Lower IT Costs through Better Anti-Virus Management

A SYMANTEC CORPORATE SOLUTION

SYMANTEC.™

Table of Contents

Executive summary

As a member of the IT community, you face challenges every day in keeping servers and workstations up and running. These challenges are complicated by the demands of an increasingly complex IT environment, limited IT resources, and often the requirements of a Service Level Agreement as well. Yet the failure to meet these challenges can result in decreased IT credibility, unanticipated organizational changes, outsourcing of IT functions, and diminished resource allocations—all of which make it even harder for you to provide excellent service in the future.

Computer viruses are among the most frustrating challenges faced by IT organizations today. They rob workers of productivity, divert IT personnel from more strategic corporate concerns, and can even jeopardize your company's information security. Yet there is no way you can keep every virus out of your company's computers. Employees unthinkingly launch executable email attachments that contain them. Newsreader programs pick up viruses attached to Usenet postings. Traveling employees bring them in on laptops after visits to customer sites.

Each time a workstation or server has problems and IT resources must be redirected to fix those problems, you incur additional costs, spend extra time, and your IT group's credibility slips just a little bit more. IT organizations therefore need strategies and robust tools to deal with the growing virus problem.

Even if you already have a strong anti-virus (AV) product, many new viruses are so complex that simply issuing new virus definitions for them isn't sufficient. These new classes of viruses require either patches or whole new revisions of the AV software.

With most AV software that means updating and producing an in-line for the entire program, because the scanning engine and the scanning application are inextricably linked together. Symantec realized that a faster, better, and less expensive solution was required to meet the needs of our customers.

That's why our Norton AntiVirus™ software features Norton AntiVirus Extension (NAVEX™) technology. This modular virus-scanning engine lets the engineers in the Symantec AntiVirus Research Center (SARC)™ quickly update and redistribute the relevant elements of Norton AntiVirus software efficiently and effectively. You not only get virus fixes faster, you get them in a form that's smaller and easier to distribute to all the workstations and servers you support.

NAVEX technology is integrated into all Norton AntiVirus products. NAVEX enables SARC to seamlessly update the scanning engine during normal virus definition updates. It's the only solution of its kind available to users of AV software today.

This white paper describes the current computer virus situation, how most AV vendors are dealing with it, and how Norton AntiVirus products—with their NAVEX technology—provide a faster, simpler, and significantly more cost-effective way to keep all your computers protected from viruses.

The escalating virus problem

Initially there were only a few computer viruses, so programmers of anti-virus products could spend a significant amount of time analyzing each new virus that was discovered, building a customized solution for it into their products, and re-releasing their programs.

However, as viruses became more prevalent, it was no longer practical to create a new version of an AV product in response to each new virus. Thus the next step was for AV vendors to create engines that could look for a virus's fingerprint. A fingerprint is a unique sequence of bytes known to be contained in a given virus. This new approach allowed AV researchers to simply add new fingerprints to the existing database used by their product when new viruses were discovered. This technique made product development faster and easier, reduced the amount of data that needed to be sent out to customers (a database update instead of a whole new software release), and eliminated the need to build a new product from scratch every time a new virus was discovered.

Unfortunately, virus writers are motivated to write code that's hard to detect and/or repair. So over the years, whole new classes of viruses emerged that were able to evade the traditional detection-and-repair algorithms of AV programs. Adding traditional fingerprints was useless in treating these viruses; new technology had to be constructed to eliminate them.

Viruses that the technology of the time couldn't handle included unusual encryption routines for hard drives (such as the One_Half virus) and attempts to conceal viral routines in memory (such as the Stealth virus). These types of viruses could necessitate a complete change in a program's AV engine. In other words, AV vendors were back to the original problem of having to spend a lot of time developing new versions of their products to eradicate the new threats.

Special case viruses that have required new AV technology to eradicate.

Boot viruses
Polymorphic viruses
Cluster viruses
32-bit Windows viruses
Variable-entry viruses
Microsoft® Office 2000 viruses
Resident viruses
Access® viruses
.HLP file viruses
Microsoft® Excel viruses
Windows® 3.1 viruses
PowerPoint® viruses
Microsoft® Office 97 viruses
Device driver viruses
Stealth viruses
Microsoft® Word viruses
VBScript viruses

Today, there are even more viruses have been developed (well over 40,000 today) and more people using AV programs. These factors mean that troublesome viruses are more common and, at the same time, it's even more costly to keep all of a company's computers updated effectively.

The cost of building, testing, and manufacturing new products is high for AV developers, and the cost—and logistical hassle—of continually reinstalling, testing, and distributing the AV software is high for customers. IT organizations end up spending valuable resources on this constant upgrading, and everyone from upper management to end users may get the impression that IT is not really on top of the virus situation if they keep having to install new AV software.

What are AV vendors doing about this frustrating situation?

Traditional anti-virus software architecture

In order to understand why the Symantec Norton AntiVirus solutions are so powerful, it's helpful to first consider the fundamental design of AV programs and how other vendors are dealing with complex viruses.

The scanning application and the scanning engine

The typical AV program comprises two major components: the scanning application and the scanning engine.

The scanning application provides a user interface, alert functions, and logging mechanisms. The application determines which files to scan and how to react when a virus is found. However, it knows absolutely nothing about computer viruses. Every time it scans a file or a floppy disk, it calls upon ***the scanning engine*** to detect computer viruses in the designated location.

If the scanning engine locates a virus, it reports back to the scanning application. The scanning application then informs the user of the infection and prompts the user to repair the file. If the user chooses to do so, the scanning application again calls upon the scanning engine to repair the infected file or disk.

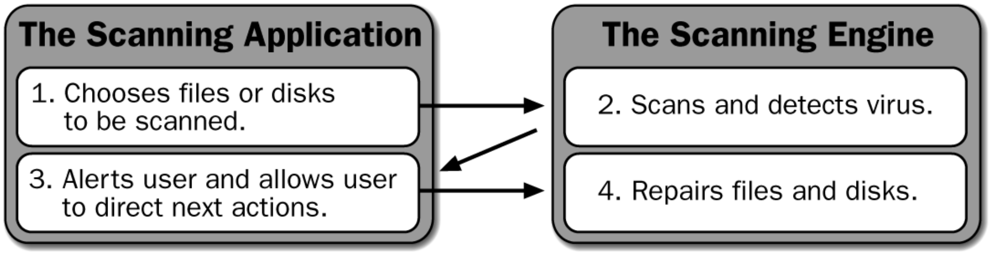

The Scanning Application
1. Chooses files or disks to be scanned.
3. Alerts user and allows user to direct next actions.
The Scanning Engine
2. Scans and detects virus.
4. Repairs files and disks.

Figure 1: How the scanning engine and scanning software work together

The scanning engine comprises dozens of complex searching algorithms along with CPU emulators and elaborate program logic. In contrast to the scanning application, the engine knows nothing about user interfaces, which files to scan, or what to tell the user when it finds a virus. It only knows how to detect and repair viruses. It simply examines the file or disk the scanning application directs it to, and determines whether there are any viruses present.

Typically, scanning engines work by scanning each file or disk for thousands of virus fingerprints. These fingerprints are stored in the virus definition data files that users around the world download each week when they obtain their virus software updates.

In all AV programs except the Norton AntiVirus family, the scanning application and the scanning engine are fused into one inseparable component.

The obstacles to successful enterprise-wide AV protection are numerous, and virus eradication is time-consuming and expensive.

Drawbacks to the traditional AV architecture

The inflexibility of traditional AV architecture, with its combined scanning application and scanning engine, becomes apparent when an IT organization is faced with a complex new virus. The obstacles to successful enterprise-wide AV protection are numerous, and virus eradication is time-consuming and expensive. Some of the consequences in applying typical AV programs to special case viruses are:

- A new version of the AV product must be released to eradicate a special case virus. When a virus is discovered that cannot be handled by a simple fingerprint update, the entire AV program must be updated and reinstalled. Even if no changes are required to the scanning application itself, changes to the scanning engine require new deployment of the entire product.
- The AV software on each supported platform must be updated to include the new scanning engine logic. And each of these new product in-lines must be deployed by the IT organization.
- Platform releases are staggered over time, leaving an IT organization with inconsistent protection across desktops, servers, and gateways until all the platforms are updated. Producing new code for each AV platform is time-intensive and costly, and forces the typical AV vendor to develop and deploy their full spectrum of product support over a period of months.
- Every AV installation requires IT time, money, and resources.
- End user productivity continues to be affected until complete AV protection is achieved across the enterprise.

AV vendor strategies to counteract product drawbacks

The costs to update and deploy comprehensive AV protection are high. To lessen expenses – to themselves and to their customers – AV vendors have tried to implement various alternative strategies.

Selective virus protection

One vendor strategy to reduce AV costs is to select only certain classes of viruses to eradicate. Sometimes this choice is made because creating a robust solution is very difficult; other times it results from the vendor's inability to integrate a solution cleanly and quickly. The major drawback in this cost-cutting strategy is the viruses that are not addressed, and leaving the customer open to infection.

Releasing temporary stand-alone tools

Another cost-cutting strategy is to build a stand-alone tool to deal with each new class of virus, distribute that tool to customers, and then integrate the new capability into the main program later. This is a stopgap solution that addresses immediate virus threats, but prolongs distribution and administration for IT.

Stand-alone tools are not platform-independent. They are usually command-line utilities written only for DOS. End users must be trained to use them, and must remember to use them regularly in addition to their normal AV software to scan files and email attachments.

When the AV vendor has eventually integrated and tested this new technology on all its AV platforms, customers must upgrade all their workstations and servers again to take advantage of the new product.

Grouping solutions together in large releases

This final cost-cutting strategy is a compromise position between the previous two choices. Here, the AV vendor waits (potentially months) until several new complex viruses are discovered and then updates the AV product line all at once to handle the latest set of virus threats. This method reduces IT administration and deployment time, but leaves the enterprise without updated AV protection for a period of time.

The length of this unprotected period can vary, but AV vendors often need six months or more to update an entire line of AV products across all platforms—perhaps first the Windows 32-bit scanner, then the NLM, then the NT server product, and finally the gateway products. So even after the first new products have been released, many other computers in customers' companies can remain unprotected.

As we have seen, the standard architecture of AV products can cause serious delays, expenses, and loss of productivity for the companies who use them. Businesses need a new anti-virus architecture that can be modified, distributed, and installed quickly and cost-effectively when new classes of viruses are discovered.

NAVEX™: A unique technology in Norton AntiVirus™ products

Symantec looked at the drawbacks of the traditional AV software architecture—and the ineffective solutions that it pressures vendors into making—and realized that a new design was needed to better serve customers.

"Abnormal" viruses have become the norm. Unless detection and repair for complex viruses can be implemented with the same ease as the fingerprinting technology of the past, creating and maintaining a robust AV solution becomes impossible. Therefore, powerful new detection and repair strategies must become part of the normal virus definition update.

The result of our research was Norton AntiVirus Extension (NAVEX) technology, which separates the scanning engine from the scanning application. The scanning engine can now be updated on its own, improved on its own, and redistributed as part of the standard Norton AntiVirus virus definitions through all available update methods. NAVEX enables Symantec to provide customers with compact, easy-to-distribute, easy-to-install updates to all our Norton AntiVirus products.

Support for all Norton AntiVirus products and platforms

The NAVEX engine's source code is platform-independent. In response to a complex new virus, or new classes of viruses, (such as Office 2000 viruses) Symantec can quickly compile a single set of engine source code for every computer platform supported by Norton AntiVirus, protecting your entire enterprise at once.

All Norton AntiVirus products on all platforms support NAVEX. That includes all on-demand components, real-time components, background scanners, server products, gateway products, and groupware products. When your enterprise upgrades to the latest definitions, your desktop systems, Windows NT® servers, and NLM will all have the latest engines and databases, and therefore the latest protection.

...Symantec can quickly compile a single set of engine source code for every computer platform supported by Norton AntiVirus, protecting your entire enterprise at once.

Consistent protection across the enterprise

Each update of the NAVEX engine is generated from one set of source code. That means SARC engineers only need to modify the program logic once in order to properly update the scanning engines for all Norton AntiVirus products—for both real-time and on-demand scanning functions. This single code-base approach gives you consistent AV protection across your entire company.

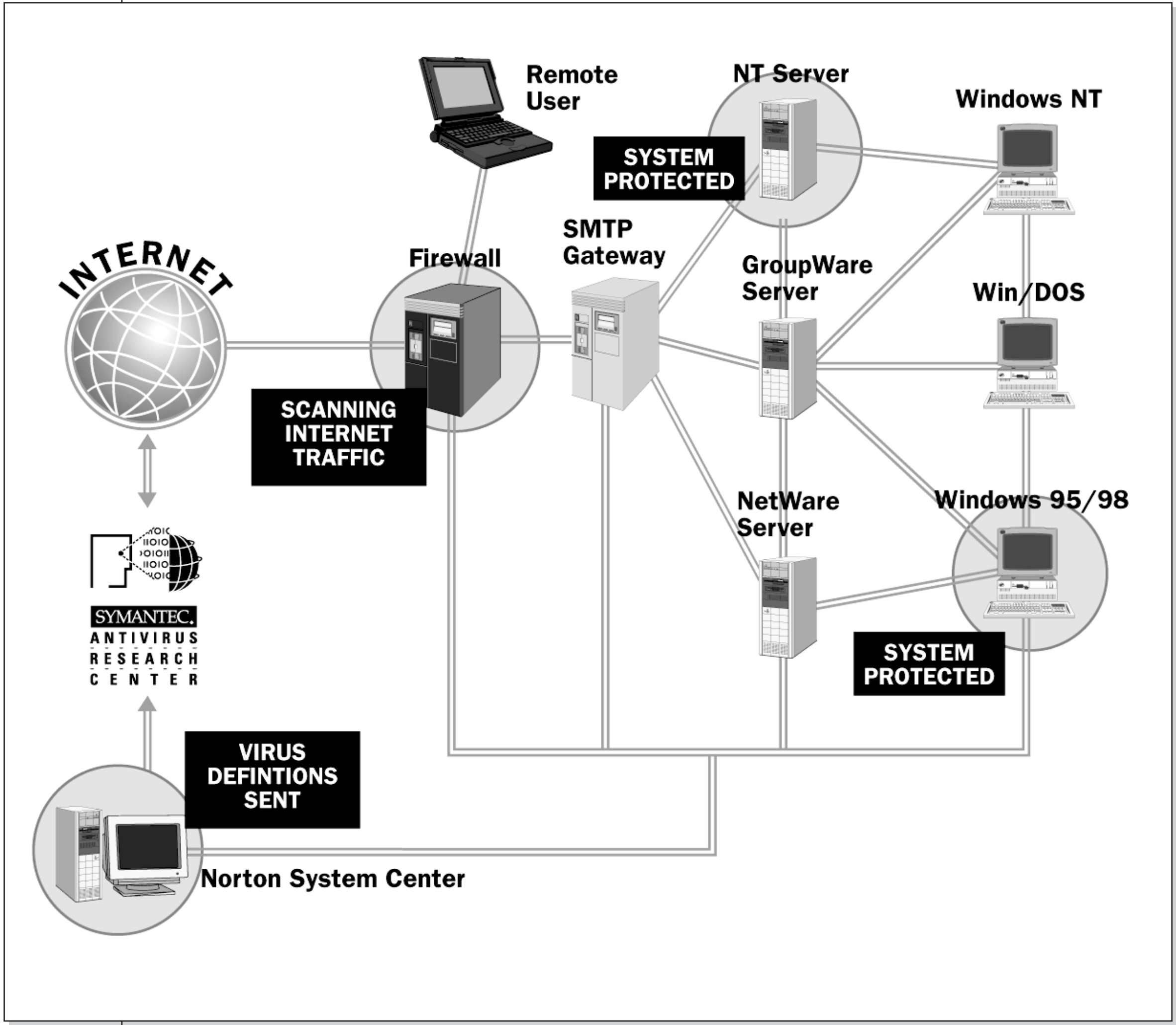


Figure 2: How one set of Norton AntiVirus source codes deploys to protect the entire enterprise.

No workstation or server downtime

All Norton AntiVirus products can be upgraded with new NAVEX engines without having to reboot the computer or even shut down the AV scanner. There's no need to take down your file servers, groupware email servers, or users' desktop systems, so you get updated virus protection without lost productivity.

Easy distribution

The modular Norton AntiVirus architecture enables Symantec to send out compact updates to the NAVEX engine instead of the full software updates required by other AV products. This approach makes it far easier for you to get updates from Symantec and then distribute them to your staff and end users.

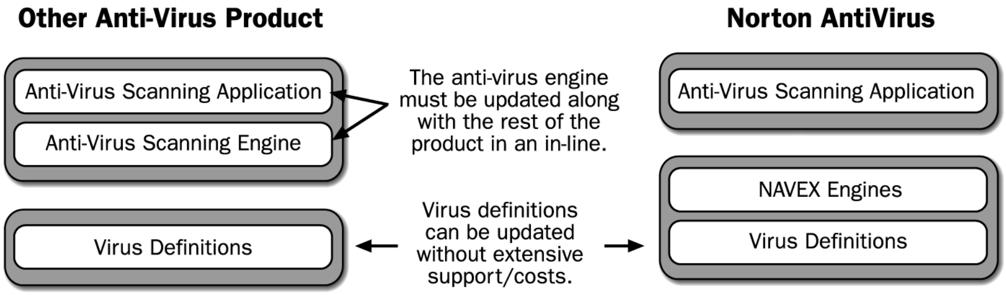

Other Anti-Virus Product
Norton AntiVirus
Anti-Virus Scanning Application
Anti-Virus Scanning Engine
The anti-virus engine must be updated along with the rest of the product in an in-line.
Anti-Virus Scanning Application
NAVEX Engines
Virus Definitions
Virus definitions can be updated without extensive support/costs.
Virus Definitions

Figure 3: Updating with Symantec and NAVEX vs. updating with other AV vendors

Here are three easy ways you can get virus updates from Symantec:

- LiveUpdate™ sessions, in which the Norton AntiVirus software dials in to a Symantec server to download the latest updates to virus definitions.
- Downloads from the Symantec web site
- Scan and Deliver responses. Scan and Deliver is a feature of Norton AntiVirus that emails newly detected virus strains to the Symantec AntiVirus Research Center for identification. (To protect the privacy of your company's documents, only the virus is sent, not the entire infected file.) SARC researchers can then respond via email with a new virus definition to treat the infection. If necessary, the new virus definition can include a new NAVEX engine.

Because virus definition updates containing new NAVEX engines are so small, you can use your choice of file and web servers, email attachments, and so on to distribute the updates to your IT staff and end users.

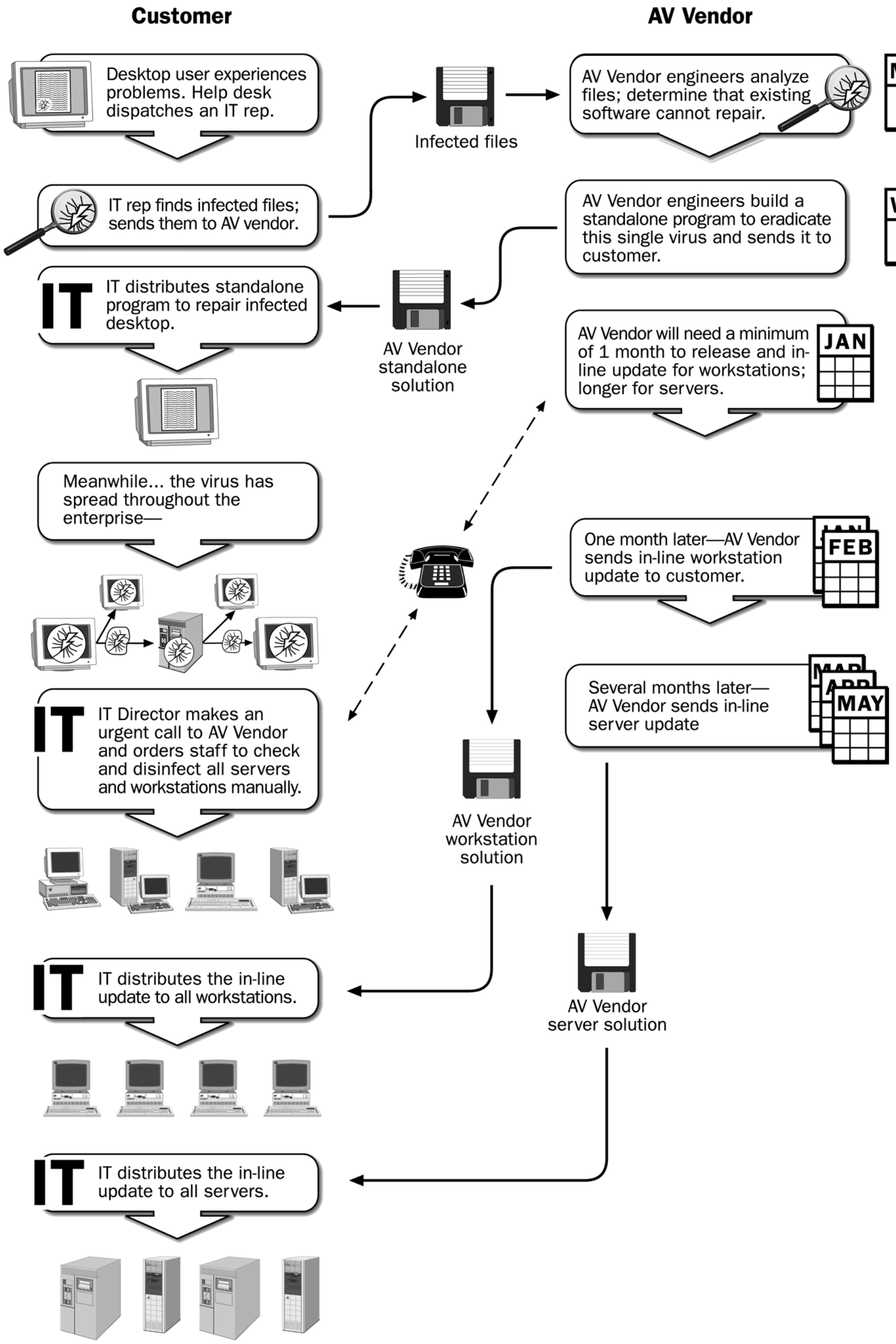
When users receive an update, virtually a single click lets them incorporate it into Norton AntiVirus. They never have to install and learn a new stand-alone tool in order to deal with a specific new virus.

Virus Eradication Scenarios

Virus authors revel in their attempts to confound AV researchers. And while most viruses use the same techniques to spread, some viruses break the mold. There are also "special case" viruses that use common techniques to spread but have some sort of nasty side effect that can't be undone without modifying the scanning engine.

This section describes two scenarios: how the vendor of a typical AV program would deal with a special-case virus, and how Symantec, with its unique NAVEX technology, would deal with it.

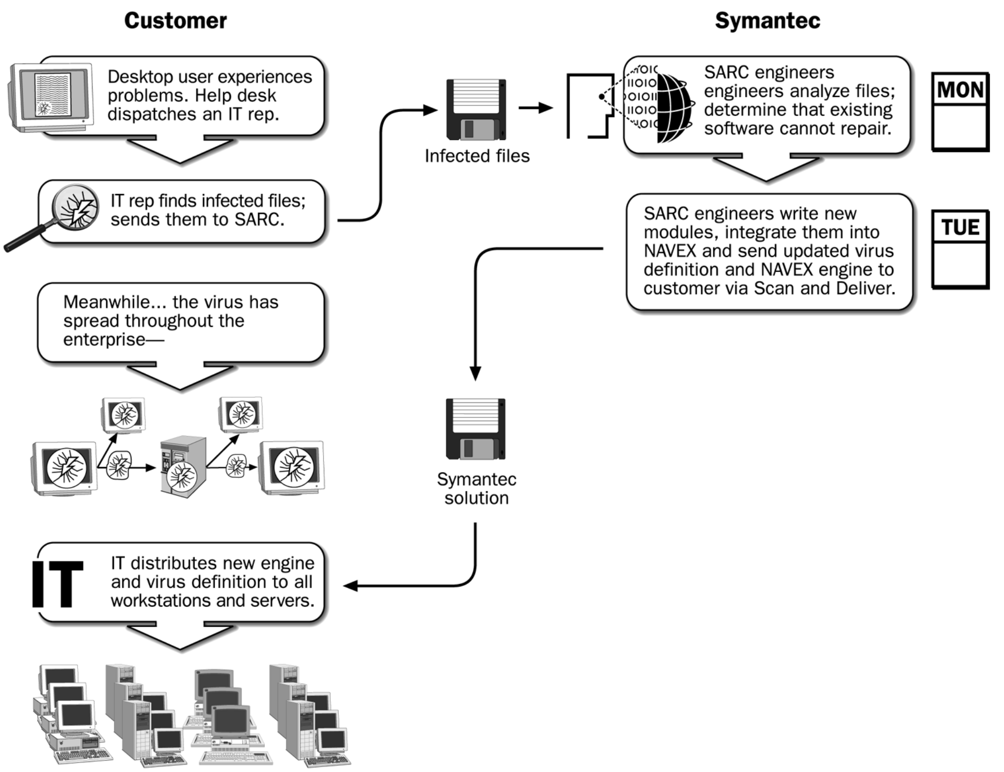
Virus eradication: the traditional AV software solution



Customer
AV Vendor
Desktop user experiences problems. Help desk dispatches an IT rep.
Infected files
AV Vendor engineers analyze files; determine that existing software cannot repair.
MON
IT rep finds infected files; sends them to AV vendor.
AV Vendor engineers build a standalone program to eradicate this single virus and sends it to customer.
WED
IT
IT distributes standalone program to repair infected desktop.
AV Vendor standalone solution
AV Vendor will need a minimum of 1 month to release and in-line update for workstations; longer for servers.
JAN
Meanwhile... the virus has spread throughout the enterprise—
One month later—AV Vendor sends in-line workstation update to customer.
JAN
FEB
IT
IT Director makes an urgent call to AV Vendor and orders staff to check and disinfect all servers and workstations manually.
Several months later—AV Vendor sends in-line server update
MAR
APR
MAY
AV Vendor workstation solution
IT
IT distributes the in-line update to all workstations.
AV Vendor server solution
IT
IT distributes the in-line update to all servers.

Figure 5: the 6-month virus update solution

Virus eradication: the NAVEX solution



Desktop user experiences problems. Help desk dispatches an IT rep.

IT rep finds infected files; sends them to SARC.

Meanwhile... the virus has spread throughout the enterprise—

IT distributes new engine and virus definition to all workstations and servers.

SARC engineers engineers analyze files; determine that existing software cannot repair.

SARC engineers write new modules, integrate them into NAVEX and send updated virus definition and NAVEX engine to customer via Scan and Deliver.

Figure 6: the 2-day Norton AntiVirus update solution

Virus eradication: the traditional AV software solution

Virus eradication: The traditional AV software solution

- *The first signs of trouble.* An employee's workstation crashes over and over. She calls the company's IT help desk.
- *Escalating the problem.* Several hours later, an IT representative arrives. He notices that a number of executable files appear to be corrupted and begins to suspect a computer virus, so he sends the files to the company's AV vendor.
- *A new virus is discovered.* The AV vendor's researchers analyze the files and realize they're dealing with a new virus that's too different for their existing AV product to detect or repair.
- *A stopgap solution.* The AV engineers realize that they cannot quickly update their main product, so they create a temporary DOS-based stand-alone program to deal with this virus and send it to the IT director at the client company.
- *The workstation cure is distributed.* The IT director distributes the tool to her staff so that they can clean up the infected workstations. Two days after the initial outbreak, the employees affected by the problem are finally able to work again.
- *More infections throughout the enterprise.* In the meantime, IT detects the virus the company's file and email servers; it has spread and reinfected some workstations. The AV vendor promises a new version of workstation software in about a month, and the server version in several more months.
- *Manual labor.* IT personnel fan out to scan all the local site's file and email servers manually, hand copies of the disk to all infected workstation users, and send copies of the program to all of their company's other sites.
- *New workstation AV software.* One month later, the AV vendor ships an in-line update for the desktop version of their AV product.
- *New server AV software.* Several months later, the AV company ships its server product to the customer. More than half a year after the new virus was discovered, the situation is finally under control. At least, until the next unusual virus appears…

Summary

This scenario is typical of virtually all AV companies and their clients. It took a month for the AV vendor to provide a software update just for workstations—months more for servers. Meanwhile, in order to protect users against this virus, the IT staff needed to manually scan dozens or even hundreds of machines, then later reinstall AV software on thousands of machines. Because the original solution was not part of the normal AV program, the virus was able to spread again when it was not completely eradicated or was reintroduced into the enterprise.

Unfortunately, this scenario happens frequently in many corporations around the world. Companies may lack protection against key viruses for months at a time. Employees must manually scan files with special purpose tools, losing productive time from their work schedules. Administrators must sift through email servers to track down and eradicate infections. IT personnel are forced to spend time dealing with virus eradication instead of working on strategic company IT plans. Today's enterprises simply can't afford to waste the time of their IT staff and general employees in this way.

Virus eradication: the NAVEX solution

Virus eradication: The NAVEX solution

- ***The first signs of trouble.*** An employee's workstation crashes over and over. She calls the company's IT help desk.
- ***Escalating the problem.*** Several hours later, an IT representative arrives. He notices that a number of executable files appear to be corrupted and begins to suspect a computer virus. He sends the files to the Symantec AntiVirus Research Center (SARC) using the efficient Scan and Deliver feature built into Norton AntiVirus.
- ***A new virus is discovered.*** SARC researchers analyze the files and realize they're dealing with a new virus that's too different for the existing version of Norton AntiVirus to detect or repair. SARC promises to deliver a solution within the next 24 hours.
- ***More infections throughout the enterprise.*** In the meantime, IT detects the virus in the company's file and email servers. SARC promises a comprehensive solution for all supported platforms within the next 24 hours.
- ***Updating Norton AntiVirus, with no stopgap solution needed.*** SARC engineers update the NAVEX engine to deal with the new virus. Because the full Norton AntiVirus engine can be modified so easily, there's no need to settle for a stopgap stand-alone solution. When the new virus definition set is ready, SARC sends to the IT director at the client company.
- ***The cure is distributed.*** The IT director gives the Norton AntiVirus update to her top engineer. He uses the company's standard distribution tools to disseminate the new virus definitions to all workstations, file servers, email servers, and gateways. He then initiates virus scans across the enterprise. He also sends the update to all other corporate sites for deployment. Two days after the initial outbreak, the employees affected by the problem are able to get back to work—and their workstations and all other computers in the company are protected from future infections by this virus.

Summary

That's how Symantec responds to a difficult new computer virus: quickly and effectively.

In both scenarios, it took roughly the same amount of time for the AV engineers to develop a solution for the virus. However, the other AV vendor had to create a temporary stand-alone tool—one that required manual intervention at every step and wasn't integrated with their regular AV software. By the time the vendor updated the AV offering on each and every platform, the customer's IT staff and other employees had lost hundreds of hours of work time. By contrast, because of Symantec's NAVEX technology, the Symantec customers got a comprehensive, integrated, multiplatform solution within two days.

The costs of distributing new anti-virus protection

The following scenarios illustrate the costs of updating Norton AntiVirus, with its innovative NAVEX technology, compared with updating a competing AV product to handle the same virus.

In both instances, we'll assume that:

- The company has 5,000 computers: 300 are Windows NT® 4.0 servers and 4,700 are Windows® 95 and Windows NT clients.
- The company's network administrator makes $60,000 a year, an approximate hourly rate of $41.00 including benefits.* We'll make the same salary assumption for the other employees mentioned in this case study.

  *Using a benefits load factor of 1.37, we get a true cost of $82,200. At 2,000 working hours a year, that yields the hourly rate of $41.00.

Updating a typical anti-virus program

There are several levels of cost to an IT organization when updating a traditional AV product to provide detection and repair for a new virus threat, such as Microsoft® Office 2000 macro viruses:

Update costs for a new virus threat:

- **Testing.** A network administrator tests an in-line version of an AV product for an average of 60 hours before deploying it across the enterprise. While in-lines often fix many problems for users, they also frequently create new issues or have incompatibilities with existing software. Thus the need for extensive testing. At the administrator's rate of $41.00 an hour, this 60 hours of testing will cost approximately $2,460.00.

- **Rolling out the new in-line.** With software distribution in place, the rollout effort would probably take around 32 hours of the administrator's time, costing about $1,312.00.

  Without software distribution in place, the administrator would probably post the in-line on a publicly available file or web server and then notify users about the update via email. All users would then be responsible for updating their own computers. If we assume that it takes the average user 20 minutes to find the in-line on the server, install it, and then reboot the desktop system, this update would take a total of 1,500 hours for the company's 4,700 workstation users. Assuming an average pay rate of $41.00 per hour for the workstation users, the distribution will roughly cost the company $61,500.00.

- **Help desk support.** Let's assume that some users will have problems installing the new update and will need to call the help desk. Even with a failure rate of only 5 percent, these problems will result in 150 calls to the help desk, at approximately 20 minutes each. That adds another 50 hours of support time at an additional cost of $2,050.00.

Table 1 summarizes the costs of in-lining a non-NAVEX-based AV product to support a hard new virus or new class of viruses:

Task	Rough estimate cost
Testing of the new version of the anti-virus software, configuration of settings, etc.	$ 2,460.00
Rollout with software distribution tools	$ 1,312.00
Calls to the help desk at 5% rate	$ 2,050.00
Total cost	**$ 5,822.00**

Task	Rough estimate cost
Testing of the new version of the anti-virus software, configuration of settings, etc.	$ 2,460.00
Manual rollout	$ 61,500.00
Calls to the help desk at 5% rate	$ 2,050.00
Total cost	**$ 66,010.00**

Table 1: Costs to update a competing AV product to support a new threat, across the enterprise, with either manual distribution or using software distribution technologies.

And other virus update costs:

Those viruses that do not require scanning engine updates. Regular virus definition updates must still be distributed to yield protection against new viruses that don't require engine updates (such as to protect against new Office 95/97 macro viruses, DOS viruses, or BOOT viruses). If we assume that competing AV products have a distribution mechanism similar to Symantec's LiveUpdate, this will cost an additional $1,312.00 per update. However, because competing products may require a reboot of desktop machines and a shutdown of the file or groupware server during the update, the administrator and end users will incur additional unproductive downtime during definition updates.

Updates to each platform as solutions become available. Because most AV vendors must in-line multiple products on multiple platforms to cope with a new virus, it can be months before an enterprise has complete protection across desktop systems, file and email servers, groupware servers, and the gateway. This incomplete and inconsistent protection makes the enterprise victim to repeat infections and the increased costs of maintaining the non-NAVEX solution.

Updating Norton AntiVirus

Now consider the costs of distributing an update to Norton AntiVirus:

Update costs for a new virus threat:

In order to detect and repair a completely new threat such as Office 2000 viruses, the administrator needs to distribute the latest virus definition files – these include the new NAVEX engine – to all desktops and servers.

- **Testing.** Most administrators test new virus definitions before a full rollout. We will estimate 16 hours of testing before this rollout. Because the software being tested includes only a set of virus definitions, rather than an in-line update of the entire application, much less testing is required than with typical AV products. Assuming once again a $41.00 per hour pay rate for an IT administrator, testing will cost approximately $656.00.

- **Distribution.** Once the administrator is assured of the stability of the new virus definitions, he posts the virus definitions on the corporate LiveUpdate server. LiveUpdate is a pull technology that all Symantec products use to obtain updates. Administrators can maintain intranet LiveUpdate servers and post new virus definitions to them as required. Client Symantec software, such as Norton AntiVirus, can be scheduled to pick up these updates as often as necessary. LiveUpdate servers can use virtually any operating system and platform, as long as the platform supports UNC, FTP, or HTTP access.

  We will estimate two hours to post the new virus definitions on the LiveUpdate server – the administrator will incur a cost of about $82.00. After the virus definitions are posted, all Norton AntiVirus desktop, server, and gateway versions can download them when appropriate.

Other virus update costs: none. Because Norton AntiVirus does not require rebooting when new virus definitions are obtained, no additional administrative effort is required to update all Norton AntiVirus products across the enterprise, and no employee downtime for rebooting is incurred.

The total cost of updating Norton AntiVirus in this situation therefore amounts to $738.00.

Task	Cost
Testing of new virus definitions	$656.00
Deployment of new virus definitions to Live Update server	$82.00
Total cost	**$738.00**

Table 2: Cost to update Norton AntiVirus to support a new threat, across the enterprise.

Summary

As the examples above show, it can cost roughly from 7 to 89 times more to update a typical AV product to handle hard viruses or new classes of viruses than to update Norton AntiVirus products. This is an example of how NAVEX technology saves you time, money, and frustration.

A special note to Microsoft® Office 2000 purchasers

As your users or business partners begin to use Microsoft Office 2000, your enterprise will need protection against new virus threats.

If you're using a competing anti-virus offering, and intend to in-line your solution as you did for Office 97, consider the following: for the one-time cost of switching to Norton AntiVirus, you'll never again have to deploy in-line upgrades of your anti-virus software to stay protected against new viruses.

Conclusion

With complex new viruses becoming the norm rather than the exception, it is more important than ever to employ an AV product that has a modular engine. This architecture can save countless hours of testing, updating, manual virus elimination, and calls to the help-desk.

Competing AV vendors offer a number of ad hoc solutions to deal with new virus threats until they can in-line their existing AV protection. However, these solutions are not cost effective, and provide varying levels of AV protection in different areas of the enterprise, and often require manual end-user intervention.

Finally, when in-lines of the competing AV product finally do become available, they require extensive testing, distribution, rebooting of workstations and servers, and end-user support.

Without NAVEX technology, there are two choices: pay a lot more for good protection, or stay unprotected.

With the NAVEX technology built into all Norton AntiVirus products, your entire enterprise can be quickly and efficiently updated to the latest level of protection—for a fraction of the cost of less-effective solutions. That's the Symantec advantage.

About Symantec

Founded in 1982, Symantec Corporation is the world leader in utility and communications software for business and personal computing. More than 50 million people worldwide use Symantec products. And Symantec products occupy the number one or two position in every software category in which they compete – categories like Java™ development tools and utility and mobile worker software, that Symantec created with its innovative, first-to-market solutions.

Symantec is dedicated to providing its customers with the highest-quality, most cutting-edge software products available, and the superior service and support to back them up. With its charter to create products and solutions that maximize user productivity and minimize support from IT, Symantec is poised to build upon its 15 years of market excellence and leadership.

Appendix: New types of virus threats

How often do computer viruses actually necessitate the updating of an AV product's scanning engine? The answer these days, unfortunately, is "all too often."

Here's a partial list of new viruses and virus classes that have required fundamentally new AV engines just in the past two years. Each of these problems forced Symantec's competitors (and their customers) to in-line their AV software in order to provide updated virus protection.

Office 97 viruses

The release of Microsoft Office 97 suite included a change in the basic macro language of the office applications. Existing macro detection strategies had to be researched and reengineered to understand the new file formats. Viruses of this type already make up roughly 5% of viruses known to be spreading "in the wild."

32-bit Windows viruses

The number of 32-bit Windows viruses has risen significantly in the last 18 months and many of these viruses are complex polymorphic (self-mutating) viruses. The first one, HPS, was discovered in May, 1998, and a more recent polymorphic virus (Win95.Marburg) has been found in many locations. While most AV products contain excellent technology for detecting DOS polymorphic viruses, detecting new 32-bit Windows polymorphic viruses is a whole new game—requiring a whole new engine.

XF.Paix

The XF in Paix's name stands for "Excel formula." This virus employs a new type of attack on Microsoft Excel spreadsheets. Scanning engines had to be redesigned to scan these Excel files more robustly, especially since Paix is spreading unfettered. The leading Norton AntiVirus competitor took many months to provide in-lines that protected all platforms against this now-prevalent class of virus.

Remote Explorer virus

The high profile Remote Explorer virus has the unusual characteristic of compressing and storing the original host within itself (using the gzip algorithm). Norton AntiVirus was the first AV product to provide an integrated, cross-platform solution for this virus. At the time of this writing, most competitors still lack detection and repair for this virus across all platforms, in both real-time and on-demand products.

PowerPoint viruses

The first Microsoft® PowerPoint® viruses emerged in 1998 (PP97M.Master.A). Already, strains of these viruses have made the Wildlist. As usual, a new virus class requires a new detection strategy.

Microsoft Access virus

A97M.AccessiV.A was discovered in the beginning of 1998, and is the first virus to infect Microsoft® Access® macros.

Java viruses

Strange Brew, found by Symantec's Seeker™ web-spider technology, was the first known Java™ virus. Since its discovery, at least two more Java viruses have been developed. New scanning strategies are needed to scan Java files efficiently.

Office 2000 viruses

Microsoft has shipped a new suite of Microsoft Office utilities in 1999 that provides a new target for viruses as Office 97 did. Companies that use Norton AntiVirus will not need to update to a whole new product in order to get protection against Office 2000 viruses. Our standard virus definition updates, including NAVEX, already protect your enterprise.

WORLD HEADQUARTERS
10201 Torre Avenue
Cupertino, CA 95014 USA
1 (800) 441-7234
1 (541) 334-6054

World Wide Web Site
Corporate:
http://www.symantec.com

Australia (Sydney): +61 3 9850 1000
Australia (Melbourne): +61 3 9823 6204
Brazil: +55 11 530 8869
Canada: 1(416) 441-3676
France: +33 1 41 38 5700
Germany: +49 n2102 7453 0
Hong Kong: +852 2528 6206
Italy: +39 2 69 5521
Ireland: +353 1 820 5060
Japan: +81 3 3476 1156
Korea: +82 2 3452 1600
Malaysia: +60 3 7567662
Mexico: +52 5 661 7978
New Zealand: +64 9 309 5620
Netherlands: +31 71 535 3111
Russia: +7095 238 3822
Singapore: +65 239 2000
Sweden: +46 8 457 3400
Switzerland: +41 71 626 20 40
South Africa: +27 11 804 4670
Taiwan: +886 2 729 9506
UK: +44 1628 592 222

SYMANTEC.™

4/99 07-71-00992