# WHY YOU NEED A NEXT-GENERATION FIREWALL

**INTRODUCTION: The tech landscape is constantly evolving. Cloud computing, virtualization and mobility have dramatically changed how organizations conduct business. At the same time, creative threats are coming from new angles, presenting security professionals with an ongoing challenge of protecting their organization's assets. To stay ahead of the threats, it's time for IT to embrace next-generation firewalls. This paper provides a checklist for selecting the right solution.**

## BUILDING THE BUSINESS CASE

The ongoing trend toward consumer-driven IT has not only led to a mass explosion of new mobile devices entering the workforce, it has also resulted in an evolving threat landscape. Simply put, how people prefer to work has changed dramatically in just a few short years.

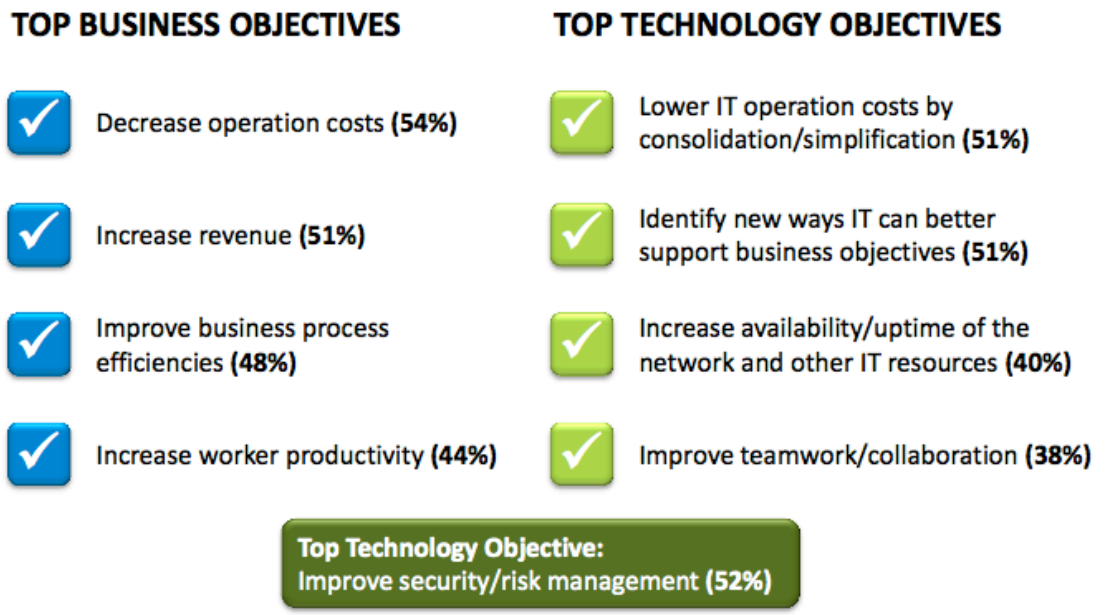
Unfortunately, this change has also forced enterprise IT leaders to deal with a host of new vulnerabilities. For instance, it has become commonplace for employees to access company data on their mobile devices while working from a local coffee shop. This situation represents a significant point of weakness, especially considering today's complex attack matrix. Hackers are now attacking different vectors simultaneously, and are more creative as they hide malware within packets or within applications.

As the entire threat landscape continues to transform, the firewall market is evolving as well from simple stateful firewalls to next-generation firewalls. Fortunately, next-generation firewalls demonstrate promise as IT leaders seek solutions to current security problems.

Gartner first defined next-generation firewalls in 2009 in its *Magic Quadrant for Enterprise Network Firewalls* report as having "integrated deep packet inspection, intrusion detection, application identification and granular control." Furthermore, the next-generation firewalls differ from previous offerings in intrusion prevention system (IPS) effectiveness, as demonstrated through third-party testing under realistic threat and network load conditions, and granular policy enforcement across the most popular and often targeted business applications.

This movement toward reduced complexity is echoed in the *Network World 2012 State of the Network Study*, in which 51 percent of respondents cited simplification as a top IT objective. "Companies are looking to consolidate their network infrastructure to achieve less complexity," says Jennifer Ellard,

NETWORKWORLD
Custom Solutions Group




SOURCE: 2012 State of the Network Study, Network World, October 2012

**80 percent of smartphone usage is for applications.**

2013 comScore report

**77 percent of mobile apps tested demonstrated data leakage vulnerabilities.**

HP 2012 Cyber Risk Report

director of product marketing at HP Enterprise Security Products, a leading provider of end-to-end security solutions. "Customers want their intrusion prevention device footprint to include the application visibility and control of a firewall within the same space."

## *UNDERSTANDING THE PAIN*

There are three primary reasons why next-generation firewalls make sense as organizations build and fortify their environments for the future and go beyond looking at IP addresses, ports and protocols for classifying and controlling network traffic.

**REASON 1: Application Access.** Today more than ever, the ability to monitor and act upon activity at the application level is crucial. As HP Security Research demonstrates, up to 84 percent of breaches take advantage of vulnerabilities within applications. This is a prime example of attackers innovating and evolving their approach as they move from networks to OS environments to applications. While it speaks to the intensified need for security-driven code development, it also reinforces the importance of having application-level control. In addition, protecting one point in the system is not sufficient. The entire pathway to the data must be secure. If there is any vulnerability along that path, then the entire system is vulnerable. Hackers are ingenious about discovering new pathways.

"Application-level control is crucial because it allows organizations to set user-specific policies for each application," says Martha Aviles, product marketing manager, HP Enterprise Security Products. "Everyone is demanding more bandwidth, and there are more applications running on corporate networks. Having application-level control can alleviate some of the pains here."

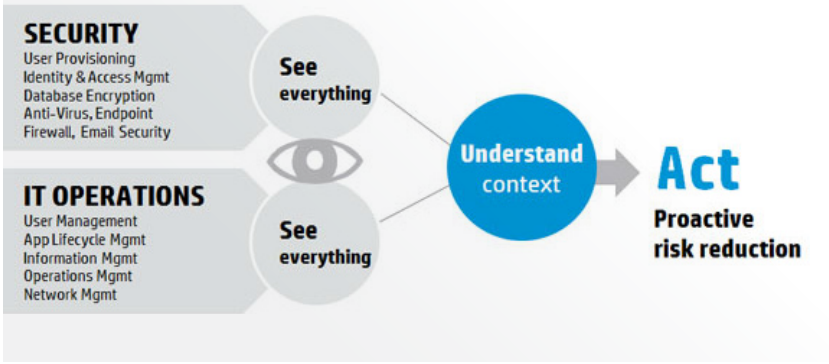
When armed with up-to-date security vulnerability prevention, a next-generation firewall can limit traffic to only approved applications, thereby avoiding risks from unnecessary applications, explains Ellard. "A byproduct of this is also reduced bandwidth consumption from unnecessary traffic," she says. "A next-gen firewall should also have the ability to scan good applications for a wide variety of threats—even confidential data leaks."

**REASON 2: Mobility Madness.** Dealing with the explosive number of new mobile devices entering the enterprise is only part of the equation for security professionals. Mobile applications are also growing at phenomenal rates. According to an April 2013 comScore report, 80 percent of smartphone usage is for applications. The problem is that mobile apps are rife with vulnerabilities. For instance, according to the *HP 2012 Cyber Risk Report*, 77 percent of mobile apps tested demonstrated data leakage vulnerabilities.

## About HP Enterprise Security

Using an end-to-end methodology is the best way to defend an enterprise successfully in today's environment. After all, enterprises and governments are experiencing the most aggressive threat climate in the history of information technology. Disruptive computing trends greatly increase productivity and business agility—but at the same time introduce a host of new risks and uncertainty.

Based on market-leading products HP ArcSight, HP Atalla, HP Fortify and HP TippingPoint, the HP Security Intelligence and Risk Management platform enables businesses to take a proactive approach to security that integrates information correlation, deep application analysis and network-level defense mechanisms—unifying the components of a complete security program and reducing risk across the enterprise.




Mobile is indeed adding a new layer of security challenges to IT. According to the *Network World study*, 48 percent of respondents said that supporting increasing numbers of devices is the top security-related challenge and obstacle their organizations face.

"For most enterprises, the network is becoming more like Swiss cheese, with mobile employees logging in, cloud-based solutions providing access to company data as well as remote employees utilizing an array of configurations to login," says Aviles. "Today's constantly growing mobile and remote workforce brings forth significant challenges. Even a mobile or remote workforce needs to be secure, but it doesn't have to be much different than how you secure your normal course of business. You can secure the network transmission. Consolidation and the ability to deploy easily make the difference."

**REASON 3: Ever-Evolving Environment.** Today's hacker attacks are not the same as in previous years. Advanced persistent threats (APTs) are increasing in number, and the targets have extended beyond the largest company to include any organization potentially harboring what an attacker views as valuable data. This is quite evident in the *Network World* study: 84 percent of respondents said they are focusing on finding better ways to safeguard APTs as a top security priority.

At the same time, organizations have unprecedented levels of data housed within enterprise systems. While this data provides enterprises with the ability to make powerful decisions, it also serves as an attractive target that is increasingly harder to monitor.

This evolving climate in itself presents a host of challenges. Businesses are tasked with monitoring threats and risks in an environment of borderless networks, persistent threats and enterprise risks. To maintain pace with attackers, IT needs the ability to collect, store and analyze any log or event data from any system within the borderless network. It also needs to be able to correlate system events, flow information, and user and application activity to help answer the Who, What and When of everything that has happened or is currently happening in the organization.

### *PATHWAY TO SUCCESS*

According to the *Network World* study, the move to next-generation firewalls to manage applications and people instead of ports is a top priority, with 80 percent of respondents currently utilizing, deploying or actively exploring options.

However, finding the right fit can be a complex and stressful endeavor for an often already overtaxed IT department to undertake. Fortunately, there are proven steps IT leaders can follow as they evaluate and ultimately embrace a next-generation firewall.

**STEP 1: Understand organizational needs.** Whether it's an application or a next-generation firewall, a solution will only succeed if it fulfills the organization's individual requirements. As such, it's crucial to take the time to distinctly identify requirements first. Key considerations should center on management capabilities, ease and speed of the deployment, acquisition costs, IT organization support capabilities, as well as the ability to integrate with the established security and network infrastructure.

**The move to next-generation firewalls to manage applications and people instead of ports is a top priority, with 80 percent of respondents currently utilizing, deploying or actively exploring options.**

Network World study

"Not every company is going to benefit from the same firewall," explains Ellard. "Businesses need to pay close attention to the total cost of ownership. While one option may have a low purchase price, it's important to look at the administration burden on IT staff as well," she says. "What is the full-time equivalent of staff needed to make sure the results are as desired? Since most organizations have limited resources, it's important to focus on finding a solution that provides the right mix of manageability and complexity in order to protect the organization while optimizing the budget."

When considering ease of use, it's essential to explore whether the solution can support both local and centralized management options, operating within a set-and-forget environment as well as an easy-to-understand and fully customizable dashboard to facilitate ongoing usage.

"Reliability should also be at the core of any successful next-generation firewall," explains Aviles. "HP built reliability into the core of our next-generation firewall by developing it on our next-generation IPS engine with a 99.99999 percent network uptime track record. In addition, we have low latency and inline deployment," she says. "Likewise, security effectiveness with continuous threat protection, including weekly HP Digital Vaccine Labs [DVLabs] updates, also have played an instrumental role in demonstrating HP's commitment to security. To date, HP has more than 7,400 filters blocking vulnerabilities across wired and wireless devices."

**STEP 2: Improve security posture.** When deploying a next-generation firewall in today's environment, there is significant value in aligning with an experienced partner like HP Enterprise Security Products, which is capable of providing end-to-end solutions.

"Consistently we have been leaders in addressing the vulnerability and threat landscape environment from a research perspective," says Aviles. "This translates into a significantly higher level of security intelligence. For instance, we have HP DVLabs, where digital vaccine researchers are focused on constantly creating filters for vulnerabilities. HP also has HP Zero-Day Initiative spearheaded by a group of White Hat security researchers who are determined to identify vulnerabilities as they reach the wild." ■

**Click here for more information about how HP TippingPoint can help you defend against cyber attacks.**