



Intelligent Defense for Enterprise Assets The Need for Host Intrusion Prevention

At the same time that organizations are providing deeper access to their networks for employees, partners and customers enabling flexible work environments and more efficient business relationships – organizations are faced with an increasingly hostile threat environment as well as rising complexity associated with corporate and regulatory compliance. This whitepaper looks at the security challenges faced by organizations and explains how Host Intrusion Prevention (HIP) plays a critical role in an organization's overall security strategy.



TABLE OF CONTENTS

EXECUTIVE SUMMARY	2
ENTERPRISES ARE UNDER SIEGE.....	3
THE CHANGING THREAT ENVIRONMENT	3
INCREASING RISKS.....	4
THE REGULATORY IMPERATIVE	5
SECURITY FORECAST: WORSE TO COME	5
COMMON SECURITY APPROACHES ARE NECESSARY BUT NOT SUFFICIENT....	6
THE PERIMETER IS POROUS	6
PATCHING ALONE IS NOT THE ANSWER.....	8
ECONOMICS OF THE SHRINKING PERIMETER	8
TODAY’S SECURITY BEST PRACTICES	9
A DEFENSE-IN-DEPTH STRATEGY IS IMPERATIVE.....	9
HOST INTRUSION PREVENTION IS YOUR BEST, LAST LINE OF DEFENSE.....	9
BATTLEGROUND: WHERE DOES HIP MAKE SENSE	10
PROTECTING YOUR ORGANIZATION: THE NEED TO ACT NOW.....	10
ABOUT THIRD BRIGADE	11

“Third Brigade”, “Third Brigade, Inc.”, “Payload Normalization”, “Deep Security Solutions”, and the Third Brigade logo are trademarks of Third Brigade, Inc. and may be registered in certain jurisdictions. Other Third Brigade graphics, logos, page headers, button icons, scripts, product names, and service names are trademarks or trade dress of Third Brigade. All other company and product names are trademarks or registered trademarks of their respective owners.

The material provided in this document is for information purposes only. It is not intended to be advice. THIS DOCUMENT IS PROVIDED BY THIRD BRIGADE ON AN "AS IS" BASIS. THIRD BRIGADE MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, AS TO THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS DOCUMENT.

Executive Summary

Internet-based attacks against enterprise networks are unrelenting, more sophisticated and, because today's attackers are motivated by profit, more dangerous to the data and systems those networks hold. Compounding the heightened threat environment, regulatory pressures associated with information security have also increased dramatically. In the new regulatory environment, information security executives must succeed in the battle against these attacks and demonstrate continuous improvement in their defenses. Compliance is not an end state but a process, subject to continuous monitoring, verification, and improvement.

Defense-in-depth is the only viable strategy for data and system protection, but the environment is constantly evolving. Regulators demand the timely deployment of effective solutions. Because malicious code can now evade conventional defenses and penetrate deep into networks, today's security best practices are redefining the perimeter and incorporating host intrusion prevention (HIP) as the last line of defense in comprehensive defense-in-depth security strategies.

While providing many of the same proven security technologies used in perimeter security, such as firewall and anti-virus scanning, HIP solutions also focus on protecting applications by means of application data inspection to provide comprehensive host protection.

Being implemented at the host also means that, in order to be adopted, good HIP solutions need to embody specific characteristics, or be relegated to the shelf as impractical. They must:

- Provide comprehensive protection
- Have minimal performance impact on the host
- Be extremely robust and reliable
- Offer low cost of ownership

With an organization's regulatory compliance, good corporate reputation, brand equity and customer satisfaction at stake, it is imperative that HIP be considered a critical part of the overall information security strategy and that organizations evaluate potential solutions to ensure they are doing everything they can to mitigate the growing risk to their organizations.

Enterprises Are Under Siege

Information security has never been a tougher challenge. At the same time that organizations are providing deeper access to their networks to employees, partners and customers enabling flexible work environments and more efficient business relationships – organizations are faced with an increasingly hostile threat environment as well as rising complexity associated with corporate and regulatory compliance.

Under these pressures, traditional approaches to information security are no longer sufficient to ensure an organization's regulatory compliance, and protect its brand and maintain customer satisfaction. As a result information security professionals are incorporating proven technology in new and innovative ways to better meet the challenge and mitigate security risks.

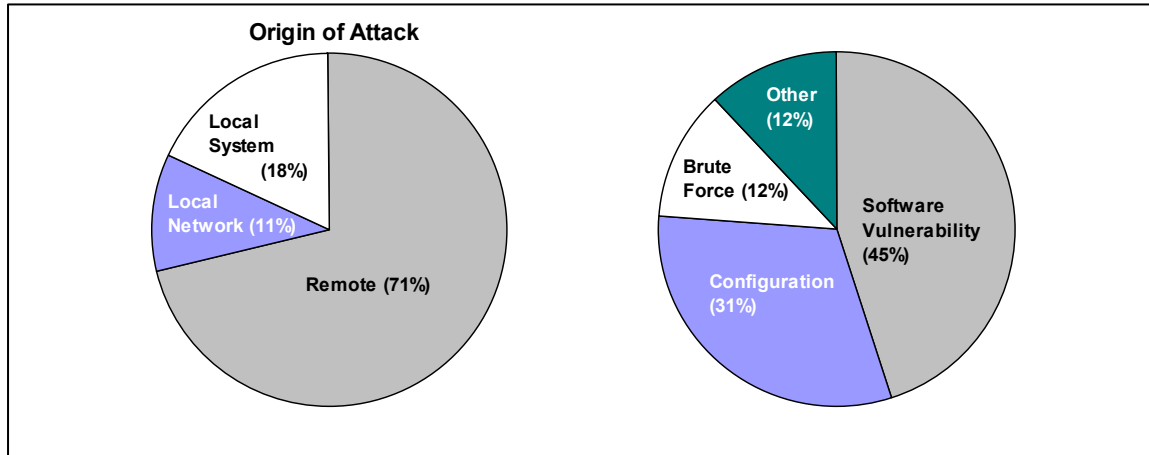
The Changing Threat Environment

Internet-based attacks against enterprise networks are unrelenting, more sophisticated and, because today's attackers are motivated by profit, more dangerous to the data those networks hold. The environment is so hostile that according to recently published tests the average lifespan of a poorly protected PC connected to the Internet is a mere four minutes. The fastest attack observed during the testing took a mere 30 seconds before the machine had been taken over.¹

Not only has the frequency and likelihood of an attack increased, so has the nature of attacks. Compared to a few years ago, there have been significant changes with respect to where attacks are originating and what attackers are exploiting. Today, a greater percentage of attacks are occurring over the network and software vulnerabilities have become the primary point of attack (Figure 1).

¹ Gregg Keizer, TechWeb.com, November 30, 2004 (2:40 PM EST), Unprotected PCs Fall To Hacker Bots In Just Four Minutes, URL: <http://www.techweb.com/wire/security/54201306>

Figure 1: Origin and Types of Attack



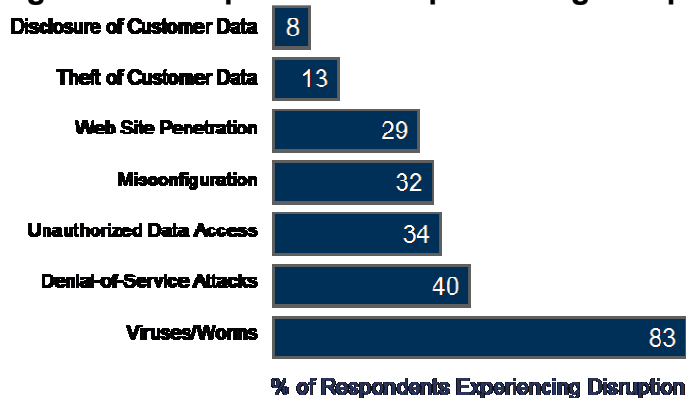
Sources: zone-h.org and Secunia.com Feb. 2005

Increasing Risks

The rising threat environment is not the only thing driving the increased security risks faced by organizations. The consequences of a security breach are also fueling this escalation. Not only are the direct financial damages associated with for profit-cybercrime a concern, so are indirect costs such as lost productivity, erosion of brand equity as well as the consequences associated with regulatory non-compliance.

According to Aberdeen Group, an average company loses \$2 million and 22 hours in downtime to an Internet-based attack. With the majority of organizations experiencing multiple types of incidents in any given year, the direct financial costs are significant. In a recent Yankee Group survey, viruses and worms topped the list of security incidents, with 83% of surveyed organizations reporting this type of attack (Figure 2).

Figure 2: Enterprises Are Experiencing an Epidemic of Security Incidents



Source: The Yankee Group, 2004



The Regulatory Imperative

In today's environment, law-makers and regulatory agencies have made it clear that confidential data must be protected. Individuals and organizations have no alternative. The penalties for failure are severe and not strictly financial penalties but may also include criminal, class-action and civil legal actions against the organization and its directors.

The Health Insurance Portability and Accountability Act (HIPAA) mandates civil fines as high as \$25,000 a person for every violation of a single standard in a given year and violations leading to gain or harm can bring fines up to \$250,000 and ten years in prison. Penalties under Sarbanes-Oxley legislation are even harsher – as much as \$5 million in fines or 20 years in prison. Violations of the Gramm-Leach-Bliley Act (GLBA) requiring banks and financial institutions to protect consumer information can lead to fines of up to \$100,000 per violation for officers and directors, and prison terms up to five years.

According to the Federal Information Security Management Act (FISMA), federal departments and agencies are required to implement "risk-based, cost-effective approaches to secure their information and systems, identify and resolve current IT security weaknesses and risks, as well as protect against future vulnerabilities and threats."

Security Forecast: Worse to Come

Sophisticated attempts to penetrate a corporate workstation or server will almost certainly succeed – the odds approach 100 percent – and such attacks are increasing. Application level threats range from generic threats such as worms which have been created to apply to a wide set of systems, to more targeted and sophisticated attacks such as SQL injection attacks. Firewalls and virus scanners cannot detect or prevent these and similar attacks.

More and more vulnerabilities are being published, enabling attackers to create more malicious code in a shorter period of time, often before software vendors can create and release patches. And with the proliferation of new and easy-to-use hacking tools, the skills necessary to launch attacks is decreasing.

Common Security Approaches Are Necessary But Not Sufficient

Most organizations as a minimum deploy a common set of network defenses to establish a security perimeter or multiple security zones. Generally this includes network firewall, anti-virus and network intrusion detection capabilities.

Unfortunately due to the nature of the modern network and the sophistication of the attackers, perimeter security defenses are often circumvented. To address these deficiencies, organizations have turned to patching as quickly as possible as a means of eliminating vulnerabilities – unfortunately this is a race that attackers regularly win.

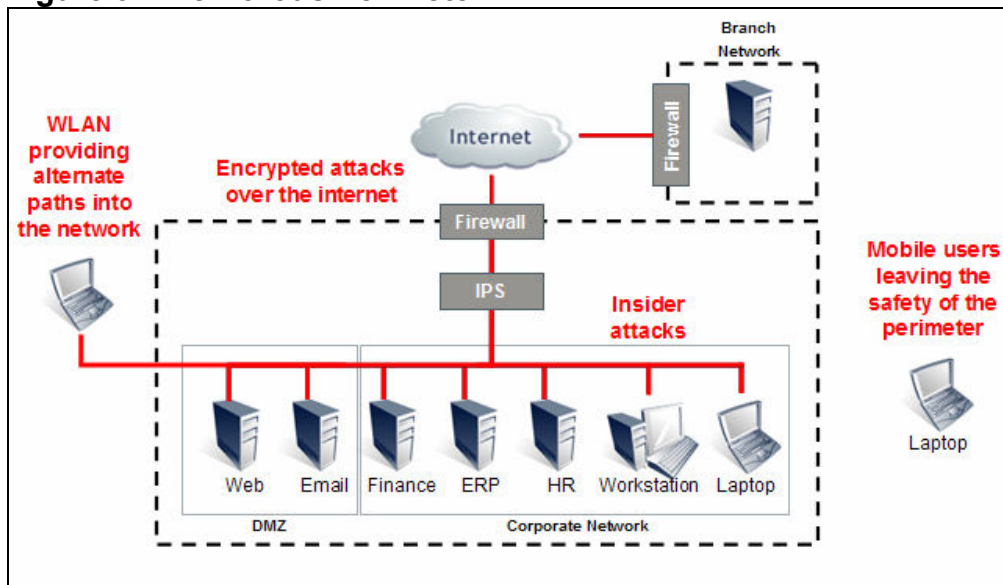
The Perimeter is Porous

The traditional network perimeter is changing to accommodate globalization, consolidations, systems modernizations, mobile computing, and wireless LANs. Together these are forcing networks to be opened to partners, regulators and service providers, which make them more porous and vulnerable to attack (Figure 3). Increasingly, organizations are testing the limits of IT security, looking to web services to extend their reach and create closer links with customers and partners. The enabling technologies, however, can allow malicious code deeper into the enterprise.

“The enterprise perimeter has changed greatly during the past several years. It now passes through mobile devices, because laptops and PDAs (personal digital assistants) often are used outside the corporate firewall. Wireless LANs allow external connections that bypass firewalls. The increasing use of Secure Sockets Layer, particularly as part of Web services, and other forms of encryption (session and data) can blind perimeter firewalls and intrusion prevention systems. Threats have changed, with rapidly propagating worms causing tremendous costs to enterprises when these worms spread across the infrastructure.”

**Gartner, Inc., “Management Update: It’s Time for Host-Based Security Platforms”
John Pescatore et al, March 17, 2004**

Figure 3: The Porous Perimeter



Going over the perimeter wall

Wireless networks provide alternate paths into the organization that often by-pass perimeter security defenses. In effect this type of access not only adds ways into the network but also circumvent many the advantages offered by physical security of the network.

Leaving the protection of the perimeter

One of the major tools that attackers target as a means of launching an attack are individual PCs. Given today's flexible work environment, many of the PCs that attach to the network are mobile and travel outside the protection provided by the network or are home machines that permanently reside outside the control of the IT department. While outside the defensive perimeter, these machines are easily compromised and can be used as launching points for more sophisticated attacks against the organization the next time they connect to the network, inside the perimeter.

Tunneling through perimeter defenses

Ironically, the increasing trend towards encrypting data in transit or storage means malicious code can 'hide' from firewalls, virus scanners and other safeguards until it reaches its end point on a server. Attacks can utilize SSL/TLS or IPsec as a means of tunneling the attack all the way to the host – depending on the target of interest.

Patching alone is not the answer

The time between the publication of a vulnerability and the malicious code that exploits it has been narrowing sharply – from months and weeks down to days, and in some cases, even hours. Meanwhile, the time to create patches and distribute them to network administrators remains relatively fixed and dangerously long. Patching entails risk - IT administrators need to properly test and schedule a patch to ensure the least disruption. The fear that a hastily deployed patch could cause a major business disruption is a very real one and dictates a minimum amount of effort and time to ensure the patch isn't worse than the vulnerability it's intended to protect.

“As cyberattackers become more efficient at quickly exploiting software vulnerabilities, IT security managers will not be able to patch faster than all cyberattacks. Implement vulnerability management and intrusion prevention approaches to prevent and respond quickly to cyberattacks.”

Gartner, Inc., “Predicts 2005: Security Focuses on Attack Prevention” John Pescatore et al, October 29, 2004.

The changes observed in internet worms over the last two years provide a good indication of the risks associated with security strategies that rely heavily on patching. MS Blast, Sasser and Santy are a few examples of worms that exploited vulnerabilities where patches had been available weeks and months in advance of each outbreak. Additionally, the time between notification of a vulnerability and the outbreak of a worm that exploits it has shortened considerably from 28 days for MS Blast in 2001 to only 1 day for Santy in 2004. Mass exploits, like worms are not the only concern, targeted exploits against both known (public) and unknown vulnerabilities in OSs and application is on the rise. Unfortunately, all indicators strongly point to this trend continuing and with critical patches coming out monthly, no organization can guarantee that they can patch on time.

Additionally, patching can not protect organizations against vulnerabilities that they are unaware of. Often referred to as unknown vulnerabilities – this type of risk is the result of an attacker becoming aware of a vulnerability and generating a exploit for it, before either the application vendor is aware of the issue or has created a patch and notified the all the potential targets. Exploits taking advantage of unknown vulnerabilities represent a significant percentage of successful attacks and it is clear that in these types of situations organizations need to turn to compensating controls other than patching for protection.

Economics of the Shrinking Perimeter

Another approach to the problem has been to employ the same perimeter security techniques to continually shrinking security zones. From a security perspective this is advantageous because it introduces layers of defense as well as providing the ability to tune the control to the specific needs of the asset or assets being protected. However, the economics of this approach have a meaningful impact on the nature and scope of these controls. As the perimeter shrinks the use of hardware based solutions to protect

smaller and smaller zones becomes too costly and at some point necessitates a software based approach. Additionally, while the size of the zones shrinks the number of zones increases, putting an increased value on the ability to centrally manage large number of zones in a cost effective way. Taken to the extreme, the perimeter shrinks to the boundary of the host itself.

Today's Security Best Practices

Traditional network security, firewalls, and detection systems are important elements of a secure computing environment but insufficient on their own. Given the ways that the traditional network perimeter can be breached, today's security best practices implement a defense-in-depth strategy to protect organizations from attack.

A Defense-in-Depth Strategy is Imperative

Defense-in-depth assumes that no single component, policy or process can assure security. The modern computing environment is too complex and diverse. Attackers have access to the same vulnerability bulletins as everyone else, and a growing range of automated tools with which to exploit them. The potential risk of failure and regulatory penalties requires security managers not just to arm themselves against a minimum standard of documented threats but to anticipate the unknown: in effect, to 'prove a negative', and show they are not insecure.

Defense-in-depth is a dynamic process, involving a continuing cycle of risk assessment, response, and evaluation. An initial deep penetration and security audit, with special attention to servers with critical information establishes a security baseline. Once that is established, a solid defense-in-depth strategy can be created.

Host Intrusion Prevention is Your Best, Last Line of Defense

With the relative ease that many types of attacks by-pass perimeter security, security professionals are implementing multi-layered defenses with the last line of defense implemented at the host itself. This last line of defense is the role that Host Intrusion Prevention (HIP) solutions play in a comprehensive defense-in-depth security strategy.

While providing many of the same proven security technologies used in perimeter security, such as firewall and anti-virus scanning, HIP solutions also focus on protecting applications by means of

"Host-based intrusion prevention (HIP) systems have exploded onto the market to preserve the integrity of server configurations against network attacks. Network-borne intrusions have demonstrated the ability to easily pass through layers of network defenses before slamming into the hosts that are serving critical business applications over the Web...Business demands a solution that will protect application revenue streams and ensure compliance with corporate audit requirements."

**The Yankee Group, Phebe Waterfield,
March, 2005**



application data inspection and application behavior control to provide comprehensive host protection.

Being implemented at the host also means that, in order to be adopted, good HIP solutions need to embody specific characteristics, or be relegated to the shelf as impractical. They must:

- Provide comprehensive protection
- Have minimal performance impact on the host
- Be extremely robust and reliable
- Offer low cost of ownership

Battleground: Where Does HIP Make Sense

The purpose of information security programs and controls is to cost-effectively reduce security-related business risks to an acceptable level. When using risk as the measure to determine where HIP makes the most sense, organizations are looking at:

- High threat environments such as the DMZ where probes and attacks are frequent
- High value hosts where the value of the asset either to the organization or the attacker is significant and warrants additional controls
- Hard to patch environments that remain vulnerable longer because they are not easily patched.

Protecting Your Organization: The Need to Act Now

Today, attackers can analyze a vulnerability and develop an exploit so quickly that traditional protection is inadequate. With no patch to plug the hole, or no signature to identify and block the malware, the enemy is within the gates before you know it. And the problem is becoming more critical. Even while security managers struggle to protect their networks, senior management is demanding greater openness, through mobile computing, wireless networking, Web applications and closer online relationships with suppliers and customers.

With an organization's regulatory compliance, good corporate reputation, brand equity and customer satisfaction at stake, it is imperative that HIP be considered a critical part of the overall information security strategy and that organizations evaluate potential solutions to ensure they are doing everything they can to mitigate the growing risk to their organizations.

For organizations looking for a layered defense-in-depth strategy that includes HIP, find out more about products and solutions offered by Third Brigade, please visit www.thirdbrigade.com.



About Third Brigade

Third Brigade specializes in providing intrusion prevention systems (IPS) to health care, government, telecommunications, financial services and other organizations that need to prevent attacks that exploit vulnerabilities in commercial and custom software, including web applications. It enables you to create and enforce comprehensive security policies that proactively protect critical applications, sensitive data, and hosts, ensure regulatory compliance, and maximize the performance of your people, processes and hosts. Unlike other intrusion prevention systems, Third Brigade's is not intrusive. It has been architected from the ground-up for intrusion prevention, and is smaller, faster and simpler.

For more information, please visit www.thirdbrigade.com, or contact us at:

Corporate Headquarters

40 Hines Rd
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 20190
USA
Toll free: +1.866.684.7332
Local: +1.703.903.4479
Fax: +1.613.599.8191