Understanding Strengths and Weaknesses of Host-Based Intrusion Prevention Styles

Gartner RAS Core Research Note G00137366, Neil MacDonald, 30 January 2006 RA1 06132006

No single style of host-based intrusion prevention provides sufficient protection. By using multiple styles of protection, you can create, overall, a more effective host-based intrusion prevention system strategy appropriate to your needs.

ANALYSIS

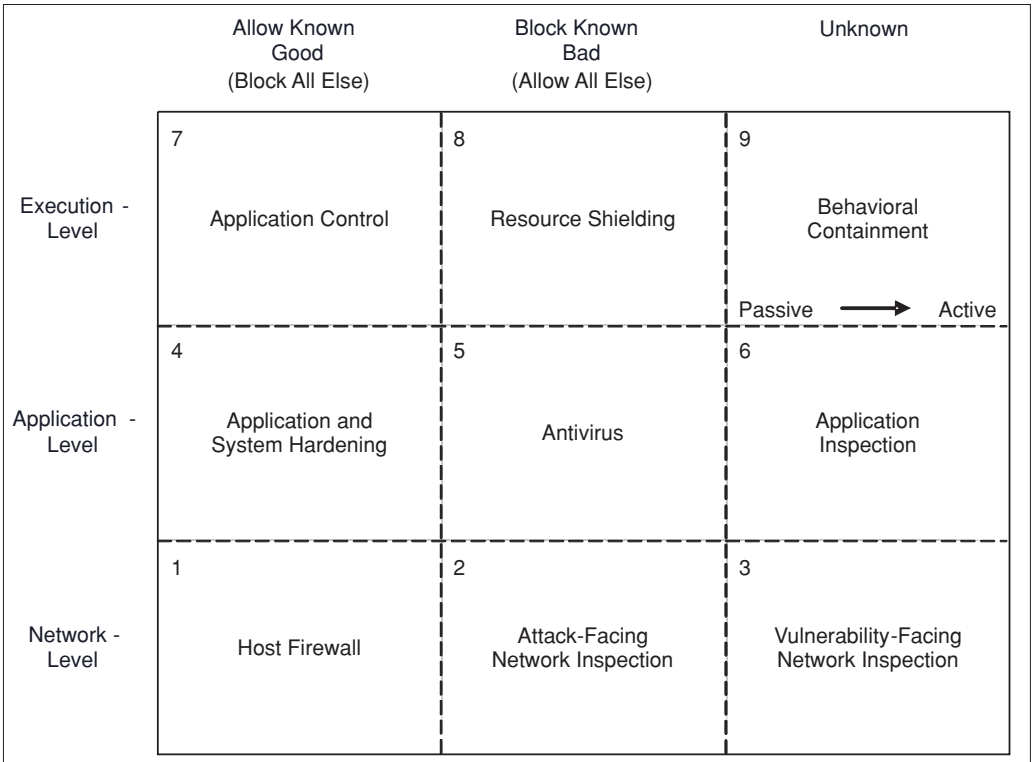
In previous research we introduced a framework for understanding the different protection styles and technologies in the market for host-based intrusion prevention systems (HIPSs). Since then, we have been asked, "What's the best HIPS protection style?" The answer is that there is no "silver bullet." No single protection style alone provides sufficient protection, and different organizations have different needs. Each style has its strengths and weaknesses. By combining styles, you balance these for a more effective intrusion prevention *system* – the "S" in HIPS. Through 2010, the best HIPS strategy for desktops and servers will use a combination of HIPS protection styles. Furthermore, your HIPS protection strategy for protecting servers will likely be different than for desktops, which will be different than for embedded devices, which will be different than for other organizations with different protection needs.

Enhancing Gartner's Nine Styles of HIPS Framework

Since introducing the HIPS framework, we have made some slight changes to make it easier to apply (see Figure 1):

- We have made the lines between the styles dashed. Many of the technologies will overlap in their protection styles as the offerings converge during the next several years. Nine different solutions are not needed!

Figure 1. Three Levels and Nine Protection Styles of HIPS



Source: Gartner (January 2006)

Gartner

- We have reordered the columns, placing the "allow known good" styles of protection in the first column (discussed in more detail later).
- We have renamed the top level of the model from "behavior-level" to "execution-level" to more accurately represent the protection this level provides (see Note 1).
- We have clarified the naming of Style 1 protection from "personal firewall" to "host firewall" to clearly include both desktop and server-based firewalls.
- Finally, we have modified the names slightly of Styles 4 and 7. Style 4 has been expanded from "system hardening" to include "application and system hardening." Style 7, previously described as "application hardening," is now more accurately described as "application control."

Analyzing the Strengths and Weaknesses of Each Level in the Framework

Level 1: Network-Level HIPS

Strengths

HIPS protection styles that operate at this level have the advantage of identifying and preventing threats in the network traffic stream before they have a chance to get on the machine. Thus, these styles avoid having to deal with the difficult issue of removal of the malicious code later. They also catch outbound threats before they have a chance to leave the machine, reducing the chance of malicious code propagation. Whether inbound or outbound, many network-based worms never manifest themselves as files, so the best place to catch them is in the network traffic stream. By deeply inspecting the network traffic stream based on knowledge of vulnerabilities, this level should provide protection against unknown attacks. Because the protection styles at this level typically operate at Layer 3 in the Open Systems Interconnection (OSI) model, they are largely transparent to the applications that run on the machine (other than CPU overhead). Network perimeters are porous and for highly distributed networks or encrypted traffic, such as Secure Sockets Layer (SSL), network-based intrusion prevention systems may not provide full protection, and HIPS solutions at this level may be the best place to perform inspection. This level of protection is important for mobile devices that will move outside of network perimeter security protection (for example, Style 1 should be in all laptops).

Note 1
"Behavioral"
The execution level of HIPS protection analyzes the interaction of an application with its host (for example, system calls, resource access and kernel calls) as the application executes; thus, "execution-level" or "system-level" interactions more accurately describes what happens here. The term "behavioral" is overused in the industry and contributes to confusion over how different HIPS solutions provide protection. True behavioral analysis occurs only in Column 3 of the framework, and the most-complex behavioral analysis occurs in application simulation before applications execute (Style 6) or as applications are executing (Style 9).

Weaknesses

Delivering Styles 2 and 3 of protection requires deeper packet inspection, which will introduce processing overhead on the machine and latency into application traffic streams and may not be appropriate for heavily loaded servers or extremely latency-sensitive applications. This level of protection is also a candidate to be performed entirely using network-based IPS technologies for nonmobile desktops and servers. The ability to detect file-borne viruses at this level is minimal, because scanning file attachments for malicious code requires file reassembly, slowing performance and introducing more latency. While network-level encrypted traffic is decrypted and inspected, application-level encrypted traffic is an issue. HIPS solutions at this level only analyze the network stream and therefore miss attacks that may be introduced via a different channel – for example, CD, DVD, Universal Serial Bus (USB), Bluetooth and so on. There is the possibility that dropped packets created by a false positive could create a denial of service on applications above it. Finally, other than malformed protocol attacks, it is more difficult to detect a true

© 2006 Gartner, Inc. and/or its Affiliates. All rights reserved. Reproduction of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

zero-day or targeted application attack that is based on an unknown vulnerability with protection styles at this level.

Level 2: Application-Level HIPS

Strengths

HIPS protection styles at this level have an advantage in that the files they examine are on the machine, making this level the best place to catch malicious code that manifests itself as a file by checking files already on the machine, as they are stored or before they are executed. Style 4 offers application and system hardening capabilities before deployment to protect these systems and applications in deployment. Hardening is best-suited for systems and applications that rarely change (such as embedded systems) or where you want to introduce strong change management controls. Legacy antivirus products hold the anchor position in Style 5. File-based, signature-based malicious code protection (also known as antivirus) is not "dead"; it is simply commoditized and no longer sufficient for comprehensive HIPS protection. Because this level deals with application files, any malicious code identified should not be allowed to be saved onto the machine or, if it is saved, must deal with the issue of quarantine and, ideally, removal of the malicious code from the machine and repair of the infected file as appropriate – a strength of legacy antivirus products.

Weaknesses

This level of protection styles misses malicious code that never manifests as a file (for example, network-based worms). Style 4 hardens known good systems and applications before they are deployed, reducing the attack surface, but it still leaves open the possibility for attacks on vulnerabilities that were not hardened against. Style 6 provides protection against unknown vulnerabilities using a simulated execution environment, but it is extremely difficult to fully understand what a piece of code may do without executing it and observing its interactions with the machine and user.

Level 3: Execution-Level HIPS

Strengths

HIPS protection styles at this level provide protection as the application is executing by monitoring interactions of the code with its host system (typically, with kernel-level drivers). This is the best way to prevent "good code gone bad" – attacks against unknown vulnerabilities in underlying applications or zero-day attack protection against unknown vulnerabilities. Style 9 at this level should detect abnormal behavior in applications as they execute, potentially providing detection of targeted attacks, zero-day attacks, and inspection of potentially malicious software not yet known to be good or bad. Because these styles monitor interactions with system resources, solutions at this level should also control access to system resources, such as USB ports and other types of removable media.

Weaknesses

Any of the HIPS protection styles at this level can introduce denial-of-service conditions on applications they protect if the application is determined to be malicious and shut down. For this reason, some organizations are reluctant to deploy protection styles at this level on production servers. Also, protection styles at this level typically don't deal with the important issue of malicious software removal because most solutions do not keep a full record of what the software did during the installation process. Finally, using multiple kernel-level driver-based products increases the chance of conflicts.

Analyzing the Pros and Cons by Column: An Alternative View of the Framework

We have moved the "allow known good" styles of protection into the first column in the revised framework in Figure 1 so that as we move from left to right in each of the three columns, the protection styles progressively screen more and more malicious code (see Note 2).

We represent this progressively finer, layered filtering approach to HIPS in the overlaid pyramid shown in Figure 2 and separately in Figure 3. Ideally, HIPS protection styles in Column 1 are used as the first layer of defense to detect and prevent malicious code. Protection styles in Column 2 form the second line of defense. The final column of protection styles is the final line of defense and is used for code that we don't know is good or bad.

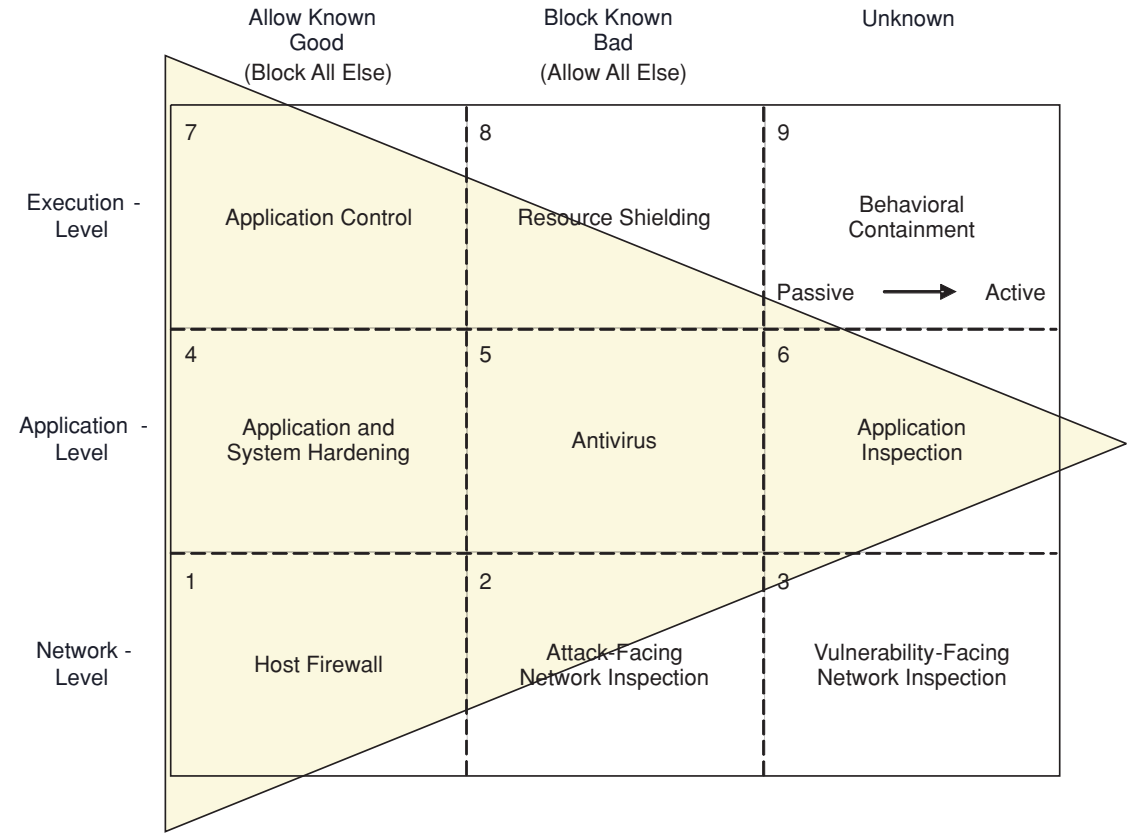
Note 2

Three Levels of Progressively Finer Filters

As an analogy, think of progressively filtering rocks with three sets of filters. The first set of filters has bigger holes but blocks the biggest rocks. The next set of filters gets the medium ones, and the final set of filters is used when something has made it past the first two sets of filters. Each filter has its strengths and weaknesses, but combined together, they create an efficient and effective filtering system. The same is true with HIPS protection styles.

Another analogy would be the human immune system, in which the first level of protection is provided by the skin, mucus membranes, sweat, enzymes and other types of perimeter protection. By blocking most attacks at the perimeter, the rest of the immune system can focus on threats within the body. In other words, the rest of the immune system works best when it doesn't have to. The next level in the human immune system would be represented by phagocytes. Most often this involves macrophages cleaning up the known bad marked with antibody signatures. The final level in the human immune system would be represented by the specific (adaptive) immune system, in which new threats (antigens) are identified through a learning process, thus providing the ability to respond to previously unknown threats. In either analogy, the first layer provides the bulk of the protection, the second layer provides more protection than the final layer and the final layer protection is adaptive, to be used in detecting the truly unknown threat.

Figure 2. Three Layers of Defense



Source: Gartner (January 2006)

Column 1 (Bottom Layer of Pyramid)

Column 1 becomes the foundation of the pyramid shown in Figure 3. This layer of the pyramid represents "allow known good" (also known as whitelisting) styles of protection – often referred to as "firewalling" technology (network firewalls, application firewalls and so on). Protection styles in this column depend on an accurate rules and configuration database that tells the protection styles what defines "goodness" at each level.

Strengths

Protection styles in this column introduce the least chance of a false positive as long as the rules and configuration database that define "goodness" at each level is configured correctly and up to date with the most recent system and application changes.

Weaknesses

Protection styles here work great for a point in time, but systems and applications change, especially on desktops. To reduce the chance of a false negative, protection styles in this column may set very granular rules – for example, Style 7 process-level controls on network, registry, file system and system application programming interface (API) access – but this creates a significant issue with the ongoing care and feeding of the rules configuration database (see Note 3). Finally, protection styles in this column won't protect against "good applications gone bad" – that is, where a legitimate application is compromised by an exploit against an internal vulnerability – if the compromised application still conforms to the rules defined for it.

Column 2 (Middle Layer of Pyramid)

Protection styles here are represented by the middle layer of the pyramid in Figure 3. This layer represents the "block known bad" styles of protection – often referred to as "signature-based" (also known as blacklisting) protection styles, the best known of which is file-based antivirus protection technologies. Protection styles in this column depend heavily on up-to-date signatures that tell the protection styles what defines "badness" at each level.

Strengths

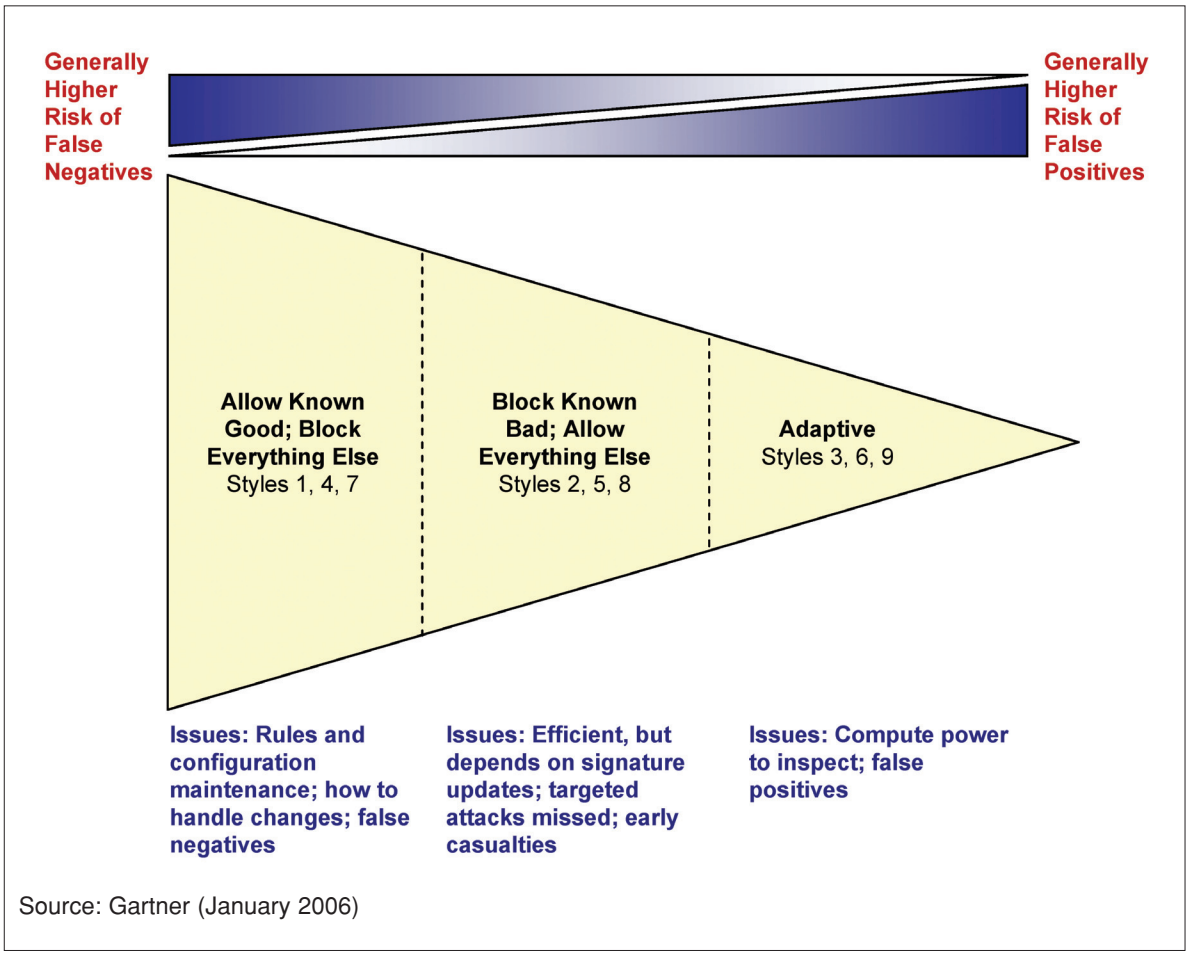
Protection styles in this layer provide the best balance of false positives and false negatives against known threats. Signature-based detection of malicious code is efficient and effective, assuming the signature files are up-to-date and high quality.

Weaknesses

The signatures must be up-to-date. Thus, solutions here must deal with the issue of providing signatures to remote and mobile users with cached or alternative sources of signature feeds. Ideally, the

Note 3
Care and "Feeding" of Application Control Products
To offset the chance of false negatives, Style 7 products can tightly control applications as they execute. However, the complexity and resources required to maintain an accurate rules and configuration database is the single biggest issue with products, such as Cisco CSA, McAfee Entercept and Symantec CSP, and other products that provide solutions that provide very granular application control. Some vendors, such as Sana Security, overcome this drawback by monitoring the application's behavior over time and building the rules and configuration database automatically. This introduces its own set of issues if the application environment changes frequently (for example, a desktop in which users are allowed to download and execute unknown applications and browser helper objects). In these scenarios, the configuration may never settle down enough for the product to provide useful protection. Alternatively, other basic application control solutions provide little granularity (for example, controlling only whether the application runs or not) but incur an increased chance of a false negative. Ideally, the rules and configuration database would be automatically built as applications are developed and deployed, but this evolution will take years.

Figure 3. Three Layers of HIPS Protection



Source: Gartner (January 2006)

updated signatures could be received from any network connection; however, if users are without any network connectivity for an extended period, they are vulnerable to newer attacks in which the signature has not yet been received. Also, the signature-based model is very much dependent on a certain threshold of users being attacked. Targeted attacks are missed. Variants of attacks that evade existing signatures are missed and potentially result in large numbers of signature updates (and large signature files) for file-based signature approaches (see Note 4). Some exceptions exist to the issues associated with signatures in Style 8 (see Note 5).

Column 3 (Top Layer of Pyramid)

Strengths

Protection styles here are represented by the top layer of the pyramid in Figure 3. This layer of the pyramid represents the "adaptive" styles of HIPS and represents the most promising but least mature of HIPS solutions. Protection styles in this layer of the pyramid offer the best protection against targeted and zero-day attacks against truly unknown vulnerabilities. These protection styles require contextual inspection and typically provide a way of learning and modeling goodness and badness to detect and prevent unknown attacks against known and unknown vulnerabilities.

Weaknesses

Because of the contextual inspection required by these protection styles, more system resources typically are needed. Because of the heuristics, learning and modeling involved, protection styles in this layer of the model tend to have the highest chance of producing a false positive. For these reasons, these styles of protection are reserved at the top of our pyramid.

Note 4
Example of the Variant Problem
A piece of malicious software known as "Tibick" was identified in 2004. As of this writing, Symantec lists more than 329 variants on its Web site. From July through December 2005, Prevx tracked 2,151 unique Tibick variants (various name and payload combinations), 761 of which contained unique payload signatures. For traditional file-based signature products (also known as antivirus), carrying around large monolithic signature files of every possible variant of malicious code a user might ever encounter is inefficient. As an alternative to file-based signature approaches, Prevx is one example of an execution-based signature approach that overcomes some of these issues.

Note 5
Style 8
A subset of HIPS Style 8 protection styles provides a "big bang for a security buck" solution without the huge complexity of managing signatures. Essentially, some Style 8 HIPS solutions enforce the simple rule/signature that there are some things executing applications should never do. Buffer overflow is one example. Overwriting system files is another. Here, these "universal signatures" of badness are relatively static and as such are easy to manage (a buffer overflow is always bad; users don't need to have a signature update to tell them this). We are frequently asked, "What HIPS solution will give me the biggest bang for my security investment?" Our answer is to purchase no execute (NX)-enabled hardware, upgrade to XP service pack 2 (SP2), and activate NX protection at a minimum on the Windows operating system and system files, and ideally on all applications.

Note 6
Vulnerability-Facing Inspection
One technique used here is to model what bad behavior would look like based on specific knowledge of underlying vulnerabilities. For example, if you know that lsass.exe is subject to a specific type of buffer overflow, then you inspect for code that uses lsass.exe and if so, inspect the code more deeply for any attempt to overflow the vulnerable buffer, thus catching all variants of malicious code that may attempt to exploit the vulnerability. Vulnerability-facing inspection is a powerful technique at this level.

One of the main concerns with any protection style in this column is how to reduce the chance of a false positive while analyzing unknown code. One approach is to model what bad behavior would look like and then inspect for similar bad behaviors in the unknown code to determine if it is bad (see Note 6). Alternatively, you could model what good behavior looks like and inspect for differences from the good behavior in the unknown code to determine if it is bad. Some vendors use heuristics (multiple techniques), which combine knowledge of good and bad application behaviors to develop an overall assessment of an application's goodness and badness to help in the final determination of whether an application is malicious.

Bottom Line

There is no host-based intrusion prevention system silver bullet. No single protection style alone provides sufficient endpoint protection. The best HIPS strategy uses multiple styles of protection for an overall comprehensive HIPS solution. By combining multiple styles of protection, you can balance false positive and false negatives, optimize your resource requirements, and provide robust threat protection against known and unknown attacks and vulnerabilities that is appropriate to your needs.