symantec™

The Digital Immune System

Enterprise-Grade Anti-Virus Automation in the 21st century

INSIDE

- The Benefits of Automation
- The Digital Immune System technology
- Virus Submissions: Prioritizing, Analyzing and Processing
- The Workflow System

Contents

Overview

This paper describes the evolution of computer viruses, the problems they cause and the responses to them, with emphasis on a new level of anti-virus response called the Digital Immune System. Customers of Symantec anti-virus products will be especially interested in the descriptions of each Digital Immune System component.

Evolution of the virus problem

Computer viruses are a major threat to users worldwide, but the damage they have done is relatively light when compared to the potential destructive force of the computer worm.

Viruses are computer programs designed to spread from one file to another on a single computer. A virus might rapidly infect every application file on an individual computer, or slowly infect the documents on that computer, but it does not intentionally try to spread itself from that computer to other computers.

Viruses are spread when users send email messages with attached documents, trade programs on diskettes, or copy files to file servers. When the recipient opens an infected file, the virus gains the opportunity to spread on the new computer. Because most computer users send email messages to small groups of correspondents, the spread of viruses is limited.

Evolution of the anti-virus response

Virtually all advances in anti-virus technology over the past decade have centered on improving the scanning engines of desktop and server anti-virus products. (Anti-virus engines are the core component of anti-virus software. They are designed to "parse" through complex file structures and locate likely virus hiding places. They then look for virus fingerprints in these hiding places.)

Advances in anti-virus technology have addressed two major problems:

THE LACK OF SOPHISTICATION IN EARLY ANTI-VIRUS ENGINES. Due to their technological limitations, some classes of complex viruses required hours or days of analysis before an engineer could extract a working fingerprint and add it to the anti-virus software.

New technology has enabled researchers to simplify the process of adding fingerprints for complex new viruses by improving the anti-virus engines. By simplifying this process, the anti-virus vendor dramatically speeded response times to new viruses.

One of the more notable improvements in this area was the adoption of the CPU emulator. Today, virtually every anti-virus product uses a CPU emulator to detect polymorphic computer viruses. (Polymorphic computer viruses mutate themselves each time they spread to a new file or diskette, concealing consistent fingerprints from older anti-virus programs.) By running suspect files in a "sandbox" environment, the anti-virus software can coax the polymorphic virus into revealing itself and then detect its fingerprint. This innovation drastically reduces the time it takes to analyze self-mutating viruses from days or weeks to hours or minutes.

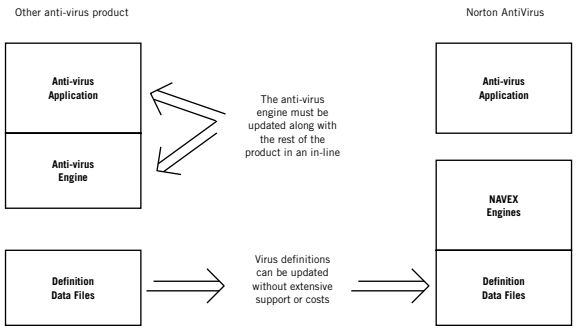


Figure 1: Traditional anti-virus architecture vs. NAVEX architecture

An even more important innovation was the advent of the modular anti-virus engine. Symantec created the first modular anti-virus engine, called NAVEX (Norton AntiVirus™ Exchange), which enables Symantec Security Response researchers to quickly create entirely new cures for unknown virus strains or whole new classes of viruses, and then deliver the cures to Symantec customers as part of a standard virus definition.

NAVEX enables fast response on even the most complex viruses or new classes of viruses. All Symantec AntiVirus products can have their NAVEX protection upgraded without rebooting the computer or shutting down the anti-virus scanner. There is no need to restart file servers, take down GroupWare email servers, or reboot users' desktop computers to update anti-virus protection; nor is there a need to re-install or distribute in-line releases. The result is consistent protection across the enterprise within a simple virus definition update; and a fully cross-platform, automatically delivered modular engine with fast response—technology that few other vendors offer.

The second major problem addressed by anti-virus vendors was the inability of fingerprint-based anti-virus software to recognize new or unknown virus strains. During the decade of the '90s, anti-virus companies invested significant efforts in building "heuristic" detection engines to find new and unknown virus strains. This effort has paid off to an extent; however, heuristic systems still fail to catch a small but significant number of new virus and worm strains.

Clearly, the anti-virus paradigm that characterized the '80s and the '90s was one of manual activity. Humans participated in—and often slowed—every step of the virus analysis and response process. With the relatively slow-spreading viruses of the last two decades, the manual analysis paradigm was a workable, albeit inefficient, method of operation. It is not sufficient to meet current or new threats.

Worms: a new threat

The sole purpose of a worm is to infect as many machines as possible on a network. The purpose of a virus is to spread many copies of itself onto a single computer. Worms are insidious because they do not rely upon human behavior in order to spread.

A worm focuses on infecting as many machines as possible on the network, instead of spreading many copies of itself on a single computer like a computer virus. The prototypical worm infects or causes its code to run on a target system only once; after the initial infection, the worm attempts to spread to other machines on the network.

A worm can spread itself without human intervention. The notorious Explore.Zip worm gained control of thousands of machines with the launch of a single program. Computer worms can exchange information quickly with large groups of people.

The infamous Melissa worm required only that a user open a single infected document and it spread to thousands of users. Melissa is actually a worm and a virus, a simple piece of computer logic that evaded virtually every anti-virus product and its intrinsic heuristics. It was not a complex polymorphic virus and didn't require CPU emulation or other complex engines to detect. It was a simple, run-of-the-mill piece of computer code that could be analyzed in minutes.

So why did Melissa cause so much trouble? The majority of corporations around the world had the most-recent anti-virus software deployed on system desktops and servers. The ideal heuristic scanner could have caught Melissa. However, there is no perfect heuristic virus detection system. Some new or unknown viruses are bound to be missed. The problem was not the anti-virus software, but the ability of anti-virus software companies to:

A. Rapidly capture the virus through improvements in engine technologies such as NAVEX, heuristics, and Norton AntiVirus behavior-blocking approaches

B. Use intelligent filtering to recognize that this virus required immediate attention, versus the hundreds or thousands of other submissions that are received on a daily basis

C. Analyze the virus, produce a cure, and test the cure

D. Spread the cure faster than the virus could spread itself, i.e., distribute a cure to all customers, all the way down to the desktop, the file server, and the gateway before the virus could gain a foothold in the network.

Each of these proficiencies is essential for dealing with worm-like threats. Because worms can spread so quickly, standard response paradigms may not be sufficient.

A Solution: Automation

While the predominant focus of the '90s was on the desktop, Symantec believes that a closed-loop communications system coupled with intelligent automation has the potential to dramatically reduce the damage from fast-spreading computer viruses and worms. Symantec began work on the Digital Immune System, in early 1998, to automate the detection, analysis, and response to new computer viruses and worm threats as intrinsic parts of the system.

A closed-loop anti-virus system manages the entire anti-virus process from virus discovery on the desktop to virus analysis at the anti-virus provider and deployment of a cure to the affected desktop. In a closed-loop system, the entire virus response process is automatic and managed, with nothing left to chance.

The goal of the Digital Immune System is to reduce the cycle time between when a virus is first found and when a cure is deployed to all susceptible systems. By automating many of the traditionally manual tasks involved in the submission, analysis, and distribution processes, the Digital Immune System dramatically reduces the severity and virulence of numerous virus threats.

The Digital Immune System has enabled customers to easily submit increasing numbers of new computer viruses, worms, and Trojan horses for analysis and processing. And, as the user community grows, so does the number of new viruses that are submitted. Each time the Digital Immune System automatically resolves a new computer virus, all members of the community reap the benefit of rapidly updated virus definitions.

The Digital Immune System

IBM® and Symantec designed the Digital Immune System as a closed-loop automated system to deal with Melissa-class threats, orders-of-magnitude increases in submissions, floods, and denial-of-service attacks. The Digital Immune System:

1. Detects a high percentage of new or unknown threats at the desktop, server, and gateway.
2. Makes the full system highly scalable.
3. Provides secure submission of virus samples and secure distribution of new definitions.
4. Provides intelligent filtering of submissions to focus system resources on the most critical threats.
5. Provides high-speed analysis capabilities.
6. Reduces instances of false positives.
7. Provides full end-to-end automation of submission, analysis, and distribution of new definitions.
8. Provides real-time status updates on all submissions.
9. Manages common flooding conditions and denial of service attacks.
10. Provides the administrator with the ability to set the level of automation.

The Closed-Loop Process

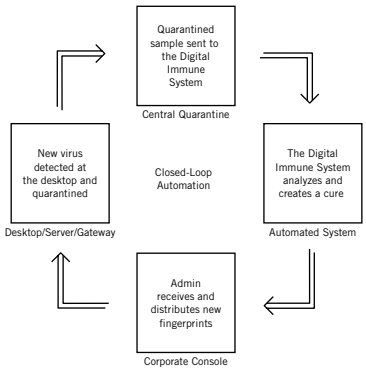


Figure 2: A high-level state diagram of the Digital Immune System closed-loop system.

Detecting A High Percentage of New Threats at the Desktop, the Server, and the Gateway

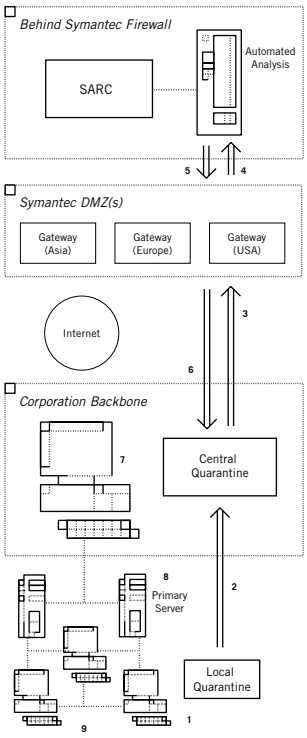
THE FIRST GOAL IN A CLOSED-LOOP, ANTI-VIRUS AUTOMATION SYSTEM IS TO DETECT AS MANY NEW AND UNKNOWN VIRUSES AS POSSIBLE ON THE DESKTOP, SERVER, AND GATEWAY.

The first step in building an automated anti-virus analysis and response system is detecting new or unknown threats at the desktop, the server, and the gateway. Suspicious files can then be forwarded for automatic analysis and processing.

Symantec has developed effective heuristic technologies for the desktop, the server, and the gateway. This technology, called Bloodhound™ heuristics, can detect a majority of new or unknown virus strains. Based on internal tests at Symantec Security Response, Bloodhound can detect:

1. 75-90% of all new or unknown Word and Excel macro viruses
2. Up to 70% of new or unknown DOS file viruses
3. Up to 80% of new or unknown boot-record viruses.

TO ARRIVE AT THESE FIGURES, TESTERS AT SYMANTEC SECURITY RESPONSE PRODUCED AN EMPTY VIRUS DEFINITION SET THAT CONTAINED ONLY HEURISTIC VIRUS DETECTION TECHNOLOGIES. THIS STRIPPED-DOWN VIRUS DEFINITION SET WAS THEN USED TO SCAN EXTENSIVE COLLECTIONS OF EACH OF THE TYPES OF VIRUSES MENTIONED ABOVE.



1. New/unknown viruses quarantined
2. Local quarantine forwards samples to corporate quarantine
3. Corporate quarantine securely forwards samples to regional Symantec gateway
4. Gateway forwards samples to back-end automation
5. Back-end automation forwards new cure/fingerprints to gateway
6. Gateways securely forward status and fingerprints to corporate quarantine
7. Corporate quarantine forwards fingerprints to master management server
8. Master servers automatically forward samples to primary servers
9. Primary servers roll out definitions to clients

Figure 3: The Digital Immune System. All numbered pathways are automatic and require no user intervention.

Submit Suspect File(s) To Symantec Security Response For Analysis

ONCE SUSPICIOUS FILES HAVE BEEN ISOLATED, THEY ARE SENT TO SARC FOR ANALYSIS AS RAPIDLY AND SECURELY AS POSSIBLE.

If configured to do so at the customer's location, Norton AntiVirus™ automatically isolates potential new or unknown viruses in a local quarantine on the desktop, server, or gateway. Norton AntiVirus automatically forwards these suspected infections from the local quarantine to the corporate Central Quarantine.

Using the Central Quarantine component, administrators can quickly obtain an enterprise-wide or site-wide view of all suspected infections. From corporate quarantine, administrators can examine all infected files, select the desired automated operations, or manually submit files to Symantec Security Response.

Before submitting files to Symantec Security Response, Central Quarantine scans each file with the latest virus definitions. If the definitions can cure the virus submission, they are quickly sent back to the workstation from which the virus came. This constitutes the first stage of automated analysis with improved response times for all machines at a customer location.

When a submission must be sent on to Symantec Security Response, and when configured to do so, Central Quarantine automatically encrypts and sends the submission using the Digital Immune System. Central Quarantine automatically strips all non-essential contents (e.g., text) from Word for Windows® documents and Excel spreadsheet files. This ensures data confidentiality while providing Symantec Security Response with the information it needs to determine whether a virus is present so it can create a cure.

At each stage of the automatic submission process, the system checks for available new definitions. If available, new definitions are immediately sent to Central Quarantine for distribution in accordance with the administrator's system configuration.

Make the full system highly scalable

SINCE THOUSANDS OF USERS SUBMIT SAMPLES TO SYMANTEC SECURITY RESPONSE EVERY WEEK, AN EFFECTIVE AUTOMATED SYSTEM MUST BE ABLE TO HANDLE FLOODS OF SUBMISSIONS AND OTHER ANOMALOUS NETWORK CONDITIONS.

The Digital Immune System has dramatically improved scalability by introducing the concept of a gateway computer that is a dedicated server with the following responsibilities:

1. It filters all submissions moving toward the Digital Immune System back-end.
2. It pushes customer submissions towards the Digital Immune System back-end either directly or through one or more gateways.
3. It pushes real-time status information down to the Central Quarantine Console either directly or through other gateways.
4. It pushes new virus fingerprints and information down to the Central Quarantine Console either directly or through other gateways.

Gateways reduce the number of submissions that reach the Digital Immune System back-end by eliminating duplicate submissions. Since virus replication and analysis is a computationally expensive process, by deploying a hierarchical set of gateways with appropriate filters the system reduces the load on the back-end and improves response time. Gateways also test submissions to determine whether a new definition already exists. If a definition exists, it is immediately sent to Central Quarantine at the customer site.

Provide secure submission of samples and secure distribution of new definitions

Email messages are no longer a reliable means of communications in emergency situations. Viruses can threaten the very existence of email, either because the corporation shuts down mail systems as a precautionary measure during a virus outbreak or because the email server crashes due to an overload of traffic.

The Digital Immune System uses a secure, HTTP-based protocol for all communications between the customer and Symantec. The communications architecture is based on the standard Secure Sockets Layer (SSL) and ensures confidentiality on all submissions. It also provides authentication of all packages sent from Symantec to the customer, ensuring legitimate virus fingerprint databases and new engines.

In addition to the security afforded by the Digital Immune System, the new communications mechanism ensures guaranteed delivery of virus samples and fingerprints. Administrators are notified in real-time of the success or failure of every transaction with the Digital Immune System gateways and back-end.

Prioritize, Analyze, and Process All Submissions

ONCE THE DIGITAL IMMUNE SYSTEM RECEIVES A VIRUS SUBMISSION, PROPER PRIORITIZATION IS CRITICAL TO ENSURE RAPID TURNAROUND AND ERADICATION OF FAST-SPREADING THREATS.

The Digital Immune System has two separate processing queues: one for corporate or government customers and one for consumers. To ensure scalability and availability, Symantec has deployed separate computer hardware to manage each of these queues, ensure that a glut of submissions on one queue will not encumber the other, and protect against denial-of-service attacks.

If necessary necessary, Symantec engineers can also add additional computing hardware to the queues, with each queue potentially using dozens of servers working in parallel to process customer submissions. This network and hardware architecture enables the Digital Immune System to process an ever-increasing number of submissions.

In order to improve response time on all submissions, Symantec engineers created highly specialized workflow, analysis, and filtering systems, which are collectively called “back-end automation.” This system performs an analysis on each submission, automatically processing submissions in the shortest possible amount of time, and prioritizing for Symantec Security Response researchers any submissions that cannot be resolved by automation.

UPON RECEIVING A NEW SUBMISSION, THE BACK-END AUTOMATION SYSTEM:

1. Tracks the submission in a database.
2. Filters files in the submission to reduce manual processing.
3. Attempts replication of suspect document and spreadsheet files to generate cures for new and unknown macro and DOS viruses.
4. Prioritizes submissions that must be handled manually.
5. Responds to customers with status data, resolution information, and fingerprints.

Database Tracking and Confirmation

RIGOROUS TRACKING OF ALL SUBMISSIONS IS KEY FOR QUICK RESOLUTION.

Before processing a submission, the back-end automation adds all submission information to a tracking database. During the automated analysis process, the Digital Immune System inserts subsequent information into a database for reference and accounting purposes. If the submission is subsequently deferred for manual analysis, all logs from the analysis and filtering steps are available to the human analyst.

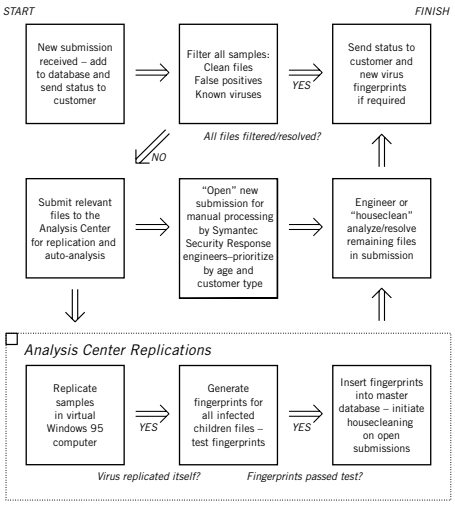


Figure 4: The different states in the automated analysis process for the Digital Immune System.

Submission Filtering

WITHOUT EFFECTIVE FILTERING, HUMAN RESEARCHERS MUST MANUALLY EXAMINE EVERY SUBMISSION.

Submission filtering eliminates as many files as possible from manual processing. Ideally, the filtering system categorizes submitted files into one of three categories: known clean, known false positive, or infected and repairable.

The back-end automation system filters every file in a given submission. If all files within a submission can be filtered automatically, the entire submission can be closed out and its status can be sent to the customer. The status response can also include a new virus fingerprint database if the customer submitted one or more computer viruses.

THE DIGITAL IMMUNE SYSTEM FILTERS AUTOMATICALLY RESOLVE APPROXIMATELY 87% OF ALL SUBMISSIONS, WITH AN EXPECTED INCREASE TO 95% AS NEW AUTOMATED ANALYSIS MODULES ARE ADDED TO THE SYSTEM.

CASE 1: CLEAN FILE FILTERS The Digital Immune System maintains a database of over 700,000 clean programs found on PCs running the Windows operating system. If a file in a submission matches a file in the database, the back-end system records the result in the database and eliminates the file from further consideration.

CASE 2: FALSE POSITIVE FILTERS A false positive occurs when an anti-virus program incorrectly identifies a clean program as being infected with a virus While anti-virus companies attempt to minimize false positives, they are inevitable and commercial-grade automation processes must be able to handle such a scenario.

If an anti-virus software company distributed a new virus fingerprint that identified false positives on millions of computers around the world, it could cause a large subset of users to submit files to the Digital Immune System for analysis. Therefore, the back-end automation system must have a mechanism to identify and respond appropriately when a submission is incorrectly labeled as positive.

The back-end automation system leverages a database of known false positive files to automatically identify false positives in submissions. If a file in the submission matches exactly with one in the false-positive database, the back-end system records the result in the database and excludes the file from further consideration.

CASE 3: KNOWN VIRUS FILTERING In the final stage of submission filtering, the back-end system scans all remaining files with Norton AntiVirus, using the very latest virus definition files. The back-end attempts to repair all files detected as viruses, and if the repair is successful, IT automatically records this result in the database. This filtering step enables the back-end system to automatically resolve submissions that contain new but only recently identified viruses. Because Symantec Security Response updates its virus definition files several times per day, this filtering step can quickly identify new viruses and ensure that customers quickly get the most up-to-date cures.

Quick analysis capability

ANALYSIS CENTER REPLICATION MODULES CAN REPLICATE AND COMPLETELY ANALYZE A NEW MACRO VIRUS IN APPROXIMATELY 30 MINUTES. AUTOMATIC VIRUS REPLICATION ENABLES DIGITAL IMMUNE SYSTEM COMPUTERS TO REPLICATE NEW AND UNKNOWN COMPUTER MACRO VIRUSES, CHARACTERIZE THEIR BEHAVIOR, AND AUTOMATICALLY GENERATE A CURE-ALL WITHOUT HUMAN INTERVENTION. RAPID REPLICATION AND AUTO-ANALYSIS OF NEW THREATS IS KEY TO COMBAT THREATS LIKE MELISSA. THIS IS THE FIRST SYSTEM IN THE WORLD TO PROVIDE AUTOMATIC PROTECTION AGAINST COMPUTER VIRUSES.

The Digital Immune System from Symantec deploys a back-end system analysis architecture, called the Analysis Center—created by scientists at IBM's T.J. Watson Research center—which offers:

1. Fast replication and auto-analysis of Word and Excel macro viruses, and of DOS viruses.
2. Multiple, simultaneous, replication and analysis sessions to support multiple customer requests.
3. Improved filtering of clean files and false positives.
4. An extendable architecture.

The Analysis Center automatically replicates and analyzes DOS, Word, and Excel macro viruses. If any of the files in a submission appear to be Word documents or Excel spreadsheets, those documents are queued for processing by the Analysis Center Macro replication module. If the files contain a DOS virus, they are routed to the DOS replication module.

Symantec and IBM Research engineers are in the process of adding and rolling out additional auto-analysis modules for 32-bit Windows viruses, and for computer worms within virtual email networks such as Explore.Zip and Melissa.

The Analysis Center is a fully contained network-within-a-network. Its replication system feeds each submitted sample (e.g., a Word document) into a simulated Windows computer running on an enterprise-grade server, and attempts to coax any viruses or worms within the document or spreadsheet to infect the virtual system.

If the document or spreadsheet contains no viruses, this will be apparent after the replication session; however, just because no viral activity was detected doesn't mean the file is not infected. Specifically, the file in question might contain a "picky" virus that fails to spread itself during the replication session. Consequently, the replication system inserts all log files and other data into the database for reference purposes, and the file is manually examined by Symantec Security Response researchers.

If the file in question does contain a computer virus, and if that virus replicates itself within the simulated environment, then the replication system gathers all potentially infected files and analyzes them. If all infected files show similar infection characteristics, the replication system automatically generates a new virus fingerprint for the virus.

Next, the replication system creates a test virus fingerprint database containing the new fingerprint and launches Norton AntiVirus, with this new database, to scan the virus and all of its child infections. If the test fingerprint database correctly detects and repairs all of the infections, the Digital Immune System provisionally certifies the new fingerprint.

Finally, the back-end system obtains a copy of the latest virus fingerprint database, without the new fingerprint, and scans all of the viral samples once more. If the most recent fingerprint database fails to detect the infections, the back-end inserts the provisional fingerprint into the master database. This final check is performed to reduce the likelihood that redundant virus fingerprints will be inserted into the fingerprint database. A new set of definitions is then built including the newly created fingerprint, and automatically returned via the Digital Immune System gateway to Central Quarantine at the customer site.

Once the back-end system has replicated and analyzed an infected file, and created a new fingerprint database, it initiates a house-cleaning session to check whether any currently open submissions contain the same virus; these submissions can be automatically re-filtered, eliminating the need for manual processing.

Reduced False Positives

PATENTED TECHNOLOGIES CHOOSE FINGERPRINTS THAT HAVE A 1-IN-10,000,000 CHANCE OF GENERATING A FALSE POSITIVE.

When extracting a fingerprint from a new virus, researchers must choose from thousands of possible fingerprints. Poorly chosen fingerprints may fail to detect virus variants (new strains) and may cause false positives, making this a difficult chore. Today, many anti-virus companies solve this problem by hiring experienced researchers to select appropriate virus fingerprints for distribution. However, even experienced researchers can pick less-than-optimal fingerprints.

To solve the problem of which virus fingerprints to use and distribute, researchers at IBM invented and patented techniques to automatically evaluate and select new fingerprints from a virus. The patented technology in the Digital Immune System uses Markov Chains to rank fingerprints according to their likelihood of false-positive occurrences and, according to IBM research, offers a 1-in-10,000,000 false-positive rate for new virus fingerprints—far better than the rates of human researchers.

The Workflow System

A ROBUST WORKFLOW SYSTEM ENABLES ENGINEERS TO EFFICIENTLY RESOLVE DIFFICULT SUBMISSIONS THAT CANNOT BE HANDLED BY AUTOMATION. SUBMISSIONS CANNOT BE LOST BECAUSE THE WORKFLOW SYSTEM TRACKS EVERY SUBMISSION.

If a submission has not been handled by the automated back-end system, the entire submission, including all log files and any other information gleaned during the analysis process, is placed onto the "open issue" file server. The back-end automation system then updates the submission database, telling Symantec Security Response engineers which "Open Issue" files are pending inspection. Symantec Security Response engineers use the HTML-based issue-tracking system to track all open issues submitted by all customers around the world. Open issues are prioritized based on submission time, customer support level, and other factors. Open issue submissions are visible from the Web-based Symantec Security Response issue-tracking system.

Symantec Security Response engineers and Analysis Center automation systems work around the clock to analyze new computer virus threats. Several times each day, engineers or the back-end replication system add new virus fingerprints to a master fingerprint database, while the housecleaning system monitors the database for changes. Whenever new fingerprints are added, the House cleaning system re-filters all open issues with the latest databases to clear open issues not resolved during the initial filtering process.

Automated Response

After the back-end automation system or Symantec Security Response engineers have examined all files within a given submission, the back-end system closes out the entire submission and sends a response to the customer describing the submission status. If the customer needs new virus definitions, the Digital Immune System automatically sends them to Central Quarantine at the customer site. Central Quarantine distributes definitions based the administrator's system configuration, and automatically sends definitions to the infected machine or to a larger group of machines, including desktops, servers, and gateways.

Real-Time Status Updates On All Submissions

Central Quarantine delivers real-time status updates on all submissions to the Digital Immune System. The Quarantine Console tracks each submission separately, displaying the stage of processing for each submission (development, quality assurance, automatic replication), and detailing the set of virus fingerprints that will help resolve the virus submission.

Full, End-To-End Automation

The Digital Immune System provides 100% automation of the closed-loop process, on both the up-link (virus submission) and down-link (fingerprint distribution to the enterprise, and its desktops, servers, and gateways). Administrators can configure the Digital Immune System to run automatically without any user interaction and to:

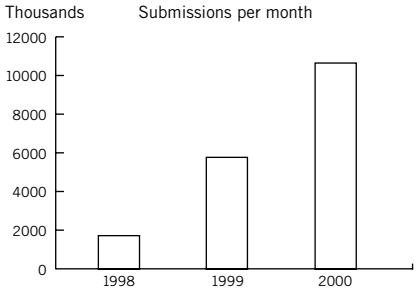
1. Automatically detect and quarantine new and unknown viruses.
2. Automatically filter and forward samples to Symantec Security Response for analysis (stripping sensitive content, if desired).

3. Automatically check for new virus fingerprints and status updates.

4. Automatically deploy new fingerprints to the infected machine or to a larger distribution of machines.

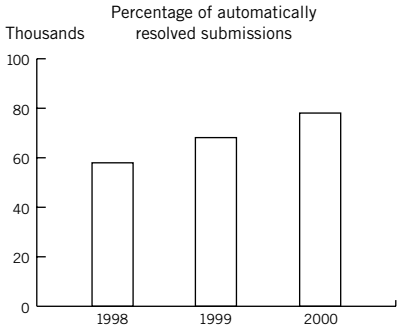
Results

WHILE SUBMISSION RATES HAVE INCREASED DRAMATICALLY, THE AVERAGE SUBMISSION RESPONSE TIME HAS DECREASED 50% FROM THE ORIGINAL 21.6 HOURS WHEN THE SYSTEM WAS FIRST DEPLOYED IN 1998, AND HAS DECREASED 79% FROM THE 48 HOURS REQUIRED DURING MANUAL PROCESSING BEFORE 1997.



The next graph shows the percentage of customer submissions that are handled automatically (without any human intervention) by the Digital Immune System.

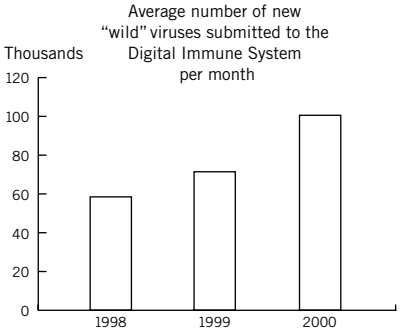
The Digital Immune System enables customers to easily submit increasing numbers of new computer viruses, worms, and Trojan horses. As the user community grows, so does the number of new viruses submitted. Each time the Digital Immune System automatically resolves a new computer virus, all members of the community reap the benefits of rapidly updated fingerprints.



The following chart shows the increase of new "wild" viruses submitted to the system each month.

Conclusion

To quickly, automatically and efficiently distribute virus cures–this is the main purpose of the Digital Immune System.



The latest computer viruses and worms are propagating at an ever increasing rate, forcing anti-virus companies to re-evaluate their strategies and technologies. These new threats have necessarily shifted the focus away from the endpoint to the network and the desktop. No matter how effective desktop and server anti-virus software may be, if new cures can't be created and distributed quickly enough to protect against the latest threat, there is no benefit to the customer.

Upon receiving a possible new virus, the Digital Immune System can replicate, analyze, create, and test a cure in approximately 45 minutes. This gives customers a total turnaround time of roughly one hour for automatically processed macro viruses. Within the next few years, Symantec researchers expect to reduce the closed-loop response time for a new virus threat to under 30 minutes from virus discovery on the corporate desktop, server, or gateway to distribution of new fingerprints back to the desktop, server, gateway, or entire organization.

The Digital Immune System automates the virus cure creation and distribution entire process, leaving nothing to chance or human error. Only with such a system can cures spread faster than today's viruses can spread themselves.

SYMANTEC, A WORLD LEADER IN INTERNET SECURITY TECHNOLOGY, PROVIDES A BROAD RANGE OF CONTENT AND NETWORK SECURITY SOLUTIONS TO INDIVIDUALS, ENTERPRISES, AND SERVICE PROVIDERS. THE COMPANY IS A LEADING PROVIDER OF VIRUS PROTECTION, RISK MANAGEMENT, INTERNET CONTENT AND EMAIL FILTERING, REMOTE MANAGEMENT, AND MOBILE CODE DETECTION TECHNOLOGIES TO CUSTOMERS. HEADQUARTERED IN CUPERTINO, CALIF., SYMANTEC HAS WORLDWIDE OPERATIONS IN MORE THAN 33 COUNTRIES.

WORLD HEADQUARTERS

20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
1.408.253.9600
1.800.441.7234

www.symantec.com

For Product Information
In the U.S., call toll-free
800-745-6054.

Symantec has worldwide operations in 36 countries. For specific country offices and contact numbers please visit our Web site.