



# HOST INTRUSION DETECTION & PREVENTION



## PERIMETER E-SECURITY

- ▶ Providing a single, complete source for all your security needs since 1997
- ▶ Constant, around the clock monitoring with over 150 security personnel analyzing information 24/7/365
- ▶ Continuous third party assessments including an annual SAS 70 Type II and Cybertrust security audit
- ▶ Three redundant data centers and seven offices nationwide
- ▶ Servicing over 2,000 financial institutions in the United States

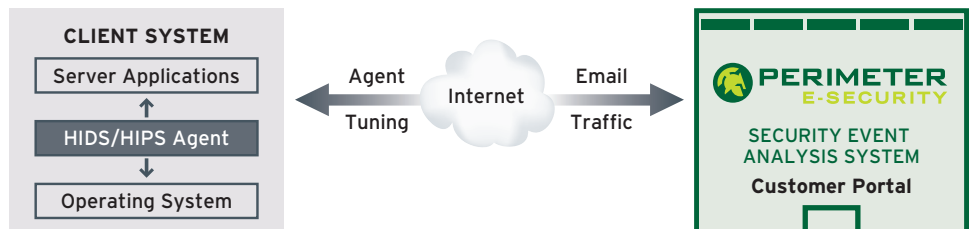
## PERIMETER E-SECURITY HOST INTRUSION DETECTION & PREVENTION OVERVIEW

Perimeter's Host Intrusion Detection and Prevention System (HIDS/HIPS) is our premier service designed to protect your most critical data and servers on your network. It provides an additional layer of defense beyond services such as a managed firewall, Network Intrusion Prevention Systems (NIPS) and signature-based anti virus software. HIDS/HIPS relies on a learning pattern for both known and unknown types of malicious activity. Rather than relying on signature matching for specific attacks, the behavior-based rules associated with HIDS/HIPS products monitor and deny malicious activity patterns. HIDS/HIPS monitors and alerts security operations personnel if activity is suspicious. Security engineers can then analyze the suspicious activity and discuss remediation procedures if necessary with the client.

Because data is often a company's most critical asset, the financial impact of an exploit executing before a signature is released can easily reach millions of dollars for a single outbreak. Accordingly, the cost-avoidance return on investment for the behavioral-based protection offered by HIDS/HIPS can be substantial.

Given the proliferation of new viruses and exploits across the Internet, the ability to proactively stop a new and unknown attack the first time it appears is a tremendous benefit of the HIDS/HIPS approach. With behavioral rules and Perimeter's team of security professionals in place, signatures do not need to be developed and continually maintained to protect systems from the latest attacks.

## HIDS/HIPS PROVIDES THIS BEHAVIORAL SERVICE IN THREE STEPS:



**STEP 1: Setup, install, and tune HIPS agent based on system type & activity**

Complete pre-deployment worksheet → Setup and deploy HIPS agent

Sign off on deployment acceptance form ← Monitor traffic for two weeks and refine rules

**STEP 2: Allow legitimate activity, auto-block certain malicious activity, and alert on possible threats**

**STEP 3: Analyze alerts on possible threats, take action as necessary, and generate reports in Customer Portal**

Call Us Toll Free: 800.234.2175

C W S D Sales Sheet



# HOST INTRUSION DETECTION & PREVENTION

## THE PERIMETER HOST INTRUSION DETECTION & PREVENTION SERVICE

Perimeter's HIDS/HIPS service utilizes the latest On Demand technology which differs from anti virus, network firewall, and NIPS services in that it analyzes activity via customizable behavioral rules to block malicious activity within the system infrastructure. It assumes that companies and employees put their systems at risk by making necessary and productive use of a wide range of Internet resources. Consequently, the service works within each system defined by the customer to monitor and control network actions, local file systems, and other system components while maintaining an inventory of legitimate activity.

Malicious system actions are immediately detected and disabled while other suspicious actions are permitted and alerted on if deemed necessary by security engineers. Both actions take place transparently, without any interruption to the user. If an encrypted piece of malicious code finds its way onto a system via email or web access, for example, as it attempts to unexpectedly execute or alter Cisco Security Agent-protected system resources, it is immediately neutralized and a notification is sent to Perimeter's Security Operations Center.

## THE BENEFITS OF PERIMETER'S SERVICE

Key Features	Benefits
<b>Single Agent Protection</b>	One agent provides preventative protection against entire classes of attacks including port scans, buffer overflows, Trojan Horses, malformed packets, and email worms
<b>Zero Day Attack Prevention</b>	You are protected from known and unknown attacks. You have the ability to enforce your own software patching rules based on your specific needs. Industry leading protection for Unix and Windows servers and Windows desktops
<b>Multiple Agent Support</b>	Perimeter supports both the 32-bit host-based Cisco Security Agent (Platinum Bundle) and the 64-bit signature-based eEye Blink Endpoint Protection Agent (Gold Bundle)
<b>Flexible Agent Architecture</b>	The agent is architected to meet the specific needs of your organization's corporate policies
<b>Customizable Solution</b>	No need to buy multiple agents for multiple systems. Perimeter customizes an agent customized to fit your network

Call Us Toll Free: 800.234.2175