Anti-Virus and the Layered-Defense Approach:
What You Need to Know For True Full End-Point Protection

Whitepaper

By Byron Hynes, CISSP

Last modified: September 8th, 2014

Layered Defense and Anti-virus

Business networks must be protected. That's your job as part of the IT staff.

Deploying anti-virus software sounds like a no brainer. Everyone must have it, lest their networks fall to bad guys, quickly. Except it turns out that it's not quite a "no brainer." An informed IT professional needs to ensure that the Anti-virus solution they choose strategically matches the goals of their company IT department.

In this paper, we set out to describe the role of anti-virus software – but specifically how it fits into a bigger layered defense security architecture. We will examine several elements of a comprehensive strategy to protect your network, and focus on defending the end-point—user workstations, such as PCs and laptops.

Layered defense

Security isn't a product. You cannot simply buy one single tool and magically enable security. Ensuring security is about doing what you can – at multiple levels – to ensure the bad guys keep stumbling over various blocks that you put in their way.

When discussing this idea of multiple levels or layers of defense within computer security, such terms as "Defense in Depth", "Layered Security" and "Layered Defense" are often used. Security experts sometimes draw nuances between them, but in practice, these terms are used interchangeably. They refer to the idea of using several steps to protect your network.

When networking was starting to become popular, organizations depended on a single primary approach or device to protect their entire computing infrastructure. In the modern world of attacks, that has proven to be wholly inadequate. To effectively protect a computer network, you need to build in several defenses. You also need to be thorough, and sometimes redundant. Having repetitions of the same type of technology applied at different points, or different approaches, or layers where one layer covers the potential weaknesses of another is important.

For example, most networks include some form of anti-virus protection that is deployed at different levels. For instance, a company could choose to have anti-virus protection on the email server to scan incoming and outgoing email, and the firewall to scan network traffic, and also on each individual PC to scan specific process activity. Implemented together, the fragmented solutions form a layered defense approach that creates a more robust overall protection. A classic and sometimes overused example is of a castle protected by a moat with alligators, thick castle walls, skilled archers– all combining to prevent the bad guys from stealing the "crown jewels." This image is a good portrait of how layers combine to repel attackers.

The idea of layered defense is not new, but security experts often don't explain why it is a good idea. Later in this white paper we'll address some of the layers you likely already have, and what you can do to make those layers more effective. For now, let's explore some excellent reasons why you should leverage a multi-layered model in your security efforts, if you're not already heading in that direction:

- Different layers of security help defend you even if an attacker finds a weakness in one of the layers. Attackers are always probing and always switching tactics. A firewall stops a lot of bad issues from getting onto your network. Unfortunately, some attacks will find their way past a firewall. To stop those attacks from escalating, another layer of defense needs to be present at the attacker's next stop on your network, be it a desktop or a server.

- Layered defense helps you stop attacks initiated from different places. For example, it makes sense to inspect inbound email at the email server for spam, phishing attacks and viruses. However sometimes, malware can originate locally, already "inside". A user with a USB thumb drive could just plug it in, and start a big problem. Anti-virus protection on the client PCs helps address this threat.

► Some industry standards, such as PCI (Payment Card Industry) requirements are strict in precisely what must be put in place. In these cases, you are probably under an obligation or expectation to exercise due diligence in building a robust, complete system that is effective. Quite often end-customers themselves may want assurance you are doing all you can to prevent a security breach.

Elements of layered defense

What makes up the elements of a layered defense model? The various elements aren't always exceptionally obvious. Each element is required to have some teeth behind it, lest the bad-guys find a way inside. Let's examine several individual elements of layered defense for a modern computing environment.

People, policies, training

Honestly, it's shocking that this category – "People, policies and training" is often completely disregarded when it comes to defense-in-depth. You could pay upwards of many thousands of dollars for a security assessment and never see any mention of these three critical elements.

It's interesting to see security recommendations and reports that don't even mention people. Sometimes called, with tongue in cheek, "Layer 8" of the OSI networking model, people are an essential part of the security equation, and you must address how they are managed within your security goals.

A study undertaken by the Computer Technology Industry Association (CompTIA) found that in over 63 percent of identified security breaches, human error was a major, underlying factor, and that 80 percent of respondents said that a lack of IT security knowledge, training or failure to follow security procedures were the root causes of these human errors. This human error was found to be the leading cause of security failures (http://www.trainingpressreleases.com/newsstory.asp?NewsID=582).

Therefore, to secure your network and computers, you must have clear security policies supported by executive management; you must train your users, and gain their support. Having users onside is not only effective security, but it also makes your job much easier.

Physical security

Just as the people problem is sometimes overlooked, so is the space problem. Sometimes technologists fail to recognize that a simple locked cabinet or electronic door control can go a long way in reducing risk and protecting data.

Physical security includes things like locking cabinets, limiting access to server rooms and server consoles, keeping track of where backup media is stored, and in some cases, hiring security officers, or providing traditional, physical surveillance with cameras or other tools.

Network firewalls

Network firewalls continue to have a place in security. In the past, a network firewall served to keep the bad on one side of the boundary, while the good could exist peacefully on the inside. While firewalls have always had some limitations, the role of network firewalls is markedly different now. Before you can really consider how to effectively deploy a network firewall, you have to figure out where your boundary now is.

What is the role of a network firewall when your users are located world-wide using laptops or connected through mobile phones, and accessing data stored in your own enterprise and in a cloud storage service?

The answer has two main parts, which keep firewalls relevant. First, use a firewall to keep a substantial amount of easy attacks out of your corporate networks. By throwing away attacks before they enter your LANs, you are reducing your exposure to danger. A firewall deployed this way also helps protect the performance of your internal network and make it easier to concentrate the other protection technologies where needed.

Secondly, firewalls can and should serve to segregate internal networks. Even as enterprises begin to flirt with cloud computing, most still have in-house servers—internal email mailbox servers, file servers, Active Directory domain controllers, etc. By grouping those servers together, defining what services those servers offer, and using firewalls to protect those segments, you make it considerably more difficult for them to be attacked. In essence, you treat all consumers of these services as potential attackers – which can be an unfortunate truth for some organizations.

Network inspection tools

Network inspection tools are common in larger enterprises, but less so in smaller businesses. They can be complicated to maintain, and sometimes generate so much information that it requires a dedicated team to review the data, particularly in the case of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).

An IDS and an IPS perform similar functions: both monitor either a network segment or a particular host and look to recognize patterns of traffic or access that represent an attack. An IDS generates logging information or alerts, and is considered a negative, or reactive approach, whereas an IPS automatically takes some action, such as modifying a firewall rule or breaking a TCP connection. An IPS is considered a positive or proactive solution.

Another form of network inspection is scanning inbound email at the server level. Specifically, network appliances or software running on the email server tries to determine if a piece of email is spam, and even if not, if it might contain a virus. This is usually repeated again by an endpoint anti-virus scanner. Scanning email at the server level allows it to be rejected before reaching the user's mailbox, and protects network and server performance.

Endpoint protection: your desktops and laptops

In many organizations, everything described so far is considered essential. However, it pales in comparison to the importance of protecting your endpoints—your desktop PCs and your laptops.

There are five elements to discuss in the context of layered defense with regard to endpoint protection—your desktops, laptops and virtual machines. Using them together builds a very solid endpoint protection scheme that goes a very long way to keeping PCs secure and users productive.

These include:

► **Appropriately keeping up-to-date with patches**

Any PC that is not kept reasonably up-to-date is just waiting to be attacked. A software publisher issuing a security update is similar to a vehicle manufacturer issuing a safety recall. However, unlike in the vehicle analogy, once an update is announced, hundreds of malware writers immediately begin trying to find ways to target and exploit unpatched systems.

Consider using Windows built-in automatic patching systems, or any one of a number of tools built for enterprise-wide testing and management of updates.

► **Using host-based firewalls**

Although a network firewall can only protect at the boundary of network segments, the host-based firewall can drop unwanted packets at the point where they reach the PC, regardless of where they originated. This comes with no performance penalty, and single-handedly stops many worms and denial-of-service attacks. However, to be most effective, this requires active consideration of how the host firewall is configured. Again, consider enterprise-wide tools to manage the firewall built into every modern client operating system.

- **Using desktop anti-spam**

In some environments, spam is an almost uncontrollable problem. In others, it's just a nuisance. In addition to anti-spam at the mail server, solutions that run on the client PC are also available (the most common is the Outlook Junk Mail feature). Running anti-spam on each client PC may allow greater control for each user's individual preference and tolerance. Anti-spam should be considered in your security plan, because spam is the leading source of initial virus distribution and phishing, a practice of stealing personal information for fraud or identity theft.

- **Application control or whitelisting**

Locking down what applications are allowed to run on a client workstation or a server is an excellent strategy. By preventing unknown executables from running in the first place, you can help protect systems and increase user productivity. Some application control functionality is built into Windows, but additional protection and management can be found, for instance, from the sponsor of this whitepaper. For more information, learn about Faronics Anti-Executable, which was discussed in the companion paper "Defense in Depth: How Application Whitelisting Can Increase Your Desktop Security."

- **Instant system restore**

The ability to quickly recover after any breach of security is essential. While it's best not to have a problem in the first place, a complete layered defense plan will discuss how to respond to a problem, and how to respond quickly. Re-imaging a computer from bare-metal to a baseline image is tedious and time-consuming. And, when complete, the users' data and personalized settings are simply gone. Consider using a product like Faronics Deep Freeze, which allows an instant recovery to a known pristine state without losing user data or personalized configuration settings.

This also gives the ability to recover from non-security events, like user error, software misconfiguration, and to re-provision or retask computers immediately.

- **Anti-virus**

Anti-virus is last on this list, but it isn't last on the list of importance. We'll discuss this crucial element in detail in the next section. It is essential in today's corporate world of information that endpoints—PCs and Laptops—be protected with an effective anti-virus solution.

Focus on anti-virus

Let's turn our attention now, specifically to anti-virus: why it's necessary, what current solutions tend to include, and what an ideal solution might look like. Occasionally, you may encounter people who don't feel anti-virus is necessary. They may be concerned about costs, or about performance degradation, or others who think that the firewall will stop all the bad guys, or others who feel they are protected adequately with other layers such as application whitelisting.

Consider the following points:

- **Cost**

Anti-virus costs less than a security breach. As the phrase goes, "An ounce of prevention beats a pound of cure."

- **Performance**

It is important to choose an anti-virus product that performs well. You'll want to find a balance between effectiveness in virus scanning and protection and the leverage of resources on the PC. Investigate solutions that are available and show no perceptible performance degradation on modern hardware performing standard business tasks.

- **What if I already have application whitelisting?**

Some applications simply must be allowed to run, and some of them can still be at risk from virus packaged in common containers, such as JPEG or Adobe Flash, both of which have seen vulnerabilities at various times.

More importantly, however, is the class of non-executable viruses: malware lurking in innocent-looking non-executable files that are not checked by the application whitelist.

In addition, IT needs to ensure that the reference machine is free of threats. Of course, the whitelist should be double-checked to ensure that "bad" applications don't allow any viruses to be downloaded or executed!

- **Compliance & Expectations**

Almost all public and regulated businesses will be considered to be required to have anti-virus as part of due diligence. In other words, you may not have a choice whether or not to deploy anti-virus due to regulatory compliance; in which case you should make the best choice of what to deploy.

"Ideal" anti-virus

Let's turn our discussion to what would make an anti-virus solution an ideal candidate for adoption. What features and properties would give most business environments a good balance of what's needed?

The task that you face when you select an anti-virus solution is finding a product that marries the features and facets that matter to you. As you're evaluating an anti-virus solution, here are some things IT managers and IT pros should be particularly concerned about:

- **Rock-solid underpinnings**

It is absolutely essential that the anti-virus engine be stable and reliable. Normally, the engine is going to be involved in every file operation conducted on the PC, so the anti-virus application must always work reliably and in a rock-solid fashion.

- **Minimal impact on the operating system and applications**

This area has seen great improvement over the last few years, but there are still some anti-virus products that impose too much of a performance hit on the operating system itself, and therefore slow down overall operations for users. When performing an on-demand virus scan as a foreground application, we would expect the anti-virus impact to be obvious; however, when scanning in the background, you want to minimize degradation.

Ensure that the product doesn't add much to the computer's start-up time as well. This is a commonly overlooked problem, and one that doesn't get enough attention.

- **Detection rates**

No anti-virus product detects everything. Examining test results, such as the RAP testing done by the Virus Bulletin (http://www.virusbtn.com/vb100/vb200902-RAP-tests) shows that the top nine products detected upwards of 90% of the known viruses in the test sample, there are still vendors that identify as low as 23%.

Since detection is quite high across the industry leaders, various differentiators ought to be used to determine which anti-virus solution is right for you. That is, the other categories in this section should have a higher weight than detection because detection is quite good amongst all the top vendors.

- **Heuristics**

The attackers and virus authors constantly change their tactics. One way in which they do so is to either automatically or manually create infinite variations on existing attacks. Heuristics in an anti-virus program means that the software extrapolates from a known threat and applies algorithms to detect that a new threat may exist. When designed badly, heuristics can lead to false positives; but when done correctly, they can be a valuable tool in your arsenal against new threats.

- **Publisher's quick response to new threats**

When a new virus is released, it is important that the anti-virus publisher can update their signature files quickly, and get them propagated out to your site and each client on your network, quickly. This means that the publisher needs to have enough staff and infrastructure to respond in a timely way.

The increase of zero-day attacks, where a piece of malware appears before the software publishers have published a code patch, makes the responsiveness of the publisher of great importance. Also look for products which include a method to protect against attacks that haven't been created yet: for example, if Microsoft announces a security update to Windows, you can be assured that attackers immediately start coding to exploit it. The better anti-virus producers start working on ways to identify those potential attacks immediately, as well. This approach is also a key benefit of application whitelisting.

- **Management**

A good anti-virus program should be easy to manage. This can mean one of two approaches: either the anti-virus solution must slide seamlessly into existing tools and processes, or the vendor provides a management tool with added value and features not available as part of current processes or tools, that clearly shows value that makes it worth adopting.

When you're auditioning an anti-virus vendor's management tools, ensure that it fits in with the way your team works or is easy to slide in to your existing IT processes.

- **Deployment**

Along with being easily managed, it must be easily deployed. You shouldn't need to personally touch each PC during deployment, or, worse, to troubleshoot it. It's essential that new computers can automatically receive the anti-virus programs and settings during the regular provisioning onto the network.

Like management, you want to ensure that the anti-virus client deployment fits in with your existing IT processes or, if it's a new process, is similarly easy to fit in with existing processes.

- **Configuration**

The anti-virus solution should work out of the box, but allow the IT administrator to tweak settings as needed. You'll want to ensure that notes and messages added to the bottom of outbound emails by your anti-virus product can be reworded or turned off; pop-up notifications should be able to be suppressed; heuristics should be able to be adjusted or disabled; etc. This allows you to adjust the product to your environment, your risk tolerance, and your needs.

- **Appropriate amount of information**

Too many products deluge the end-user with too much information, creating unnecessary help desk calls or inciting panic attacks when the user sees a big red "x" with a virus warning. On the other hand, some products simplify the interface and reporting information so much that the administrator cannot get any details, either. Information needs to be available when needed, but not pushed out needlessly as interruptions.

► Granular reporting

For management and analysis, a corporate anti-virus program needs to provide both summary and detailed information. Often this is in the form of "drill-downs" or interactive reports. Ideally, reports can be customized and new reports can be created by the IT administrators on demand.

► Seamless updates

Anti-virus products generally rely on having up-to-date signature files that describe the latest threats. Clients will normally update themselves through a hierarchy on the local network, which also provides an opportunity to update settings and policies specific to your organization, and to receive reports back. However, if the endpoint PC is mobile, as many are, they may not be able to receive the updates from the LAN.

Therefore, clients must be able to update from the office LAN or from the public Internet, seamlessly and without user intervention.

► Integrate with other levels of protection

Earlier, we described many levels of defense that should be combined to work together. Unfortunately, too often these levels do not coordinate well with each other; sometimes even within one product line.

A great example of layer miscommunication is when the application whitelisting is inadvertently configured to prevent the anti-virus application from updating. Another example is when a quick-recovery product automatically undoes the latest signature update.

It's important that your anti-virus solution and the rest of your defenses work together – not against – each other layer. Ideally, these products will use common management tools, interfaces and reporting.

► Quality of customer support

The quality of customer support that an anti-virus vendor can provide your team is paramount. Support should be responsive and knowledgeable, ensuring any issues experienced are dealt with immediately without exposing your environment to any additional risks or threats.

► Cost effective

Lastly, this has to be cost-effective. One of the premises of security is that you don't spend more to protect something than what it's worth. It's hard to place a value on data and user productivity, but that doesn't mean you can spend limitless amounts on anti-virus.

In fact, by examining things like management, deployability, seamless updates and integration with other levels of defense, you can usually maximize your investments, and often lower your costs.

From Byron Hynes and Faronics – Introducing Faronics Anti-Virus

When evaluating the options provided by current anti-virus products, consider Faronics Anti-Virus Enterprise. In this section you can learn if Faronics Anti-Virus is right for your environment. Here are some common questions and answers:

Q: I understand that deployment of the anti-virus client should be easy. What is Faronics' solution to easy deployment and management?

A: Faronics Anti-Virus is managed and deployed with Faronics Core, Faronics' complimentary network management platform. You have one central place to see all managed computers in your environment, even if they are not members of a Windows domain.

Faronics Core can quickly discover computers on your network, send the anti-virus client to them and do the installation without any user interaction.

Optionally, you can send an installation package to the client via Group Policy, SCCM or your own software management system. Or, you can also use the package to manually install clients across a network or from removable media.

Q: Management is often the hardest part of any system. What does Faronics Anti-Virus do to help me manage my new investment?

A: Once the end-point is in the Faronics Core database, each computer can be configured, examined and reported on. Anti-virus settings can be defined in policies and remotely applied to an individual computer, a group of computers, or your entire enterprise. Selection parameters are very flexible, computers can be grouped by their configuration settings, or physical location.

Q: I am interested in a layered defense approach. What other solutions can I utilize to establish a solid layered defense perimeter?

A: In addition to anti-virus, Faronics offers an application whitelisting solution, Faronics Anti-Executable, and an instant system restore product called Deep Freeze.

Although Faronics Anti-Virus is one of the most effective anti-virus solutions on the market, it cannot control unauthorized or unlicensed applications that are not malicious. Faronics Anti-Executable automatically creates an approved "whitelist" of applications permitted to run, and denies all other programs from running.

Faronics Anti-Executable is also the most effective method for preventing new "Day Zero" executable malware from running on your systems. It was designed to work with Faronics Anti-Virus and accommodate virus definition and engine updates without reconfiguring the whitelist or relaxing security policies.

Download a free 30 day trial of Anti-Executable here.

Deep Freeze is 100% effective in removing any configuration changes on a protected workstation with every restart. The absolute majority of malware requires a reboot in order to become active. Even if such threats penetrate the layer of active anti-virus or application whitelisting, Deep Freeze can eliminate such threats upon restart. Deep Freeze was designed for integration with Faronics Anti-Virus, allowing definition updates to be retained between restarts even on protected end nodes.

Download a free 30 day trial of Deep Freeze.

Q: How will I notice malware found in my organization?

A: The Faronics Core console includes extensive reporting options. In addition to a variety of detailed and summary reports for anti-virus, reports for Anti-Executable and Deep Freeze can be created.

Q: Is Faronics Anti-Virus proven, stable and fast?

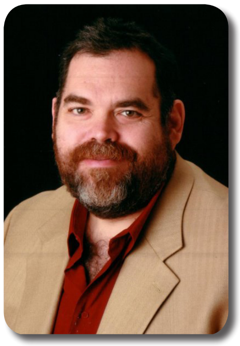
Although the Faronics Anti-Virus solution is new, it is built on Sunbelt Software's highly regarded VIPRE anti-virus technology. VIPRE is well-known for being light-weight in resource usage but a "heavy" in detection and protection. West Cost Labs, a prominent security certification and accreditation organization has awarded Faronics Anti-Virus its feature Checkmark certification. You can also visit www.faronics.com to check out recent testimonials and case studies of Faronics Anti-Virus, Anti-Executable, and Deep Freeze.

Q: How will I address my various Windows machines (Windows XP, Windows Vista, Windows 7, Windows 2003, Windows 2008, Windows 8.1)?

A: Faronics Anti-Virus is available for all currently supported versions of Windows, including 32 and 64 bits versions of Windows XP, Windows Vista, Windows 7, Windows 8.1, Windows Server 2003, and Windows Server 2008.

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. 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 Anti-Virus ensures proactive, resource-efficient malware protection without compromising system performance. It combines anti-virus, anti-spyware, and anti-rootkit technologies into an efficient solution that seamlessly integrates with Deep Freeze, so definition updates will occur even while workstations are protected in a Frozen state.

Deep Freeze helps reduce IT costs and requests by making computer configurations indestructible. Once Deep Freeze is installed on a workstation, any changes made to the computer, regardless of whether they are accidental or malicious, are automatically eradicated with every reboot. User data can still be saved in Thawed (unprotected) partitions.

Faronics Anti-Executable and its whitelisting technology ensures total endpoint productivity by only allowing approved applications to run on a computer or server. Any other programs, whether they are unwanted, unlicensed, or simply unnecessary, are blocked from ever executing. Systems and users remain in full-compliance at all times without the need for constant IT attention.

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.

Contact Us

Address: **USA**
100, W. San Fernando Street, Suite 465
San Jose, CA 95113, USA
Phone: +1-800-943-6422
Fax: +1-800-943-6488

Canada
1400-609, Granville Street, PO Box 10362
Vancouver, BC V7Y 1G5 Canada
Phone: +1-604-637-3333
Fax: +1-604-637-8188

Web: www.faronics.com
Email: sales@faronics.com

Europe
8 The Courtyard, Eastern Road,
Bracknell, Berkshire,
RG12 2XB, England
Phone: +44 (0) 1344 206 414
Email: eurosales@faronics.com

Singapore
20 Cecil Street, #104-01 Equity Way,
Singapore, 049705
Phone: +65 6520 3619
Fax: +65 6722 8634
Email:
internationalsales@faronics.com.sg

Copyright