

CA Host-Based Intrusion Prevention System r8.1

CA HOST-BASED INTRUSION PREVENTION SYSTEM (CA HIPS) BLENDS ENDPOINT FIREWALL, INTRUSION DETECTION, INTRUSION PREVENTION, OPERATING SYSTEM SECURITY AND APPLICATION CONTROLS CAPABILITIES TO CREATE A CENTRALIZED, PROACTIVE DEFENSE AGAINST KNOWN AND UNKNOWN ONLINE THREATS. BEHAVIOR-BASED REAL-TIME PROTECTION COMPLEMENTS SIGNATURE-BASED TECHNOLOGIES, PROVIDING SUPERIOR SECURITY FEATURES, ACCESS CONTROL, POLICY ENFORCEMENT AND INTRUSION PREVENTION MANAGEMENT UNDER A SINGLE, INTUITIVE CONSOLE.

Overview

Malicious code and blended threats are evolving too quickly for traditional threat protection to keep up. You need a blended defense that combines and layers endpoint security.

CA HIPS combines endpoint Firewall, Intrusion Detection, Intrusion Prevention, Operating System Security and Application Controls capabilities complementing signature-based technologies with centralized, proactive protection against known and unknown online threats.

Benefits

By adding CA HIPS to your existing threat defenses, you enhance your endpoint protection with centralized access control and policy enforcement.

CA Hips is designed to block a variety of known and unknown threats effectively blocked, helping to reduce the risks of downtime and, data breaches that result in remediation expenses and help desk costs, improve operational efficiencies, boosting end user and IT staff productivity and facilitate service continuity.

CA Advantage

CA HIPS complements other CA threat management products and, with them, provides a comprehensive and multilayered defense against known and unknown threats.

CA security solutions are a fundamental component of CA's broader Enterprise IT Management (EITM) vision to unify, simplify and secure the management of technology.

CA HIPS Counters Blended Threats with a Blended Defense

The malware phenomenon has evolved from a hacker sport, populated by amateurs seeking bragging rights, to a criminal enterprise, populated by software professionals looking for ill-gotten gains. These crimeware authors are using sophisticated combinations of attack techniques to defeat traditional threat-protection products, target the rapidly growing and increasingly diverse population of remote and mobile endpoint devices, and exploit the opportunities that zero-day vulnerabilities present.

Signature-based anti-virus and anti-spyware products play an important role in endpoint security, but they are reactive technologies suffering from a real-time gap that is highlighted by the advent of blended threats and zero-day attacks. Blended threats mandate a blended and layered defense, and zero-day attacks require proactive, behavior-based protection.

CA HIPS creates a powerful five-in-one threat protection solution for business desktops, laptops and servers by combining endpoint Firewall, Intrusion Detection, Intrusion Prevention, Operating System Security and Application Controls capabilities under central, policy-based management. With CA HIPS, you can monitor network traffic and system behavior and spot the anomalies that often herald new threats.

This host-based software continues to protect endpoints even when they are off the network. When users reconnect, the HIPS client automatically retrieves new policy updates down to their devices.

CA HIPS fronts a sophisticated policy management with a highly intuitive interface. You can base security rules on a number of factors — such as the user’s geographic location, the time of day and the individual user’s role in the organization — and apply them dynamically. Your administrators can use these highly granular policy-setting capabilities and a “learning mode” to tailor CA HIPS to the way your business already uses software.

Key Capabilities

THREE THREAT PROTECTION TECHNOLOGIES IN ONE A combination of endpoint Firewall, Intrusion Detection, Intrusion Prevention, Operating System Security and Application Controls capabilities provides proactive endpoint protection against known and unknown threats. You manage access control, policy enforcement and deployment from an intuitive web-based console.

BEHAVIOR-BASED REAL-TIME PROTECTION CA HIPS has a learning mode you can use to baseline your existing system behavior and create or adapt security policies accordingly. As a result, you can fine-tune anomaly detection to help reduce false alarms, and customize threat protection to match your business needs.

CENTRALIZED POLICY MANAGEMENT With centrally managed policy creation, deployment and maintenance, the ongoing administration of security policy across the business is both easy and flexible. From the intuitive graphical interface, you can set policies that apply rules for user groups, types of endpoint devices, security functions and security levels.

GRANULAR POLICY AND RULE SETTING Administrators can determine the level of access and control applied to systems, groups of users or individual users. They can also establish a policy that applies to specific users during certain hours, or when they are operating in specific roles or in specific locations.

COMPREHENSIVE EVENT MANAGEMENT The CA HIPS server collects and records the events that occur on each client, and provides filters that the administrator can use to sift for important events. The filtering criteria are offered through a convenient drop-down menu.

POLICY-BASED CLIENT USER INTERFACE CA HIPS provides an intuitive client user interface for end users. Depending on policies set by the system administrator, your end users can see and modify CA HIPS defensive measures for their own PCs, helping to block new attacks on the desktop if necessary. This feature is controlled centrally and can be turned on or off at the administrator's discretion.

GRAPHICAL TECHNICAL AND BUSINESS REPORTS Using the graphical reports in CA HIPS, you can track incidents and look for patterns. Reports allow you to collate, analyze, understand and present threat information, displaying it in tables, pie charts or bar charts.

MULTIPLE LANGUAGES FOR GLOBAL DEPLOYMENTS CA HIPS supports English, French, Italian, German, Simplified Chinese, Brazilian Portuguese and Spanish.

ADMINISTRATOR'S MAIN SCREEN

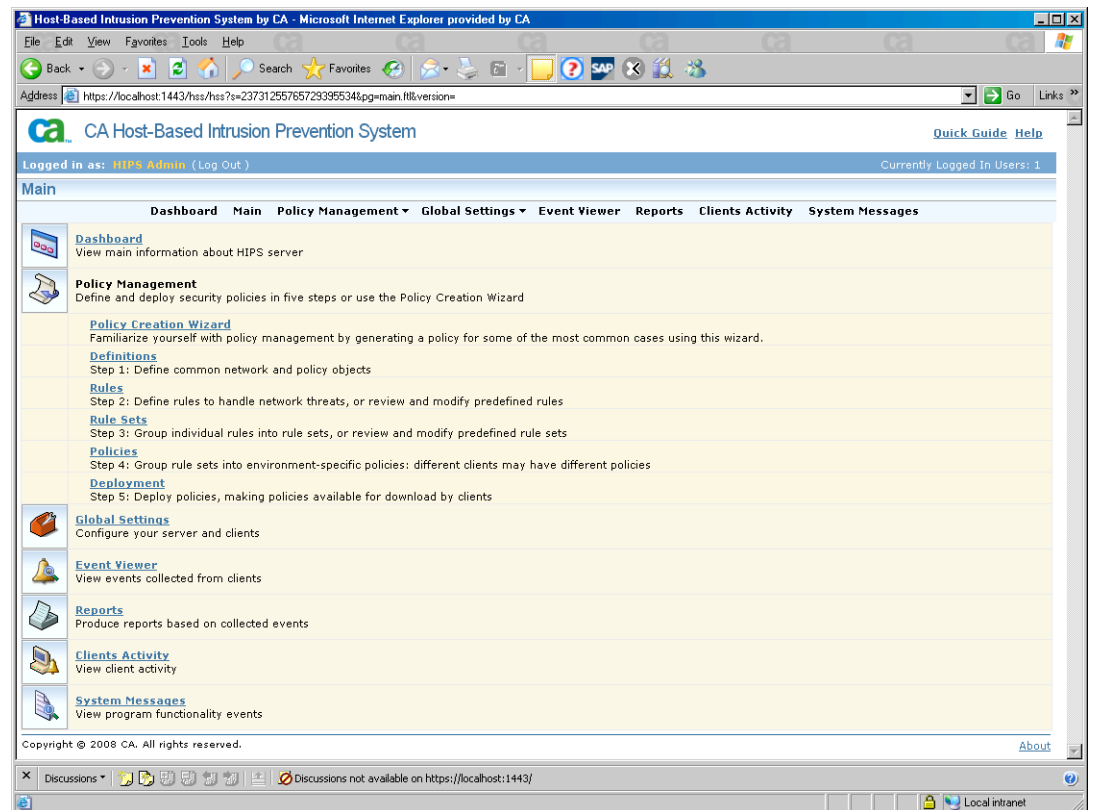


FIGURE A

The CA HIPS Main Screen controls the CA HIPS software in your environment. The Administrator can create and distribute policies and rules to all of the CA HIPS clients in the organization.

CLIENT USER INTERFACE

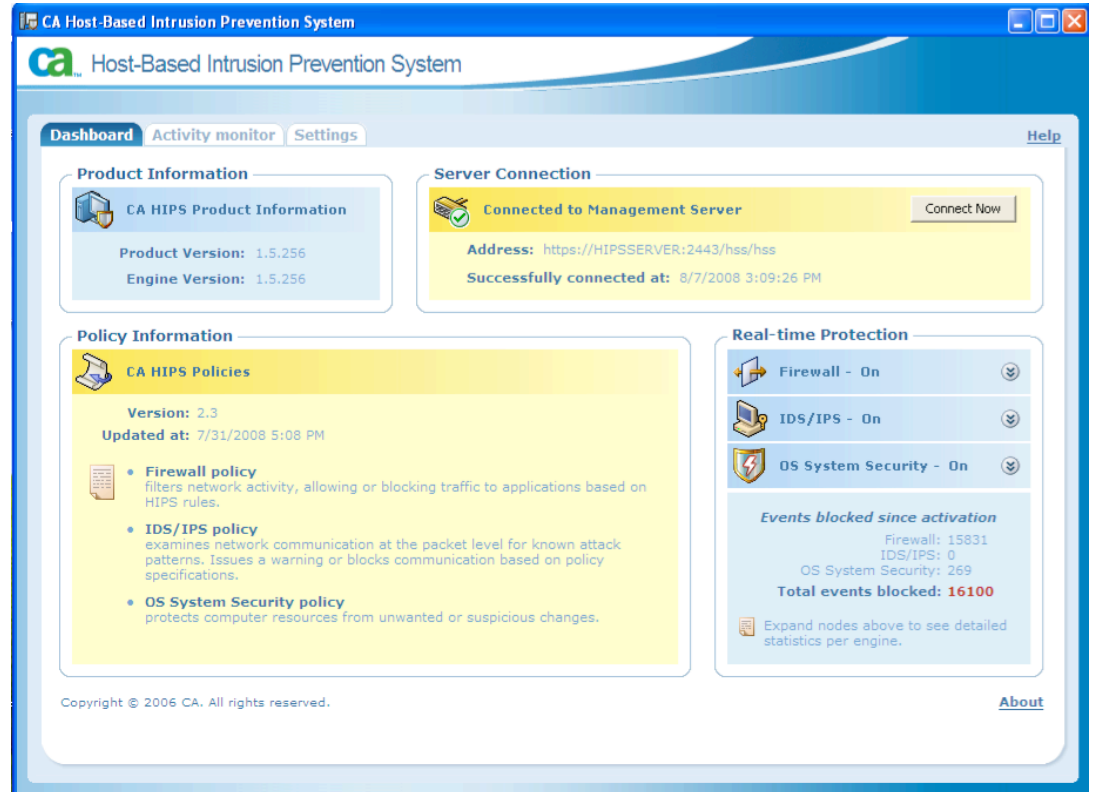


FIGURE B

The CA HIPS Client GUI makes it easy for end users to view security events on their desktops.

CA HIPS Protects Assets, Reduces Downtime and Improves Operational Efficiencies

By applying the real-time, proactive protection — the centralized access control and policy enforcement in CA HIPS — you enhance your endpoint protection against known and unknown threats. CA HIPS helps reduce the risk of downtime by preventing malware, spyware and rogue software from using endpoints to gain access to your network. And fewer threat infections mean lower remediation and help desk costs and greater operational efficiencies.

The proactive anomaly detection in CA HIPS facilitates, service continuity in the face of zero-day threats. Using key intelligence in CA HIPS, system administrators can learn normal system and application behavior and create policies to make anomalies stand out. As a result, you can better protect your IT resources and processes and keep them operating safely in the absence of signature updates. You can use this same intelligence to adapt threat protection to your business instead of the other way around.

Proper security and threat protection are good business practices and depending on the information and IT assets protected, are often mandated by state and federal government regulations. You can use the rich logging and reporting capabilities in CA HIPS to help ease the burden of regulatory compliance. CA does not provide legal advice. No software product referenced herein serves as a substitute for your compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, standard, policy, administrative order,

executive order, etc. (collectively, "Laws")) referenced herein or any contract obligations with any third parties. Please consult with competent legal counsel regarding any such Laws or contract obligations. CA HIPS also leverages existing investments in traditional signature-based endpoint protection solutions, combining with them to create a multilayered threat defense that can detect and remove threats at one layer that may have evaded detection at another.

PRODUCT	FUNCTION	FEATURES	BENEFITS
CA HIPS	Enhances Windows endpoint protection by monitoring network traffic and system behavior proactively and identifying anomalies	<ul style="list-style-type: none"> • 5-in-1 protection • Behavior-based • Centralized policies • Robust reporting 	<ul style="list-style-type: none"> • Easy to install and manage • Real-time protection • Granular control • Easy data analyses

System Requirements and Platforms Supported

The following requirements must be met or exceeded for the CA HIPS server to install and run correctly:

- Intel® Xeon® 3 GHz processor or higher (x86/x64)
- 2 GB RAM
- 80 GB or larger hard disk
- 100/1000mbps network interface card

Supported Server platforms

- Windows 2000 Professional with SP4 Rollup 1
- Windows 2000 Server with SP4 Rollup 1
- Windows 2000 Advanced Server with SP4 Rollup 1
- Windows XP Professional with SP2 (32/64 bit)
- Windows 2003 Server with SP2 (32/64 bit)
- Windows 2008 Server (32/64 bit)

The following requirements must be met or exceeded for the CA HIPS client to install and run correctly:

- 1.6 GHz processor
- 512MB of RAM
- 20 GB or larger hard disk

Supported Client platforms

- Windows 2000 Professional with SP4 Rollup 1
- Windows 2000 Server with SP4 Rollup 1
- Windows 2000 Advanced Server with SP4 Rollup 1

- Windows XP Professional with SP2 and SP3 (32/64 bit)
- Windows Vista with and without SP1 (32/64 bit)
- Windows 2003 Server with SP2 (32/64 bit)
- Windows 2008 Server (32/64 bit)

CA Advantage

CA HIPS complements other products within the CA Threat Management solution, combining to provide a comprehensive, multilayered defense against viruses, spyware, adware, rogue software and other known and unknown threats. CA's integrated threat management strategy is an important part of CA's overall approach to transforming IT management. CA's EITM framework helps you unify and simplify IT management across the enterprise for greater business results.

Next Steps

CA HIPS is a business-ready product that enhances and streamlines existing threat Management. It can help you boost employee productivity, optimize IT resources, ease regulatory compliance and improve service continuity.

Discover how CA HIPS can enhance your endpoint protection against known and unknown threats.

To learn more, and see how CA software solutions enable organizations to unify and simplify IT management for better business results, visit ca.com/products.

Copyright © 2008 CA. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. Windows, the Windows logo, Outlook and Windows Vista are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Intel Xeon are trademarks of Intel Corporation in the U.S. and other countries.

Use of this product is subject to applicable license agreement. Provided with "Restricted Rights" as set forth in 48 CFR 12.212, 48 CFR 52.227-19(c)(1) and (2) or DFARS 252.227-7013(c)(1)(ii), or applicable successor provisions. Manufacturer is CA. CA, Inc., One CA Plaza, Islandia, NY 11749

Learn more about how CA can help you
transform your business at ca.com

