Defending Against Increasingly Sophisticated Cyber Attacks
HP TippingPoint Bolsters Enterprise Data Center Protection
The Evolving Enterprise Security Threat ................................................................. 3
Driving Trends ........................................................................................................... 3
Key Challenges ........................................................................................................... 4
Recent High-Profile Security Breaches ................................................................. 5
Protecting Enterprise Physical and Virtual Data Centers ...................................... 6
Meeting Critical Enterprise Needs .......................................................................... 6
Optimizing for a Virtualized Environment ............................................................ 8
Weighing Vendor Solutions .................................................................................... 8
Why HP? .................................................................................................................... 9
HP DV Labs’ Cutting Edge Research ........................................................................ 9
Benefits of HP’s NGIPS Technology ...................................................................... 10
The Last Word .......................................................................................................... 12
THE EVOLVING ENTERPRISE SECURITY THREAT

The modern cyber threat landscape requires enterprise organizations to be more vigilant than ever in their mission to protect sensitive data and network resources. Administrators and information security professionals seek tools that can protect networks, applications and endpoints from the most complex and furtive cyber attacks. The network intrusion prevention system (IPS) provides threat detection technologies that make it an indispensable component in a layered, “defense-in-depth” enterprise security architecture.

There are several new IPS products, technologies, and features available in the market today that can have a notable impact on security efficacy, cost, scalability and usability. Whether replacing an existing IPS deployment or evaluating an initial purchase, enterprise organizations must evaluate the solution that best meets their security and business value requirements. This paper will outline the top factors that enterprise organizations should consider when evaluating an IPS deployment.

Driving Trends

The ability to protect enterprise networks and sensitive data is the primary factor when evaluating IPS solutions. Enterprise security teams face highly sophisticated network attacks that are carefully crafted by dedicated and skilled hacker groups. Now, cyber attacks are perpetrated for much more clandestine and criminal purposes than in previous years.

Today, hacker groups are employed or sponsored by nation-states or criminal organizations. State-sponsored hacker groups engage in espionage or sabotage against specific corporate or government targets. Criminal hacker groups are more opportunistic but will still target specific organizations. In both cases, a highly motivated hacker uses sophisticated exploits and malware in a long-term, multi-stage attack campaign. This type of attack is known as an advanced persistent threat (APT).

The first stage of an APT is to penetrate network defenses undetected. The attacker will attempt to obfuscate evidence of its activities and disable other detection systems. The attacker can then move throughout a network in search of sensitive customer data, valuable intellectual property and state secrets. At this point, the attacker can perform a number of actions, such as stealing sensitive data, sabotaging systems, or siphoning computing resources. These attacks are very effective at going undetected and can continue for several months or even years.
Chart 1 illustrates the processes used in an APT attack.

<table>
<thead>
<tr>
<th>STEP</th>
<th>GOAL</th>
<th>EXAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>PENETRATE NETWORK</td>
<td>EXPLOIT A ZERO-DAY VULNERABILITY TO COMPROMISE A WEB APPLICATION SERVER</td>
</tr>
<tr>
<td>2</td>
<td>OBfuscATE EVIDENCE</td>
<td>CHANGE OR DELETE LOG INFORMATION, DISABLE ANTIVIRUS UPDATE SYSTEMS</td>
</tr>
<tr>
<td>3</td>
<td>EXPLORE AND SPREAD THROUGH NETWORK</td>
<td>FIND CUSTOMER DATABASE SERVERS AND FINANCIAL RECORDS</td>
</tr>
<tr>
<td>4</td>
<td>STEAL OR SABOTAGE DATA AND SYSTEMS</td>
<td>INSTALL BACKDOORS AND BOT SOFTWARE, EXFILTRATE DATA, MANIPULATE PLC SYSTEMS</td>
</tr>
</tbody>
</table>

Source: Frost & Sullivan analysis

**Chart 1 – The Advanced Persistent Threat Lifecycle**

Even organizations that do not store or transmit sensitive data will have computing resources that can still be used by hackers for other criminal purposes. Hackers can recruit these stolen resources to send spam and perform massive distributed denial-of-service (DDoS) attacks and as a proxy for illicit data transfers. The victim will suffer diminished availability of computing resources and will also be liable for any damages, depending on applicable laws.

**Key Challenges**

First and foremost, enterprise organizations are challenged to protect the integrity and confidentiality of corporate and customer data and the availability of network resources from skilled and persistent attackers. Moreover, businesses must defend against sophisticated attacks, while also managing a steadily growing number of traditional Web and e-mail attacks. Essentially, enterprise security teams are expected to protect against more challenging threats, often without a compensatory increase in funding.

The security process is further complicated by pressure to adopt emerging technologies such as virtualization and cloud computing, and workplace trends such as information technology (IT) consumerization and employee mobilization. Virtualization and cloud computing are technology trends that emerged in recent years, enabling businesses to maximize their return on IT investments.

Virtualization describes the technology to separate software logical layers from hardware layers. This hardware independence enables businesses to deploy multiple virtual computers on a single hardware platform in order to best leverage the hardware’s capabilities. Businesses can also virtualize memory, data storage, processing, and networking for security and efficiency purposes.
Cloud computing is simply the delivery of data processing and storage as a utility service. Large service providers pool computing resources together and then bill enterprise customers based on how much of these resources are utilized over a given time period. Cloud computing offers the advantage to shift large capital expenditures to nominal operational expenses, making this a compelling offering for enterprise organizations.

New technologies and business practices enable greater organizational efficiencies but can also increase risk. Virtualization can bypass traditional inspection technologies offered in network-based security products. Cloud computing requires businesses to rely on the service provider to secure the cloud infrastructure, but to then secure their own virtual environments and assets. Employee-owned mobile devices require the enterprise to contend with a vastly larger set of operating systems and device-specific vulnerabilities than when all connecting devices are corporate-issued and managed.

**Recent High-Profile Security Breaches**

Any organization can be the victim of a data security breach if it fails to address the challenges presented by advanced threats and new technologies. In recent years, numerous multinational corporations, government agencies, and even branches of the armed services have made headlines as victims of APTs and advanced malware.

- **Operation Blitzkrieg (2012-2013)** is a current campaign to attack and breach as many as 80 financial institutions in Western countries. The attack is based on a set of customized variants of a known Trojan virus. This malware will emulate victims’ computers to transfer funds to illicit accounts and will accompany a DDoS attack designed to disable fraud response systems.

- **Operation High Roller (2012)** is an APT targeting financial institutions in Europe and in the United States. This APT targets wealthy victims to ensure successful large fund transfers. It utilizes very advanced tactics to defeat pin-and-chip authentication systems, process fraudulent transactions through dedicated servers, and automate a database of mule accounts.

- **Stuxnet (2010), Duqu (2011), and Flame (2012)** are extremely sophisticated malware designed to target high-value targets in Iran, Syria, Egypt, Saudi Arabia, and the West Bank for espionage and sabotage purposes. These advanced viruses utilize techniques such as malware modules, rootkit functionality, evidence removal, keylogging, audio recording, authentication using stolen certificates and zero-day vulnerabilities.

A zero-day vulnerability is any software flaw that is unknown to software and security vendors until it is used in an exploit. These vulnerabilities are particularly effective when they enable hackers to execute code on targeted systems. Unfortunately, the majority of reported vulnerabilities enable code execution, as shown on the next page in Chart 2.
PROTECTING ENTERPRISE PHYSICAL AND VIRTUAL DATA CENTERS

The network IPS appliance has been the traditional method to detect anomalous behavior, malware, and intruders. Though these systems still provide protection against the majority of network attacks, enterprise organizations now face advanced threats that can evade detection by IPS signatures.

Meeting Critical Enterprise Needs

A next-generation intrusion prevention system (NGIPS) offers the best-of-breed threat detection and prevention capabilities necessary to stop advanced malware and APTs. NGIPS provides holistic contextual awareness, including visibility into endpoints, operating systems, network services, protocols, application types, content and user identity. This wealth of data improves the NGIPS's ability to analyze and baseline network traffic and events. Therefore, greater contextual awareness enables NGIPS devices to identify suspicious behavior and other indicators of slow, “under-the-radar” attacks.

NGIPS also includes advanced threat detection engines. Traditional IPS detection methods, such as vulnerability and exploit signature matching, can only detect known malware and can be defeated by slight alterations to existing malware code. To prevent IPS evasion, a NGIPS should offer advanced detection capabilities, including behavior anomaly detection, IP reputation, and heuristics. These detection methods empower enterprise organizations to defeat custom-tailored exploits, zero-day attacks and polymorphic malware, in addition to the massive amounts of daily non-specific Web and e-mail threats.
Defending Against Increasingly Sophisticated Cyber Attacks: HP TippingPoint Bolsters Enterprise Data Center Protection

Chart 3 compares NGIPS and IPS functionality.

<table>
<thead>
<tr>
<th>IPS</th>
<th>NG IPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Exploit signatures</td>
<td>• IPS functionality, plus:</td>
</tr>
<tr>
<td>• Vulnerability signatures</td>
<td>• Application awareness</td>
</tr>
<tr>
<td>• Anomaly detection</td>
<td>• Application control</td>
</tr>
<tr>
<td>• Behavior analysis/heuristics</td>
<td>• User identity awareness</td>
</tr>
<tr>
<td>• Inline blocking</td>
<td>• Advanced detection engines</td>
</tr>
<tr>
<td></td>
<td>• IP reputation</td>
</tr>
<tr>
<td></td>
<td>• Basic DLP</td>
</tr>
<tr>
<td></td>
<td>• DDoS Prevention</td>
</tr>
<tr>
<td></td>
<td>• Botnet detection</td>
</tr>
<tr>
<td></td>
<td>• Evasion detection</td>
</tr>
</tbody>
</table>

Source: Frost & Sullivan analysis

Chart 3 – Comparison of NGIPS and IPS Functionality

While security breaches are currently a top concern for enterprise organizations, customers also expect security solutions to represent a safe investment. For this reason, NGIPS products should support enterprise requirements for network latency and throughput. A NGIPS must collect and analyze an escalating amount of data to be effective, but must accomplish this with little impact to systems availability.

To support network throughput requirements, leading NGIPS products are purpose-built with custom hardware to accelerate inspection and analysis processes. Soon, NGIPS will also be expected to support other methods to increase throughput, such as combining multiple connections, also known as link aggregation.

Moreover, NGIPS should offer sufficient performance to support current network requirements as well as future organizational growth. Enterprise communications increasingly rely on IP networks, and this demand will only increase, owing to greater numbers of users, computing devices, adoption of data-intensive Web applications, Voice-over-IP (VoIP), streaming video and online conferencing.

NGIPS should deploy as a transparent bridging appliance. As such, the device can be easily deployed as a “bump in the wire” and will not require an IP address or changes to the network. This will greatly simplify the acquisition, approval and deployment process.

Platform flexibility is an essential factor that determines the NGIPS’s ability to adapt to ever-changing security requirements. Every organization will have unique security goals, compliance objectives and network environments that will be important considerations in the present. However, a NGIPS should offer the ability to easily add new security functions in order to adapt to environmental and threat changes. For example, a business may not need WAF functionality until it develops and deploys a business-critical custom Web application.
OPTIMIZING FOR A VIRTUALIZED ENVIRONMENT

Another factor that impacts business value is support for new technologies and the future-readiness of a NGIPS. For example, physical network security appliances are unable to inspect communications between virtual machines (VMs). Thus, at a minimum, a NGIPS product portfolio should include virtual appliances to monitor inter-VM communications on a single host.

Initially, virtual IPS appliances were simple ports of the software offered on a physical NGIPS appliance. Going forward, the NGIPS operating system should be designed with virtual environments in mind since virtual appliances do not benefit from dedicated or purpose-built hardware acceleration.

Virtual NGIPS appliances enable enterprise organizations to secure virtual environments. However, a combination of virtual and physical-layer NGIPS protection is essential for fully protecting private, hybrid and public cloud environments. In addition, a security solution that allows customers to migrate from physical to virtual to cloud-based infrastructures, while maintaining the same levels of protection, can accelerate the adoption of securing critical assets.

Weighing Vendor Solutions

There are key factors to consider as enterprise organizations evaluate the NGIPS options available. First, NGIPS must offer true next-generation functionality to assure security efficacy. NGIPS builds upon traditional IPS by collecting much more comprehensive contextual data from network packets. At a minimum, NGIPS should identify and control applications and end users. NGIPS must also offer advanced detection engines, including behavior anomaly detection, IP reputation and heuristics.

Leading NGIPS vendors will support these detection capabilities with ongoing research and product development efforts. Enterprise organizations should prioritize vendors with extensive and global research expertise. This research is necessary to adapt to changing and evolving threats because research labs can identify new or advanced malware and quickly update NGIPS detection systems appropriately.

NGIPS vendors must leverage purpose-built appliances with hardware acceleration in order to function at enterprise network throughput levels with minimal latency. This product performance should be validated by independent, third-party labs using realistic network traffic. NGIPS appliances must offer excellent port-density to support bandwidth requirements and should support 40GbE, which is increasingly adopted in enterprise networks. NGIPS should also support standards such as IEEE 802.1ax Link Aggregation Control Protocol (LACP).

Enterprise organizations should consider NGIPS solutions that offer deployment flexibility and expandability in order to adapt to environmental and threat changes. Hardware modules or software blade models offer the ability to easily expand security services as future requirements dictate. However, a broad line of network appliances will continue to be required as different
security functions require unique deployment scenarios. Finally, the NGIPS portfolio should include virtual appliances. Ideally, the NGIPS operating system should be purpose-built to support virtual and cloud environments.

**WHY HP?**

**HP DVLabs’ Cutting-Edge Research**

HP TippingPoint offers a compelling portfolio of NGIPS products that are supported by the HP Digital Vaccine Labs (DVLabs), a leading provider of original vulnerability research. DVLabs discovers, analyzes, and responsibly discloses vulnerabilities in enterprise software and network services. This data is then used to develop and deliver protection updates in HP TippingPoint NGIPS solutions. This is very unique for a security appliance vendor, where most research teams, by necessity, spend the majority of their efforts on simply adding signatures based on publicly known vulnerabilities versus doing actual research into discovering new ones.

This original vulnerability research is further supplemented by the HP DVLabs Zero Day Initiative (ZDI) program. ZDI encourages and leverages the expertise offered by the independent research community. HP DVLabs ZDI works with vetted independent researchers to find and report new vulnerabilities to affected software vendors. By doing so, ZDI ensures that software vendors receive reliable and actionable vulnerability reports with which to create a patch. As a result, HP TippingPoint products are continually updated with protection filters developed directly from the unique data provided by its premier research labs.

Chart 4 illustrates HP’s proficiency in the vulnerability research market.

![Chart 4 – Percent of Reported Code Execution Vulnerabilities by Source, Global, Q3 2012](chart)

Furthermore, HP TippingPoint leverages this research expertise to develop new security products and technologies.
Benefits of HP’s NGIPS Technology

In 2012, HP TippingPoint announced a new line of NGIPS products called the HP TippingPoint NX NGIPS Platform. Its architecture provides core services that provide essential protection against advanced malware and APTs and the design principle for future network security solutions, extending well beyond NGIPS.

Figure 1 – HP TippingPoint NX NGIPS Platform

HP’s NGIPS supports the ability to inspect and control traffic based on end-user identity and applications, including Web-based applications such as streaming media and social networking. This includes granular controls to block application traffic where necessary or to rate-limit this traffic when appropriate. This functionality is necessary to address the ever-increasing amount of application traffic on enterprise networks and in response to the increasing frequency of application-level attacks.

HP NX NGIPS products are updated with security intelligence feeds from the HP Reputation Services Security Module. Using Reputation Services, enterprise organizations can automatically blacklist resources known for phishing, illegal data collection, and malware hosting. HP DVLabs’ advanced security intelligence feeds further improve HP NX NGIPS products’ ability to identify and block hosts that have been compromised and are under the control of unauthorized third parties. The Reputation Services Security Module provides the extra contextual data that is necessary in order to detect the most advanced, stealthy network attacks faced by enterprise organizations.

Compromised endpoints may be converted into automated “bots” and controlled by a hacker as part of a massive botnet for additional attacks or to send spam. This software technology identifies and blocks endpoint communications with botnet command and control centers. Thus, this feature reduces the lost resources and potential liability stemming from unintentional participation in a hacker’s botnet.

HP TippingPoint NX NGIPS products also integrate Web Application Protection Module and Services. Because Web applications are unique, they are often unprotected by off-the-shelf protection services offered in IPS or NGIPS products. The HP TippingPoint Web Application Protection Module and Services analyzes custom applications in an enterprise organization, then provides protection until the application code itself can be fixed. Enterprise organizations can also create custom filters to protect legacy or industry-specific applications using the HP Digital Vaccine Toolkit.
These features help improve the security of an enterprise organization’s network systems and data. However, HP NX NGIPS platforms are also designed to meet enterprise requirements concerning scalability and flexibility. Customers can then easily expand this functionality to meet future threats, compliance requirements, or business objectives. Thus, HP NX NGIPS can be deployed as an IPS solution or with integrated vulnerability management, network behavior anomaly detection, and forensics tools. This deployment flexibility ensures that customers can implement the security technologies needed now, while easily expanding this functionality set as future requirements dictate participation in a hacker’s botnet.

HP NX NGIPS products offer excellent scalability in terms of port density and network throughput. The HP NX NGIPS platform can be reconfigured with various network modules, enabling enterprise organizations to support various network speed requirements, including up to 13 Gigabit per second (Gbps) inspection throughput. The ability to easily expand network throughput without replacing the appliance greatly improves customer value.

Enterprise organizations are also challenged to adopt cloud services in a way that integrates seamlessly and securely with existing infrastructure. HP’s Converged Cloud strategy integrates virtual and physical security technologies with HP CloudSystem and Cloud Services Automation (CSA). This strategy provides a more comprehensive solution to the security challenges presented by virtual and cloud computing environments. Integrated security and virtualization technologies from HP will enable enterprise organizations to create and implement uniform security policies and visibility across the entire infrastructure. The ability to manage and monitor the complete network infrastructure with familiar tools and processes is essential to successful adoption of a value-adding virtualization strategy.

Finally, an important factor is the integration of IPS event data into SIEM (Security Information and Event Management) platforms. HP NX NGIPS platforms provide tight integration with HP ArcSight, allowing enterprise organizations to correlate collected data with other security tools in the HP Security Intelligence and Risk Management (SIRM) platform. This level of integration is necessary to baseline network traffic, which can be used to monitor, measure and analyze network performance. This is a necessary best practice to find anomalous behavior and data breaches, and also centralizes the data archiving for baselining and auditing purposes.
THE LAST WORD

Today’s enterprises face a number of new and seemingly overwhelming cyber threats, driving the need for NGIPS products that can successfully defend network systems and sensitive data. However, NGIPS products must also meet enterprise requirements in terms of scalability and flexibility. Traditional network defenses are essential but are unable, without sufficient context and security intelligence, to sufficiently defend against the sophisticated attacks that enterprises encounter on a daily basis.

Frost & Sullivan believes that enterprise organizations must invest in a NGIPS that provides greater contextual awareness, advanced threat detection capabilities, enterprise scalability, flexibility, and comprehensive strategies for virtualization and cloud computing deployments. HP’s focus on flexibility, advanced protection features, scalability, research and integration makes the HP TippingPoint NX NGIPS platform a compelling solution for enterprise organizations.
ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today’s market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies? Contact Us: Start the Discussion

For information regarding permission, write:
Frost & Sullivan
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041