



LANDesk® Host Intrusion Prevention

Add Prevention to Protection

Increased Protection against Targeted Attacks



"If the growth in malware continues at the current pace, makers of antivirus software may not be able to withstand the onslaught."

— "Antivirus Companies Fighting Un-Winnable War?,"
Idm.net.au, quoting
Eugene Kaspersky of
Kaspersky Labs

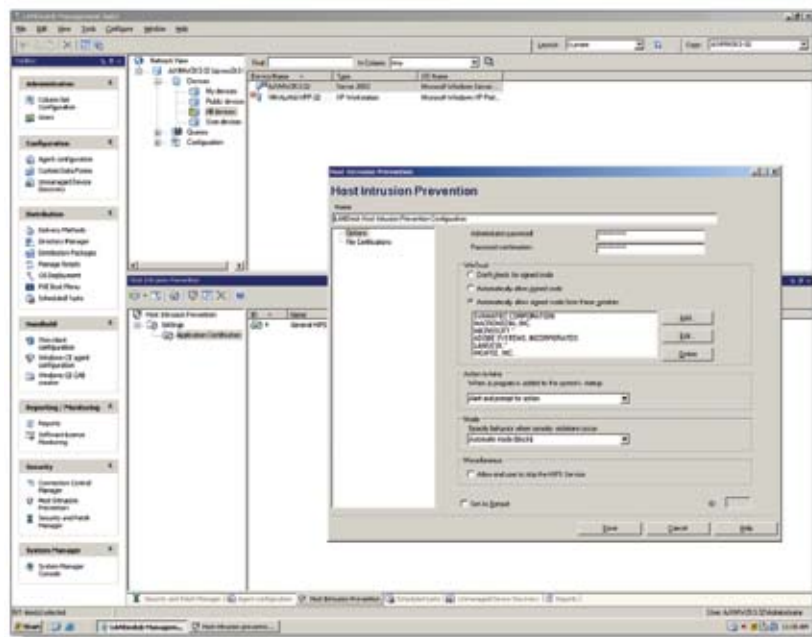
Hackers are getting faster and more devious. And the traditional ways of protecting enterprise systems—antivirus software and firewalls—are no longer enough to ensure your systems stay up and that your critical intellectual property doesn't fall into the wrong hands. Chief Research Officer Mikko Hypponen of F-Secure, a provider of security services, said that some days it receives as many as 40,000 new tainted files to create antivirus signatures for. He continued, "This is not just a battle between manufacturers of security software and some Internet criminals. It is a war between good and evil." ("Antivirus Companies Fighting Un-Winnable War?," idm.net.au)

You can wage your own war and wonder when the next zero-day threat will take out all or part of your enterprise. You can wonder what may get past your firewall or antivirus solution. Or, you can choose to reinforce your existing security efforts with protection against targeted attacks right at the host level and give your enterprise an even higher level of protection.

LANDesk® Host Intrusion Prevention: Added Peace of Mind

LANDesk® Host Intrusion Prevention helps you thwart malicious attacks with behavior-based blocking that prevents applications from executing in malicious ways right on an individual host system. What's more, LANDesk Host Intrusion Prevention runs from the same console your IT staff uses to administer LANDesk® Security Suite and LANDesk® Management Suite. You access everything you need for the most complete, layered LANDesk® security solution available, including:

- Added assurance and the knowledge that you're equipped to prevent zero-day threats even before the fix is available.
- Increased efficiency and reduced training and infrastructure costs with a single console solution for complete layered security.
- Precise control over what users can and can't run on your enterprise systems.



With LANDesk® Host Intrusion Prevention System, thwart malicious attacks with application control administered directly from the same console used to administer LANDesk® Security Suite.

Adding Prevention to Protection from a Single Console

It's critical to keep your systems patched with the latest antivirus definitions and ensure that known viruses never harm critical data or user productivity. But with the frequency of zero-day attacks rapidly increasing—there were more than 20 zero-day exploits in 2007 alone—your enterprise could still be at risk, even with the best antivirus solution available. That's where LANDesk® Host Intrusion Prevention comes in. It works in conjunction with LANDesk® Security Suite and LANDesk® Antivirus from a single administrative console to give you an added layer of protection—one called prevention.

LANDesk Host Intrusion Prevention goes beyond protecting against existing known viruses or other malicious attacks. It lets you prevent them by monitoring for and stopping suspicious behaviors—the types of behaviors typical of malicious attacks. So, even if an antivirus definition isn't available yet, you can reinforce your protection against attacks. As a mature technology, LANDesk Host Intrusion Prevention has an impressive track record, having blocked malware exploits for over 10 years, including the likes of Zotob, Storm, Code Red, Nimda and the Blaster virus, even before antivirus signatures were available.

Precise Control Using Application Whitelists

Through two distinct methods, LANDesk® Host Intrusion Prevention allows your IT staff to determine not only which applications can't be run on the host system, but which ones can be. You can use standard HIPS security protection to prevent all malicious software behaviors automatically. For an even more customized level of control, apply whitelisting security protection and execute only those applications that have made it to your "whitelist" or approved application list. All other applications are denied execution.

LANDesk Host Intrusion Prevention also lets IT determine which applications are authorized to send email, modify protected registry keys and write into executable files and protected processes. IT is empowered to prevent new, malicious applications—those that might be posing as everyday applications—from slipping through your enterprise defenses. New and emerging threats, such as buffer overflow exploits and zero-day threats can be monitored and contained as well.

An Even More Complete, Layered Security Solution—Single Console Simplicity

LANDesk® Host Intrusion Prevention is an add-on to LANDesk® Security Suite. Use it with LANDesk Security Suite and LANDesk® Antivirus for an even more complete, layered security solution and even broader centralized control over your entire network environment.

—LANDesk Security Suite extends active security management to your endpoints. Use it for quarantine capabilities, active threat analysis, spyware detection and removal, access control, configuration security tools and more.

—LANDesk Antivirus delivers enterprise-ready virus protection and rootkit detection using the single console simplicity found only with LANDesk® solutions. It lets you extend world-class virus protection to your enterprise for a lower investment than other industry-standard solutions.

Nine Protection Styles of Host-Based Intrusion Prevention

	Block the Known Bad (Allow All Else)	Allow the Known Good (Block All Else)	Unknown
Behavior-Level HIPS	7 Resource Shielding	8 Application Hardening	9 Behavioral Containment Passive → Active
Application-Level HIPS	4 Antivirus	5 System Hardening	6 Application Inspection
Network-Level HIPS	1 Attack-Facing Network Inspection	2 Personal Firewall	3 Vulnerability- Facing Network Inspection

Source: Gartner (May 2005)

127317-01

LANDesk® Host Intrusion Prevention added to LANDesk® Security Suite and LANDesk® Antivirus gives you virtually all of Gartner's Nine Protection Styles of Host-Based Intrusion Prevention.

Key Features

Single Console Control

- Allows IT administrators to use a single management console to install, configure and manage host-based intrusion prevention features for all enterprise systems.
- Lets IT quickly and easily perpetuate learned behaviors blocked on an individual host to host system enterprisewide.

File System and Registry Protection

- Recognizes malicious writes and modifications to the registry to prevent malware from running when a host system is rebooted.
- Allows IT to lock down the registry unless and/or until writes are approved by the IT administrator.
- Allows IT administrators to prevent certain malware classes from performing malicious functions in the file system by specifying which operations on which files are forbidden to which processes.
 - Processes can be “all” or certain named processes.
 - Operations can be “none” or certain predefined operations—read, write, execute, create.
 - File can be “All” or predefined file names, including wildcards. For example: “FILE.ABC”, “*.EXE” etc.
 - According to the above rules and the requesting processes certifications, the result is “allow” or “deny” operation.

System Startup Control

- Gives IT administrators a process to make a white list of applications allowed to run at host startup in addition to a blacklist of those that can't be run.
- Gives IT administrators precise control over the applications that can run on enterprise systems and how those applications are allowed to execute.
- Provides added protection against malicious attacks by preventing disguised, new and/or unknown malicious applications from slipping through enterprise defenses.
- Provides flexible configurations for different user profiles to easily enable different white lists for different users and groups.

Application Access and Rootkit Control

- Allows IT to determine whether or not applications that are running can execute other applications on a host in order to detect and prevent stealth rootkits from infiltrating enterprise systems.
- Kernel-level network filtering lets IT define an application's executable files and what is and isn't acceptable network behavior.
 - IT can filter network and block applications that attempt to connect to SMTP mail servers unless specifically authorized to send email.
- Gives IT control over which applications can read, write or modify protected files or registry parts.
 - By locking down what changes in the registry, prevents malware from launching in memory and/or making changes to the registry.
- Creates a log of malicious, uncertified rootkits—a log that can be perpetuated throughout the enterprise.

Process and File Certification

- Empowers IT administrators to certify that certain applications or files are allowed to bypass some or all protections built in to LANDesk® Host Intrusion Prevention.
 - Users can be given the right to modify protected files.
- Prevents non-certified processes from injecting into certified processes and illegally obtaining certified authorization attributes.

Visit www.landesk.com for more information.

This information is provided in connection with LANDesk products. No license, express or implied, by estoppel or otherwise, or warranty is granted by this document. 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. For the most current product information, visit <http://www.landesk.com>.

Copyright © 2007 LANDesk Software Ltd. or its affiliated companies. All rights reserved. LANDesk, Peer Download, Targeted Multicast and Trusted Access are registered trademarks or trademarks of LANDesk Software Ltd. or its affiliated companies in the United States and/or other countries. Other names or brands may be claimed as the property of others. Each customer's results may vary based on its unique set of facts and circumstances. LSI-0679E 1107/BB/NH

