Host Intrusion Detection and Prevention System (HIDS/HIPS)

THE PROBLEM OVERVIEW

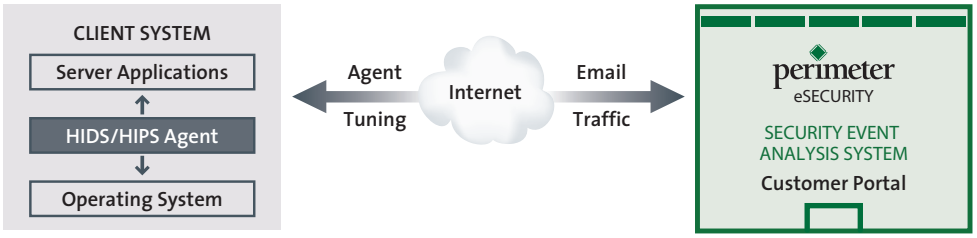
- Hackers can get through firewalls
- Network Intrusion Protection may not stop encrypted malicious traffic
- Anti virus services will stop most but not all viruses
- Internal servers & databases are vulnerable to new and unknown types of attacks
- The system to protect these critical systems needs to be constantly learning and reviewed by security professionals

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 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

perimeter eSecurity™

Complete. On Demand. Affordable.

THE PERIMETER SOLUTION

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.

To decipher legitimate activity from malicious activity, the pre-deployment process associated with this service includes a two-week activity-monitoring period. Subsequently, customized behavioral policies protect the customer's systems by allowing or denying specific system actions. Perimeter will always remain in close communication with the client to continually fine tune the service to block malicious activity, alert on suspicious activity, and ensure that legitimate activity is allowed.

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.

Legitimate activity that triggers a protective rule will be allowed, but monitored and analyzed by Perimeter to verify its legitimacy. If the allowed activity is determined to be malicious, the client will be contacted and guided through remediation procedures. The activity will also be blocked to prevent future attacks. If the allowed activity is not malicious, it will be recorded in the client portal for review and compliance reports.

THE BENEFITS OF PERIMETER'S SOLUTION

Key Features	Benefits
Provides preventative protection against entire classes of attacks including port scans, buffer overflows, Trojan Horses, malformed packets, and email worms	One agent protects against multiple attack methods and lowers cost and time to install
Offers "Zero Day Update" prevention for known and unknown attacks. Provides industry leading protection for Unix and Windows servers and Windows desktops allowing customers to patch systems on their own schedule	You are protected from the latest attack methods. You have the power to enforce your own rules on software patches based on your specific needs
Open and extensible agent architecture offers the capability to define and enforce security according to corporate policy	We architect the agent to meet your corporate policy
Instead of a one-size-fits-all solution, Perimeter provides a solution that is customized for your network	No need to buy multiple agents for multiple platforms – we customize an agent for your needs