



**Defense in Depth:
How Application Whitelisting Can
Increase Your Desktop Security**

Whitepaper

November 16th, 2009

Intelligent Solutions for **ABSOLUTE** Control

www.faronics.com

Tel: 1-800-943-6422 • Fax: 1-800-943-6488

Tel: +1-604-637-3333 • Fax: +1-604-637-8188

© 1999 – 2009 Faronics Corporation. All rights reserved. Faronics, Anti-Executable, Deep Freeze, Faronics Insight, Faronics Power Save, Faronics System Profiler, and WINSelect are trademarks and/ or registered trademarks of Faronics Corporation.

All other company and product names are trademarks of their respective owners.

Defense in Depth: How Application Whitelisting Can Increase Your Desktop Security

By Byron Hynes, CISSP

Executive Summary

There was a time when many computer professionals relied solely on one technology to protect their computers and networks. But today, most well-developed organizations use a collection of several technologies, methodologies, and products, each protecting against a particular threat. The concept of a layered protection strategy—or “defense in depth”—is fairly well known. But many IT professionals overlook what can be one of the strongest layers of defense available – application whitelisting.

No single technology guarantees security, however application whitelisting covers situations not addressed by firewalls or anti-virus utilities. This paper focuses on how application whitelisting can be effectively used as an important layer in your security scenario. It examines other security layers as well, and demonstrates how whitelisting *compliments* and augments existing defenses. Along the way, we’ll examine the limitations and difficulties inherent in various existing defenses.

All of This Has Happened Before

The concept of application whitelisting is not new, but it has definitely been out of use for many years. When computers first came into businesses as work tools, only the IT Department could run code, code that had been written and installed for that specific installation. This was the ultimate in whitelisting; nothing else could be loaded or run.

Then, the personal computer changed everything.

Smaller and much cheaper, PCs took over homes and the workplace. The ability to install off-the-shelf software, and the burgeoning software market, meant that every business, even every user, could choose what software to run. Security problems began to appear, but as compared to today, they were manageable. Viruses existed, but propagation was limited to slow dial-up connections and “sneakernet” floppy attacks. All the while, though, a problem brewed underneath the surface: people expected to be able to run whatever they wanted, whenever they wanted.

Then, the Internet changed everything—again.

Since the explosion of the Web, many IT professionals struggle to stem the flood of security threats. As the Internet has grown, so has the threat of the criminal enterprise. Organized crime and small-time crooks have moved online, because there is real money to be made by compromising computer security. Attackers are well-funded, often well-educated, and highly skilled criminals.

On the one hand, application whitelisting is a simple concept that should make this easy—simply permit only approved applications to run. But, on the other hand, it is often not a popular choice with end-users or sometimes even with IT staff. This is because even if the IT staff is on board with the concept, in practice, it has traditionally been too hard to implement, too hard to manage, or simply too restrictive.

So, as you investigate ways to build your security layers and hone your technology and processes, some of the most vulnerable parts of the infrastructure—your desktops and laptops—remain too much at risk.

Why Bother with Stronger Security?

So, why bother?

One reason is to protect the bottom line. Security matters can be costly if only retroactively addressed.

In July 2009, the largest bank in the United Kingdom was fined 3.2 million British pounds (about 5.25 million US dollars)¹ after losing media containing customer information, and sending confidential data through insecure third parties without encryption. The government regulatory agency who investigated called the company “careless” in its treatment of data. The director of enforcement said the bank had “failed their customers by being careless with personal details which could have ended up in the hands of criminals,” and that “firms must ensure that their data security systems and controls are constantly reviewed and updated to tackle this growing threat.”

Of course beyond the fine line are hundreds of thousands of dollars in costs borne by the company, and the loss of customer faith and loyalty (not to mention stock value) from the negative publicity.

¹ <http://www.cio.co.uk/news/119615/hsbc-data-security-failure-costs-it-3-million/>

“The concept of a layered protection strategy is fairly well known, but many IT professionals are overlooking what can be one of the strongest layers of defense available—application whitelisting.”

This is only one example. Security costs money, but failed security costs even more. That's why we bother.

Basic Tenets

The basic tenets of computer security in the big picture are often defined as the “CIA triad.” CIA stands for Confidentiality, Integrity, and Availability.

These are three complimentary, but distinct, goals for anyone charged with handling and protecting data. Here's how we can envision each one.

- ▶ **Confidentiality:** private data remains private and only accessible to those authorized to access it;
- ▶ **Integrity:** the data represents what it is meant to and has not been changed without authorization;
- ▶ **Availability:** the data (or systems) are available when needed.

Together, confidentiality, integrity, and availability (CIA) sum up virtually every goal in computer security. Conversely, almost any attack erodes one of those tenets.

In practical terms, we must keep our company's data protected from theft. It must not become identity-theft collateral (one of the most common goals of criminal attacks against systems). We must ensure that all data stored and managed remains correct or our business decisions will be wrong. In some cases lives may be at risk. We must avoid denial-of-service attacks that take our systems offline. (A denial-of-service can also include attacks that prevent people from doing their jobs. An attack that consumes vast amounts of staff time—sometimes called a “social attack”—can cost as much as an attack that prevents access to systems).

Legal Compliance

These protections are so important that in many industries they are codified into law or regulation, or as you have certainly heard “compliance requirements.” These span an alphabet soup of acronyms like HIPAA, SOX, GLBA, and more—and if you're an international corporation, add exciting terms like PIPEDA and Safe Harbor.

It's beyond the scope of this paper to define compliance, or even to spell out all those names, but we can sum it up by saying that most of us are legally obligated to protect the data in our care, and all of us are morally obligated to do so.

Defense in Depth

The most successful, and now the most common, approach to combating threats like this is to use a layered approach often called “defense in depth.” You may have heard the following analogy of a medieval castle:

Before an attacking hoard could spirit away the King's daughter they had to cross the wide-open plain in front of the castle (or scale a high cliff, if the King was Scottish). If they got across the plain without being picked off by archers, they faced a deep moat of foul-smelling water and possible alligators. The attackers not eaten or drowned then had to dodge the scalding oil being poured from above, and pummel on the portcullis and the heavy door. Finally inside the courtyard, they faced hand-to-hand combat with the King's bodyguards, a few more locks and doors, and maybe a maze of narrow passages and twisty stairs. Finally, absconding with their young and beautiful prize, they discover the chastity belt, which of course serves to buy enough time for our hero to ride in on horseback and rescue the maiden.

During a slow afternoon I am always amused to map each of the technologies in use today to one of those medieval layers.

Our Opponents Are Formidable

Regrettably, our modern attackers are very determined. The effect of the distributed nature of attacking, and the financial motivation of most attackers (although there are other motivators from time to time, financial gain of a criminal enterprise is far-and-away the leader) means that modern attackers have literally all the time in the world and almost unlimited resources.

If an IT staff was to place all hope in only one layer or technology, that company is bound to lose. Eventually, an attacker will compromise that one defense layer, and then all is lost. In the early days of computer security you would overhear “Oh, we have a firewall; so, we're protected.” That was a shortsighted view that defends against only one type of threat. Those who failed to adapt and consider new attacks most often became victims.

Now, other layers are needed, and sometimes one layer (such as desktop anti-virus) is heavily promoted. IT departments are wise to revisit history, lest they repeat the same mistakes.

The best practitioners use an entire arsenal of tools, each protecting a different area—or *more likely, specifically designed to counter a specific threat*. This gives two great advantages: more threats are protected against, and if one defense is compromised, a second, or third, or fourth, stands ready and must still be overcome.

A Review of Common Layers

Application whitelisting should not be presented or implemented as an all-in-one “fix-it-all” or a complete solution. However, it can greatly enhance your existing defenses and often be the “last mile” to a full solution.

In that spirit, let’s review some of the other layers.

Layers can be divided into a few sections:

- ▶ Physical and Environmental Security
- ▶ Social Defenses
- ▶ Network and Edge Protection
- ▶ Desktop Technologies

Other security guidelines may suggest other divisions, but these are reasonable layers for our discussions. They can also be based on your technology focus. If you are primarily concerned with server farms, you would have a different outlook than someone focused more on desktops.

Physical and Environmental Security

Physical security is the first line of defense. Some have called it the “gates, guards, and guns layer.” Obviously, this layer is in the most active use in the military, but often overlooked in smaller organizations, and sometimes even in larger enterprises. However, it is one of the best examples of people matching their expenditures to their perceived risk. Not everyone should have a perimeter fence with barbed wire, but even the smallest operation can benefit from securely locked server rooms and/or locked cabinets for servers and network gear.

As an organization and its assets become more valuable, the IT department can consider biometrics (hand or retina scanners), or smart-card based access. The key is to make reasonable risk/reward decisions based on your own threat level, and the value of your assets.

Social Defenses

Unfortunately, this area is often overlooked, as a small investment here can yield significant results. As technologists, we often want to jump right into the gadgets, software, and configuration; however, we need to work with people too.

Begin with written corporate security policies and guidelines, including a management-approved level (or levels) of response. What actions are unacceptable? Which ones warrant gentle reminders popping up on the screen? Which require software-enforced limits? Which are firing offenses, and when do you call the cops?

End-users should understand policies and be regularly reminded. Consult with representatives of end-users. Inform, influence, and educate the user base. In short, your IT department and company management should make sure that all staff “get it.” This makes it much easier to secure your network and to enforce policies.

Building awareness through formal and informal communications and training can be one of the least expensive but most effective ways to improve your security.

Network and Edge Protection

Any decent bookstore will have several 1,000+ page books on Network and Edge security. You can’t implement every security mechanism, but here are four common network and edge-protection technologies often found in use today:

- ▶ **Edge Firewalls:** a firewall device at the edge of your network or between subnets. These have been around as long as networking. These still have value. They keep a significant amount of evil outside your network. They restrict access from a large number of attackers, and contribute greatly to increasing the efficiency of your network (and therefore the availability part of CIA). In short, they are necessary.

However, they don’t do anything to protect against attacks originating inside your network. They also don’t protect against software purposely run— whether that software is malware being run accidentally by a well-meaning user, or a malicious tool run by a user that should not have been trusted (but is).

- ▶ **Intrusion Detection Systems (IDS):** sometimes part of a firewall, and sometimes blending with NAC/ NAP (the next section), these are hardware or software components that watch network traffic for patterns that match malicious activity. They too can serve a purpose, but they are limited by what they can see (especially on a switched network), and by the need to have pre-defined signatures or advanced heuristics. Some IDS systems also suffer from too many false positives (flagging normal traffic as dangerous).

- ▶ **Network Access Control (NAC)/Network Access Protection (NAP):** NAC/NAP products are intended to monitor the “health” or “state” of a network device, like a PC, and limit its communication on the network if it is not compliant with a pre-defined policy.

NAC/NAP implementations can help reduce help-desk costs, and improve regulatory compliance. They can encourage or force your users to use the tools you provide to protect your systems. Generally, though, they do an excellent job of ensuring that *other tools* are being utilized. For instance, NAC/NAP can check to see if a PC has a specific anti-virus (AV) solution installed and that it is kept up-to-date. But the NAC/NAP solution’s job isn’t to actually protect against a virus. If the anti-virus system doesn’t yet have a signature for a new virus, having NAC/NAP tools enforce the requirement of running anti-virus is of limited value.

- ▶ **Transit Encryption:** the two most common forms of encryption of data in transit are Transport Security Layer/Secure Sockets Layer (TLS/SSL) and Internet Protocol Security (IPsec). These are essential for sending confidential data over untrusted networks like the Internet. But, they don’t prevent bad data or malicious code from being transmitted. Indeed, too much encryption can make IDS of limited value, since an encrypted virus is more easily hidden.

Desktop Technologies

Finally, let’s examine the types of protection most directly related to where most of our users live: the desktop. Each of these has a role to play, but not one technology by itself is enough to protect your environment against all threats.

- ▶ **System Restore:** When a computer becomes unusable, many administrators prefer to simply re-image it than to try to troubleshoot and repair the damage. Many security experts say that if a computer has been compromised, the only secure choice is to completely erase, reformat, and reinstall the system. Those drastic measures are not always feasible or necessary, particularly if the “damage” is not a security issue, such as installing the wrong version of a driver. Windows includes the System Restore function to allow some changes to be undone. Applications are also offered to allow administrators to quickly and completely return the system to a known state. Microsoft offers a limited solution called Windows SteadyState. SteadyState was formerly called the Shared Computer Toolkit because it is optimized for shared computers. The most well-known commercial application of this type is Deep Freeze from Faronics. Note that System Restore solutions do not prevent problems or mitigate the risk of data leakage; rather they provide a method—potentially a very effective method—of quick recovery.
- ▶ **Encryption:** Like protecting data in transit, encryption can also be used to encrypt data at rest. Products in this category include single-file (or directory) encryption like the Encrypting File System (EFS) built into Windows, or “whole-disk” encryption suites like BitLocker™ Drive Encryption (available in some editions of Vista and Windows 7), the open-source TrueCrypt, and software from several other vendors.

These are great tools for protecting data from prying eyes, or reducing worry if a users’ laptop is stolen. Disk encryption is now commonly required for compliance. However, just as with data in transit, these products only protect against certain specific scenarios. In most cases if the computer is running and the OS is booted, the encryption software is happy to decrypt everything and execute whatever users like.

- ▶ **Execution Control:** One element in this category is the User Account Control (UAC) found in Windows 7 and Windows Vista. UAC’s purpose is to reduce the need for users to run as administrators, and to force developers to consider when they are requesting more rights and privileges for an executable than really necessary. Unfortunately, UAC has garnered a bad reputation because users and administrators found it frustrating and disliked the many pop-up warnings and prompts. In order to be effective as a security measure, the UAC settings had to be so restrictive that many people found it objectionable.

Another technology in this area is the idea of traditional blacklisting, where a particular application is *prevented* from running. We’ll talk more later about blacklisting and whitelisting, and there are still some occasions where a blacklist can be useful. However, it is impossible to know in advance every potential application that you might not want to run, thus limiting the protection that can be provided by a blacklist of executables.

- ▶ **Traditional Anti-Virus (AV):** Philosophically, anti-virus could be seen as an enhanced blacklist. Specific programs are blocked by name, by file hash, or because they contain predefined strings of known bytes and patterns. In most modern anti-virus programs, heuristics are also used to attempt to detect variations of known viruses or behaviors that are virus-like.

AV is mandated in most companies, and is often required for regulatory compliance.

Anti-virus is often not all that effective when used alone. First of all, AV needs constant updating. The

famous “Ten Immutable Laws of Security”² say that an out-of-date virus scanner is only marginally better than no virus scanner at all. Some AV products are drains on system resources. Some are nearly impossible to manage for a corporate enterprise.

The key anti-virus limitation though is it will only protect against the threats that the publisher already knew about—not the one that’s happening now. There are several types of threats that may attack before the AV vendors know about them. For example, some malware is specifically written to mutate (to change its own code) to avoid detection. Other viruses exploit vulnerabilities that have not been disclosed or patched (the “zero-day attack”), and it is common for malware writers to reverse-engineer a published patch to create a new virus—written in minutes after an OS patch is released, faster than that patch is applied, and before the AV vendors can update their signature files.

- ▶ **Application Whitelisting:** as its name suggests, is the counterpart to blacklisting.

Philosophy and Benefits

Rather than trying to identify all the possible bad applications that you never want to run, you start by identifying *exactly what you do want to run*. Therefore, the system is configured to allow *only* those specific applications to execute.

The benefits of whitelisting are quick to see. You don’t have to worry about unknown malware, because if it’s not on the list, it doesn’t run. You are dealing with a finite set of known good programs rather than the infinite set of unknown bad programs.

Software Restriction Policies and their Limitations

A form of application whitelisting has existed in Windows since Windows 2000, known as Software Restriction Policies (SRPs). SRPs continued with minor improvements into Windows XP and Windows Vista.

Regrettably, there are both logistical and technical limitations to SRPs. First of all, SRPs offer no way to easily identify all of the programs you want to allow to run. You must manually do so (although, you can whitelist entire directories such as C:\Windows\System32). Thus, you had to deploy the computer with the SRP already in place and carefully manage administrative rights (or a user or attacker could simply install the new, unwanted software in the whitelisted folder).

Also, as surprising as this sounds, the OS itself doesn’t enforce the SRP restriction. Rather, it is up to the shell or application launching the new process to check the SRP. Windows Explorer does so, but there are a number of other ways to launch a process, some of which could get around SRP without much effort. There are published exploits against existing Windows Software Restriction Policies technology.

Implementing a fully whitelisted environment using SRPs is a lot of work and needs constant maintenance. First, you need to identify every application used by employees, and then determine whether that application is productive.

An average desktop can have many dozens of processes running, all of them are providing a useful purpose. One creates a taskbar icon for the sound card driver. One notifies the user if they receive new email. The number of executables potentially used by a knowledge worker is in the hundreds or even thousands.

Most SRP documentation suggests simply whitelisting the entire Program Files directory. Most security professionals believe that even on a clean Windows installation, there are executables installed that really don’t need to be run by the average user. You either must choose to allow them all to run or identify each executable and manually add it to the list.

If an application is updated, you must repeat the process. There is no automatic way to install a patch and simply whitelist whatever changed.

AppLocker in Windows 7

In Windows 7, Microsoft changed SRPs into AppLocker™, which addressed many of the limitations. However, a few gaps remain.

There is now a wizard available to assist in creating AppLocker rules. The wizard instructions recommend preconfiguration by using Group Policy, and recommend designating that all programs present under Program Files or the system Windows folder be allowed to run, even if they are added in the future without being added to the whitelist.

2

Microsoft’s 10 Immutable Laws of Security, from the Microsoft Security Response Center. <http://technet.microsoft.com/en-us/library/cc722487.aspx>

The wizard can only automatically create whitelist rules for one folder tree at a time. If you want to include the user's profile or the whole disk in the wizard, you are limited to the types of rules you can create. The wizard is a vast improvement over Software Restriction Policies for Windows Vista and Windows XP, but it is still complicated to use, and requires a deep understanding of Group Policy, Windows, and the AppLocker infrastructure to be effective.

AppLocker, like SRPs, requires careful management of Administrative rights. If a user must be able to run an application that can only be run as an administrator, that user, by default, will be exempted from the restrictions. If you change the default, any administrator can still choose to bypass AppLocker.

In many organizations, the bigger issue will be that AppLocker is present only in Windows 7, and only in certain editions—Ultimate and Enterprise. Many business customers will be out in the cold because they are simply not licensed for the “correct” Windows 7 version, or they are not yet prepared to migrate from Windows XP or Windows Vista. This limits the usefulness of AppLocker in established environments.

Faronic's Anti-Executable

Microsoft is not the only software publisher to offer Application Whitelisting. Anti-Executable from Faronics is a commercial solution, and is discussed in detail later in this paper.

Why AV and Whitelisting Together Make Sense

AV still has a role to play, and it is a good baseline security to have. The better AV products use heuristics to help recognize malware, and there remain vast hordes of attackers using old attacks to compromise systems because there are many unpatched operating systems and even more unpatched applications out there in the real world.

In addition, even with whitelisting, there are threats that can be carried inside what used to be thought of as data. For example, you are probably going to allow a word processor, such as Microsoft Word, to execute—in other words, it's going to be whitelisted. Most modern AV scanners will look at the file being opened and watch for dangerous macros or malformed JPEGs and other well-known attack avenues after execution.

A good AV scanner interacts with all of the other layers and enhances them.

Whitelisting Benefits: Beyond the Obvious

We need to have layers of defense to protect confidentiality, integrity, and availability of data. There are also additional, non-obvious benefits when application whitelisting is employed. These benefits go beyond security and can save additional man-hours and money.

Protecting Resource Usage

In many organizations, significant resources are being used to operate unapproved and unnecessary applications. Using application whitelisting can ensure that company resources are focused more effectively on the task at hand.

Lower Help-Desk Costs

Every time a user calls the help-desk, it costs money. On the other hand, non-technical users don't understand why their computer isn't working—or why they can't get their job done—and have no choice but to call in the pros at the help-desk, even though it's often really of their own doing.

Here's a typical scenario: the IT Department delivers a new desktop, and all is well. After a few days, users install a new viewer for some unusual file format without realizing that it's an older version that conflicts with a DLL already installed on the computer. Then, while reading their personal email on the Web, they click a link to a new file (usually, a game), and inside, it's also installing a key logger program. A few days later, bored with the standard Windows screen-saver, they download, install, and run, a new whiz-bang screen saver that plays clips of a celebrity's new movie.

In just a matter of days, the user, without being malicious, created a situation where their new computer is slowing down, and where “things just don't work right.”

By keeping unauthorized applications from running, your computers remain much more stable and are run as efficiently as possible. You can eliminate unfortunate incompatibilities and ensure that what you produce in your test lab will be maintained out in the real-world after production. This eliminates needless help desk calls, and the costs associated with them, and reduces the need to re-image workstations.

Prevent Distractive Applications

Once you have established written corporate policies, it becomes easier to enforce them using application whitelisting. Similar to the need to ban certain Web sites when they take over too much employee time or network bandwidth, application whitelisting can eliminate games and other unproductive applications.

Prevent Unlicensed or Illegal Applications

No one wants to be on the end of a lawsuit. Your organization could face a software audit, the results of which could include paying thousands of dollars in license fees for applications installed without your knowledge. Even if the application isn't being used, but was installed outside of an approved trial period and not removed, you could still have to pay for it.

Application whitelisting ensures you know that only applications you've specified are being used.

Likewise, some applications could be illegal or inappropriate. Whitelisting protects you from this problem as well.

Mitigations of Zero-Day Attacks

Once software patches are produced, evildoers immediately start to reverse-engineer the patch to find how to exploit the vulnerability. Oftentimes, malware for unpatched systems is ready to go within a few short hours, during which you may not have completed testing or implementing the new patch. It also takes time for the AV vendors to catch up and have new signatures produced and distributed. Since the goal of most exploits is to cause the attackers' executable to run, you can breathe a bit easier knowing that their new executable isn't on your whitelist.

Some people hope that limiting the use of the administrator account will protect them from these kinds of attacks. Limiting the number of administrators is a good idea, a very good idea. But, non-administrators must be allowed to run approved software and must be allowed to access data—simply to do their jobs. Many malware programs are being written to run as standard users and to read or corrupt confidential data without requiring administrative rights.

Remember: If it's not on your whitelist, it doesn't run.

The road to a new AV signature is paved with the results of victims of zero day attacks. Application whitelisting, used correctly, can stave off the attack.

Summary

Application whitelisting enforces compliance with organizational IT policies. It keeps your client computers stable. It cuts help-desk costs. It keeps your computer and personnel resources focused on productive tasks. It combines with other defenses and keeps you secure.

If application whitelisting prevents even one corporate data breach due to malware, and keeps you online and out of the newspapers, it could easily repay its costs.

“From Faronics and Byron Hynes”—The Anti-Executable Solution

You have seen some of the benefits of application whitelisting, but also heard some of the difficulties and limitations inherent in the traditional solutions and options built into Windows. Anti-Executable from Faronics is designed to work with other layers of defense to give you all the benefits of application whitelisting. It is also easy to use in a small organization, and easily managed centrally in the enterprise.

Usage Examples

Let's take a look at some situations where application whitelisting—specifically Faronics Anti-Executable—can play a role in improving and protecting desktops and mobile workstations.

Corporate IT

Unauthorized applications are the bane of many corporate IT departments. Software comes into the environment through portable drives, email accounts, and web browsing. The IT department faces a constant uphill battle to keep computers running, corporate data secure, and employee productivity high, and these unwanted executables are a leading cause of trouble.

Since much of the software is malicious—keyloggers, spyware, malware, viruses, and Trojans—companies are compelled to address the situation in order to comply with legislation such as HIPAA and Sarbanes-Oxley. Other applications, such as games and instant messaging clients, are distractions to employee productivity and divert resources. File-sharing programs can be used to move corporate data to unauthorized computers and create too much risk of data-leaking. The corporate IT department is also charged with ensuring that all software is properly licensed, but users frequently download trial versions, and a few have brought in copies of software from home or tried to run non-authorized versions of commercial programs.

Anti-Executable protects users from these threats through application whitelisting—blocking all unauthorized programs from installing or running, while still providing users with the ability to access the programs that have been deemed by IT to be safe. The IT department whitelists *only* applications that have been documented as being properly licensed. Anti-Executable helps computers remain free of malicious software, helps keep corporate data secure, and enforces acceptable use policies and regulatory compliance. Anti-Executable helps ensure network bandwidth remains efficient, and IT personnel are freed from unnecessary tedious help-desk and repair requests.

Local Government

Municipal and other local governments face unique computing challenges. They handle public data as well as confidential data about their citizens. They must provide uninterrupted public services, often including police, fire, ambulance, and physical infrastructure, even during hectic and unpredictable emergency situations.

Let's look at an example of a large municipal police force. This force has patrol cars with mobile data terminals (MDTs). These MDTs run only Windows 95, with a single dedicated police dispatch application, and use a low-bandwidth, radio-based data communication link. They realize that to keep up they will need to upgrade and select a new class of equipment known as mobile data computers (MDCs). The MDCs are essentially a customized, business-class laptop for vehicles, and they run Windows XP.

Because of the new software and hardware being introduced into the computing environment, IT was concerned about new threats and possible software configuration issues. While able to do much more, the new MDCs are also potentially more susceptible to external threats such as spyware, viruses, and other malware. It is essential to prevent damage or data leakage caused by any of these threats.

In this case, the IT department chose to combine Faronics Anti-Executable with the additional layer of Faronics Deep Freeze. Deep Freeze provides the ability to reduce the resources required to fix or reimage machines, allowing users to simply reboot to a known good state, eliminating the need for the computer to be brought in or replaced.

Anti-Executable increases a user's productivity by blocking the installation of non-business-related or harmful files that could prevent the use of a mission-critical system. Because Anti-Executable proactively protects machines by only allowing authorized executables to run, tasks that are often performed to avoid software compliance problems, such as constant routine software audits, are no longer necessary when Anti-Executable is installed, thus further freeing IT staff to attend to other duties.

For more information about this real scenario in use with over 1500 mobile devices, visit the Faronics Web site ³.

Libraries, Schools, and Kiosks

The "kiosk model" and "internet café" scenarios continue to grow in popularity. In many locations and cultures, it is much more common to access the Web through a free or low-cost shared system than from home or work. The needs of the operators of public-access computers are specialized. Up-time and reliability are critical, but the nature of the clientele makes it difficult. A few users will deliberately try to sabotage the system; students will want to experiment and install the latest fad software or game; while criminals want to get a key logger (and other malware) installed to capture the next user's passwords and personal information.

Some operators (schools and libraries) must restrict what can be done on each computer. Some provide the public-access computer for a specific purpose (school research, card catalog lookup), while others want paying customers to be able to access a wide variety of tools and applications, but do not want to be caught in licensing dilemmas or fail software audits.

Any unauthorized or unwanted programs can cause problems for the operators. As in the corporate environment, software comes from portable drives, email, and web browsing.

Anti-Executable's application whitelisting protection eliminates productivity threats resulting from malware and key loggers, and limits users to those applications allowed by policy, whether that is one application only, or a library of dozens. As with business scenarios, Anti-Executable makes it easy to ensure that computers remain in full compliance with licensing requirements at all times, without constant attention from IT or library/café staff.

Questions and Answers

Here are the answers to some common questions about Faronics Anti-Executable and application whitelisting.

Security Features

Q: How difficult is it to create a whitelist?

A: Faronics is a pioneer and leader in automatic whitelist creation.

The most common scenario is to begin with a reference computer containing only the applications you want to allow to run. Anti-Executable can examine the computer and create a whitelist entry for each application already installed, automatically and in the background. Once the whitelist is created, you can remove any extraneous or unwanted executables with one click.

In addition, you can also automatically create a whitelist for a computer that is already deployed, and then examine the list to remove any entries you don't want. After doing this, you can reapply the modified list back to the same computer,

³ http://www.faronics.com/whitepapers/CaseStudy_LAPD.pdf

without ever taking it out of production or having to reimage it.

With the Anti-Executable Enterprise Edition, you can manage your whitelists centrally, and use automatic whitelist creation for remote computers (this is called Remote Scanning).

Q: I have already deployed computers to employees in remote and branch offices. I'm not totally sure what applications they are using, but I want to protect them. Can I do this without travelling to them, or re-issuing their computers?

A: Yes. Use Remote Scanning to create a whitelist for the remote computer. This will include all of the applications already installed on that computer. You then have the option to review the automatically created whitelists in order to verify that only authorized applications have been installed.

It is important to note that you will not ever need to manually create a whitelist entry. You can review the automatically created whitelist and decide whether to allow the application by leaving it on the whitelist, meaning you're approving it, or you can remove the entry. This is a great way to determine exactly what software—approved or otherwise—has been installed across your network.

Alternatively, you can automatically create a new whitelist from a reference computer, and choose to apply it to the remote site.

Once you have edited the automatically created whitelist, you can use the Faronics Core to apply the appropriate whitelist to all desired computers, no matter where they are on your network—down the hall or around the globe.

You can also use a blacklist to be absolutely sure that particular applications can never run, even if they are already installed when you automatically create a whitelist. One use for a blacklist might be to prevent a particular application from running during the time it takes you to review the automatically generated whitelists.

Centralized Management

Q: How hard is it to get an 'at a glance' status and feedback about my client base?

A: Faronics products are designed to be easy to use for homes and small businesses and enterprise-ready. The Enterprise Edition of Anti-Executable comes with and is managed by the Faronics Core.

The Faronics Core provides centralized deployment, configuration, scheduling, and control of Anti-Executable and other Faronics products, and allows you to rapidly install Anti-Executable on any or all workstations, manage and export log records of violation attempts, change maintenance schedules on the fly, and manage workstations easily using groups and filters

Q: Do I have to work with each machine individually?

A: No, the Faronics Core allows you to manage workstations in logical groups that you can define, or by filtering on a number of criteria. You can see screenshots, download trials, or register for a free live webinar that demonstrates the Faronics Core functionality at the Faronics Web site ⁴.

Compatibility Concerns

Q: Is Anti-Executable compatible with my existing anti-virus solution? Do I need to rip-and-replace or run only Faronics software?

A: Anti-Executable is fully compatible with all major anti-virus applications.

In fact, by marking an application, such as an anti-virus program, as trusted you can allow Anti-Executable to automatically whitelist any changes that application makes to its own files (for example, if that program updates its own executables). You can also use maintenance mode to install updates and update the whitelist in one step, or manage the whitelist manually).

In the first section of this paper we discussed the benefits that come from having each layer work in tandem. Anti-Executable can be an excellent compliment to your chosen anti-virus solution.

Q: Is whitelisting with Anti-Executable compatible with my investment in Deep Freeze?

A: Yes. A good security solution plays well with others. A great security product leverages all the other layers.

⁴ <http://www.faronics.com/html/screenshots.asp>

Anti-Executable is aware of Deep Freeze and integrates seamlessly with its instant system recovery functionality. Anti-Executable can be configured to honor Deep Freeze Maintenance Mode, allowing for effortless patching and regular updates.

Q: How does Anti-Executable compare with what Microsoft provides?

A: As discussed earlier in this document, Microsoft provides Software Restriction Policies (SRP) in versions of Windows since Windows 2000, and AppLocker™ in Windows 7 Enterprise and Windows 7 Ultimate.

Anti-Executable provides the following benefits compared to Microsoft technologies:

- ▶ Automatic creation of whitelists in a simple, one-step procedure.
- ▶ Enforcement of policies without relying on the launching application (or Windows Explorer) voluntarily checking the policy before spawning the new application.
- ▶ Universal application of Anti-Executable across all versions and editions of Windows since Windows XP SP3.
- ▶ Integrated reporting that can include any changes made to whitelists, any status changes (such as Anti-Executable being disabled by an authorized user), and any attempts to run programs that are not on the whitelist (violation attempts).
- ▶ Automatic updating of whitelist in Maintenance Mode. Anti-Executable enters Maintenance Mode automatically when it detects that a Deep Freeze Maintenance Event has Thawed the computer.
- ▶ Automatic updating of whitelist by trusted applications.
- ▶ Centralized and remote management through Faronics Core Console.
- ▶ Reliable and simple restrictions of local computer administrators (for example, if application compatibility requires that users have administrative rights).
- ▶ Whitelists can be imported, exported, viewed, edited, searched, merged, and sorted.
- ▶ Displays a customized violation message when a user attempts to perform an action that is not authorized by Anti-Executable.

Summary

Finding the right mix of security and flexibility has always been a balancing act, but the ease with which Faronics Anti-Executable can be deployed and maintained makes it easy to restrict applications immediately, which allows a straightforward, simple way to make changes as needed, either centrally or on each computer.

Anti-Executable also makes applying Windows and third-party updates easy and effortless. On-demand and scheduled maintenance modes allow for application updates and additions. When used with automatic whitelist population, the limits of earlier whitelisting solutions can be overcome.

A layered approach is essential to protect your digital assets in today's world, and Faronics Anti-Executable is a powerful, enterprise-ready and cost-effective layer that, when combined with other defenses, gives you the most complete threat coverage available today.

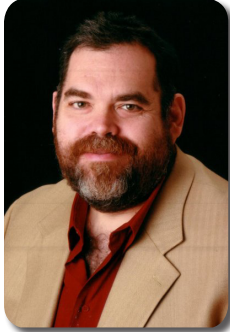
Next Steps

Faronics is dedicated to your success in securing and protecting your computing environment, and we invite you to find out more about us and our products. Here's how you can learn more about Faronics Anti-Executable:

- ▶ Browse the extensive on-line Content Library at <http://www.faronics.com>, which includes the product documentation, case studies, screen shots, and whitepapers.
- ▶ Download a free, 30-day evaluation copy from <http://www.faronics.com> and try Faronics Anti-Executable in your own environment.
- ▶ While at <http://www.faronics.com>, register for a free Webinar. Faronics Webinars include product demos and walkthroughs, and direct access to a Faronics expert for any questions you have.

About the Author

Byron Hynes is an infrastructure and security specialist with over 25 years in IT and related fields. Building on years of experience implementing networks, databases, and software, Byron also brings a talent for understanding the big picture and a love of finding ways to solve real problems with technology. His skills include a deep understanding of platforms and technologies, a proven track record in managing cross-group projects and initiatives, and sound communication skills he uses as a technical writer, conference speaker, and trainer.



Byron has worked with small startups, non-profits, mid-size companies and the largest enterprises, including over four years at Microsoft Corporation. Byron left Microsoft in 2009, after spending three years helping to create Windows Server 2008 (where he worked on features like BitLocker, Authorization Manager, and the core security functions in the OS), and then working for the Enterprise and Partner Group as a strategist and trusted advisor to Microsoft's largest customers.

You've read Byron's writing in TechNet Magazine, the Windows Server 2008 Security Guide, the Windows Server Security Resource Kit, and in several books, including ones co-authored with Mark Minasi. You may have seen Byron present at Microsoft's Tech-Ed conference, World-Wide Partner Conference, ITForum, MSDN, or TechNet events, as he's spoken world-wide.

Byron holds several industry certifications in security, infrastructure, database administration, and development, including those from Cisco, Microsoft, and ISC2/CISSP, among others.

About Faronics

With a well-established record of helping businesses manage, simplify, and secure their IT infrastructure, Faronics makes it possible to do more with less by maximizing the value of existing technology. We are market leaders in delivering solutions that lower the high costs of IT and increase the ability for IT to drive productivity improvements. Our solutions deliver total workstation reliability, complete system control, and non-disruptive computer energy management.

As a customer-centric organization, Faronics's products are researched and developed in close consultation with our end-users. We value our customers' ideas and suggestions, and depend on this feedback to provide the innovative solutions our users have come to rely on. This approach is the basis for Faronics's industry-leading customer service strategy: continually working to build and maintain lasting relationships with our users.

Faronics Deep Freeze provides ultimate safety net of instant system preservation, Faronics Anti-Executable blocks unauthorized software through application whitelisting, and Faronics Power Save lowers computer energy costs in an intelligent and non-disruptive manner.

Incorporated in 1996, Faronics has offices in the USA, Canada, and the UK, as well as a global network of channel partners. Our solutions are deployed in over 150 countries worldwide, and are helping more than 30,000 customers.

Address:

Canada & International

609 Granville Street, Suite 620
Vancouver, BC V7Y 1G5 Canada

Phone: +1-604-637-3333

Fax: +1-604-637-8188

Email: sales@faronics.com

Web: www.faronics.com

Hours: 7:00am to 5:00pm (Pacific Time)

USA

2411 Old Crow Canyon Road, Suite 170
San Ramon, CA 94583 USA

Phone: 800-943-6422

Fax: 800-943-6488

Europe

Siena Court, The Broadway
Maidenhead, Berkshire, SL6 1NJ UK

Phone: +44-1628-509008

Fax: +44-1628-509118

Email: eurosales@faronics.com

Copyright

This publication may not be downloaded, displayed, printed, or reproduced other than for non-commercial individual reference or private use within your/an organization. All copyright and other proprietary notices must be retained. No license to publish, communicate, modify, commercialize or alter this document is granted. For reproduction or use of this publication beyond this limited license, permission must be sought from the publisher.