Executive Summary

Host Intrusion Prevention Systems (HIPS) complement perimeter defenses, and play a vital role in protecting critical applications and sensitive data from a security breach. As such, the process of selecting the right HIPS – one that provides the required protection while addressing operational security concerns, and minimizing the impact on IT resources – is an important one. This white paper identifies twelve critical questions that organizations need to consider when selecting a HIPS product. These questions relate to protection, manageability, integration and speed.

Table of Contents

Executive Summary ............................................................................................................1
Introduction ..........................................................................................................................2
1. How does it minimize false positives? ........................................................................3
2. Can it prove you were protected? ................................................................................3
3. What platforms does it protect? ..................................................................................4
4. How easy is it to administer and manage? ................................................................4
5. Can it integrate with other security investments? ......................................................5
6. How long will it take to deploy? ..................................................................................5
7. Where does it stop the attacks? ..................................................................................6
8. What impact will it have on performance? .................................................................6
9. How quickly can it be updated with new filters? .........................................................6
10. What kinds of reports are provided? .........................................................................7
11. Has it been certified? ..................................................................................................7
12. How quickly will the HIPS vendor respond? ............................................................7
About Third Brigade® ....................................................................................................8
Introduction

Enterprises today recognize the importance of securing their hosts, applications and data from a security breach. They know that:

→ Financially motivated cyber-criminals are increasingly targeting enterprises;

→ Perimeter defenses, while important, can be readily bypassed or penetrated, often by insiders;

→ It can take weeks or months to fully test and deploy the latest patches for operating systems and enterprise and web applications, leaving a significant vulnerability gap that attackers can exploit;

→ The costs of a breach – including those associated with business disruption, lost revenue, customer turnover, lower productivity, and remediation and support – are high;

→ Regulations, standards, and service level agreements with customers increasingly require additional, host-based compensating controls.

Host Intrusion Prevention Systems (HIPS) have emerged as a security best-practice that address these issues. Because of the vital role that HIPS plays in a proactive, defense-in-depth strategy, the process of selecting the right HIPS – one that provides the required protection while addressing operational security concerns, and minimizing the impact on IT resources – is an important one.

To help ensure organizations evaluate and select the appropriate HIPS product for their environment, here are twelve critical questions that should be asked of every vendor, about their HIPS product.
1. How does it minimize false positives?

The accuracy of a HIPS – as measured by the number of false positives and negatives – is crucial. False positives require investigation that consumes valuable and often scarce IT resources, and can undermine the confidence of business owners. HIPS implementations that rely solely on behavioral analysis must first learn what normal behavior is for a host, and then identify and block strange or anomalous behavior. As such, they must be continuously retrained whenever there is a change to the software running on the host. In contrast, HIPS products that use a blended approach of network techniques—such as stateful firewall, signatures, and other filters that shield known vulnerabilities from unknown exploits, and enforce application and protocol behavior—can be fine-tuned for greater accuracy, and don’t require training. This blended approach also provides organizations with maximum flexibility by allowing them to adjust or tune the HIPS product based on their risk profile.

2. Can it prove you were protected?

While stopping an attack is the ultimate goal of any HIPS, it’s also important to know – and to be able to prove to auditors and other business executives – that your systems were actually protected from a specific threat. With HIPS products that use a behavioral-only approach, you don’t know whether you’re protected unless you test it by launching specific malware. In contrast, filtering-based HIPS products link vulnerabilities with specific rules, so it’s easy to determine whether the necessary protection was in place.
3. What platforms does it protect?

Most enterprises today have heterogeneous IT environments – particularly in the data center, where Windows, Solaris, Linux and other operating systems often run side-by-side – and adopt the latest releases to take advantage of new features. So in addition to supporting a wide range of platforms, it’s also vital that the HIPS vendor quickly support new platform versions (such as Solaris 10, SuSE 10). You simply can’t afford to have your migration plans be constrained or impacted by your HIPS solution. Microsoft Windows Vista and Windows Server “Longhorn” 64-bit versions include PatchGuard, a kernel protection mechanism that is problematic for some HIPS products that rely on kernel hooking. In contrast a HIPS product that uses deep packet inspection to protect vulnerabilities will be compatible with these new Microsoft operating systems.

4. How easy is it to administer and manage?

Security administrators have a lot on their plates. So it stands to reason that any new security product such as a HIPS that is added into daily operations is only going to be successfully deployed and used if it’s easy to administer and manage. One of the biggest factors affecting deployment is accuracy, and the ability to reduce false positives and negatives (see Q1). Any system that generates a lot of false positives is going to require significant operator intervention, which impacts manageability. And too many false negatives means the system isn’t working.

A HIPS product that is easy to administer and manage will have been architected and designed for enterprises. It will be scalable, integrate with directories and other security infrastructure (see Q5), and support multiple administrators by providing role-based access control, and personalized dashboards. Other features to look for include detailed, flexible reporting (see Q10), and scheduled tasks.
5. Can it integrate with other security investments?

Like any good IT security investment, HIPS is a part of the defense-in-depth strategy and should operate in a coordinated fashion with other key security controls. As such, integrating HIPS with other technologies such as Security Information and Event Management (SIM/SEM) systems is one of the best ways to leverage the value of these other investments, and maximize the ROI of the HIPS investment, while minimizing the impact on day-to-day operations. A SIM/SEM can be used to correlate HIPS events with other security events, and for collection and long-term storage of events from HIPS products. Look for a HIPS product that supports (a) a variety of event/log collection methods employed by SIM vendors, including log file forwarding, syslog forwarding, dedicated connectors and common log format initiatives, and (b) web services, to automate tasks and simplify the integration of HIPS with other products. Web services also provide a dynamic response capability, allowing changes to be made in the HIPS rules based on observations from the SIM/SEM or other security systems.

6. How long will it take to deploy?

Deployment time is a function of a number of variables. The approach used (behavioral vs. network) is one of the most important considerations. Any HIPS product that requires a system learning period will take longer to deploy because it must learn what is “normal”. Other features, to look for that will accelerate deployment include:

→ the ability to operate first in detect-only mode, before switching to active prevention;

→ the ability to scan the hosts and automatically recommend the appropriate rules to deploy;

→ the ability to deploy agents to the hosts, and update them, without a system reboot. Rebooting a mission critical server is a sensitive issue, and typically requires significant scheduling and planning.
7. Where does it stop the attacks?

There are two main approaches to HIPS: behavioral- and network-style protection. HIPS products that use a behavioral-only approach examine the characteristics of executing code and attempt to detect and block the ability of executing malicious code to damage the system. This approach to blocking malware can cause application and system instability that results in denial-of-service conditions. Also, the malicious code has the opportunity to neutralize the HIPS software itself, before detection. In contrast, HIPS products that operate at the network-level are proactive: they inspect the traffic stream and block the malicious code before it executes on the host, thus avoiding denial of service situations occurring because of your HIPS software.

8. What impact will it have on performance?

The people responsible for IT Operations are reluctant to deploy security products that have a significant or noticeable impact on system performance. Although any software will impact CPU utilization of the host, and consume some memory, look for solutions that minimize this impact with small-footprint agent software and high performance deep packet inspection.

9. How quickly can it be updated with new filters?

Because new vulnerabilities are constantly being discovered by Microsoft, Oracle and other ISVs, as well as security researchers, a HIPS solution that uses a network approach with filters will require updates. As such, the response time of the vendor to providing new filters to address these vulnerabilities, and the speed with which they can be deployed – ideally without requiring a system reboot – is an important consideration.
10. What kinds of reports are provided?

Reports are an integral part of a HIPS product. Reports provide insights into the security incidents, demonstrate the value of the investment, and provide key stakeholders, including executives, and audit and compliance officers, with the information they need. Good HIPS products come with a wide selection of out-of-the-box reports, in a variety of formats. They also have the ability to drop in new or custom reports, schedule reports and distribute them via email, filter reports based on the information the recipient has access to, and provide the ability to customize queries and export information from the management UI. Be sure to ask how easy it is to generate new reports.

11. Has it been certified?

Certifications are an important means of benchmarking a HIPS products, allowing customers to better understand its capabilities and the platforms it designed to protect, and compare it with similar systems. The Common Criteria (CC) is an international standard (ISO/IEC 15408) for computer security. It provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard manner. If Common Criteria certification is one of your selection requirements, look for HIPS products that have obtained, or are obtaining – because certification can take months – EAL 3+ or higher level of certification.

12. How quickly will the HIPS vendor respond?

Today’s threat environment is rapidly changing. New exploits and vulnerabilities are being discovered on a daily basis. Coupled with a dynamic business environment characterized by new competitive pressures, and regulatory changes it's important that the HIPS vendor be able to both quickly support new platform versions, and respond to support inquiries. Does the vendor’s size, culture and focus support rapid response times?
About Third Brigade®

Third Brigade specializes in providing host intrusion defense systems to organizations that need to detect and prevent attacks that exploit vulnerabilities in mission critical systems. Third Brigade Deep Security allows businesses to apply comprehensive security profiles to hosts that protect against known and zero-day attacks using deep packet inspection. It helps ensure compliance and the 24-7 availability of critical systems, provides a virtual patch for software vulnerabilities, and allows organizations to deliver Internet-based services with greater security and confidence. Unlike other host intrusion detection and prevention systems, Third Brigade Deep Security provides broader, faster and simpler protection.

Third Brigade. That's control.

For more information, please visit [www.thirdbrigade.com](http://www.thirdbrigade.com), or contact us at:

**Corporate Headquarters**
40 Hines Road
Suite 200
Ottawa, Ontario, Canada
K2K 2M5
Toll free: +1.866.684.7332
Local: +1.613.599.4505
Fax: +1.613.599.8191

**United States Headquarters**
11710 Plaza America Drive
Suite 2000
Reston, Virginia, USA
20190
Toll free: +1.866.684.7332
Local: +1.703.903.4479
Fax: +1.613.599.8191

**European Headquarters**
Fetcham Park House
Lower Road, Fetcham,
Surrey, KT22 9HD
United Kingdom
Tel: +44 1372 371210
Fax: +44 1372 371211

“Third Brigade”, “Deep Security Solutions”, and the Third Brigade logo are trademarks of Third Brigade, Inc. and may be registered in certain jurisdictions. All other company and product names are trademarks or registered trademarks of their owners. © 2007 Third Brigade. All rights reserved.