

Anti-Virus Is Dead

The Advent of the Graylist Approach to Computer Protection

Robin Bloor, Partner
Hurwitz & Associates





© Copyright 2006, Hurwitz & Associates

All rights reserved. No part of this publication may be reproduced or stored in a retrieval system or transmitted in any form or by any means, without the prior written permission of the copyright holder. Hurwitz & Associates is the sole copyright owner of this publication.

■ 330 Bear Hill Road, Suite 230 ■ Waltham, MA 02451 ■ Tel: 781-890-7185 ■
www.hurwitz.com

Executive Summary

In the past 20 years, Anti-Virus technology has grown to become an industry in its own right with revenues just below \$4 billion. Nevertheless the viruses that AV software is supposed to protect us against still proliferate and organizations still have to bear the high costs of virus attacks.

For those who do not analyze software technology, it must look as though there is an unending war being waged between the malicious virus writers and the noble AV technology companies. The evil viruses attack and the noble AV companies step up to do battle. There are casualties, but ultimately the latest virus threat is stopped and life continues until the next assault. This enthralling view of the software world is completely wrong.

The reality is that viruses, worms, trojans, and other forms of malware persist only because of AV technology, which became the main defense against them. Sadly, it is a terribly flawed defense. From the outset, the AV software vendors took the wrong approach to stopping malware. This truth became clear in the past two years as new Application Control/Software Authentication products emerged that took a far more effective approach to blocking rogue software.

We cannot refer to these new products as Anti-Virus products because they are far more powerful than that. They stop a wide variety of software that organizations do not want running in their networks; viruses, worms, trojans, spyware, adware, hacker tools, peer-to-peer file sharing software, games, unlicensed software, stolen software and even old versions of valid software. Instead of trying to recognize rogue software, these products focus on authenticating valid software (from a whitelist), blocking everything that is invalid (from a blacklist) and running any software that is new and unknown (the graylist) in a controlled manner until it has been authenticated or rejected. By casting such a net, these products catch many kinds of fish – a far wider variety than AV software could ever hope to catch.

In this paper, we analyze the failure of AV technology in depth. However, for the sake of this summary a single fact will suffice:

According to AusCERT, Australia's Computer Emergency Response Team, the top-selling Anti-Virus solutions let in 80 percent of all new malicious code.

From the outset, the AV software vendors took the wrong approach to stopping malware.



Anti-Virus Is Dead

If you pay for AV software, then in all probability, that's what your money is buying: 20 percent protection from new threats. It's not much of an insurance policy is it?

In the paper, we also explain how Software Authentication products work, using Bit9 Parity, one such product, as an example. So on the one hand, the paper chronicles the failure of AV technology, and on the other, it provides an insight into the technology that will inevitably supersede it.

The advent of Software Authentication products means that the age of Anti-Virus software is coming to an end. Organizations that adopt Software Authentication technology simply have no use for Anti-Virus software.

To put it bluntly, Anti-Virus is dead.

Sunset on Anti-Virus Software

Anti-Virus (AV) software is in the process of dying. You may be surprised to read this. Indeed, it seems unlikely when you consider some of the facts, but it is true nevertheless.

AV software is not just a type of software product. It is big business. It is an industry in its own right. There are not just one or two AV companies, there are about 30, including giant companies like Symantec with annual revenues in the region of \$5 billion, as well as smaller ones that you may never have heard of, like Hauri (of South Korea) or G Data (of Germany).

The annual revenues of the AV industry are somewhere between \$3 and \$4 billion. That's about 50¢ each year for every person on the planet or about \$3 for every functioning PC. And to cap it off, the AV industry has been growing at the rate of about 11% in recent years. It doesn't sound unhealthy does it?

Why Is the AV Software Industry in Trouble?

Despite the fact that the AV software industry has managed to keep a lid on viruses for the longest time, it has become abundantly clear that AV software does not solve the problem it is supposed to solve. It is also incapable of solving other PC problems which it really ought to handle, such as the problem of spyware or adware.

Despite the fact that the AV software industry has managed to keep a lid on it for the longest time, it has become abundantly clear that AV software does not solve the problem it is supposed to solve.



Anti-Virus Is Dead

Strange as it may seem, the ineptness of AV software wouldn't be particularly damaging to the AV industry were it not for the fact that there is technology that reliably protects PCs and other computers against viruses, worms, trojans, adware, spyware, and other forms of malware.

I will make it clear. The AV industry is moving into retreat because, from the moment it began, it took the wrong approach to preventing malware. Consequently, while it flourished as an industry, malware flourished too. Malware wasn't stopped in its tracks by AV; it had a great time. The more malware there was, the more you needed AV. It was a virtue-less circle.

And it was inevitable that it would continue to turn until some companies emerged that took the right approach to handling this problem. That has happened. Indeed, there are now a handful of such companies, and each one of them has Anti-Virus Is Dead stamped on its forehead.

The Anatomy of Failure

You probably remember the early days of PC viruses. I guess all of us who were using PCs in that era got hit by a virus at some point. In those days, viruses were fairly simple – thin little executables that hid in the boot sector of a floppy disk. The first chance they got, they jumped onto a host PC and wrote copies of themselves to the boot sector of all the floppies that the PC wrote files to. That's how they came to be called viruses. They replicated themselves like biological viruses.

It may have been precisely because they were called viruses that the AV vendors took the wrong technical approach to preventing their spread. They figured that you only needed to recognize these viruses and stop them in their tracks – like the body's immune system does to foreign invaders.

It was exactly the wrong paradigm. The body's immune system has a good record against threats it has met before. But the immune system is hopelessly outgunned by pathogens, including viruses and bacteria it has no experience of. Witness what smallpox did to the Aztecs and the American Indians, or how the Black Death carved its merciless way through Europe in the Middle Ages.

AV software works in the same way. It is equally inept at dealing with new threats. It is the same. Exactly the same.

...the immune system is hopelessly outgunned by pathogens, including viruses and bacteria it has no experience of.



Anti-Virus Is Dead

Let The Record Show...

Let us imagine a different world; one where the computer virus problem emerged and a software technology that actually stopped viruses, worms, and other malware emerged a little time later. What would happen? The likely scenario is this:

Some users would try the technology and thus cure the problem. Viruses would continue to circulate, but only among unhealthy computers. Gradually more and more users would adopt the solution until eventually very few computers would be vulnerable. The virus authors would then give up and move on, because there would be no real point in creating malware. Game over.

The failure of AV technology is demonstrated by the fact that the game is not at all over.



Figure 1: The Estimated Business Costs of Mass Circulation Viruses

The failure of AV technology is demonstrated by the fact that the game is not at all over. This becomes clear if you examine the record of virus propagation since 1998. The costs of the major viruses of those years are illustrated in Figure 1 using estimates made by Computer Economics (www.computereconomics.com). These cost estimates cover only the organizational use of PCs, thus they serve as a rough index of the extent of corporate infection.



Anti-Virus Is Dead

The first widespread virus was the Morris worm, which came to a desktop-near-you in 1998 and infected about 10 percent of computers connected to the Internet. That was followed in 1999 by the Melissa virus, which was estimated to have cost the world in the region of \$1.5 billion. Then came the I Love You virus, in 2000, at an estimated cost of \$8.75 billion. For the major viruses of 2001, the estimated costs were; Sircam (cost \$1.25 billion), Code Red (cost \$2.75 billion) and Nimda (cost \$1.5 billion).

It may have seemed as though the situation improved in 2002, with Klez (only \$750 million), BugBear (\$500 million) and BadTrans (\$400 million). But 2003 brought us the Slammer Worm (\$1.5 billion) and SoBig.F (\$2.5 billion). And then 2004 ushered in MyDoom, at an estimated cost of \$4 billion.

By 2004 everyone everywhere knew about viruses and organizations were well aware of the costs of dealing with virus infections. In fact, by 2003, 99 percent of organizations had AV software (according to the 2003 CSI FBI Computer Crime and Security Survey). The figures from the 2004 survey are the same. In fact, AV technology was and is deployed more than any other type of security software. The problem is that it doesn't work.

Anti-Virus Software Doesn't Work

AV-Test.org is a project of the Business-Information-Workgroup at the Institute of Technical and Business Information Systems at the Otto-von-Guericke University Magdeburg (Germany) in cooperation with AV-Test GmbH. The project regularly tests the effectiveness of AV software. AV-Test carried out a trial (reported by Datamation in 2004 – go to http://itmanagement.earthweb.com/columns/executive_tech/article.php/3316511 for further details) that involved monitoring the responses of 23 AV companies to new viruses over a 3-day period. AV-Test measured the time it took for each AV product to post an AV signature following the appearance of a new virus or virus variant.

Its results showed a wide variance, with the slowest average responses coming from InoculateIT-VET (29 hrs 45min), Symantec (27hrs 10min), and McAfee (26hrs 11min) and the fastest average response coming from Kaspersky (6hrs 51min).

Incidentally, these timings **do not** show you how long you are at risk with each

...AV technology was and is deployed more than any other type of security software. The problem is that it doesn't work.



Anti-Virus Is Dead

product, because posting an AV signature doesn't cause the automatic update of your AV software. With a few AV products, automatic updates can occur after a matter of hours, but with most products, it's a matter of days and some are set for only once a week.

So what does this mean in practice?

That depends on each particular virus and how it spreads. The worst case is a virus like the SQL Slammer worm. This worm infected Windows computers running Microsoft SQL Server 2000 or MSDE 2000, infecting new computers by scanning networks to find computers with UDP port 1434 open and then using a buffer overflow to install itself. *It has been estimated that SQL Slammer infected 90 percent of all the computers that it could infect in the space of 10 minutes.*

For any virus that spreads at such a speed, AV software offers no protection whatsoever.

Why Anti-Virus Software Doesn't Work

According to AusCERT, Australia's Computer Emergency Response Team, the top-selling AV solutions let in 80 percent of all new malicious code. AusCERT is clearly being very kind in referring to them as "solutions." This is an extraordinary level of failure, which has two specific causes.

The first we have already described; it simply takes too long for AV software to provide a defense, so it is forever slamming the stable door after the horse has bolted.

The second is the simple fact is that the virus writers are also AV customers. If your goal in life is to infect computers with your handcrafted viruses for whatever nefarious reason, then you are surely going to test your product before you bring it to market. This is exactly what the more technically skilled virus writers do, and in doing this they guarantee themselves a high level of success.

The Misdiagnosis

From the outset, the IT industry failed to diagnose the problem of software viruses correctly. AV companies sprang into existence, all taking a similar flawed approach to blocking viruses and these companies prospered. When new fast-

For any virus that spreads at such a speed, AV software offers no protection whatsoever.



Anti-Virus Is Dead

moving viruses emerged, the AV vendors would be quoted extensively in the press. They would be the first to explain exactly what the impact of any new virus was and they would usually be able to declare that “they had a fix” that would protect their users. Reporters never asked how many of their customers were infected before the fix was installed nor did it matter, as AV was the only game in town.

The Advent of Spyware and Adware

This situation, so pleasant and profitable for the AV vendors, was disturbed a little by the emergence of spyware. As a term, “spyware” is a little confusing because it has been used to describe both malware placed on your computer by a hacker who is “spying” on your activity in the hope of stealing, for example, credit card details, and also to describe software placed on a computer without the “informed consent” of the user.

Here, we are writing about this second kind of spyware, which is usually accompanied by adware – software that plagues you with pop-up advertisements. Typically you become a victim to spyware and adware because you inadvertently agree to it. You visit a web site or load an application of some kind on your computer and in the process you sign some sort of consent or license agreement. Because very few people read such agreements, they do not realize that by doing so they have volunteered to allow sporadic advertising on their PC and the collection of information about the software they use and which web sites they visit.

Such users quickly discover that their PC is now broadcasting pop-ups advertisements to them and has slowed down to a fraction of its normal speed. In fact, when infected with spyware and adware, home PC owners often conclude that the PC is hopelessly broken and simply buy another one. That’s what almost 1 million US households did in 2004 and 2005, according to a Consumer Reports survey. Taking spyware and virus problems together, the survey estimated that the cost to the US consumer was \$3.9 billion per year.

Anti-Spyware Software

AV products were not able to protect you against “legitimate” spyware. The fact that the PC users agreed, however inadvertently, to have the software run means that AV software could not simply treat it like other forms of malware it

Taking spyware and virus problems together, the survey estimated that the cost to the US consumer was \$3.9 billion per year.



Anti-Virus Is Dead

recognized and delete it on sight. In theory, at least, the PC user has to choose to delete it. This reality created an interesting new commercial opportunity for the AV vendors. They could create products that were almost identical to their AV technology, but which focused on detecting spyware and adware. So that is what they did, employing the same flawed signature techniques that they had used against viruses.

Curiously, this led to a series of lawsuits with anti-spyware vendors; with Lavasoft, Zone Labs, and Symantec being sued by other companies claiming that their software was being “falsely classified” as adware or spyware.

Cybercrime Evolves

Whether the distributors of spyware and adware were behaving illegally was open to debate. It depended on how they were getting their software installed. Some were distributing it like a virus, while others simply fooled you into agreeing to accept it. So while some distributors were suing the anti-spyware vendors, others were having to defend themselves in the courts for trespassing on people’s PCs.

The nature of the malware author was changing. The early virus writers got their kicks from getting their virus into the news. After all, not everyone has the ability to write software that brings millions of PCs to a grinding halt, and very few people have actually done it. But by 2002, viruses started to include mechanisms that were clearly meant to aid criminal activities rather than make the headlines. Some aimed at turning PCs into email broadcast points for sending out spam and phishing emails, and some planted back-door access to the PC enabling hackers to gain access.

The digital delinquents were becoming outright digital criminals. Virus writers and hackers and spammers and phishers and fraudsters and identity thieves were becoming a single threat. And viruses, password crackers, spam mail, Trojans, spyware, adware, zombie PCs, and Internet bots were the tools they had at their disposal.

The nature of the virus itself was changing. This became apparent when McAfee announced in July 2006 that it had added 100,000 “threats” to its virus database since September 2004. In less than 2 years, McAfee encountered the same amount of malware that it had registered in the previous 18 years.

In less than 2 years, McAfee encountered the same amount of malware that it had registered in the previous 18 years.

Anti-Virus Is Dead

Mass virus infections were no longer in vogue. Cybercrooks had become more interested in specific targets for which tailor-made viruses could be written. Such viruses are more difficult for AV products to detect, because they can slide in beneath the AV radar.

The cybercreek who wants to plant a back-door entry into a specific company or onto a specific computer, may now use a custom virus to do it. He has a limited target and when he gains access he will probably remove the virus and any other software tools he loaded when he makes his silent exit, with your company's money in his bank account and its data in his pocket. The virus may never be identified by any AV vendor.

Looking At It Wrong

For 20 years, the IT industry has been "looking at it wrong." It was like that optical illusion that appears to be two faces in profile if you look at it one way, but it appears to be a vase if you look at it in a slightly different way. The word "virus" pulled a trick on us all and we looked at the problem in the wrong way. It was the wrong approach to focus on the bad software – it was necessary to focus on the good.



Figure 2: A Two-Way Illusion

The Graylist Approach

Forget viruses, worms, trojans, logic bombs, back doors, spyware, adware, and any other form of malware you've ever heard of. We can stop them all without giving them names, without constructing signatures to recognize them by and without finding out what nefarious things they will do if we let them loose. All we need to do is focus on the software that is valid and allow only that software to run.

It sounds almost too simple to be true, doesn't it?

"Are you telling me that for 20 years we've been suffering the slings and arrows of outrageous viruses and we could have stopped them, just like that?"

Yes, I am.

All we need to do is focus on the software that is valid and allow only that software to run.



Anti-Virus Is Dead

The Black, the White, and the Gray

To tell the truth, it is a little more complicated than “only let the good software run,” but not much. We’ll explain the idea using Bit9 Parity as our example technology. It is one of a handful of Software Authentication products we know of that takes the right approach.

Bit9 Parity maintains a whitelist, a blacklist and a graylist – classifying software as white, black or gray according to the lists. The whitelist is the list of software that you, as an organization, approve to run. These are the PC applications and package applications and the in-house applications that a company developed, which run the business. Because not everyone has the need to run every application, a whitelist (and a blacklist and a graylist) is maintained across the enterprise.

When any new program tries to run on a computer that has Bit9 Parity loaded, Bit9 Parity immediately checks to see if it is one of the programs on the whitelist. The check is done using a fingerprint that Bit9 creates for every program it has to classify. This unique fingerprint is created by calculating the cryptographic hash of the whole executable program.

Incidentally, it is not the same signature that AV software vendors create to try to identify viruses, as the AV vendor needs to try to recognize virus variants (viruses that are very similar but not the same as a given virus). Consequently AV signatures are usually more complex than the hashes used by Bit9.

Just as there is software that should be allowed to run on a given computer, there is also software that shouldn’t. In theory this list could be very long. You could, for example, have it include every piece of malware ever detected, but actually there is no point. This list only needs to include software that has been rejected **in action** by Bit9 or which is forbidden by the company as a matter of policy.

Not long ago we came across a situation that provides a good example of the type of software a company may choose to forbid. A company on the East Coast of the US noticed one day that its Internet connection was frequently saturated with traffic and the performance of applications using the connection was suffering. It took them quite a while to discover what the problem was. The problem was an employee, who has recently joined the company and who

Just as there is software that should be allowed to run on a given computer, there is also software that shouldn’t.



Anti-Virus Is Dead

happened to have a good friend who lived on the West Coast. Both of them had set up Webcams on their desks at work so that they could smile and wave at each other throughout the day. There was no malicious intention on the part of this employee. She simply never knew that her two-way Webcam broadcasts consumed 512k of bandwidth and put other applications under pressure.

There are quite a few applications that users will load if left to their own devices and which a company probably does not want to run. Some companies, for example, have suffered network traffic problems because of staff using peer-to-peer file sharing programs such as Kazaa, Morpheus, and Limewire. Some companies have banned the use of Skype because of the unpredictable traffic level it caused. The Bit9 blacklist can be used to enforce such corporate software policy and it is entirely discretionary.

So, when a program tries to run, Bit9 calculates its hash and checks to see if it is on the whitelist or the blacklist. If it is on the whitelist, it is allowed to proceed and if it is on the blacklist, it is stopped from running. But what if it is on neither list? In that case, it is both new and unknown, so it goes on the graylist.

A graylisted item is always reported to the central Bit9 Parity server and it remains on the graylist in a “pending state” until it has been officially approved and put on the whitelist or banned and put on the blacklist. However, it may be treated differently while it is on the graylist. Bit9 provides the following possibilities:

- 1) **Lockdown Mode.** With lockdown, all graylisted software is prevented from running. This kind of policy would be applied to PCs which, for example, are only ever used for specific known applications. With lockdown, the graylisted software will not run but its attempt to run will be reported.
- 2) **Block and Ask Mode.** A PC can be set to Block and Ask, in which case when any new and unknown software is noticed, the user is asked directly to approve it or block it.
- 3) **Monitor Mode.** In this mode, users are allowed to run graylisted software; however, IT will be able to track any new and unknown software installed on their PCs and can proactively ban any specific unwanted software.
- 4) **Hybrid Mode.** Finally, there is a hybrid mode that allows the IT

A graylisted item is always reported to the central Bit9 Parity server and it remains on the gray-list in a “pending state” until it has been officially approved and put on the whitelist or banned and put on the blacklist.



Anti-Virus Is Dead

administrator to specify different policies for laptops when they are connected or disconnected. For example, when connected to the corporate network, laptops may be in Lockdown Mode, where all unsanctioned software is blocked. On the road, hybrid-protected laptops may be put into Block and Ask mode where the user can approve software as needed.

Further, by integrating with desktop infrastructure and IT processes for rolling out new software and updates, Bit9 allows IT to control applications and enforce policies with minimal effort. Bit9 enables automatic whitelist maintenance via more granular control through trusted relationships with:

- Users approved to install software
- Publishers with digitally signed software
- Auto-updaters for specific applications
- Any software needing local or global approval

Via Parity's automated software approval and trust-based whitelisting, exceptions to corporate and security policies are minimized upfront without active IT involvement.

In addition, Bit9 maintains a large database, called ParityCenter, which contains the details and cryptographic hashes of millions of "trusted" programs and executable files that are known not to be malware. (Currently the knowledgebase contains over a billion records; you can use the knowledgebase for free at fileadvisor.bit9.com). Making use of this extensive resource, Bit9 enables you to configure a computer to allow such "trusted" software to run automatically. Management can then decide later whether it wants this software on the whitelist or the blacklist.

Promoting Responsible Behavior

The avalanche of infection that sweeps across a company during a virus attack may mask the irresponsible behavior of the user who caused it. The user responsible might not even know that they were the cause. Perhaps they visited a rogue web site or accepted a file from someone in a chat room or clicked on an email attachment or allowed their 14-year-old son to play with their laptop. "Hey, malware happens, never mind."

The avalanche of infection that sweeps across a company during a virus attack may mask the irresponsible behavior of the user who caused it.



Anti-Virus Is Dead

But when you turn the situation on its head, and make individuals responsible for the decision to allow software that is “new and unknown” to run or not, they begin to behave more responsibly. No matter how technically ignorant a user is, a user normally knows or can easily get to know what is and is not likely to be “bad.” Users know the context in which they are using their software.

Consider the situation where the user clicks on an email attachment. They thought, perhaps, that an MS Word file was going to be displayed, but they discover instead that a new program wants to run. If asked whether they want to run it, most users will realize what it probably is and say “no.” There are many circumstances where the user will know from his or her context that something not on the whitelist that tries to run is probably dangerous.

Software that suddenly tries to run when you open a newly received spreadsheet is suspicious, software which tries to run when you visit a new web site is suspicious, and software which suddenly tries to run when you weren’t doing anything at all is suspicious. And if they know that software which is trying to run has never been fingerprinted then they will need to have a good reason to run it – and indeed they may have; it’s their decision.

With a clever bit of “social engineering” it may be possible for a hacker to get a user to accept some malware. But with the graylist approach, the only PC that the user will infect is their own and their error will quickly become clear to them. They won’t so easily be fooled again.

Software and Hardware

Figure 3 on the following page illustrates how Bit9 Parity works from a technical perspective. The Bit9 Parity Server is the central hub of the configuration. When the server is installed, Bit9 Agents, which unlike AV are completely transparent to the end user, are also installed on all the computers that are going to be monitored. The Agents communicate all events (i.e. the firing up of all software) to the Bit9 Parity Server in real time, giving the server a complete picture of all graylisted processes throughout the whole installation. As these events are reported using standard protocols this information can also be passed directly to system management software or displayed (as shown in the diagram) on an Enterprise Management Console.

...when you turn the situation on its head, and make individuals responsible for the decision to allow software that is “new and unknown” to run or not, they begin to behave more responsibly.

Anti-Virus Is Dead

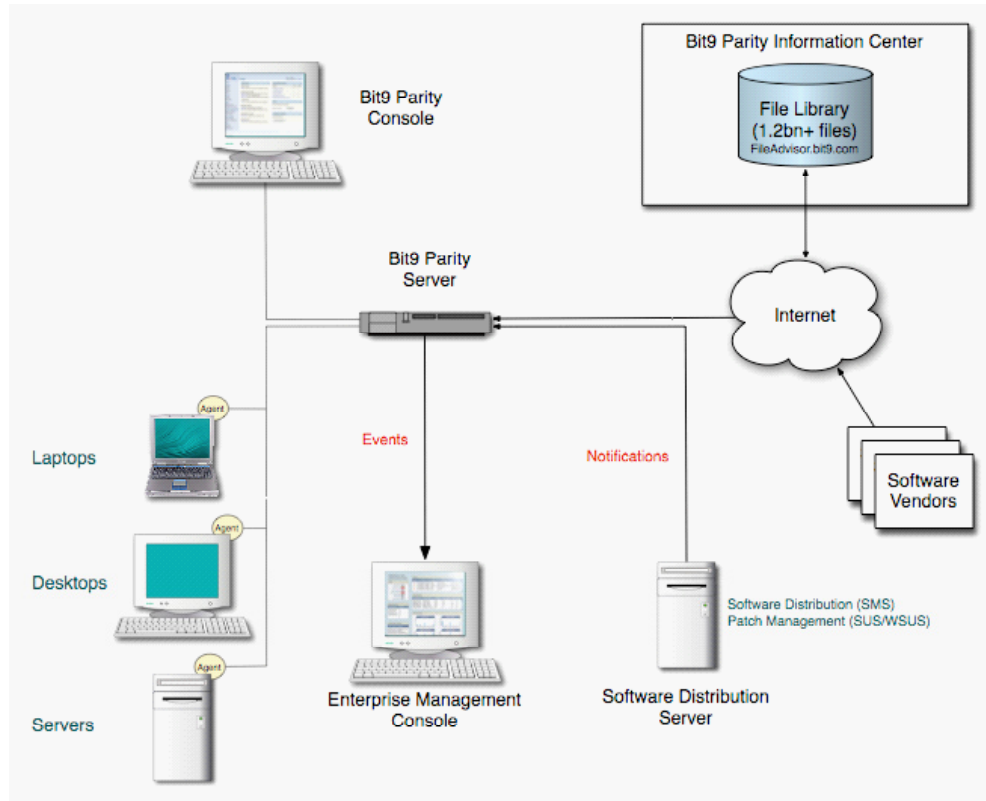


Figure 3: The Bit9 Software and Hardware Configuration

Bit9 itself is managed from the Bit9 Parity console, which reports on all graylisted software and allows IT support staff to query the network about a specific executable file; when and where did it arrive, is it still executing, who else has executed it, is it waiting for approval, etc. It is used to ban or approve software and it can also be used to designate trusted users (users that can approve software), trusted directories (specific directories containing executables, all of which can be trusted), trusted publishers (software companies all of whose executable files are to be automatically approved) and trusted updaters (companies providing updates to executables all of which are to be automatically approved). The bulk designations make it easy to get Bit9 up and running quickly and easy to maintain in dynamic environments.



Anti-Virus Is Dead

The Bottom Line

Products like Bit9 Parity are Software Authentication products. They ensure that all software that runs on a company's computers has been authenticated as valid, or if it has not, then it is running in a controlled manner and has been approved to run by someone within the organization. For that reason, Software Authentication products stop a whole host of ills, rather than just viruses and worms.

The broad nature of the protection they deliver is clear from Table 1, below.

Security Capability	Anti-Virus Products	Software Authentication Products
Prevent known viruses	Yes	Yes
Prevent new viruses	Only sometimes	Yes
Prevent uploading of hacker tools	Only sometimes	Yes
Prevent spyware and adware	Only sometimes	Yes
Software authentication process	No	Yes
Prevent use of officially banned software	No	Yes
Prevent use of new unknown software	No	Yes

Table 1: Anti-Virus and Software Authentication Compared

The simple truth is that AV software protects against very little. Most AV products will completely protect against known viruses. Statistics mentioned earlier indicate that the more popular AV products protect against only 20 percent of new viruses, primarily because most virus authors test their work against these tools before releasing their malware into the wild. The success of AV products against hacker tools is limited for the same reason.

The simple truth is that AV software protects against very little.



Anti-Virus Is Dead

That they have any success at all against new viruses is due to the fact that AV products do more than check signatures. They can provide behavioral monitoring capability (monitoring software to see what it does) or code pattern matching (matching sections of code from known viruses). Unfortunately these techniques are imprecise. While such techniques may detect malware sometimes, they can also generate “false positives,” classifying perfectly valid code as malware. This creates administrative problems, as it means that IT staff must do some manual software authentication.

Software Authentication products do not employ such flawed techniques.

It looks from the above table as though the capabilities of Software Authentication products are extensive, and indeed they are extensive, when compared with weak and inadequate capabilities of AV products. But in reality they have a single focus – the authentication of corporate software. In doing this they block a wide variety of software that companies do not want running in their networks: viruses, worms, trojans, hacker tools, peer-to-peer file sharing software, games, unlicensed software, stolen software, old versions of valid software... The list is long.

Companies that implement Software Authentication technology soon abandon the AV software that they previously deployed. Most adopters stay with the AV software for a while until they are convinced that it no longer serves any useful purpose. Then it is retired.

The number of companies moving to Software Authentication products to improve their security is growing and the IT industry is gradually learning that AV software has become a defunct technology. It is now only a matter of time before AV turns up its toes.

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.

Robin Bloor is a Partner of Hurwitz & Associates.

Companies that implement Software Authentication technology soon abandon the AV software that they previously deployed.