HURWITZ
& ASSOCIATES

The Extraordinary Failure of Anti-Virus Technology

Whitelisting Succeeds Where AV Has Failed

Robin Bloor, Partner

A HURWITZ WHITE PAPER

This white paper was originally written for Securewave in February 2007. It has been updated to reflect the merger in July 2007, between PatchLink Corporation and SecureWave S. A., which resulted in the formation of Lumension Security, Inc.

□ 233 Needham Street □ Newton MA 02464 □ Tel: 617 454 1030 □
www.hurwitz.com

The Failure of Anti-Virus Technology - A Summary

Anti-virus technology fails to prevent computers from virus infections. And because it fails, it inadvertently assists many security woes that plague the computer population.

Because viruses spread, hackers find it easier to compromise business computers, identity theft is better enabled and computer fraud is easier to perpetrate. Virus-infected computers become an exploitable resource for hackers, who assemble and control networks of thousands of "zombie" computers, which are used to mount "denial of service" attacks, distribute huge volumes of spam and distribute more viruses.

Statistics that demonstrate the ineffectiveness of AV technology are regularly produced:

- A recent Yankee Group report stated that 99% of companies had AV technology installed, yet 62% of companies suffered successful virus attacks.
- According to AusCERT, Australia's Computer Emergency Response Team, the two most popular and deployed AV products fail to prevent 80% of new viruses.

Virus writers test their new viruses against the more popular AV products before releasing them. And that is why AV technology is so ineffective. AV products have been trying for nearly 20 years to deal with the virus threat and have made very little progress. The AV technology vendors have simply taken the wrong approach. They have built "burglar alarms" that will only alert you if a known burglar tries to enter the house. The real solution is to have a "burglar alarm" that sounds when anyone you don't know tries to enter the house.

Fortunately, whitelisting technology has emerged in recent years. Whitelisting technology takes a different approach to the malware problem, recording all valid programs and preventing others from executing. Because of this approach, it can be and is used to prevent other ills, such as spyware, adware, unlicensed software or any other kind of unauthorized software. Whitelisting can be applied to device control as well, which prevents the attaching of unauthorized devices to corporate PCs and laptops.

This paper will discuss:

- Viruses and AV technology, providing a history of virus evolution and the failure of AV technology
- Five common types of security breaches, indicating how whitelisting technology prevents the activity
- Lumension's whitelisting technology and how it works
- A case study of a bank that replaced AV technology with whitelisting technology

Anti-Virus: The Underreported Failure

As the chronology provided here shows, AV technology has persistently failed to cure the primary security woes of both business and home computer users over a period of nearly two decades.

The Birth of the Computer Virus: 1982

The possibility of a computer virus – a program that could reproduce itself – was first suggested in 1949 by John von Neumann; however, it wasn't until 1982 that the first such program, called Elk Cloner, was written.

The possibility of a computer virus - a program that could reproduce itself - was first suggested in 1949 by John von Neumann; however, it wasn't until 1982 that the first such program, called Elk Cloner, was written.

Academia and Viruses: 1984

From 1984 onwards, Dr. Fred Cohen produced several academic papers that explored and defined the concept of a computer virus. Cohen defined a computer virus as "a program that can 'infect' other programs by modifying them to include a possibly evolved version of itself". The word "virus" itself was invented by Cohen's faculty advisor, Leonard Adleman, who created a virus theorem, proving mathematically that it is not possible to determine for sure whether a virus is or is not present on a computer.

First PC Virus: 1986

In 1986, first PC virus called Brain, was created by two brothers in Pakistan in an attempt to deter the pirating of a software product they had written. This virus "escaped into the wild" and spread across the globe, turning up on PCs in various US universities. The Brain's source code was subsequently used as a basis to build other viruses.

The Dawn of AV Technology: 1987

From 1986 onwards, new viruses began to appear every few months, and consequently software developers created anti-virus programs in an attempt to deal with the problem. The first such product, called Vaccine, was written in 1987 and others quickly followed.

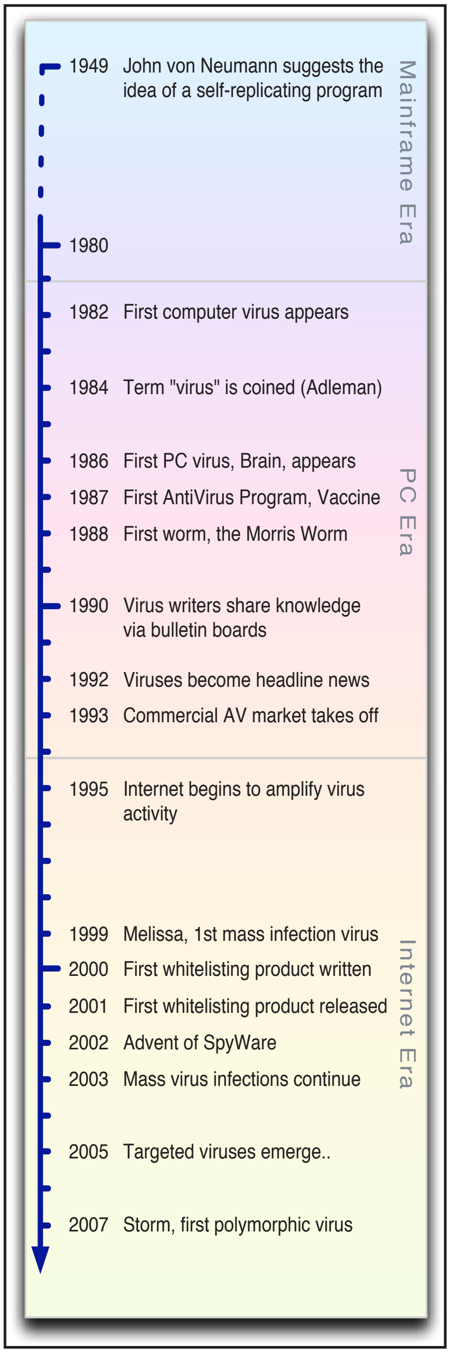
1949 John von Neumann suggests the idea of a self-replicating program
1980
Mainframe Era
1982 First computer virus appears
1984 Term "virus" is coined (Adleman)
1986 First PC virus, Brain, appears
1987 First AntiVirus Program, Vaccine
1988 First worm, the Morris Worm
1990 Virus writers share knowledge via bulletin boards
1992 Viruses become headline news
1993 Commercial AV market takes off
PC Era
1995 Internet begins to amplify virus activity
1999 Melissa, 1st mass infection virus
2000 First whitelisting product written
2001 First whitelisting product released
2002 Advent of SpyWare
2003 Mass virus infections continue
2005 Targeted viruses emerge..
2007 Storm, first polymorphic virus
Internet Era

Figure 1: The Virus Timeline

In 1989 there were about 30 known viruses, a mere handful compared with today's figures of more than 200,000.

Here Come the Worms: 1988

The Morris worm, written by Robert Morris, a student at Cornell University, was the first worm, which was released onto the Internet from a computer in MIT in November 1988. Until then viruses had been passed from one computer to another by virus files on a floppy disk. Worms introduced a new, more direct and automatic means of infection, copying themselves from one machine to another over a network. The Morris worm was originally intended to count the number of computers connected to the Internet, however it ended up bringing many of the computers it infected to a grinding halt.

The Proliferation of Virus Authors: 1990

In 1989 there were about 30 known viruses, a mere handful compared with today's figures of more than 200,000. This changed in 1990 with the advent of virus exchange bulletin boards, which had large numbers of viruses available for download along with the source code. In order to use the bulletin board, you had to upload a virus too, ensuring that the population of viruses grew more quickly.

Viruses in the News: 1992

Virus outbreaks became big news in 1992 because of the hysteria that bubbled up around the Michelangelo virus. This virus was a “sleeper” that was timed to activate on all infected PCs on March 6th (Michelangelo’s birthday). By then virus infection was commonplace and the prospect of a general meltdown of PCs in offices across the world engaged the minds of the public. It never actually happened, because the virus was less infectious than some commentators had suggested.

The Quickening: 1991-1993

By 1991, the proliferation of virus authors had begun to have its impact and viruses became increasingly sophisticated with new ways of working and concealing activities. Virus kits appeared to aid virus authors. Polymorphic viruses appeared – viruses that cannot be recognized by their signature because the virus file mutates as they proliferate. In 1993, a German virus appeared which disabled the Microsoft anti-virus product which ran on MS-DOS 6.0. From this point onwards, the AV industry bloomed trying to understand, recognize and neutralize new viruses after they appeared.

Polymorphic viruses appeared – viruses that cannot be recognized by their signature because the virus file mutates as they proliferate.

Commercial AV Vendors Prosper: 1993-2006

The commercial AV companies prospered both because the number of new viruses emerging was growing at a remarkable rate, and because viruses had become news. By 1992, most regular PC users had read the virus stories and many had experienced a virus infection. As AV vendors never actually solved the virus problem, virus infections continued to occur. This continually demonstrated the need for protection, boosting the sale of AV products because they were the “only solution available.”

The Internet Amplifier: 1995-2006

The Internet connected all the world’s computers together, providing a far more fertile environment for virus infection. In 1995 macro viruses emerged using Word and Excel files to spread themselves. Email viruses also became prevalent. An important virus-spreading technique was introduced by the I Love You virus, in 2000. As soon as an email carrying the virus with the “I Love You” title was opened, a virus executed, demonstrating the power of social engineering. If an email had the right title and came from a known source then a good proportion of recipients would open it.

Viruses began to include Trojan payloads that allowed hackers to take control of infected PCs. Viruses appeared (for example, CodeRed and SQL Slammer) that were based on a specific software vulnerability. Such viruses could achieve mass infection in hours or, in the case of SQL Slammer, in minutes. Remarkably, it took a mere 10 minutes for SQL Slammer to infect 90 percent of the computers on the Internet that had the vulnerability it exploited - long before any AV vendors were even aware of its existence.

The AdWare Epidemic: 2002

In 2002 a new phenomenon, AdWare and SpyWare, emerged. Such software was introduced by fooling the user into downloading the software and allowing it to run. Once installed, the user would be plagued with pop-up advertisements. AV technology was not able to stop this, so AV vendors created and sold "new" anti-spyware products.

From Hobby To Business: 2004-2007

By 2004, the age of the amateur virus writers was over and viruses had become a highly useful tool in the hands of the cyber-criminal, who herded together huge networks in order to distribute spam, carry out denial of service attacks and spread viruses. By 2005, virus writers were targeting viruses at specific organizations, in order to carry out some specific criminal act, such as data theft or fraud. In 2007 the first targeted polymorphic virus, the Storm Worm, appeared - specifically designed to assemble networks of zombie PCs. It had become clear that the hobbyist hackers had been superseded by professional criminals.

The Failure of AV Technology

The failure of AV technology becomes apparent if you construct a timeline of the evolution of viruses. AV technology never became a prosperous business until around 1993. By then the population of PCs was growing at a dramatic rate, viruses spread by floppy disk had become common and viruses were in the news from time to time.

If AV technology had been effective, then the problem of viruses and other associated malware would have gradually faded away. But quite the opposite happened. The Internet provided an exceptional breeding ground for viruses and helped virus authors from across the world to share their accumulated knowledge. The virus problem escalated.

If AV technology had been effective, then the problem of viruses and other associated malware would have gradually faded away. But quite the opposite happened.

By 1999 the worst possible outcome was occurring. Mass virus infections were happening regularly and the costs to businesses and computer users were extreme. The costs of mass viruses (as calculated by Computer Economics, www.computereconomics.com) tell a sorry story.

1999 - Melissa	($1.5 bn)
2000 - I Love You	($8.75 bn)
2001 - Code Red et al	($5.5 bn)
2002 - Klez et al	($1.65 bn)
2003 - Slammer et al	($4 bn)
2004 - MyDoom	($4 bn)

Incidentally, these are not the costs to businesses for all the virus infections in that year, just the cost of the major new viruses that emerged in that year.

Year after year, new viruses were introduced and proliferated causing billions of dollars of damage. AV technology was not even coming close to fixing the problem. Some recent security reports from 2006 tell the story:

- The Information Security Breaches 2006 survey, conducted by the UK Department of Trade and Industry (DTI) in conjunction with PriceWaterhouseCoopers, stated that “in the past two years, virus infections have been the cause of 50 per cent of businesses’ worst security incidents.” The report goes on to say that about two-fifths of these incidents had a serious impact on the affected business.
- In a paper released by Microsoft’s Anti-malware Team, in June 2006, Microsoft claimed that of the 5.7 million computers it had run its anti-malware software on, 62 percent of them had been infected with backdoor Trojan software.

The high rate of malware infection in commercial organizations around the world can only be attributed to the fact that AV software doesn’t do the job for which it is designed.

Why Doesn’t Anti-Virus Software Work?

The high rate of malware infection in commercial organizations around the world can only be attributed to the fact that AV software doesn’t do the job for which it is designed. The reason why it is ineffective is simple; if it cannot recognize software as malware, it lets it run.

AV technology employs a variety of techniques in order to try to detect malware, but whether it’s the relatively simple technique of using a “digital signature" or the more complex techniques of trying to recognize code sequences or known virus behavior traits, the outcome remains consistent. New malware tends to get through. AV technology is equivalent to having a burglar alarm that only works when a known burglar attempts to enter your house. If a burglar is not recognized by the alarm and doesn't behave suspiciously, then the alarm stays silent and the burglar gains access.

There is a solution to this problem: Don't try to recognize the malware; just identify the software that you want to be able to run and either prevent anything else from running, or let software that is new run in a quarantined environment, until its validity can be verified. This is the security approach that was first formulated by Lumension in 2000, as it became clear that AV technology was fundamentally flawed.

There is a solution to this problem: Don't try to recognize the malware; just identify the software that you want to be able to run...

The Whitelist Strategy: Five Use Cases

The whitelist approach fixes the virus problem, and provides a variety of other security benefits. Its impact is illustrated with the following five "use cases," each of which provides a different IT security threat and explains how whitelisting provides a defense.

Use Case 1: The Virus Writer/Distributor

The ultimate goal of a virus writer varies quite considerably. Early viruses were written for research purposes, but nowadays, such virus "innovators" may just post the source code of a new virus to a web site and let someone else compile and distribute it.

Viruses have been released as irresponsible pranks, as political messages that flash up on the screen when the virus runs, as outright vandalism, to attack specific products, to generally infect PCs with Trojans, as demonstrations of virus craftsmanship and as direct attempts to steal data. There have even been some examples of viruses that tried to fix known problems or add improvements to programs.

The modus operandi of the virus writer is as follows:

1. Design the virus, deciding on how it will spread and what it will do to the host machine that it infects.

2. Write the virus, patching in source code from the virus libraries that exist.
3. Test the virus on several PCs each of which is running a popular AV product. Tweak the virus until it evades detection by some or all of the AV products.
4. Release the virus into the wild, using an Internet cafe and anonymous accounts.

A virus prepared in this fashion will spread, guaranteeing a week or two of success, if not more.

How can this be prevented?

Infection will not occur on any computers running whitelist technology and it may be stopped by some of the AV products that the virus wasn't tested against. Eventually, the AV products that it was designed to circumvent will block the virus and in time it will gradually become less infectious - although it may continue to exist and infect new computers for years. If all PCs ran whitelisting technology, the virus would not be able to execute and therefore would not spread.

Infection will not occur on any computers running whitelist technology and it may be stopped by some of the AV products that the virus wasn't tested against.

Use Case 2: Your Global Neighborhood Hacker

Since 2002 many of the viruses released into the wild have included code that opened up "back door" access into an infected computer. This explains how, in 2005, Dutch cyber criminals managed to assemble a network of 1.5 million "robot" PCs. The ineffectiveness of AV technology in combination with viruses that planted Trojans on infected PCs made it possible.

There are a multitude of things that a hacker can do with a network of PCs controlled via backdoor Trojans. The hacker can set up email engines to distribute both Spam and phishing attacks and viruses, or mount Denial of Service attacks on web sites to put them out of action or steal data that identifies an individual. If a hacker can assemble a network of robot PCs, it is possible to mount any of these activities for almost no cost.

In order to gain access to and control a PC, the hacker needs a way in:

a) Find PCs infected by viruses that have planted a backdoor Trojan, by running an automated scan on the internet to find such PCs. Once found, the door is open.

b) Use known security weaknesses to gain access. Security weaknesses are announced quite regularly and the hacker only needs to keep abreast of this.

c) Use social engineering tricks to persuade users to load software that will open up a back door into a PC. This time consuming, manual method is rarely used when assembling a network of robot PCs, but is used when there is a specific target.

Once a hacker has PC access, they will load software onto it.

How can the hacker be discouraged?

AV technology does very little to discourage the hacker, while whitelisting software is almost impossible to subvert. Even if a hacker does manage to gain access, for example, through social engineering, any attempt to load and execute any other software will reveal the hacker's presence.

Use Case 3: The Focused Hacker

Since 2005, there have been few mass infection viruses like those that had caused so much financial damage in previous years. However there were a much greater number of new, targeted viruses being released and the financial damage for impacted organizations was and continues to be high. According to Network Associates, between September 2004 and June 2006, as many new viruses appeared as had done so in the previous 18 years.

A new trend was emerging. Viruses were being released that were specifically targeting individual companies or organizations.

A new trend was emerging. Viruses were being released that were specifically targeting individual companies or organizations. Such viruses are, incidentally, just one weapon in the armory of the "focused hacker" who has a specific corporate target in mind. In the most sophisticated attack, a "focused hacker" may unleash a whole series of security attacks on a target. It could include a denial of service attack, combined with automated hack attempts on known security weaknesses plus a mass email virus attack and additionally a few emails with macro attachments. Highly sophisticated attacks of this kind are aimed at distracting security staff with a whole series of ineffective threats that will allow one simple undetected attack to get through.

The use of a targeted virus as the specific attack vehicle stems from the fact that the hacker can probably find out which AV software is in operation in the target company, and write a virus to get around it. The hacker then only needs to introduce the virus - a spoofed email from a trusted person is a technique that is commonly used.

The motive may be fraud, attempting to steal financial information or the hacker may be hired by a competitor. If the hacker is successful, the corporate cost will be very high.

How can the focused hacker be stopped?

Whitelisting technology will clearly prevent focused virus attacks and will prevent the attacker from ever loading any new software onto the computer network to achieve whatever is planned. The whitelisting shield is likely to encourage the hacker to choose other companies as targets, because it provides such a rigorous defense. The only strategy that could potentially be successful against such defenses is to try social engineering techniques on the security staff who authorize the addition of new software.

Use Case 4: The Data Thief

The average cost of a data loss, according to a recent CSI/FBI survey is $167,713 although the cost can reach many millions in high profile situations. Data loss is the third most expensive type of security breach that a business can experience, after virus infection and hacker intrusion. The CSI/FBI survey estimated that 75 percent of US fortune 1000 companies suffered data theft in 2005.

From the hacker's perspective, getting access to valuable company information is more difficult than skipping around AV software. For that reason, most data thefts are "inside jobs." The insider knows where the data is and has some idea of how to get at it.

...most data thefts are "inside jobs." The insider knows where the data is and has some idea of how to get at it.

Currently the most effective tool for the data thief is the memory stick. It's small, easy to plug in and nowadays memory stick capacities are measured in gigabytes – large enough to store whole databases. PDA's that have file transfer ability to a desktop PC can also be useful. Passing stolen data files of any size out of the company through the corporate network is riskier as the transaction may well be noticed.

In a recent survey of CIOs/IT Directors, 60 percent of those surveyed admitted that they did not monitor device usage. Yet, in most cases, the data thief is already working for the organization and steals data when the opportunity presents itself. External attacks or planned recruitment of insiders are less common.

How can data theft be stopped?

The whitelisting of software is unlikely to stop data copying as the software used to copy data is quite valid. However, there is an equivalent process to whitelisting of software described as device control. Device control software keeps a list of which devices are allowed to be used on a specific computer and by whom. It can thus block or allow the use of any device that can be connected to a computer. Such software can also provide a "shadowing capability" for allowed devices that records which files and what specific data were copied, when and how. Limitations such as file types or size limits provide further controls and reduce the risk of data leakage, while enabling legitimate use of these devices. One of the benefits of implementing such controls is that it combats the tendency of clever users to find unsafe ways to get things done. Data theft can happen through carelessness as well as through direct intent. Implementing device control has the beneficial effect of making computer users more aware of the dangers and thus less likely to be careless with corporate data.

Use Case 5: The Rogue Employee

The FBI gives the following figures as a guide to the level of people's honesty: 5% of people are completely honest, 15% are entirely dishonest, and the remaining 80% form a spectrum of relative honesty between these "honest" and "dishonest" poles.

Even if you have remarkably effective recruitment capabilities, you have staff who, although they might not be entirely dishonest, will behave irresponsibly. A recent illustration of this was when an IT Security officer at a US company bought a handful of memory sticks, loaded some software on them and then scattered them around the company's parking lot. Several employees found the memory sticks, plugged them into their PCs or laptops and ran the software "just to see what it was."

...an IT Security officer at a US company bought a handful of memory sticks, loaded some software on them and then scattered them around the company's parking lot.

Many organizations trust their staff, but unless their use of technology is effectively policed, some employees will misbehave. Staff misbehavior often includes the following:

- Loading unapproved software onto PCs and laptops. Sometimes the culprit is actually the teenage child of the employee rather than the employee themselves.
- Loading peer-to-peer file-sharing software on company PCs and downloading music or other files. Aside from possibly being illegal, it can saturate the network bandwidth of an organization and thus prevent important applications from running properly.
- Loading unlicensed software onto PCs and laptops. It is estimated that about 27% of all software loaded on company PCs and laptops is unlicensed and most of that is loaded by employees. Fines for a company discovered to be running unlicensed software average out at $91,000. Staff can, without actually realizing it, put a company at risk.

How can the problem be contained?

All of these issues are addressed by whitelisting software that prevents the execution of any software that has not been approved. Whitelisting software prevents any software that is not explicitly authorized. The addition of a capability that prevents the attachment of new devices to a PC, as described in the previous example, further reinforces the protection of the corporate network.

__The addition of a capability that prevents the attachment of new devices to a PC ... further reinforces the protection of the corporate network.__

Without some connection capability, employees are less inclined to think they have a right to load software. Where staff are delegated the right to load software, whitelisting software keeps a log of any application that attempts to execute so any new software is immediately reported when use is attempted and can be quickly removed if there are, for example, insufficient licenses.

Sanctuary: Application Control and Device Control

Lumension's Sanctuary technology is the leading whitelisting product, protecting more than 2 million computers, providing both application and device control. Sanctuary provides control of both the software that runs on a computer and the devices that can be attached to a computer.

Sanctuary uses a fingerprinting technique to uniquely identify software so it is able to identify any piece of software without error.

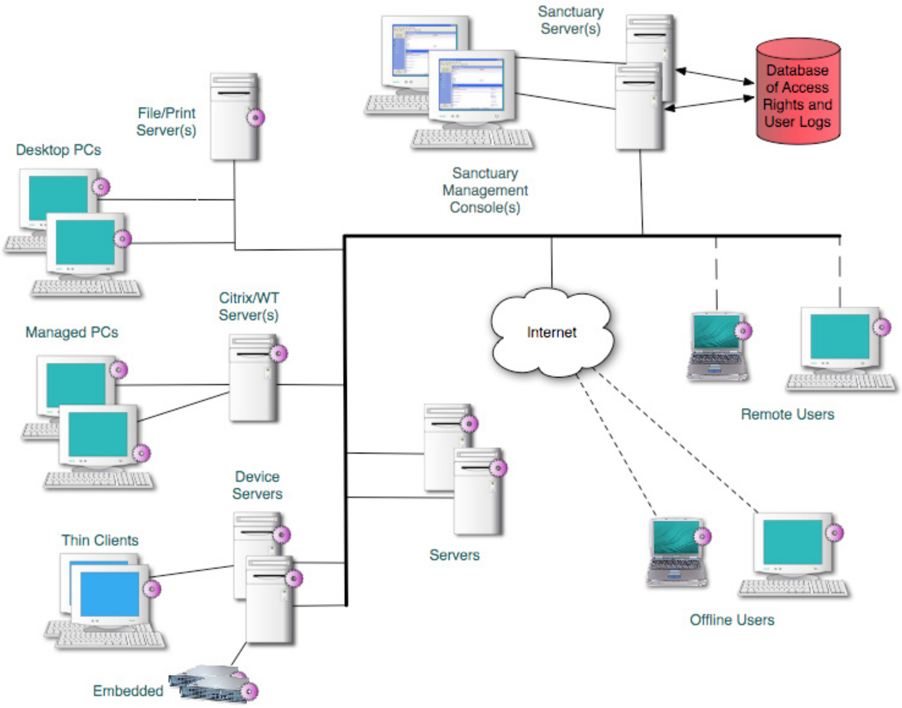

Figure 2: The Sanctuary Architecture

Figure 2 illustrates how Sanctuary delivers application and device control. The central components of the architecture are the Sanctuary database of access rights, the server(s) which enable the Sanctuary agents to access the database when needed and the Management Console.

Additionally Sanctuary places a client agent (illustrated as small cogs) on each device that is protected. This agent runs within the kernel of the operating system so that it has direct access to and knowledge of operating system activity and minimal resource utilization. There may be more than one console and server if there are a large number of devices in the network. Sanctuary scales by adding extra servers and consoles.

How Sanctuary Works

When a user logs on to any computer, this client agent sends basic identification information to the Sanctuary server (machine ID, user ID, Domain ID, Group ID, policy version, etc.) using a purpose-built secure protocol. The server checks to see if a more up-to-date version of the policy is available with access rights for both application access and for device access, and securely passes any updates back to the client computer. (Application Control and Device Control are separate options, which are managed together but can be implemented separately if required).

Once this interaction with the server occurs, the control of the computer is managed locally by the client agent referring to the downloaded access rights information. Policy changes added to the central database of access rights are downloaded at next login, at scheduled times, on demand by the user or as pushed by the administrator.

With this architecture, it is possible to disconnect the computer (as would happen with a laptop) and Sanctuary still protects as if it were connected. A user can be locked down completely so that it is impossible to run any new software, or the user can be trusted to run new software. However, any new software is prevented from executing anywhere else in the network, until it is approved and added to the access rights. Sanctuary uses a fingerprinting technique to uniquely identify software so it is able to identify any piece of software without error. Sanctuary keeps a log of all software that is denied and allowed to run.

There are a variety of ways that a program can execute on a computer; directly when run, as a plug-in to another application, as an application run from a web site, as a macro attached to a file and so on. Ultimately though there is only one situation; some executable code is requested to run either by a computer user or by some piece of software. Sanctuary simply intercepts the executable code as it attempts to run, authenticates the file, and either blocks or allows the program to run.

Sanctuary simply intercepts the executable code as it attempts to run, authenticates the file, and either blocks or allows the program to run.

Similarly, computers have a variety of ports that are connection points of one sort or another that are specifically designed to allow other hardware devices to connect to the computer and work with it. With the evolution of the PC, a large variety of possible computer connection ports now exist, including; serial (COM), printer (LPT), card connection points PCMCIA, infrared connection (IrDA), USB, FIREWIRE and Bluetooth. Sanctuary only needs to intercept the computer at the point that it tries to connect to the variety of devices that can connect to these ports and again authenticate the device and either allow or deny access. In the case of allowed devices, Sanctuary can provide further controls and policy enforcement mechanisms such as copy size limits, file type filtering, read/write permissions, data encryption enforcement and more.

Sanctuary - At A Texas Bank

The First National Bank of Bosque County is a full-service consumer bank with four branches in the Valley Mills area of Texas. Like many organizations, the bank had deployed anti-virus and anti-spyware software but had nevertheless suffered problems. So in March 2006, before its Symantec licenses were about to expire, Brent Rickels, the bank's VP in charge of technology, re-evaluated its security infrastructure.

"We were having our fair share of spyware problems despite deploying anti-spyware software. It was obvious that because anti-virus and anti-spyware solutions are reactive by definition, they did not offer the complete malware protection we were after," said Rickels.

Valley Mills is a developing area and the bank only recently acquired a dedicated internet connection, something that Rickels regarded as a double-edged sword that would improve capabilities but increase security problems. The prospect of increased risk combined with the failure of the AV/AS products from Symantec led Rickels to examine and then purchase Sanctuary Application Control from Lumension.

"Without a comprehensive enforcement solution, you still have to depend on users to manage their own computers and inevitably, you will have some employees either purposely or unintentionally create a problem," said Rickels. "We looked at a variety of solutions from many different vendors, but most were reactionary and others only isolated and quarantined malicious executables. Sanctuary actually prevents them from running, and it is far easier to manage."

"Without a comprehensive enforcement solution, you still have to depend on users to manage their own computers and inevitably, you will have some employees either purposely or unintentionally create a problem..."

The Customer Experience

With assistance from Lumension engineers, Rickels scanned the bank's computers and built the application whitelist in a single day. Installing the client agent took about three minutes per machine, all done from the central management console.

Subsequently the bank implemented a policy of no games. Attempts to run

Windows Solitaire or Minesweeper prompted a pop-up message explaining that those applications were not allowed. Two other application types that Rickels elected to remove from the whitelist were peer-to-peer and instant messaging (IM) programs, which Rickels regarded as presenting unnecessary security risks and offering little benefit to the bank.

Prior to Sanctuary, Rickels spent hours every week checking each machine for viruses and making sure the anti-virus was set up correctly and properly updated. Since deploying Sanctuary, the First National Bank of Bosque County has not experienced a single malware incident.

"I spend about an hour per month updating Sanctuary," said Rickels. "I am able to deploy the patches at my own pace because I know that Sanctuary will prevent any of the vulnerabilities from being exploited. The administrative overhead required to manage Sanctuary is minimal. Sanctuary solves all the problems. It is cheaper than anti-virus so it has paid for itself already."

Into the Future

Symantec chairman and CEO John Thompson declared in October 2006 that the problem of "worms and viruses is solved." Unfortunately, he failed to mention that Symantec isn't the company that had solved it.
The problem is indeed solved – by the handful of companies, led by Lumension, that deliver an effective whitelisting-based solution. However, the global problem of viruses will not be solved until the adoption of whitelisting technology quickens. Right now less than one percent of computers are protected by whitelisting technology. Most of the rest are vulnerable to virus infection and consequently capable of assisting in virus proliferation. The ease with which viruses spread will not be diminished until a far greater number of computers have effective protection.

Right now less than one percent of computers are protected by whitelisting technology. Most of the rest are vulnerable to virus infection and consequently capable of assisting in virus proliferation.

It is estimated that somewhere in the region of eight percent of home computers are infected by Trojans and available to be corralled into the zombie networks that cyber criminals assemble. These networks are themselves a menace and it is, for the most part, viruses that have spread the Trojan software and laid the foundations required to build such networks. This curse will not be lifted until whitelisting technology proliferates and clips the wings of the cyber-criminals.

About Lumension Security

Lumension Security, a company formed by the combination of PatchLink® Corporation and SecureWave® S.A., is a global security management company, providing unified protection and control of enterprise endpoints for more than 5,100 customers and 14 million nodes worldwide. Leveraging its proven Positive Security Model, Lumension enables organizations to effectively manage risk at the endpoint by delivering best-of-breed, policy-based solutions that simplify the security management lifecycle. This includes automated asset discovery, vulnerability assessment, remediation and validation; application and device control; extensive policy compliance reporting; and integration with leading network access control solutions. Headquartered in Scottsdale, Arizona, Lumension has offices worldwide, including Virginia, Florida, Luxembourg, the United Kingdom, Spain, Australia, Hong Kong and Singapore. More information can be found at www.lumension.com.

About Hurwitz & Associates

Hurwitz & Associates is a consulting, research and analyst firm that focuses on the customer benefits derived when advanced and emerging software technologies are implemented to solve pragmatic business problems. The firm's research concentrates on understanding the business value of software technologies, such as Service-Oriented Architecture and Web services, and how they are successfully implemented within highly distributed computing environments. Additional information on Hurwitz & Associates can be found at www.hurwitz.com.