Gartner

Research

Publication Date: 27 May 2005 **ID Number: G00127317**

Understanding the Nine Protection Styles of Host-Based Intrusion Prevention

Neil MacDonald

Many technology providers are entering the market with host-based intrusion prevention systems using markedly different protection approaches. The multiple offerings are distilled into three levels and nine distinct protection styles. The best HIPS will use multiple protection techniques.

© 2005 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.

WHAT YOU NEED TO KNOW

All security frameworks should include a comprehensive, layered approach for providing host-based intrusion prevention. Use our framework of the nine host-based intrusion prevention system protection styles to understand which style or combination of styles is right to protect your servers and desktops. We believe, at a minimum, in addition to personal firewalls, that any endpoint security strategy should provide for network-level intrusion prevention system traffic inspection — whether done in the network or on the endpoint — by the end of 2005. Through 2010, we believe the best HIPS strategy for desktops and servers will use a combination of HIPS styles across all three levels for optimal protection.

ANALYSIS

The time for a more complete approach to host-based intrusion prevention is here. Traditional antivirus and personal firewall solutions are no longer sufficient to protect endpoint systems against targeted application-level attacks, and we can't keep our systems patched as quickly as new vulnerabilities are announced. As a result, we have seen a large number of products enter the market, and they are described as host-based intrusion prevention systems (HIPS) (see "Host-Based Intrusion Prevention: Ready for Servers, Not PCs"). However, the technologies and mechanisms to perform the detection and blocking of intrusions vary greatly, and some of them overlap with existing antivirus and personal firewall functionality. We introduce a three-level framework for comparing the nine foundational protection styles of HIPS so that you can better understand where providers and solutions fit, how each style differs in its approach to providing protection, and how traditional antivirus and personal firewall products fit into an overall host-based intrusion prevention strategy.

The Three Levels (and Nine Protection Styles) of HIPS

Consider a piece of code designed to be executed on a desktop or server. The three possible states the code will be in are as follows:

- In the process of entering the machine
- Already present on the machine but not yet executing
- Executing on the machine

These map to the three broad levels of HIPS functionality: network-level, application-level and behavior-level. Each one of these represents a row along the left-hand side of Figure 1.

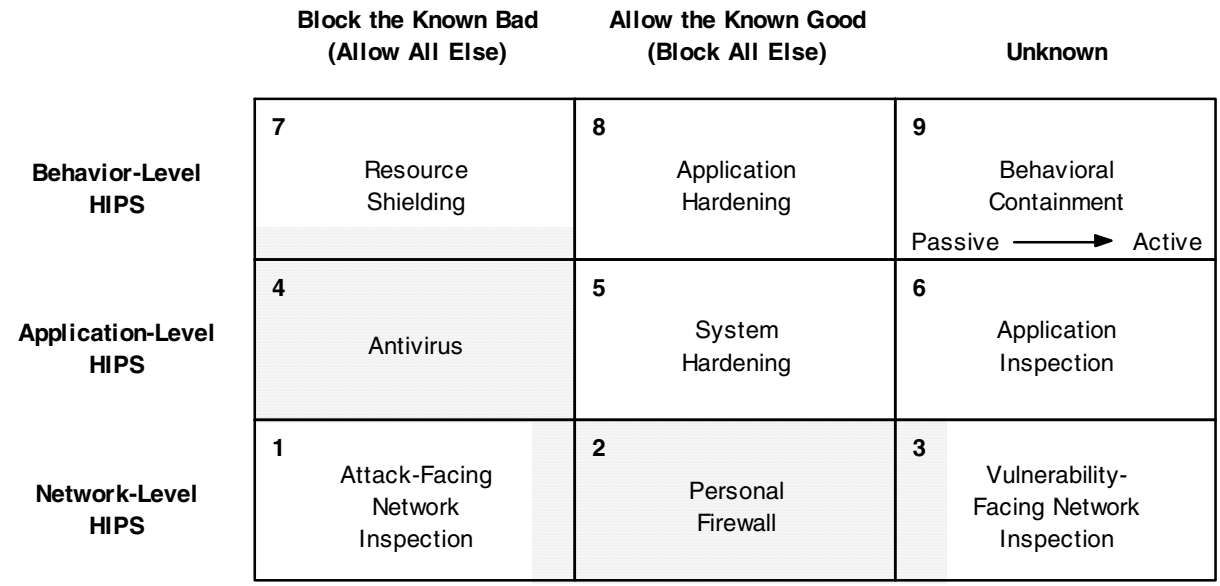
Now consider what we know about the code and its behavior at each level:

- It is known to be bad, so we want to block it (and allow everything else, also known as blacklisting)
- It is known to be good, so we want to allow it (and block everything else, also known as whitelisting)
- It is unknown.

These three levels of knowledge about the code are listed across the top of the three columns in Figure 1.

© 2005 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

Figure 1. Three Levels and Nine Protection Styles of HIPS



127317-01

Source: Gartner (May 2005)

By looking at all the possible combinations, we have collectively described the nine protection styles of host-based intrusion prevention. Each style has its strengths and weaknesses. For styles in the first column, blacklists are the least likely to create false positives but are reactive. In the second column, whitelists are straightforward to implement but require lockdown, and many IT departments can't lock down applications, especially for desktops. The third column is the most proactive and flexible, but it has the highest potential for false positives, and the contextual inspection required is typically more resource-intensive. Of the nine styles, it is likely that you have two of the styles already installed on many endpoints (that is, antivirus and personal firewall functionality). By looking across the nine styles of HIPS, you can more easily compare vendors, functionality and applicability and determine which combination of styles makes the most sense for your endpoint protection strategy. Many of the HIPS providers incorporate multiple styles of protection. Just as in network intrusion prevention system (IPS), Gartner believes the best HIPS will use multiple techniques.

Network-Level HIPS (Styles 1, 2 and 3)

Network-level HIPS (see Notes 1, 2 and 3) examine the incoming (and, ideally, outgoing) network traffic stream to provide protection against malicious code with the goal of detecting, blocking and removing the malicious code before it ever gets onto the machine. As shown in Figure 1, personal firewalls are well-established in the second column to provide network-level system protection by configuring what known good applications need to access the network and setting the firewall rules to allow this. Some provide screening for known and unknown attacks, overlapping with Columns 1 and 3. Emerging network-level HIPS provide capabilities beyond most traditional firewalls. The first column of network-level protection examines the network traffic stream for the signatures of known bad traffic — also referred to as attack-facing signatures. Protection at this level performs pattern detection and removal of known bad bits by using a signature "blacklist" of known attacks (for example, worms, port-scanning, operating system (OS)-fingerprinting, malformed protocols and so on). Deep packet inspection products in this category (for example, Third Brigade Deep HIP) can detect obfuscated attacks that span multiple packets and, in the

© 2005 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

future, viruses in reassembled attachments. The third column of network-level protection examines the network traffic stream for unknown malicious code but doesn't rely on attack-facing signatures for detection. In this HIPS style, vulnerability-facing behavioral filtering techniques are used for malicious traffic detection and removal. For example, rather than look for every variant of the Sasser worm using signatures, by inspecting network traffic for specific buffer overflow techniques, a single vulnerability-facing filter would detect all attacks, known and unknown, aimed at exploiting the Local Security Authority Service (LSASS.EXE). Vulnerability-facing behavioral filtering is more complex and resource-intensive than attack-facing inspection and requires deep-packet inspection, with some level of vulnerability contextual awareness — in some cases, by disassembly and simulation of embedded code (such as Check Point). In most cases, when malicious code is detected, vendors simply drop the malicious packets. However, some providers enable the ability to modify content within the packets. With deeper inspection, some providers offer the ability to understand the context of the conversation — for example, check for malformed HTTP and Structured Query Language (SQL) queries — and to modify content within an application context.

Application-Level HIPS (Styles 4, 5 and 6)

Application-level HIPS (see Notes 4, 5 and 6) examine the characteristics of an application's code on the machine with the goal of detecting, blocking and removing malicious code before it is executed. In the first column, traditional antivirus solutions are well-established and use signatures to detect and remove known malicious code. As shown in Figure 1, most antivirus solutions also will perform some real-time scanning of memory during execution and provide "known bad" memory protection as applications are executing, overlapping somewhat with the resource-shielding style above. The second column contains a style of HIPS that will lock down a system (also known as system hardening) based on a known good application configuration so that no other application can execute. Some providers also include the base OS in the hardening process. This style works well for embedded systems, fixed-function servers and kiosks that rarely change and that don't have users downloading unknown applications. The third column of this level represents the most complex style of an application-level HIPS. Here, the solution must inspect the application's code, look at the types of system calls and application programming interfaces (APIs) that are used, contextually understand the activities that the application would perform if it was executed and block potentially malicious code. This can be achieved by exercising the application's code paths using a simulated environment (for example, Internet Security Systems [ISS] Proventia Desktop) or by using reverse-engineering techniques to inspect code to determine malicious characteristics before the application is allowed to be saved or executed on the machine.

Behavior-Level HIPS (Styles 7, 8 and 9)

Behavior-level HIPS (see Notes 7, 8 and 9) examine the characteristics of executing code with the goal of detecting, blocking and removing the ability of executing malicious code to damage to the system. This level represents the last line of defense, because the malicious code has entered the system and is now executing. In the first column, we already discussed how some antivirus products will scan for the signatures of known bad executing applications. Furthermore, many HIPS providers can block signatures of known bad application behaviors (for example, no application should ever execute code from memory flagged for data usage, and no application should ever change OS files). Because many worms and viruses depend on buffer overflow techniques to install their malicious payload, this HIPS style detects and prevents installation of the payload but may result in a denial of service to the underlying process. Some of this style of HIPS is delivered as part of most OSs today (see Note 10).

In the second column, application hardening provides the ability to lock down a known good application's access to only those system resources it legitimately needs, including network ports,

© 2005 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

APIs, areas of disk, memory and areas of the registry. For known, profiled applications, the HIPS provider should include a rich library of application and usage profiles out of the box (see Note 11). Application hardening HIPS should also provide a learning mode for applications so that organizations may create additional profiles. Some newer OSs provide this style of HIPS today (refer to Note 10), and providers offer value by adding greater manageability and consistency across platforms. If the OS doesn't provide granular resource-blocking capabilities, application hardening HIPS providers either inset "shim" code between applications and resource access to "virtualize" or "sandbox" the application from its resources, or run the known applications in their own virtual machine. Then, rules are applied to enable known good applications to access only the resources they need to execute.

One of the drawbacks of application hardening is how unknown, unprofiled applications are handled. The final column of behavior-level HIPS — behavioral containment — contains the potential malicious behavior of unknown executing applications. Multiple technology approaches range from passive to active behavioral containment. Passive behavioral containment typically uses "sandboxing," virtualization or lower-privileged accounts to limit the damage from malicious applications. Here, HIPS providers (such as GreenBorder and SecureOL) create a completely virtualized environment for the execution of unknown code ("unknown" being contextually defined, such as all code from the Internet). Little or no attempt is made at behavioral monitoring or blocking. The malicious code is allowed to execute, but no damage to the underlying system is possible (but it also may affect the usefulness of the application). More-active containment solutions (for example, Finjan Software) apply rules for allowed and disallowed behaviors of the unknown code in the virtualized environment. Other active behavioral containment HIPS styles don't rely on virtualization and, instead, inspect and monitor the behavior of the application to detect and contain applications determined to be malicious. Some HIPS providers (such as Sana Security) monitor the application over time and look for changes in activities and divergence from normal patterns of memory access, systems access and so on, and typically they require a learning period to baseline normal behavior. Other behavioral containment providers (such as Whole Security) heuristically inspect executing applications against a large set of good and bad application behaviors to determine and stop malicious intent without requiring a learning period.

Key Issues

How will opportunities in the market be affected by competition, technology, and evolving user requirements?

Note 1

Examples of Network-Level, Attack-Facing HIPS Providers and Solutions

- eEye Digital Security Blink
- ISS Proventia Desktop (network inspection component)
- Kerio ServerFirewall (network inspection component)
- McAfee Entercept (network inspection component)
- snort_inline
- Sygate Personal Firewall Pro
- Third Brigade Deep HIP
- Panda Software ClientShield

© 2005 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

Note 2

Example of Network-Level, Personal Firewall HIPS Providers and Solutions

- See "Magic Quadrant for Personal Firewalls, 1H05"

Note 3

Examples of Network-Level, Vulnerability-Facing HIPS Providers and Solutions

- Check Point (Malicious Code Protector component)
- eEye Digital Security Blink
- ISS Proventia Desktop (network inspection component)
- Third Brigade Deep HIP
- Panda Software ClientShield

Note 4

Example of Application-Level Antivirus Providers and Solutions

- See "Magic Quadrant for Enterprise Antivirus, January 2005: Vendors Must Address New Malicious Code Threats"

Note 5

Examples of Application-Level System Hardening HIPS Providers and Solutions

- Solidcore
- Verdasys
- SecureWave's Sanctuary Application Control Desktop and Server

Note 6

Example of Application-Level, Application Inspection HIPS Providers and Solutions

- ISS Proventia Desktop (virus prevention system component)
- Panda Software ClientShield (genetic heuristics engine)

Note 7

Examples of Behavior-Level, Resource Shielding HIPS Providers and Solutions

- Bastille Linux
- ISS Proventia Desktop (buffer overflow protection)
- Sana's Attack Shield Worm Suppression (WS) (memory protection)
- Sana's Primary Response
- Symantec IPS

© 2005 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

- Check Point Integrity (memory protection)
- Kerio ServerFirewall (code injection protection)
- Windows' Data Execution Prevention
- NX hardware flag support in Linux, Solaris and Windows
- Prevx Enterprise
- Determina Memory Firewall
- eEye Digital Security Blink (Kevlar protection in v2.0)
- Windows System File Protection

Note 8

Examples of Behavior-Level, Application Hardening HIPS Providers and Solutions

- Argus' PitBull
- Cisco Security Agent (technology acquired from Okena)
- Kerio ServerFirewall (behavioral blocking component)
- Immunix
- ISS Proventia Desktop (application control component)
- McAfee Entercept
- Sana's Primary Response
- Symantec IPS
- Check Point Integrity (application control component)

Note 9

Examples of Behavior-Level, Behavioral Containment HIPS Providers and Solutions

More passive:

- Sun Microsystems' Solaris 10 containers
- BSD Jail
- GreenBorder
- SecureOL
- VMware ACE
- Microsoft Virtual PC
- Check Point Integrity Clientless Security Secure Browser

More active:

© 2005 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

- Finjan Software's Vital Security for Clients
- Sana's Primary Response (Active Malware Defense Technology)
- Whole Security
- Panda Software ClientShield (autonomous behavior analysis)
- Cisco Security Agent

We expect more vendors and OSs to provide capabilities in this area, as multicore and software- and hardware-based virtualization techniques become more common.

Note 10

OS-Based HIPS Capabilities

Microsoft has built-in support for the hardware-based NX flag with XP Service Pack 2 (SP2) and Windows Server 2003 SP1 and supports applications compiled with the “/GS” and “/SSEH” flags (see "Deploy Microsoft Windows XP SP2 in 2005"). Also, since Windows 2000, Microsoft has provided “System File Protection” for the protection of the Windows OS files. With Longhorn, we expect Microsoft to provide its initial process-level access controls for application hardening (technology acquired from Pelican). Solaris 10 provides support for the NX flag when running on x86 hardware and also adds support for Solaris containers and process-level access controls (capabilities brought over from Trusted Solaris). Linux has provided NX support since Linux 2.6.8, and SELinux provides process-level access control and application hardening capabilities.

Note 11

Pre-configured Applications, Roles and Usage Profiles

- Server applications — Web server software, database packages, Microsoft Exchange, Lotus Notes, enterprise resource planning packages and customer relationship management packages
- Server roles — Database server, e-mail server, file/print server, Active Directory server, domain controller and Web server
- Desktop applications — Internet Explorer with common plug-ins and Microsoft Office
- Desktop and server usage profiles — In addition to application and role templates, HIPS providers should include templates for different levels of lockdown (strict, medium or loose). For less-vulnerable applications, products should be able to operate with fewer rules to ease configuration management and testing issues.

Acronym Key

API	application programming interface
HIPS	host-based intrusion prevention systems
IPS	intrusion prevention system
ISS	Internet Security Systems
LSASS.EXE	Local Security Authority Service
OS	operating system
SP2	Service Pack 2

© 2005 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

SQL	Structured Query Language
SSEH	safe structured exception handling

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Level 7, 40 Miller Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Latin America Headquarters
Av. das Nações Unidas 12.551
9 andar—WTC
04578-903 São Paulo SP
BRAZIL
+55 11 3443 1509

© 2005 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

Gartner