

# LANDesk® Host Intrusion Prevention System

---

A New HIPS Solution that Stops Zero-Day Attacks in their Tracks



White Paper



## Table of Contents

Executive Summary .....	3
The Gathering Malware Storm .....	3
An Intelligent Defense: Host-Based Intrusion Prevention .....	4
Toward Layering and Consolidation of Security Techniques.....	6
Today’s State of the Art: LANDesk® Host Intrusion Prevention System .....	6
New Client HIPS Functionality .....	6
New Console HIPS Functionality .....	7
LANDesk® Host Intrusion Prevention System: A Feature Summary .....	8
Arm Your Enterprise for Today and Tomorrow .....	8
References .....	9

Copyright © 2007 LANDesk Software Ltd. or its affiliated companies. All rights reserved. LANDesk and Targeted Multicast are registered trademarks or trademarks of LANDesk Software Ltd. or its affiliated companies in the United States and/or other countries. Avocent is a trademark or registered trademark of Avocent Corporation or its subsidiaries. Other names or brands may be claimed as the property of others.

This document contains confidential and proprietary information of LANDesk Software, Ltd. and its affiliates (collectively “LANDesk”) and is provided in connection with the identified LANDesk® product(s). No part of this document may be disclosed or copied without the prior written consent of LANDesk. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in LANDesk’s terms and conditions for the license of such products, LANDesk assumes no liability whatsoever. LANDesk products are not intended for use in medical, life saving, or life sustaining applications. LANDesk does not warrant that this material is error-free, and LANDesk reserves the right to update, correct, or modify this material, including any specifications and product descriptions, at any time, without notice.

LSI-0624 05/07 JBB/NH

## Executive Summary

Zero-day attacks. No other vulnerability today strikes more fear into an IT administrator responsible for protecting the company's most valuable assets—its strategic information and the systems that store, process and communicate that information.

Firewalls and antivirus software remain an important line of defense against malicious code entering your computing environment—or worse, actually executing on employee desktops. But these traditional security techniques depend on the ability to stay ahead of the hackers by patching known vulnerabilities, identifying signatures of known malware and rejecting applications of unknown origin or function.

Sophisticated hackers know this, and are increasingly mounting attacks that take advantage of the unknown and unseen. They've even learned how to install rootkits to steal passwords and other sensitive information, create zombie computers, launch denial-of-service and spam attacks, and more—essentially controlling systems for their own purposes while remaining undetectable.

It used to be that a vulnerability could go exposed for months without being attacked, giving vendors plenty of time to create and distribute a patch. No more. Now it's the hackers who have the head start in the security race.

As hackers learn to maximize the damage they do, we're seeing a new epidemic of zero-day attacks. These exploits are designed to infect systems before vulnerability has been recognized and patched, or before a malware signature has been identified and incorporated in antivirus software.

## The Gathering Malware Storm

Antivirus software has long been the mainline IT defense for most companies, and is likely to continue to be an important security component for some time. But an antivirus solution, by itself, is no longer enough.

Writing for *NetworkWorld*, Ellen Messmer quotes Robin Bloor of the consulting firm Hurwitz & Associates as saying, "The criminals working to release these viruses against computer users are testing against antivirus software. They know what works and how to create variants. [It] isn't about viruses, it's about what should be running on a computer." In the same article by Messmer, Andrew Jaquith, security analyst at Yankee Group, notes that there has been an "explosion" in cumulative malware variants, with 220,000 unique variants expected this year—ten times the number released in 2002. Jaquith likens the flood of variants to a denial-of-service attack against antivirus labs, forcing far more signature changes than the labs can possibly handle.<sup>1</sup>

Antivirus solutions are effective only once a new threat has actually been discovered, a signature identified and published, and the signature installed on enterprise desktops and servers. In the same way, patching a software vulnerability requires time to discover the vulnerability, create a fix, publish the fix and install it. As illustrated by Microsoft's infamous "Super Tuesday," this patch detect-fix-deploy cycle can take a month or more.

While LANDesk's efforts have prevented infection in countless machines, even that kind of responsiveness by itself can't stop the damage of a zero-day attack. In the time it takes to notice a zero-day attack, analyze the corresponding software vulnerability, create a patch, make it publicly available, download and install it, millions of machines can potentially be infected with devastating results.

These zero-day attacks are on the rise. According to the eEye Research Team's Zero-Day Tracker, an informational archive for zero-day vulnerabilities, at least 38 zero-day vulnerabilities had already been discovered by the middle of the second quarter of 2007, ranging from a few to several hundred days of exposure. At least five of these vulnerabilities were still active (unpatched) as of May 8, 2007. And keep in mind that any given zero-day exploit may have been unleashed well before it is discovered, and may still be affecting machines well after a patch has been created.

As hackers are learning they can make money from such exploits—turning PCs into spam bots, mounting denial-of-service attacks, extorting software vendors and more—the problem will only continue to grow.

In fact, it has already grown out of control. Reporting on the 2007 CeBIT exhibition in Hannover, Greg McNevin quotes Mikko Hypponen, the chief research officer at F-Secure, a worldwide provider of antivirus solutions. Hypponen complained that the company can receive more than 40,000 tainted file submissions on any given day. “How can we deal with this avalanche? This is not just a battle between manufacturers of security software and some Internet criminals. It is a war between good and evil.”<sup>2</sup>

## An Intelligent Defense: Host-Based Intrusion Prevention

While traditional antivirus software and vulnerability patching remain crucial, they’re no longer sufficient to keep up with the arms race between unknown malware developers who can launch an unforeseen attack at any time, from anywhere in the world. That’s why enterprises need to fortify their reactive security systems with additional layers of security that take a more proactive approach, rooting out and rejecting malicious code before the vulnerability has been diagnosed and patched.

Host-based intrusion prevention systems (HIPS) are designed to protect servers and workstations by placing software agents between applications and the operating system’s kernel. Using predetermined rules based upon the typical behavior of malware attacks, these systems evaluate activities such as network connection requests, attempts to read or write to memory, or attempts to access specific applications or registry keys. Behavior known to be good is allowed, behavior known to be bad is blocked, and suspicious behavior is flagged for further evaluation.

Evaluation and blocking can happen in multiple ways, at multiple levels. In the May 27, 2005 Gartner report entitled *Understanding the Nine Protection Styles of Host-based Intrusion Prevention*, Gartner analyst Neil MacDonald introduced a framework for understanding the different protection styles and technologies in the market for host-based intrusion prevention systems. In January 2006, Gartner published *Understanding Strengths and Weaknesses of Host-based Intrusion Prevention Styles* and made some slight changes in the HIPS framework to make it easier to apply.<sup>3</sup> Gartner’s nine protection styles can be visualized as a matrix, with security applications that work at the network, application and execution levels, each evaluating incoming code that’s known to be good, known to be bad or unknown:

**Figure 1. Three Levels and Nine Protection Styles of HIPS**

	Allow Known Good (Block All Else)	Block Known Bad (Allow All Else)	Unknown
<b>Execution-Level</b>	7 Application Control	8 Resource Shielding	9 Behavioral Containment  Passive → Active
<b>Application-Level</b>	4 Application and System Hardening	5 Antivirus	6 Application Inspection
<b>Network-Level</b>	1 Host Firewall	2 Attack-Facing Network Inspection	3 Vulnerability-Facing Network Inspection

Source: Gartner (January 2006)

137366-1

While traditional security products are targeted toward individual boxes in the matrix, the growing number and sophistication of attacks—especially zero-day attacks—requires a more comprehensive approach. This means going beyond traditional antivirus and firewall solutions to identify legitimate applications while proactively detecting, blocking and removing suspect behavior such as hidden processes, process injection, rootkits and more. This expansion and multilayering of the security landscape to block known and unknown threats at every level—as well as permitting applications known to be good—is called host-based intrusion prevention, or HIPS.

Gartner's MacDonald states, "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." <sup>4</sup> In the following are excerpts from *Understanding Strengths and Weaknesses of Host-based Intrusion Prevention Styles*, MacDonald discusses some of the strengths of the HIPS framework at the network, application, and execution levels:

### **Level 1: Network-Level HIPS**

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).

### **Level 2: Application-Level HIPS**

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.

### **Level 3: Execution-Level HIPS**

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.

## Toward Layering and Consolidation of Security Techniques

The HIPS concept of top-to-bottom and across-the board security is relatively new. Just five or six years ago, most desktop security was based on personal antivirus systems that depended largely on the compliance and self-management of individual users. Since then, companies have added antispyware and personal firewalls at the desktop level, as well as network access control (NAC), patch management and other capabilities at the enterprise level. Today's enterprise security environment typically includes multiple layers, with each designed to catch a vulnerability or threat that other layers may have missed.

Alongside this layering of complementary security techniques, there has been a trend toward consolidation of security products—so that antispyware is typically bundled with antivirus, personal firewalls are bundled with operating systems, and so on. The natural trend is toward a comprehensive suite of security solutions covering all nine styles in the matrix, with consolidated and centralized control over the whole suite. In short, the goal is a true HIPS system.

## Today's State of the Art: LANDesk® Host Intrusion Prevention System

Intrusion prevention solutions can be implemented at the network level in the form of network inspection tools, and at the endpoint level in the form of one or more security clients residing on desktops and servers. For endpoint-based HIPS, the ultimate goal is a consolidated solution that covers the entire security landscape—blocking of known-bad code, whitelisting of known-good software and behavioral containment of unknown code—with all features managed through a single console.

Companies looking to achieve that goal now have a solution from the pioneer and a leader in desktop management: LANDesk.

If you're a LANDesk customer, you're already familiar with LANDesk® Antivirus, LANDesk® Patch Manager and LANDesk® Security Suite—three of the leading security applications among the many IT management products we offer. Together, these products offer significant security coverage in the areas of personal firewall, antivirus and resource shielding.

Now, LANDesk has combined these capabilities with new features that further strengthen existing security features, while adding new HIPS coverage in the areas of system hardening, application control, and behavioral containment. And unlike add-on security products that make management and compliance increasingly problematic with each new area of coverage, LANDesk provides a single console for managing the entire desktop security environment.

We've put it all together in our newest product for enterprise endpoint security: LANDesk® Host Intrusion Prevention System, or LANDesk® HIPS.

LANDesk HIPS provides application whitelisting to give you precise control over the code that can run on enterprise systems, as well as application control blocking technology to control how applications are allowed to execute. Its leading-edge security features include kernel-level, rule-based file system and registry protection, system startup control, multiple layers of protection from stealth rootkits, kernel-level networking filtering, process and file certification, and more.

With this new plug-in for LANDesk Security Suite, we're extending our layered security to cover every client-based security style in the HIPS matrix. We're making it possible to manage all of these client-based security features, on all your Windows desktops and servers 4 through a single console—significantly decreasing the IT burden while ensuring consistency and compliance. And we're committed to continuously strengthening security across the matrix in the coming months, adding even more capabilities in the areas of buffer overflow, personal firewall and more.

LANDesk is placed in the Leaders Quadrant of the *Gartner Magic Quadrant for PC Configuration Life Cycle Management, 2006*.<sup>5</sup> As PC security becomes an ever-more critical issue, and with the May 2007 release of LANDesk HIPS, we expect our new security capabilities to solidify our position as an unsurpassed leader in PC management.

Let's take a look at some of the features available with new LANDesk HIPS.

## New Client HIPS Functionality

When you add LANDesk® Host Intrusion Prevention System to LANDesk® Security Suite, you get our highest level of protection for desktop and server systems. While traditional firewall and antivirus solutions block malware based on IP addresses, ports and known virus signatures, LANDesk HIPS adds the ability to drive policy decisions based on application content and behavior. It's specifically designed to address zero-day threats by blocking malware before a new signature or vulnerability has even been discovered, as well as to allow IT administrators to control precisely what can execute on a given machine.

The LANDesk client uses proven heuristic and behavior-recognition techniques to recognize typical patterns and actions of malicious code. For example, a file that attempts to write to the system registry, or a rootkit that attempts to create a kernel hook, would be blocked and flagged as potentially malicious. The LANDesk HIPS client uses a variety of proprietary techniques to reliably detect malware even before a signature has been identified.

Two goals in any client-based security system are to minimize the impact on system resources and performance, as well as to minimize false positives. LANDesk achieves both of these goals by applying the industry's smartest and most efficient technology for profiling malware behavior in the absence of a known signature. And to provide even more efficiency and accuracy, the LANDesk HIPS client also offers a "whitelist" that can be continuously updated to identify the applications known by an enterprise to be benign.

The new LANDesk HIPS client gives administrators a powerful new tool for controlling what applications run on enterprise desktops and servers, and how those applications are allowed to execute. Just as important, it runs automatically and efficiently, allowing users to concentrate on their jobs without interruption—and without worrying about the integrity of their systems and data.

## New Console HIPS Functionality

One of the downsides to client-based security management has always been the difficulty of managing individual machines throughout the enterprise—or worse, depending on users to manage their own PC security environment. LANDesk® Security Suite was created around the philosophy that the enterprise security team should always be in control of security policy, and the IT staff should always have an easy way to implement and enforce policies. This philosophy is realized through a centralized console that provides endpoint discovery, inventory, patch management, access control, compliance enforcement, audit reporting and other security needs for the entire organization.

At the same time, the LANDesk Security Suite philosophy recognizes that different users have different access and application requirements. The console must allow for different user profiles and system configurations, while maintaining consistent, centralized control that minimizes the IT burden even in the most complex and multifaceted organization.

This philosophy is further reinforced with the new HIPS plug-in for LANDesk Security Suite and LANDesk® Patch Manager. With the addition of LANDesk® Host Intrusion Prevention, administrators now have a single console for installing, configuring and managing host-based intrusion prevention for all connected and disconnected endpoints throughout the enterprise. For IT departments using only LANDesk Patch Manager, the capabilities of LANDesk HIPS provide protection before patches are available.

Centralizing control over HIPS clients provides enormous benefits for IT management efficiency, consistency and control. For example, as users on each client PC identify new whitelist applications, they are stored in a central repository where IT administrators can manage the entries and automatically distribute them to other PCs that need the same whitelist information.

At the same time, LANDesk HIPS provides administrators with the ability to define and manage separate profiles for different user groups. For example, employees in the call center may only require access to the company's troubleshooting and support applications, and perhaps one or two off-the-shelf applications such as email and instant messaging. Other user groups, such as the sales force or the finance department, may require much broader application access—for example, financial applications, customer databases and VPN software to connect securely while traveling.

LANDesk HIPS accommodates the needs of any and all user groups by allowing administrators to create multiple, highly flexible configurations for different user profiles. Each profile can include separate whitelists, application control and behavior-based blocking policies. In our example, LANDesk HIPS makes it very easy to develop and manage separate whitelists for the different user groups, and it's just as easy for the system to "learn" as needs change—for instance, to add to the call center whitelist when a new service portal comes online.

Antivirus, antispymware, application blocking, resource shielding and other host-based security features are the last line of defense against attack. Most security solutions available today only provide one or two features from the complete HIPS matrix, and each solution must be managed independently of other solutions, on a per-machine basis. But with LANDesk HIPS, you have full coverage for every endpoint security function—along with centralized configuration and control to ensure that all your users have the functionality they need while complying with the security requirements you specify.

## LANDesk® Host Intrusion Prevention System: A Feature Summary

LANDesk® Host Intrusion Prevention System adds several new layers of security to LANDesk® Security Suite and LANDesk® Antivirus, providing powerful behavior-based blocking technology to catch zero-day attacks and other malware that signature-based blocking might otherwise miss. Features of LANDesk® HIPS include:

- **Kernel-level, rule-based file system and registry protection:** Rules specifying which operations on which files are forbidden to which processes.
- **System startup control:** A process that controls the programs allowed to run upon startup.
- **Detection of stealth rootkits:** Two methods for detecting the presence of rootkits:
  - Kernel hooks detection, which identifies and logs malicious drivers while insulating them from the operating system.
  - Hidden process detection, which looks for discrepancies between the list of processes seen by the software's user-mode service and the list seen by the software's kernel driver.
- **Kernel-level network filtering:** Filters the network connection requests for applications, allowing or denying them in accordance with policy settings and process certifications (described below).
- **Process and file certification:** A mechanism, based on a list of authorized applications and files, that bypasses some of the protections listed above while protecting against injection of non-certified code at runtime.

LANDesk HIPS integrates all of these protection barriers with the signature-based protection found in LANDesk Security Suite and LANDesk Antivirus, while allowing installation and control of all endpoint security features from a single console. It gives you unprecedented ability to:

- **Detect and remove hidden processes and rootkits.**
- **Protect system services, startup programs, Activex and toolbars.**
- **Protect against process injection and kills.**
- **Provide rule-based file-system and registry protection.**

## Arm Your Enterprise for Today and Tomorrow

While no security system can guarantee perfect success in blocking all malware with no false positives, we submit that no solution on the market today provides more complete coverage, more reliable protection against zero-day attacks, or more robust and flexible management with full IT control than LANDesk® Host Intrusion Prevention—and all from a single console. When it comes to host intrusion prevention, LANDesk leads the pack—and we intend to build aggressively on that lead in the months and years to come.

Learn more about how easy and affordable it is to add LANDesk Host Intrusion Prevention to LANDesk® Security Suite for unmatched protection, even against unknown threats. Call LANDesk today at 1-800-982-2130. Or visit us at [www.landesk.com](http://www.landesk.com). You can be certain that the next zero-day attack is already being prepared. Now is the time to mount your best defense.

## References

- <sup>1</sup> Ellen Messmer, “Has the End Arrived for Desktop Antivirus?” Network World, April 5, 2007.
- <sup>2</sup> Greg McNevin, “Antivirus Companies Fighting Un-winnable War?” idm.net.au, March 19, 2007.
- <sup>3</sup> Neil MacDonald, “Understanding Strengths and Weaknesses of Host-Based Intrusion Prevention Styles” Gartner Research, January 30, 2006.
- <sup>4</sup> Ibid, p. 1
- <sup>5</sup> See the LANDesk website for supported versions: [www.landesk.com](http://www.landesk.com).
- <sup>6</sup> Ronni J. Colville, Michael A. Silver, Terrence Cosgrove, “Magic Quadrant for PC Configuration Life Cycle Management, 2006”, Gartner Research, December 4, 2006.

The Magic Quadrant is copyrighted December 4, 2006 by Gartner, Inc. and is reused with permission. The Magic Quadrant is a graphical representation of a marketplace at and for a specific time period. It depicts Gartner’s analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor, product or service depicted in the Magic Quadrant, and does not advise technology users to select only those vendors placed in the “Leaders” quadrant. The Magic Quadrant is intended solely as a research tool, and is not meant to be a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.