## Symantec Critical System Protection 5.0 overview and feature comparison with Symantec Host IDS 4.1.1 & Intruder Alert 3.6.1

***December 2005***

**Purpose:**

This document assists in explaining the differences between Symantec Host IDS, Symantec Intruder Alert and their recent update called Symantec Critical System Protection 5.0. The document contains three sections. The first section outlines the differences between the host intrusion prevention of the solutions. Section two provides an overview of the out of the box intrusion prevention policies for SCSP 5.0. Section three provides an overview of the out of the box detection policies included in SCSP 5.0.

**Audience:**

The audience for this document is the security architect, security analyst or IT manager responsible for server based intrusion prevention as well as system monitoring & auditing. This document is specifically written for existing Symantec Host IDS or Intruder Alert customers who are reviewing the opportunity to upgrade to Symantec Critical System Protection 5.0.

**Section 1 – understanding the differences**

This section outlines the functionality differences between the two solutions. For the most part, Symantec Critical System Protection 5.0 is a super-set of the Symantec Host IDS and Intruder Alert solutions. Symantec Critical System Protection leverages the high value functionality from Symantec Host IDS and incorporates an entirely new set of functionality that protects serves from day zero threats and provides enterprise wide proactive security policy enforcement.

*(Note: The light yellow boxes denote an advantage for Symantec Critical System Protection 5.0)*

| | Feature Description | Symantec Host IDS 4.1.1 | Intruder Alert 3.6.1 | Symantec Critical System Protection 5.0 |
|---|---|---|---|---|
| | **Intrusion Prevention** | | | |
| 1 | Process Monitor – watch critical processes, restart based upon policy (this was a Host IDS specific function) | Yes | No | The IPS component proactively protects critical processes from being terminated by validating system calls against security policy. The system monitoring component can watch for process termination and can restart or alert. |
| 2 | Process Blocker – blocks processes from starting (this was a Host IDS specific function) | Yes | No | Prevents new processes from starting by validating system calls against security policy |
| 3 | Process Reporter – a complete view of processes running on the system (snapshot – this was a Host IDS specific function) | Yes | No | No snapshot of processes is provided in SCSP. |

| | | | | |
|---|---|---|---|---|
| 4 | Exploit prevention | No | No | Utilizes behavior control descriptors for O/S functions, services and applications. These descriptors define acceptable behavior and prevent hijacking by security risks. Any attempt by system services, applications or users to access system resources that is not acceptable will be automatically blocked and logged. Exploit prevention is automated through the use of "out of the box" policies. See section 2 for more details. Exploit prevention does not have to be implemented. But if it is implemented, it may operate in audit (prevention disabled) mode or enforcement mode. |
| 5 | Application profiling tool | No | No | Includes an application profiling tool to enable administrators to create a baseline behavior control descriptor for legacy applications or other applications that may not be included in the Symantec policy library |
| 6 | Restricts application usage of network resources | No | No | Restricts applications and services to their known good network activity. This prevents exploits from taking advantage of an application and forcing it to use the network in malicious ways |
| 7 | Prevents registry changes | No – HIDS has registry watch | No | Locks down the registry (or sections of the registry) to prevent modification. This assists in stopping unknown attacks that leverage registry setting changes as one of their attack vectors. |
| 8 | Executable white listing | Yes | No | Explicitly defines the set of applications and services that may execute on the endpoint. This allows administrators to create hardened systems that perform limited functionality to reduce the risk of exposure. |
| 9 | Executable black listing | Yes | Yes | Explicitly defines the set of applications and services that may NOT execute on an endpoint. This allows administrators to proactively enforce policy across the enterprise and ensure that unwanted applications do not reside on any servers. (for example prevent the running of P2P file sharing programs or multi-player game software) |
| 10 | Active protection of system configuration | No | No | Explicitly protects system configuration settings. This protection will prevent any user from tampering with or changing system settings no matter the level of user credentials. |
| 11 | Active protection of system resources | No | No | Explicitly protects system resources such as the registry, file systems and even default printers. This protection will prevent any user from tampering with or changing system settings no matter the level of user credentials. |
| 12 | MS Windows buffer | No | No | Detects and stops the execution of buffer |

| | | | | |
|---|---|---|---|---|
| | overflow protection | | | overflow threats that exploit the operating system. (Symantec also has a separate memory firewall solution available to augment the buffer overflow protection provided by Symantec Critical System Protection) |
| 13 | Default O/S & interactive protection policies | No | No | Default policies are listed in section 2. By providing out of the box systems can be protected upon initial installation |
| 14 | Device controls | No | No | Prevents the use of (either reading or writing to/from) USB devices, removable media, drive mounting, Bluetooth devices, etc based upon policy |
| 15 | Server firewall | No | No | Server firewall monitors incoming and outgoing traffic, blocks ports and protocols based upon policy. |
| 16 | Policy enforcement | No | No | Enforces security policy across the enterprise without requiring reconfigurations at each end point. Global policy enforcement can reduce the impact of configuration errors and reduce the amount of time required to enforce policy compliance. |
| | | | | |
| | **System Monitoring** | | | |
| 17 | File watch | Yes | No | Yes |
| 18 | Audit log tracking | Yes | Yes | Yes |
| 19 | Custom log tracking | Yes | Yes | Yes |
| 20 | Customizable intrusion detection policies and responses | Yes | Yes | Yes |
| 21 | Smart event response | Yes | Yes | Yes |
| 22 | Threshold based alerting | Yes | No | Yes |
| 23 | System monitoring policy library | Yes | Yes | Yes |
| 24 | Global flags and timers | Yes | Yes | No |
| 25 | Bulk log transfers | No | No | Provides the administrator with the ability to bulk transfer the security event log to the central management server. |
| 26 | Tamper resistant log files | No | No | Log files are fingerprinted via a check sum and then securely transmitted to prevent tampering. |
| | | | | |
| | **Centralized Reporting & Alerting** | | | |
| 27 | Customizable rule sets | Yes | Yes | Yes |
| 28 | Reporting | Yes | Yes | Yes |
| 29 | Predefined queries & custom queries | No | No | Yes |
| 30 | Integrated with | Yes | Yes | Yes |

| | | | | |
|---|---|---|---|---|
| | Symantec Security Information Manager | | | |
| 31 | Alerting – Email | Yes | Yes | Yes |
| 32 | Alerting – SNMP | Yes | Yes | Yes |
| 33 | Alert management console | Yes | Yes | Yes |
| 34 | DeepSight Threatcon integration | No | No | Symantec DeepSight Threatcon information is integrated into the home page of the management interface. This allows administrators to keep up to date on the Theatcon level and provides links to important information about current threats. |
| | | | | |
| | **Platform Support** | | | |
| 35 | Windows 2000 | Yes | Yes | Yes |
| 36 | Windows NT | Yes | Yes | Yes |
| 37 | Windows XP | Yes | Yes | Yes |
| 38 | Windows 2003 EE | Yes | Yes | Yes |
| 39 | Solaris 8 SPARC | Yes | Yes | Yes |
| 40 | Solaris 9 SPARC | Yes | Yes | Yes |
| 41 | HP/UX 11i | Yes | Yes | Monitoring & Auditing (IDS) only in 5.0 |
| 42 | HP/UX 11i v2 | Yes | Yes | Monitoring & Auditing (IDS) only in 5.0 |
| 43 | AIX 5.2 & 5.3 | Yes + AIX 5.1 | Yes | Monitoring & Auditing (IDS) only in 5.0 |
| 44 | Redhat Linux ES 3 | Yes | Yes | 1st half 2006 |
| 45 | Redhat Linux 7.3 | Yes | Yes | 1st half 2006 |
| 46 | SuSE Linux Enterprise Server 8 | No | No | 1st half 2006 |
| 47 | SuSE Linux Professional 9 | No | No | 1st half 2006 |
| 48 | IBM DB2 | Yes | No | No |
| 49 | Microsoft SQL Server | No | No | Yes |
| 50 | Management Server language variation | U.S. English | U.S. English | U.S. English |
| 51 | Agent platform language variations | U.S. English | U.S. English | U.S English |
| 52 | SESA Management Console | Yes | No | No, utilizes SESA collector at the management server (not the agent) to integrate with the Symantec Security Information manager 4.0 |
| | | | | |

**Section 2 – Overview of the "Out of the Box" prevention policies for Windows & UNIX**

| | **Windows Prevention Policy Library** | **Symantec Host IDS/Intruder Alert** | *For full detection policy details, please see document titled "Symantec Critical System Protection Prevention Policy Reference Guide"* |
|---|---|---|---|
| 53 | Windows NULL Policy | Yes | Allows all processes to perform all functions |
| 54 | Windows Core OS Policy | No | Provides general integrity protection. Includes protection for processes and shared libraries that are loaded without user intervention. |

| | | | |
|---|---|---|---|
| | | | Confines many of the system services and applications to acceptable behavior. Policy limits the ability of a service or application to harm the integrity of the system or O/S. Policy is configurable. |
| 55 | Windows Strict OS Policy | No | Provides all of the protection of the core policy plus adds restrictions for interactive programs including blocking (admin can create white lists of acceptable programs) Also by default blocks changing of screen saver, blocks com object registration and ActiveX component installation, blocks changing of network services (such as DNS), blocks changing of default printer and blocks recognition of Bluetooth devices. Policy is configurable. |
| 56 | Windows Limited Execution Policy | No | Blocks the execution of all interactive programs except those listed by the administrator as approved applications. Suitable for dedicated workstations with a small set of applications that require a high level of control. (for example, a kiosk or an appliance like server) |
| 57 | Default protection policies for Microsoft IIS, Exchange, SQL Server, Outlook and Offfice | No | Yes – see prevention policy reference guide for more detailed information |
| | | | |
| | **Unix Prevention Policy Library** | | |
| 58 | Solaris Standard Policy | No | Provides a general integrity protection policy. It confines many of the operating system daemons that have been identified as vulnerable as well as some common applications. |
| 59 | Solaris NULL Policy | No | Allows all processes to perform all functions |
| 60 | Apache Policy | No | Yes – see prevention policy reference guide for more detailed information |
| 61 | Sendmail Policy | No | Yes – see prevention policy reference guide for more detailed information |
| 62 | Postfix Policy | No | Yes – see prevention policy reference guide for more detailed information |
| 63 | Linux Standard Policy | No | Provides a general integrity protection policy. It confines many of the operating system daemons that have been identified as vulnerable as well as some common applications. |

**Section 3 – Overview of the "Out of the Box" detection policies for Windows & UNIX**

| | **Windows Detection Policy Library** | **Symantec Host IDS/Intruder Alert** | For full detection policy details, please see document titled "Symantec Critical System Protection Detection Policy Reference Guide" |
|---|---|---|---|
| 65 | Domain Trust Configuration – detects a creation or removal of a | Yes | Yes |

| | | | |
|---|---|---|---|
| | trusted domain configuration | | |
| 66 | Agent Status – Monitors the status of SCSP at the endpoint | Yes | Yes – In addition, can proactively prevent the shutdown of its agent processes |
| 67 | File Tampering – detects changes to critical system files | Yes | Yes – In addition, can lock down system files and prevent write access so that files may not be modified |
| 68 | ISS scanner probe – detects a heavy probe | Yes | Yes |
| 69 | Malware – detects the effects of malicious applications on the Windows system – signatures identify 12 common known exploits | Yes | Yes – In addition, can automatically prevent known and unknown exploits from gaining a foothold into the system by restricting applications & services to known good behaviors. This prevents multi-vector attacks from hijacking a system service and forcing it to do alternative tasks. |
| 70 | Microsoft Front Page activity – detects requests made to the front page server | Yes | Yes, In addition can proactively prevent Microsoft Front Page activity based upon security policy |
| 71 | Microsoft IIS Security Configuration – detects changes to IIS security settings | Yes | Yes – In addition, can proactively prevent changes across the enterprise. |
| 72 | Microsoft IIS vulnerable CGI scripts – detects web access to vulnerable CGI scripts | Yes | Yes |
| 73 | Network communication configuration – detects changes to settings that impact network communications | Yes | Yes – In addition, can prevent changes to system configuration settings |
| 74 | Symantec AntiVirus client communication – detects alerts from Symantec Antivirus | Yes | Yes |
| 75 | Sans – Detects Microsoft Windows issues from the SANS Top 20 list | Yes | Yes – In addition, can proactively enforce security policy across the enterprise according the recommendations of SANS (for example, disable IIS on all servers that don't require it – After defined in policy, SCSP could prevent IIS from running on any server without having to re-configure every server) |
| 76 | System Audit Tampering – detects system audit changes and the clearing of audit logs | Yes | Yes – in addition, can proactively protect audit settings and prevent changes and clearing of audit logs based upon policy. |
| 77 | System Authentication Configuration – detects changes to Windows Active Directory authentication and encryption settings | Yes | Yes |

| | | | |
|---|---|---|---|
| 78 | Autorun detection – detects if changes are made to the autorun which would execute code upon startup (such as a CD Rom) | Yes | Yes |
| 79 | Windows Failed Access – detects when a user has failed to authenticate either locally or via a domain | Yes | Yes |
| 80 | System file protection status – detects events by the Windows File Protection system which monitors critical system files which should remain available, detects file restorations | Yes | Yes, In addition can proactively prevent system files from modification or deletion |
| 81 | System Group Management Changes – detects creating, enabling or changing of security groups | Yes | Yes, In addition can proactively prevent the administrator from making changes |
| 82 | System Hardening – detects changes to user configured registry keys | Yes | Yes |
| 83 | System Logon Success – detects all successful local and remote Windows logons | Yes | Yes |
| 84 | System remote logoff – detects all successful Windows logoffs. | Yes | Yes |
| 85 | System security configuration – detects changes to registry keys that impact security settings | Yes | Yes, In addition can proactively prevent changes to registry keys |
| 86 | System Shares Configuration - detects the creation or removal of a share | Yes | Yes, In addition can proactively prevent the creation or removal of a share |
| 87 | System Startstop Options – detects changes to system startup and shutdown settings | Yes | Yes, In addition can proactively prevent the changes to system startup and shutdown settings |
| 88 | System User Configuration – detects changes made to user accounts | Yes | Yes, In addition can proactively prevent changes to user accounts |
| 89 | USB Device Activity – detects connection and disconnection of USB devices | Yes | Yes, In addition can proactively prevent the use of USB drives as well as other removable media |
| | | | |
| | **UNIX detection policy library** | | |

| | | | |
|---|---|---|---|
| 90 | Apache Vulnerable CGI Scripts – detects activities of certain (59) vulnerable CGI scripts | Yes | Yes, In addition can proactively prevent CGI scripts from executing |
| 91 | Agent Status – Monitors the status of SCSP at the endpoint | Yes | Yes – In addition, can proactively prevent the shutdown of its agent processes |
| 92 | File Tampering – detects changes to critical system files | Yes | Yes – In addition, can lock down system files and prevent write access so that files may not be modified |
| 93 | NetRecon – detects a scan by Symantec NetRecon | Yes | Yes |
| 94 | Sans – Detects issues from the SANS Top 20 list | Yes | Yes – In addition, can proactively enforce security policy across the enterprise according the recommendations of SANS |
| 95 | Sendmail Brokenpipe messages – detects broken pipe error messages | Yes | Yes, In addition has a default policy to protect Sendmail from exploitation. See intrusion prevention policy library. |
| 96 | Stack Execution Denied – detects attempts to execute instructions stored in the O/S stack | Yes | Yes |
| 97 | Syslogd tampering- detects when the syslog daemon isn't running | Yes | Yes |
| 98 | System Logon Failure – detects failed logon attempts from the local console or remote access | Yes | Yes |
| 99 | System Logon Success – detects successful logon attempts from the local console or remote access | Yes | Yes |
| | | | |