



Advanced Virus Detection Technology for the Next Millennium

The evolution of malicious code detection and
cleaning technology for advanced code inspection

Table of Contents

Introduction	2
Before Viruses Made Headlines.....	3
Don Quixote in the “Floppy” Virus Era: 1980–1994.....	3
Defense Against Macro Viruses in the “Macro” Virus Era: 1995–1998.....	3
Viruses and the Bottom Line: 1999 and the New Millennium.....	4
Network Associates Virus Scanning Technology Today.....	4
Battle-Tested Engine Technology	4
Versatile Virus Detection “Language” Base.....	5
Efficient Virus Variant Detection	5
Accurate Detection of New Viruses	6
Faster Virus Cleaner Availability	6
Virus List Update Stability.....	7
Encrypted Virus Detection	7
Polymorphic Virus Detection.....	8
Patented Algorithmic PSDE Analysis.....	8
VirusLogic “Double Heuristic” Analysis.....	9
Negative Heuristics	10
False Alarm Elimination	10
Macro Heuristics	11
The Problem with Heuristic Sensitivity Tools.....	11
Expanded Malicious Code and Other Scanning Capabilities.....	11
Malicious Web-Based Attacks	11
Java Applets	12
ActiveX Controls	12
Extended Internet Code Protection	12
Recursive Decompression Scanning	12
Email X-Ray Scanning.....	13
AutoImmune and The Future of Virus Detection	13

The information in this guide has been provided by Networks Associates Technology, Inc. To the best knowledge of Network Associates, these companies offer the types of products described. These companies are solely responsible for their software, distribution, and support services. Network Associates disclaims any and all liabilities for and makes no warranties, expressed or implied, with respect to these products, including, without limitation, the implied warranties of merchantability and fitness for a particular purpose. Distribution of these products, or information concerning these products, does not constitute Network Associates’ endorsement of the products, the companies, or support services. Product information is subject to change without notice.

Introduction

“Businesses worldwide have lost a total of at least \$7.6 billion in the first two quarters of 1999 at the hands of Melissa, the Explore.Zip worm and other viruses. This is a conservative number in that not everyone tracks cost, and most companies tend to undercount and underreport.”

—Computer Economics Inc., June 18, 1999

The war against viruses continues to escalate, with losses in the billions of dollars and lost data offering partial evidence of the latest electronic attrition rates. While virus defense systems of the past kept pace with the then-adolescent stage of virus patterns, scanners for the new millennium have been forced to evolve. Their in-depth inspection techniques and statistical behavior pattern marking reflect the equally evolved nature of viruses.

No longer are traditional methods sufficient for fighting viruses. In an interconnected web of networks, viruses, worms and trojans have erased borders and have emerged as complex security threats. Fighting this war has forced Network Associates to effect the same level of change. The end result is an advanced engine design and next-generation code scanning unlike anything the industry has ever seen.

The particulars of these evolutionary virus scanning changes, a clear description of their impact, and an outline of new virus warfare weaponry for business are discussed in this white paper.

Before Viruses Made Headlines

Don Quixote in the "Floppy" Virus Era: 1980–1994

It may have looked like a fight against windmills in previous decades as anti-virus pioneer John McAfee, an engineer at US defense systems leader Lockheed, wrote “programs that decoded other programs”. In his time, the late 1980s, it was a \$20 bet with fellow engineers that spurred his development of the first anti-virus weapon, not thousands of virus outbreaks. Unlike today, when more than 400 new viruses appear every month, the early virus era of McAfee’s emergence questioned whether someone could even write a malicious program.

As a result of such a limited virus environment, weapons like McAfee’s first anti-virus scanner were simplistic in nature. Based on hypotheses of what future threats could occur, the defense was based more on remote threat than real-world crisis. Virus samples had to be collected from a small circle of acquaintances, haphazardly, in insecure environments. Designed with his friend vs. foe expertise developed through his years in the defense industry, McAfee’s early scanners focused on pattern matching techniques that had to fully identify a known virus, then match a fix against it. “Friendly” code, that which could not be fully matched, was allowed through in the hopes that no unknown virus was embedded in the file.

By the early 1990s, well-known viruses began to reach computers in larger numbers. Still, more than 90% of transmitted files were spread by floppy. Scanners remained localized, reading floppies upon access, and matching known viruses against the list. McAfee could spend days analyzing a sample, since outbreak was unlikely unless many diskettes with the infection were passed around.

Defense Against Macro Viruses in the “Macro” Virus Era: 1995–1998

By the mid-1990s, however, scanning technology had to be updated to combat a huge surge in occurrence of viruses. It soon became common practice to scan all outside diskettes, but a new type of virus also changed the nature of fighting. Macro viruses, which took advantage of existing code inside word processing tools, exploited the rush to office-enabled computer programs and made localized battles a thing of the past. Pushing through documents by riding on the macros, these viruses reached further, faster than their predecessors.

Scanners, as a result, were stretched to the limits. Advanced algorithms had to be compressed into technology that could rapidly detect such macro viruses, and kill them instantly. While a floppy virus could be isolated and quarantined for later cleaning, macro viruses afforded scanners no such luxury. Speed had to be enhanced, and cleaning had to match the speed with which the virus was detected. New virus signature files had to be ready within hours, otherwise rapid proliferation could result.

Viruses and the Bottom Line: 1999 and the New Millennium

Viruses today affect vast numbers of computers in locations throughout the world. With interconnected computers afforded by the Internet, viruses need only hit once to strike deep. Lightning speed connections make time-consuming grunt-scans obsolete, and the sheer number of viruses—estimated at more than 45,000—makes pure pattern matching impractical. Together with the dramatic increase of viruses per month, the advanced state of virus attacks has significantly affected the virus detection and cleaning engines in use today.

Network Associates Virus Scanning Technology Today

By engineering an integration of several past and newly emerged technologies, Network Associates has brought to life technical advantages formerly unavailable in any cohesive scanner engine in the marketplace¹. Particularly for corporate organizations with large installed bases of server and desktop computers, the new Network Associates integrated virus detection and cleaning engine has marked a changed approach to virus defense. Specifically, this engine has added the following technical advantages. Detailed descriptions of these technical attributes follow this bulleted list.

- Battle-Tested Engine
- Versatile Virus “Language” Detection Base
- Advanced Heuristic Analysis
- Expanded Scanning Capabilities
- AutoImmune Virus Capture

Battle-Tested Engine Technology

The evolution of virus defense weaponry at its earliest stages faced the challenge of having no precedent to have learned from. Just as generals study war plans of famous battles of history, anti-virus developers need precedents to look for clues on combating present and future threats. Such a history helps developers add in features that are new, or change the scope of features already in the product.

Besides using history to their advantage, researchers at Network Associates have taken advantage of another phenomenon. Documented software industry trends reveal that first generation technologies inevitably contain technical inefficiencies that are difficult to measure in a lab setting prior to product integration. Only through real-world testing across multiple platforms, in large-scale environments, can engines be benchmarked. Once measured in these

¹ The Network Associates engine is included in all Network Associates 4.x series products under the Total Virus Defense product line (VirusScan, NetShield, GroupShield, WebShield) and in Dr Solomon branded products versions 7.9x and above.

scenarios, the engine can then be further developed and re-engineered to suit specific customer requirements. Later generations incorporate all the previously learned techniques and are often selected for mission critical applications.

The Network Associates engine is currently in its fourth generation. This engine has already been proven successful for over 50 million customers around the world and 80% of the Fortune 100, more than double that of its nearest competitor. Over the years, the Network Associates engine has been proven for robustness and quality necessary to achieve superior levels of virus detection and virus cleaning. Using the war analogy again, the Network Associates engine is like troops that have already been battle-tested and fought wars on various continents, under diverse conditions, across a period of time.

The fourth generation engine, with excellent detection and cleaning, has since been successfully inserted into both desktop and server environments. As a mature, stable, and proven engine, it has also been further developed for application across a complete virus defense spectrum, applying strong cleaning and detection in both the high demand mail server environments as well as to the relatively low-demand desktop scanning for DOS. This flexibility of design gives Network Associates a unique advantage as virus risks change over time.

Versatile Virus "Language" Detection Base

As the nature of viruses changed, so did scanners. The Network Associates engine architecture is especially geared towards the latest levels of threats. Specifically, the technical design of a virus defense engine can critically affect its ability to detect and clean new virus strains as they emerge. If too tight in design, the engine's "language" may miss new variants of virus threats. If too open-ended, it may drain performance and affect too many components in a routine computer task list. In addition, it may generate a large number of false positives that take up system resources and distract IS personnel from mission critical activities. Especially during a virus outbreak, engine design and the language it is based upon can drastically affect time and accuracy of virus detection and cleaning.

Efficient Virus Variant Detection

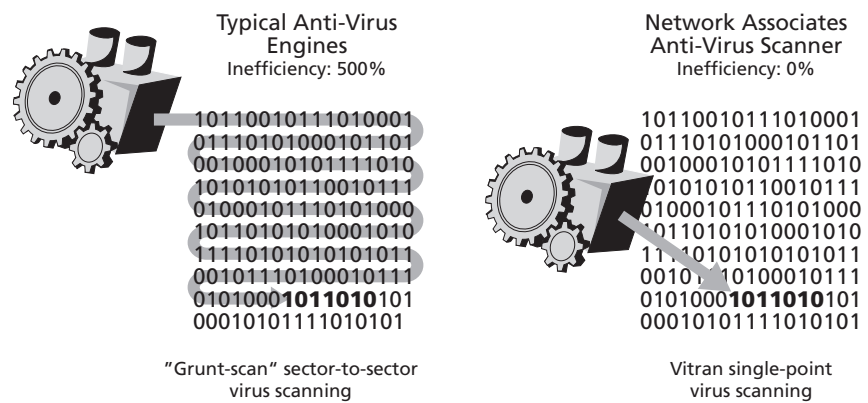
The Network Associates engine uses **Virtran**, a unique proprietary virus detection language invented and perfected by renowned European anti-virus expert Dr. Alan Solomon.² Because it is specifically designed for virus detection and cleaning, the engine applies an extremely efficient method for detecting numerous virus variants.

² Network Associates acquired Dr. Solomon's software in 1998.

Virtran works by enabling the scanner to locate the specific point in a file, boot sector or MBR (Master Boot Record) containing the virus code. The scanner does not need to “grunt-scan” for virus code from one end of a file or sector to the other. Instead, it employs a “single-point” scanning technique. NAI Labs AVERT (Anti-Virus Emergency Response Team) researchers can thus determine where, within the file, the virus code is located. This knowledge, built into the driver, allows the scanner simply to search for the virus in a specific location within the file. If the specific sequence of bytes sought for (sometimes called a signature, or definition) is not there, it is concluded that the virus sought after is not present.

FIGURE 1.

Single-point virus scanning enabled by the Network Associates engine's use of the Virtran “language” creates faster and more accurate virus detection.



Accurate Detection of New Viruses

With the Virtran-enabled engine, virus defense technologies can look for specific code points in viruses and inherently detect and repair more variants of viruses than other virus defense approaches. If one virus generates several family member viruses, for example, Virtran can detect all variants and not just the source virus. To test the engine in its initial form in mid-1998, it was run against a collection of 15,000 new viruses submitted to Network Associates by a skilled, anonymous virus writer.³ The engine was able to quickly detect and clean nearly 100% of these previously unknown virus variants without installing new updates of any kind.

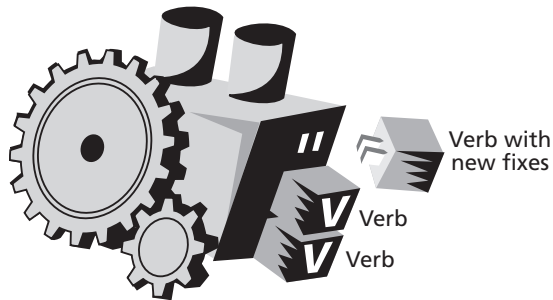
Faster Virus Cleaner Availability

Many new viruses, however, still require updates to the engine itself to ensure accurate detection. Here again, Network Associates holds a significant technology lead over its nearest competitor. To combat new viruses spread rapidly over the Internet, updated virus signatures must be posted within hours of a virus’ first appearance. The unique nature of the Virtran language offers not only more efficient and more accurate virus detection, but also greatly enhances the speed in which virus cleaning files can be developed. Using Virtran, an AVERT

³ Virus writers occasionally let loose viruses in security vendor environments in the hopes the virus will attack a commercial product and exploit a vulnerability. In this case, it is unclear why the virus writer chose to expose the large private collection to a commercial vendor. Rather than cause damage, the submitted collection actually helped Network Associates speed its research into new strains of viruses by providing virus samples that could then have fixes produced before the viruses went public.

researcher can write a detector and cleaner that covers an entire family of viruses, rather than just one particular virus. Built-in components of the Network Associates engine, usually referred to as “verbs,” provide a variety of technical suggestions for virus cures. Generating additional verbs and incorporating them into the Network Associates engine is a compact, clean process.

Network Associates Engine



Virus List Update Stability

The original McAfee engines that updated virus defense systems by adding code, or expanding the pattern matching capabilities, are primitive compared to today’s Network Associates engine. Sliding detection for new viruses quickly into the engine is now possible at the integration level with the Network Associates engine architecture. While many anti-virus products still use outdated techniques to simply add code upon code, Virtran’s integration into the Network Associates engine stabilizes the defense system allowing new “verbs” to be inserted rapidly.

This design feature also eases the task of developing virus cleaners. This capability, in turn, speeds availability of cleaners, a prime benefit in the event of a virus outbreak. While “grunt-scan” methods waste time simply detecting virus presence, the Network Associates engine helps developers spend less time figuring out detectors and more time getting fixes out to customers quickly, before virus infiltration is widespread. Building code upon code, as in the past, just doesn’t match up to the heat of the battle in today’s networks.

Encrypted Virus Detection

Earlier virus scanning designs took into consideration very few types of viruses, since very few existed. As mentioned, floppies carried the majority of viruses until a new type, macro viruses, came on the scene. Today, it is important for a virus detection engine to not only detect a wide variety of virus variants, but to detect the more difficult *types* of viruses as well. Once again, the Network Associates engine has a clear technical advantage in this area, particularly in its detection of polymorphic viruses.

FIGURE 2.

The efficient architecture of the Network Associates engine, using the Virtran language, enables virus researchers to quickly draw on existing engine “verbs” to develop new verb language structures that detect entire families of viruses. These structures integrate easily into the engine. Inferior designs avoid integration and simply add code upon code.

“It is estimated that over 80% of all encrypted communications on the Internet today are protected with Network Associates PGP encryption technology...this expertise offers a tremendous benefit when detecting and cleaning polymorphic encrypted viruses, the most difficult in existence today.”

Virtually unheard of in the early 1990's, polymorphic viruses have continued to rise, using encryption to hide themselves and continue their infection spread. As the developer not only of anti-virus technology, but also encryption tools, Network Associates has been able to successfully map the advanced expertise of its cryptography researchers to its advanced Total Virus Defense division. It is estimated that over 80% of all encrypted communications on the Internet today are protected with Network Associates PGP encryption technology. Just as the army uses the field technique of camouflage to hide its inventory and valuables, today's companies use PGP to hide their Web-borne information. On the other side, these same companies can use the Network Associates advanced virus scanner to dig out viruses from encrypted messages and traffic at the desktop. Having fully supported and funded developers in both sectors, anti-virus and encryption, adds to the strength of both products used by a company defending its networks.

Polymorphic Virus Detection

For most viruses, it is possible to identify a virus using a specific sequence of bytes. This sequence of bytes is stored within the virus signature file. If the sequence of bytes matches the sequence in the signature, then the file is infected and the virus detected. However, a polymorphic virus is variably-encrypted; the sequence of bytes in the virus code changes with each infection. There is no constant sequence of bytes for which to search. Polymorphic viruses are known to be difficult to detect and repair, as they constantly change their sequence of bytes to outmaneuver pattern matching detection methods.

The Network Associates engine design includes a unique patented PolyScan Decryption Engine (PSDE) that provides excellent capabilities to detect polymorphic viruses. The PSDE portion finds the encryption routine, runs it in a virtual machine until it can understand the encryption algorithm, then uses that understanding to “see through” the encryption to the virus itself. The result is an advanced polymorphic detection rate, which in turn affects the speed of understanding and recognizing new virus strains, even as they change. For corporate enterprises, this rapid polymorphic detection rate helps prevent further spread or virus damage. The PSDE enables the scanner to detect, identify and remove polymorphic viruses.

Patented Algorithmic PSDE Analysis

Just as John McAfee was first with his anti-virus scanner, the heritage of virus defense remains with Network Associates—first to develop the PSDE, which is patented in its approach to polymorphic virus detection. The PSDE analyzes the algorithm used in the decryptor-loader of the polymorphic virus, that is, what the virus uses to decrypt its own code before executing.

The PSDE then applies the algorithm to the encrypted code. Once the virus code has been decrypted in this manner, a standard sequence may be used to identify the virus positively. This enables the engine to find all the instances of a polymorphic virus. In addition, it does not produce false alarms, and enables researchers to clean the infected file or disk sector.

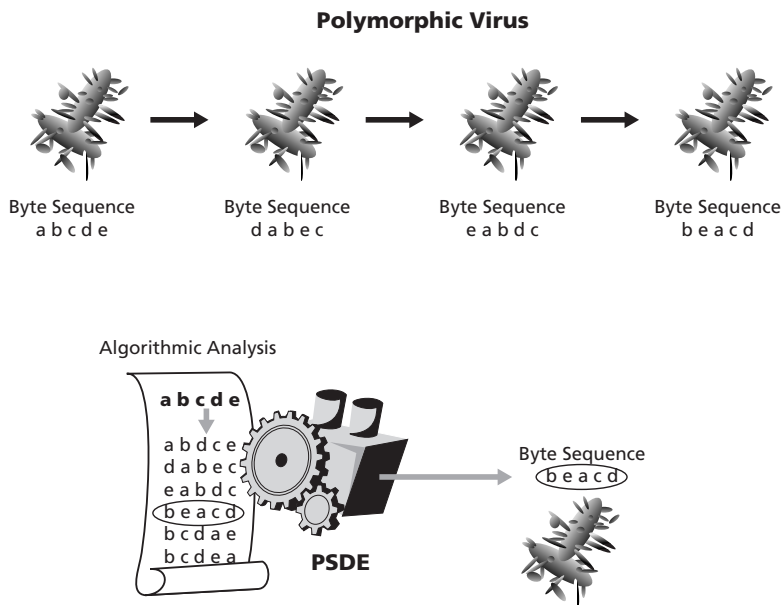


FIGURE 3.

Polymorphic viruses are one of the more difficult virus types for engines to detect because of their dynamic nature. Such viruses change their sequence of bytes with each infection.

The patented PolyScan Decryption Engine (PSDE), exclusive to the Network Associates virus scanning engine, analyzes polymorphic viruses to determine a sequenced encryption routine. Once the PSDE determines the sequence, it then applies the encryption routine to the next appearance of the same polymorphic virus to detect it, even in its changed form.

VirusLogic "Double Heuristic" Analysis

Perhaps most exciting in the emergence of new levels of virus detection and cleaning has been the approach towards intelligently estimating a virus. Most major anti-virus approaches today use some form of this analysis, known as *heuristics*, to detect new viruses that have not been seen before. This involves searching through the code in a file to determine whether that code takes actions that appear to be actions typical of a virus even if it does not specifically recognize a known, existing virus. The more virus-like code that is found, the more likely that a virus is present. Once the level of virus-like code reaches a pre-determined threshold, the scanner identifies a possible infection. While virus scanners of the past could rely on the tables of signatures to match the known variants, the significant rise in the number of new viruses developed each day prompted Network Associates to find newer ways to catch unknown viruses. Catching them before damage could be done also became a priority, as companies hooked up to the Internet and left their corporate assets vulnerable to outsiders.

VirusLogic, Network Associates' "double heuristics" technology analyzes virus logic by employing both negative and positive heuristics, enabling organizations to catch the rising number of e-mail-borne viruses and variants such as the ExploreZip.worm, without causing

false positives generally associated with such technologies. The powerful scanning engine scans not only for virus-like behavior, such as unprompted modification of files, invocation of mail clients or other means of self-propagation, but also searches for “legitimate,” non-virus-like behavior, such as prompting the user before taking action. Based on this level of analysis, the scanning engine can catch new viruses while avoiding the cost and time associated with addressing the “false positives” that can result from the inefficiencies of less evolved scanning engines.

Negative Heuristics

While most organizations seek tight control over security, CIOs understand the trade-off that could result is an inability for the business to perform basic functions. If security technologies shut down functions at the user’s every turn, security becomes only an obstacle. With anti-virus scanners in particular, the danger is a high level of *false positives*. The heuristic technology deployed by most anti-virus products, unfortunately, generates many false alarms because of the inefficiencies of most heuristic detection engines.

The Network Associates engine uses not only traditional heuristic analysis technique, but also performs a sophisticated “non-virus” identification approach called “negative heuristic” analysis. While the scanning engine is searching through code to determine whether it contains any virus-like commands, it also searches for code that is distinctly not like a virus. This negative heuristic analysis enables a simultaneous, bi-directional virus analysis. It is an approach that reflects the changed nature of viruses, and the realization that to be a virus defense expert, one must think like a virus writer.

False Alarm Elimination

Approaching virus detection from both angles, ViruLogic also speeds the rate of virus recognition, again affecting the speed with which researchers can provide virus cleaners to customers to prevent virus proliferation. This *double heuristics* approach greatly reduces the likelihood of false alarms, which explains the high heuristic detection rates possible with products using the Network Associates engine. It is the third point of reduced false alarms that can particularly be of importance to today’s enterprise, which deals with hundreds of technologies and management tools, and cannot afford to take attention away from another task to deal with threats that are in fact, just engine inefficiencies. Eliminating false alarms removes another disruption and works toward more seamless virus defense operations.

Macro Heuristics

To deal in particular with the advent of macro viruses, the advanced heuristic scanning in the Network Associates engine includes macro heuristics for detection of macro viruses. Macro viruses currently represent the biggest threat to corporate systems as the most common viruses, and often infect Microsoft Word and Excel applications by inserting unwanted words and phrases, modifying formulas, or even destroying data. The advanced ViruLogic double scanning method of positive and negative heuristics in the Network Associates engine significantly improves macro virus detection rates.

The Problem with Heuristic Sensitivity Tools

Advanced heuristic scanning eliminates the need for so-called sensitivity tools that adjust scanning sensitivity due to its elimination of false alarms. While more primitive first generation anti-virus tools still offer such settings to reduce sensitivity, next generation engines from Network Associates do not trigger false alarms and thus do not need such fixes. Such advanced scanning is a technical advantage particularly to large organizations, which, with first generation anti-virus scanners, could generate huge false alarms lists. Virus defense systems that promote the use of sensitivity tools are frequently attempting to disguise vast inefficiencies in their scanning technologies, many of which are leftover from the floppy virus era.

Expanded Malicious Code and Other Scanning Capabilities

In addition to the initial engine design benefits of mature technology, an efficient language base, and advanced heuristic analysis, the Network Associates engine also enables expanded capabilities for new virus vehicles. In the ever-escalating war, it is not just files carrying viruses, but Internet code in the form of Java and ActiveX, e-mails, forwarded zip attachments, trojans and even Internet “worms.”

Malicious Web-Based Attacks

An emerging threat to computer users with Internet connectivity is the potential of hostile code that is automatically downloaded and executed on a user’s computer when connecting to hostile sites on the Internet. Although a comparatively small number of malicious applets have been discovered at this time, malicious code, also known as “mobile code,” has the strong potential of being the preferred vehicle of future virus writers.

Java Applets

“Java applets” typically refers to executable code written in Java, a Sun Microsystems technology, that is frequently found on Web sites in the form of animation such as a rotating stock ticker. Java is also used increasingly in corporate applications such as Lotus Notes, and intranet tools. Java applets are automatically and transparently run through a Java Virtual Machine that is part of commonly used Internet browsers such as Netscape Navigator. The extensible and efficient Network Associates engine includes defense against malicious Java applets that break Java Virtual Machine sandbox restrictions or perform otherwise potentially hazardous actions.

ActiveX Controls

“ActiveX controls” typically refer to executable code written in ActiveX, a Microsoft technology, also found frequently throughout the World Wide Web. ActiveX controls automatically and transparently run through Web-based browsers such as Internet Explorer. The extensible and efficient Network Associates engine includes defense capability against malicious ActiveX controls, particularly important due to the lack of an advanced security model for ActiveX code.

Extended Internet Code Protection

Although such Internet code is, in fact, more reminiscent of a security breach rather than a virus, its malicious actions make it possible for detection and cleaning through the Network Associates engine. In addition, as has been documented in various virus industry journals, viruses are increasingly using multiple forms to carry out attacks. The extensible and efficient Network Associates engine includes defense capability against Java, ActiveX, and JavaScript. VisualBasic Script is scanned through the macro virus capabilities.

Recursive Decompression Scanning

Virus writers often attempt to hide viruses inside compressed files. When a file is compressed, the contents of the file are essentially encrypted. Any sequence of bytes sought after by the scanner are likewise encrypted. Thus, the bytes sought after may be re-arranged, or absent altogether. The only way to find viruses within compressed files is to understand the compression format. The Network Associates engine is able to detect viruses within the most commonly used compression methods, including PKZIP, ARJ, PKLITE, LZEXE Microsoft compression, RAR, TAR, GZIP, and others. The Network Associates engine is also able to look recursively within several layers of compression, through a ZIP file within a ZIP file inside an ARJ, for example.

Email X-Ray Scanning

New e-mail-based viruses and Internet worms like Melissa and Explore.zip spread around the world at unprecedented speeds, affecting millions within a matter of hours. While most leading anti-virus vendors publish new updates when such viruses are discovered, end users who rely on these products have no way of knowing whether an incoming message is infected until they actually attempt to open the potentially infected message, allowing their anti-virus scanner to inspect its contents. If their scanner is not updated correctly, or the update patch improperly applied, it is unfortunately too late. The infected attachment, once opened, will begin its work immediately, spreading itself to other users and, in some cases, deleting critical files on the infected machine.

To effectively combat today's rapidly spreading e-mail viruses, Network Associates has incorporated a technique known as Email X-Ray scanning in its popular VirusScan, an industry-first for desktop anti-virus products. Through its Email X-Ray feature, VirusScan actually examines attachments inside incoming e-mail messages before they are opened. If infected attachments are discovered, users are warned long before they attempt to open it, greatly reducing the possibility of inadvertently spreading the infection to others.

AutoImmune and The Future of Virus Detection

Virus defense was once a localized, simple process that involved matching known threats against a list, with no delivery deadlines or virus fix timetables. In the networked world of the Internet, such weapons are almost obsolete, and the demands of virus defense users have changed. Today's engines require updated capabilities against new world threats, as well as new techniques to speed the development of virus signatures. In addition, Network Associates engines have evolved significantly in order to catch viruses that have never before been seen. The Network Associates engine, tested in real-world scenarios, versatile in its infrastructure, efficient and broad in its scanning abilities, and advanced in several key technical areas of virus defense engine design, offers an unprecedented approach to dealing with the continuing war against viruses. Its flexible design and patented architecture also allows it a successful continued life as new virus threats appear. These attributes have made the Network Associates engine the industry's leading virus defense method, in particular for corporations, as well as the military and many government agencies fighting multi-national virus attacks.

But just as virus writers evolve and develop their attacks to more sophisticated levels, researchers at NAI Labs are working towards continued advancement and innovation on the virus security front. In particular, the collaboration among Network Associates security researchers is helping further evolve a breakthrough new approach to virus detection known as *AutoImmune*.

AutoImmune simulates the human immune system, further reducing the time required to create detectors and cleaners for new viruses. Unlike similar efforts by other anti-virus vendors which have remained in the research stage for years, the initial phases of AutoImmune technology are already shipping in products like VirusScan today.

AutoImmune is part of a larger initiative at Network Associates known as Active Security. Active Security allows individual security products such as virus scanners, firewalls, vulnerability scanners and intrusion detection monitors to communicate with each other automatically when security breaches are detected—tightening security policies, shutting down intruders and creating cures for new viruses on the fly. Network security products such as CyberCop (intrusion detection) and Gauntlet (firewall) already communicate with each other through Active Security integration today. AutoImmune represents a natural extension of Active Security, combining the discoveries of multiple security researchers at NAI Labs to combat the most costly security problem facing network administrators today.

Further Network Associates efforts will streamline the communication between virus scanners, firewalls, and other security devices to create active communication that knows what to do on all fronts when a virus attacks. Automatically today, AutoImmune technology embedded in Total Virus Defense products already detects, removes and creates a cure for previously unknown viruses. The AutoImmune initiative takes anti-virus protection to the next level by automating processes that formerly required intervention by network administrators, thereby lowering the total cost of ownership of an organization's security solution by stopping new viruses before they have a chance to spread.

In the near future, the evolved Network Associates engine technology will ensure closer coordination among different levels of the customer network, but also, closer work between Network Associates researchers and the customer. In whatever form viruses take to bypass a company's security, Network Associates will develop viable security systems to limit risk, protect data, and prevent the spiraling costs of virus outbreaks in particular. This paper highlights only the virus scanning engine efforts to date. More innovations, already under confidential development today, are soon to be launched commercially to the market. All such efforts will continue the successful Network Associates heritage for our 50 million customers around the world.



Who's watching your network

For more information on products, services, and support,
contact your authorized Network Associates sales representative

CORPORATE HEADQUARTERS

3965 Freedom Circle
Santa Clara, CA 95054
TEL: (408) 988-3832*
FAX: (408) 970-9727

**Call for additional Worldwide Sales Offices*

Visit our Website



<http://www.nai.com>

McAfee, VirusScan, NetShield, GroupShield, WebShield, Total Virus Defense, PGP, CyberCop, Dr Solomon and Gauntlet are registered trademarks of Network Associates, Inc. and/or its affiliated companies in the U.S. and/or other countries. All other registered and unregistered trademarks in this document are the sole property of their respective owners. All specifications may be changed without notice.

©1999 Networks Associates Technology, Inc. All rights reserved.

6-TVD-AVD-001 8/99