comes fully equipped with a generic security plan and predefined events, which can be easily implemented or customized to suit the particular security needs of any organization. Using the eTrust Antivirus policy manager tool, an administrator can set up any number of security plans for the different divisions, departments or individuals in an organization, allowing the company's security policy to be diverse and flexible.

Q. Can eTrust Antivirus manage more than one gateway?

A. Yes. The eTrust™ Control Center in all eTrust Antivirus editions provides a single, centralized management station that can support multiple distributed gateways.

Q. What about real-time performance?

A. eTrust Antivirus intercepts objects at the gateway, where both the analysis and comparison of each executable with the security plan is done on the fly in real time — without decreasing network performance.

Q. Is the size of an organization or network a concern when using eTrust Antivirus for perimeter protection?

A. eTrust Antivirus was designed and can be customized to protect small, mid-sized, large and even very large global organizations.