

LANDesk® HIPS

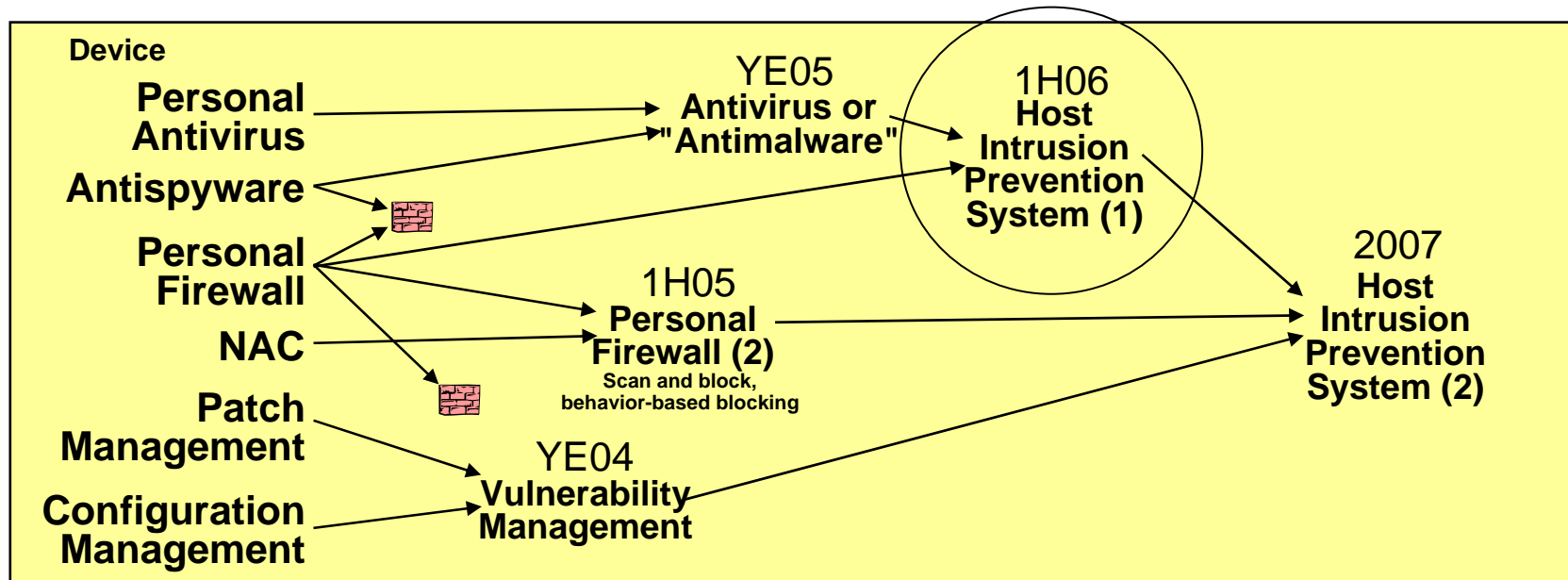


Jan Buelens
Technical Sales Manager
LANDesk Software



What is Host-based Intrusion Prevention (HIPS)?

»» HIPS protects endpoints by combining signature-based detection (AV, anti-spyware) with personal firewall with behavioral detection.



Zero-day Threat and HIPS

- »» (February 2nd, 2007) ... Microsoft's **fifth zero-day** exploit since December 2006.
- »» Feb 9, 2007: 30 publicly known threats for which no vendor patch is available.

Malicious code is changing too rapidly for traditional defenses to keep up. Firms must look to a suite of client security products — typically, antivirus, antispyware, client firewall, and at least some host intrusion prevention (HIPS) capability — to protect endpoints from malware.”

- Forrester Research, June 22, 2005
The Forrester Wave™: Client Security Suites, Q2 2005

The screenshot shows the top portion of the eWEEK.com website. On the left is the eWEEK.com logo. To its right is a navigation bar with the text "ENTERPRISE NEWS & REVIEWS" and a list of menu items: "NEWS · REVIEWS · OPINIONS · CASE STUDIES · TOPICS · IN". Below the navigation bar is a search box with the word "SEARCH" inside. Below the search box is a dark grey banner with the word "Security" in white text.

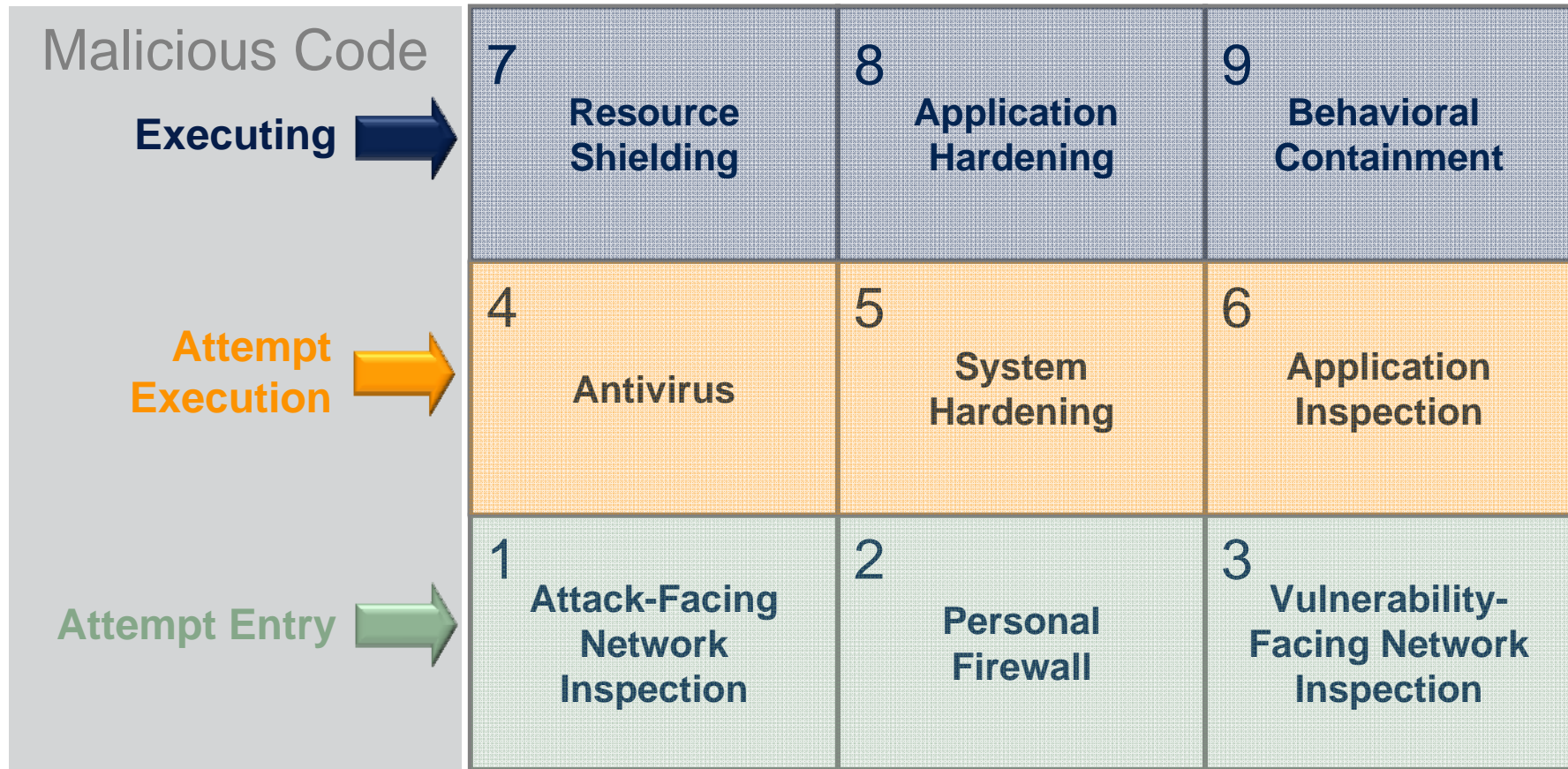
Microsoft, Zero-Day Flaws Dominate SANS Vulnerability Rankings

By Matt Hines
November 15, 2006

TALKBACK
Comment on this article
▶ Be the first to comment on this article

»»
LANdesk
An Avocent Company

Gartner HIPS framework



Gartner HIP Framework – Which to use?

Known Bad	Known Good	Unknown
Resource Shielding	Application Hardening	Behavioral Containment
Antivirus	System Hardening	Application Inspection
Attack-Facing Network Inspection	Personal Firewall	Vulnerability-Facing Network Inspection

Nine Protection Styles of Host-Based Intrusion Prevention *NEW! With LANDesk HIPS:*

	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

■ = Covered by LDMS 8.7

■ = Added Protection from LD HIPS

What is LANDesk® HIPS?

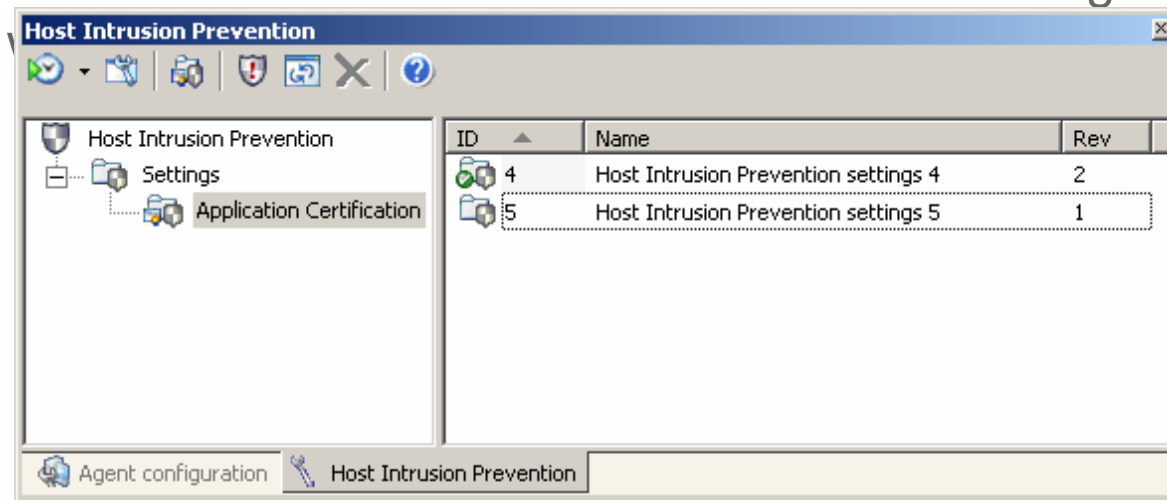
- »» A new plug-in for LANDesk® Security Suite
- »» Introduced with 8.7 SP3
- »» behavior-based blocking” technology :
 - Rule-based File System Protection
 - Rule-based Registry Protection
 - System Startup Control
 - Detection of Stealth Root Kits
 - Kernel-level Network Filtering
 - Process and File Certification
- »» Requirements:
 - OS: Windows 2000 / XP (32-bit) / 2003, Vista
 - AV: LANDesk Antivirus, Symantec Antivirus, McAfee Enterprise

Backup



How Does LANDesk HIPS Work?

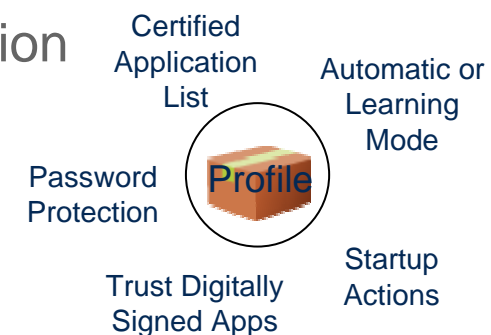
- »» Requires LANDesk® Security Suite (stand-alone or add-on)
- »» Requires LANDesk® Antivirus, Symantec Antivirus, or McAfee VirusScan Enterprise 8.5i
- »» Allows the LANDesk user to manage HIPS behaviors that will later be applied to managed clients
 - This is done within the LANDesk console using the HIPS tool



Host Intrusion Prevention Tool Window

Working with HIPS Tool Window

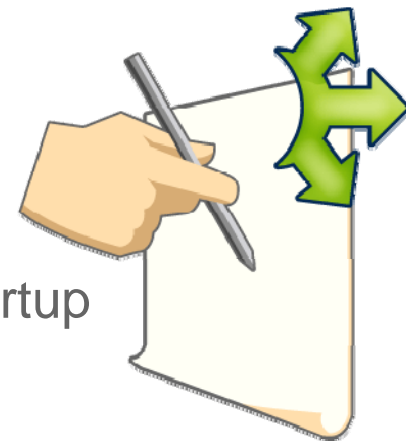
- »» The LANDesk user accesses tool from within console
- »» This tool is used to create profiles defining just how client machine is to be protected using HIPS protection
- »» Options include:
 - Setting an Administrator password
 - Selecting WinTrust functionality options
 - Selecting actions to take (on the client's machine) when an application is added to the startup group
 - User can be alerted and prompted for action
 - Event can simply be logged
 - Application can be removed again
 - Setting *Automatic* or *Learning* mode
 - File Certification
 - *White list* of approved applications



More on File Certification

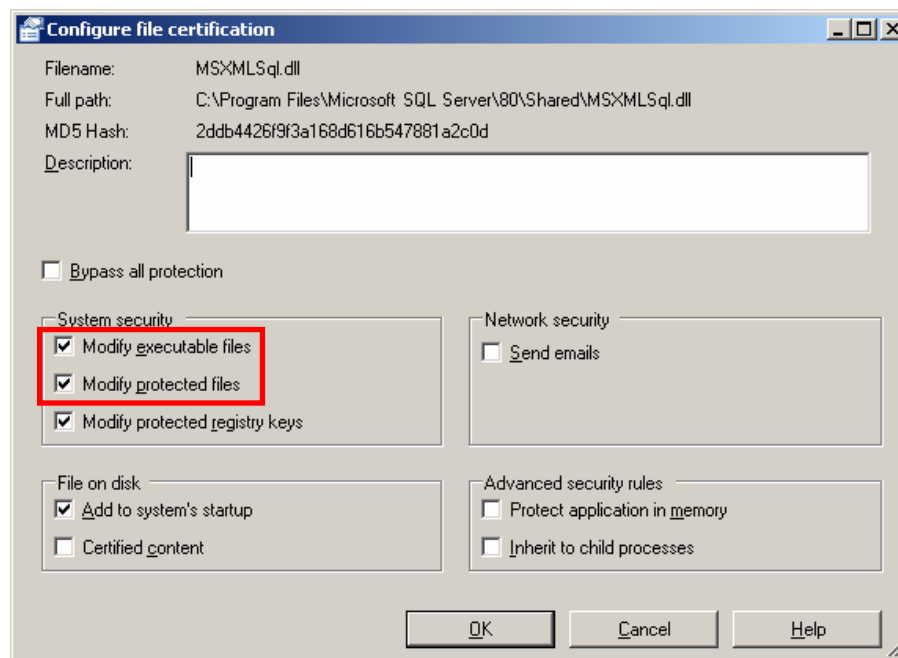
»» File Certification lets the LANDesk user create a *white list*, which are applications that automatically have rights to perform certain functions on the client's computer without generating violations. Functions that applications can perform, include:

- Bypassing all protections previously defined by rulesets
- Modifying executable files
- Modifying protected files
- Modifying protected registry keys
- Sending emails
- Adding things to the client's system startup
- Protect applications in memory
- inherit to child processes



Rule-based File System Protection

- »» Used to protect files used by applications on the system
- »» Whenever non-certified apps attempt to modify a file on the system, a violation is generated and the operation is prevented



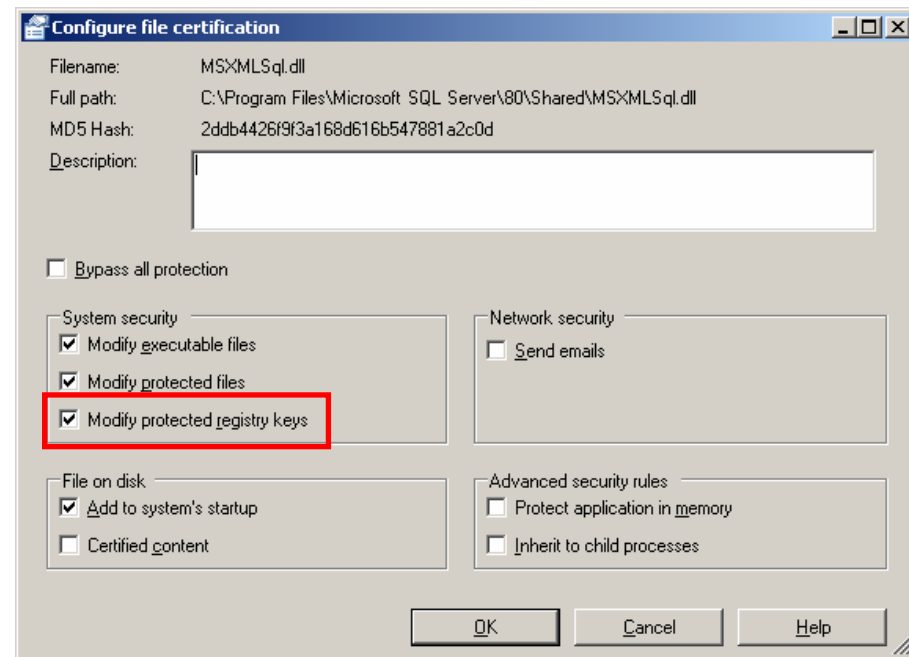
Configuration Dialog

- Once an app is certified, it is either granted or denied rights to perform that operation on protected executables and files
- All other applications executing on the system that attempt to modify executables or protected files, will generate a violation

Rule-based Registry Protection

- »» Used to protect Registry Keys used by applications on the system
- »» Whenever non-certified apps attempt to modify protected registry keys, a violation is generated and the operation is prevented.

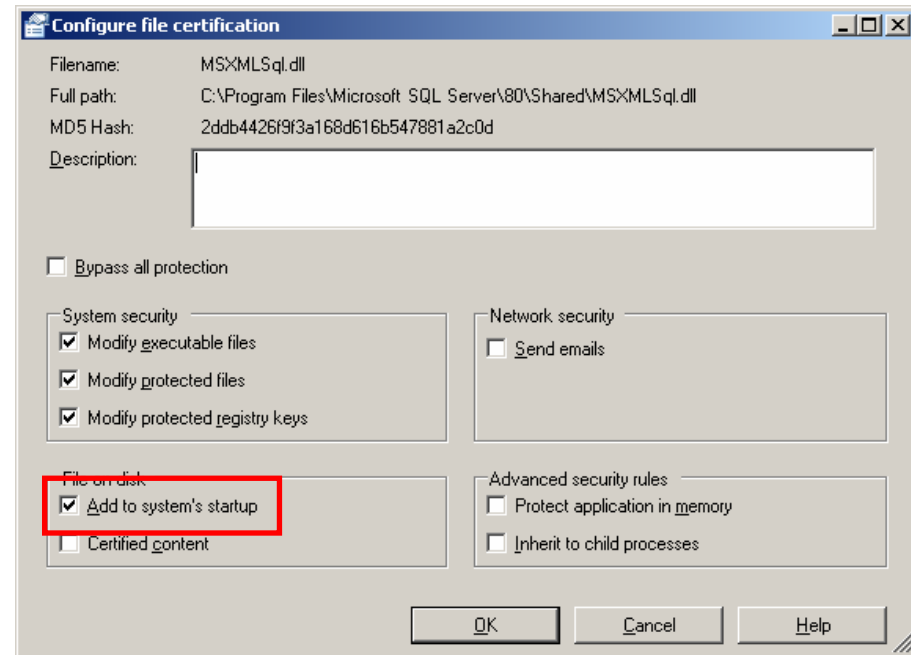
- Once an app is certified, it is either granted or denied rights to perform that operation on protected executables and files
- All other apps attempting to modify registry keys, will generate a violation



Configuration Dialog

System Startup Protection

- »» Used to protect files from being added to the system's startup
- »» Whenever a non-certified app attempts to add another app to the system startup, a violation is generated and the operation is prevented



Configuration Dialog

- When this feature is applied to a certified application, that application is either granted or denied rights to perform that operation. All other applications executing on the system that attempt to add apps to the system's startup, will generate a violation.

Detection of Root Kits Protection

- »» This feature is used to determine if malicious or non-certified drivers are trying to modify the system. If detected, the system can identify and log the event.
- »» In order to detect Root Kits (stealth Kernel drivers), the two following detection mechanisms are used:

- **Kernel hooks detection**



- Upon system boot, a “fake” virtual SSDT is built and shown to any driver that loads into the system. Drivers that try to modify the SSDT will only modify this “fake” SSDT. If this is a malicious or non-certified driver, LANDesk HIPS identifies the driver and logs it.

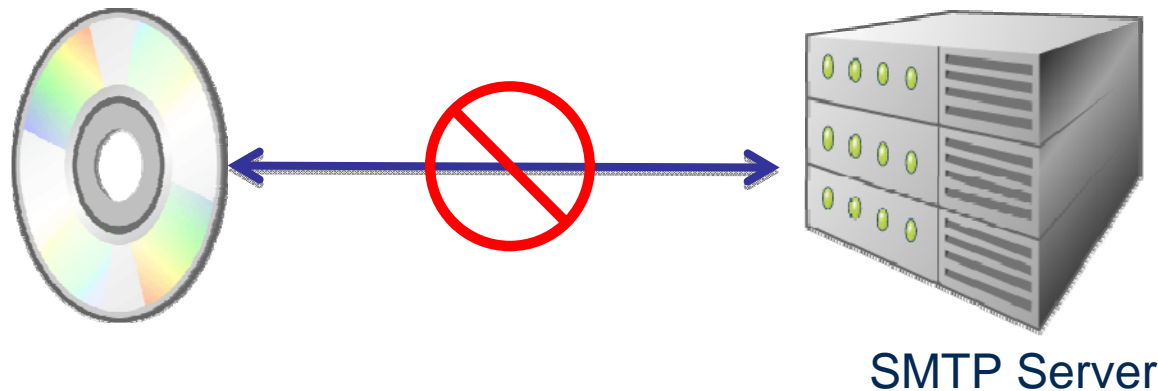
- **Hidden processes detection**



- By comparing lists of processes, LANDesk HIPS can detect processes hidden from User-mode processes.

Kernel-level Network Filtering

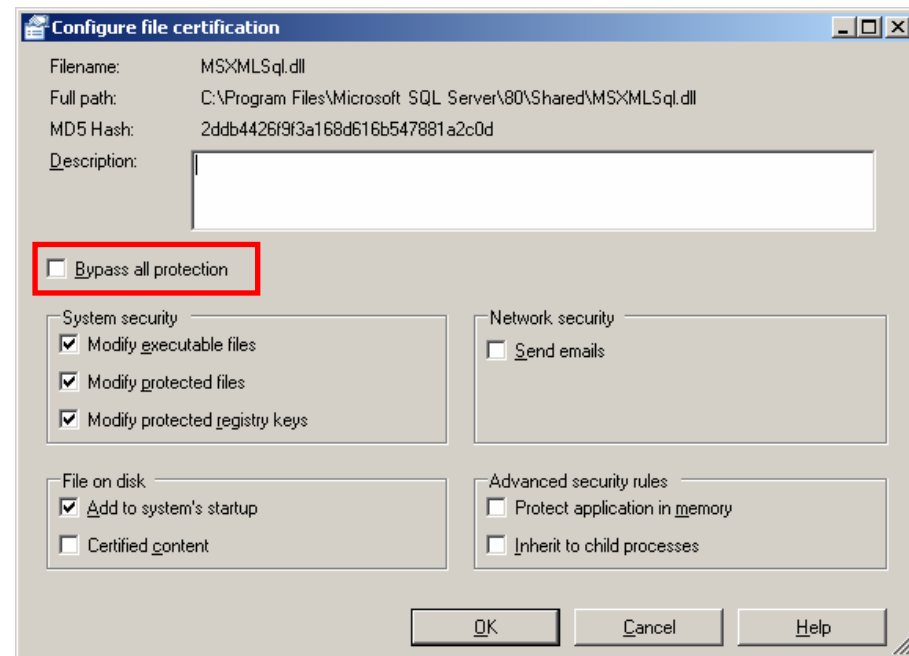
- »» This feature is used to filter applications' network connections requests
- »» According to policy settings, connections are allowed or denied
- »» In particular, applications that attempt to connect to SMTP mail servers are blocked unless specifically authorized to send e-mail



Process and File Certification

- »» Used to bypass previously mentioned protections
- »» By certifying an app you are approving it for use on the system
- »» Process

- Administrator deploys LANDesk HIPS agent set to *Learning* mode to collect information about app use
- Once info is collected, Administrator creates white list of certified applications and fine-tunes their ability to perform operations
- LANDesk HIPS agent config is set to *Automatic*, and updated on the client



Configuration Dialog