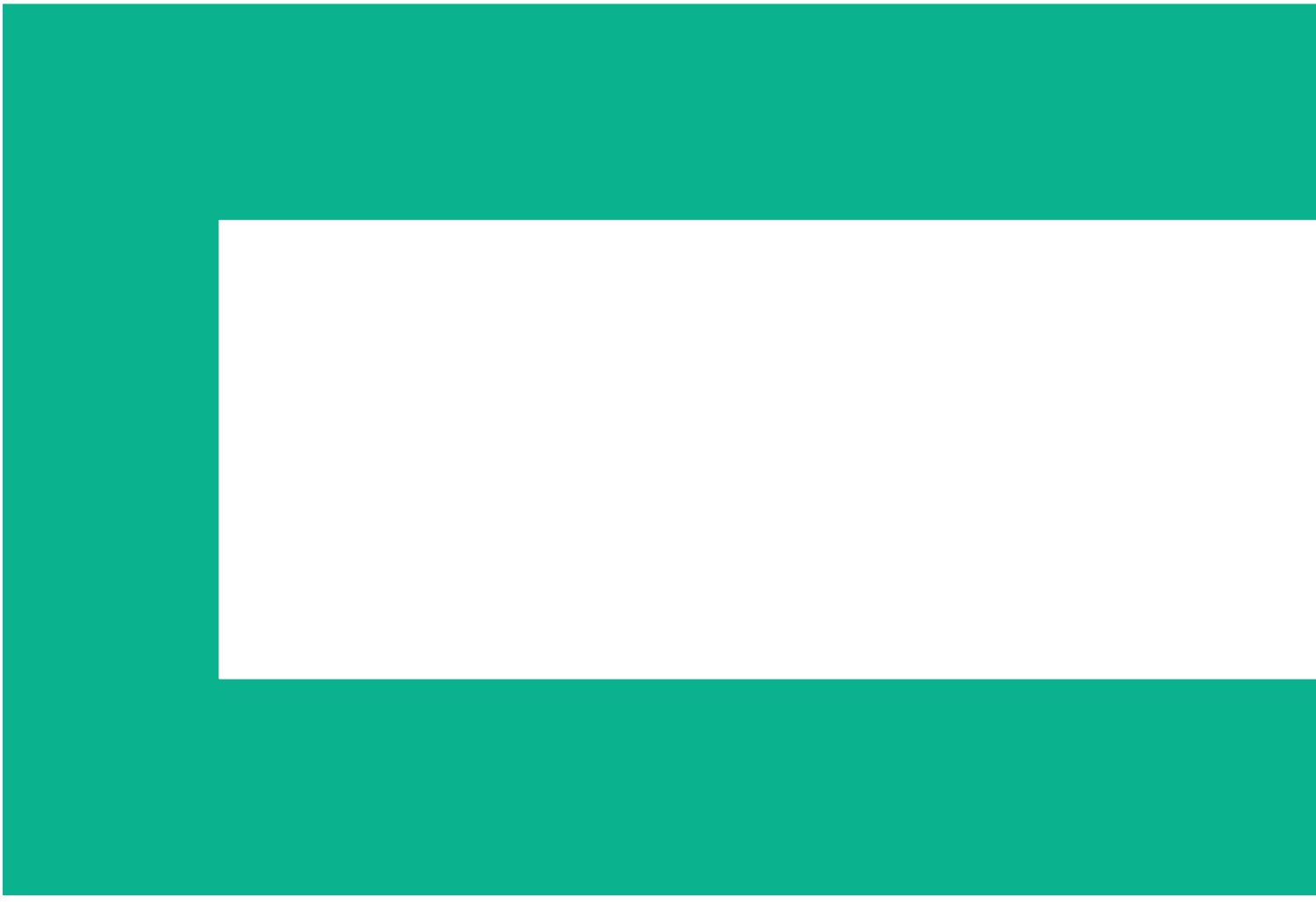
Hewlett Packard Enterprise

Business white paper

Enhance network security

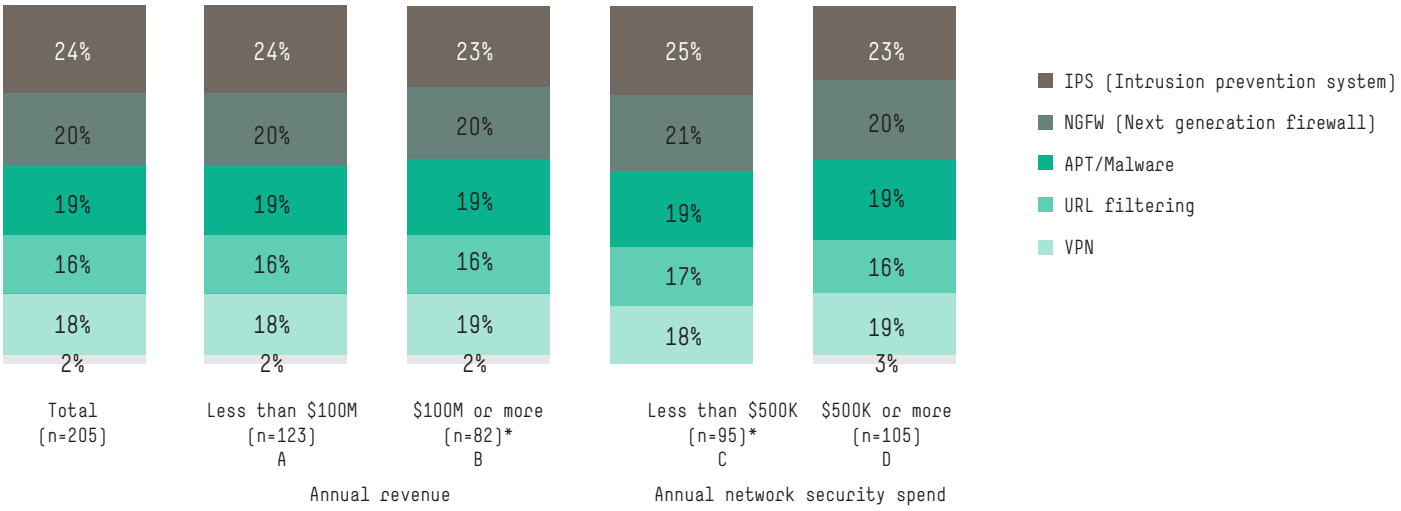
A survey by Ipsos Observer for Hewlett Packard Enterprise



Much of the industry's perception of network security is driven by the headlines. But planning investments in security programs and technology requires real data. "State of Network Security," a survey sponsored by Ipsos and Hewlett Packard Enterprise, explores the challenges faced by 205 network security professionals in the United States. It examines their main concerns, their experience with cyber threats, and their use and planned use of network security technologies.

Survey findings

Spending On average, firms are spending about $2.6 million annually in network security, and more than 60 percent expect to spend more in the next 12 months. The greatest area of investment—45 percent of total network security spending—is for intrusion prevention systems (IPS) and next-generation firewalls (NGFW). Additional spending categories include advanced persistent threat and malware detection and URL filtering technology .



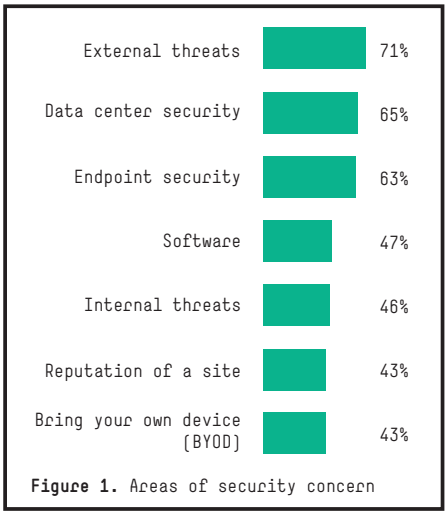


Figure 1. Areas of security concern

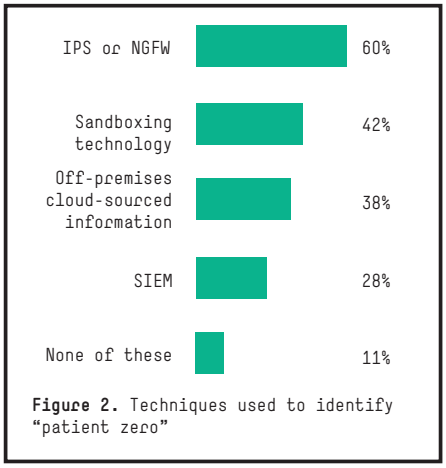


Figure 2. Techniques used to identify "patient zero"

Top IT security initiatives The top IT security initiative identified by respondents was to embrace the cloud or virtualization (82 percent). But other security-related issues followed close behind. Breach detection, for example, was identified as a top initiative by 70 percent of respondents, and among companies who spend more on security, 77 percent identified breach detection as a top initiative.

Concerns When asked about areas of security concern, 71 percent of respondents are "very concerned" about external threats with data center security and endpoint security following close behind. Looking specifically at security concerns with applications, more than half are very concerned with file sharing and almost as many with cloud-based applications.

Attacks experienced Respondents identified the types of attacks experienced by their organizations. The most widely cited was phishing with untargeted spam and concealed malware following closely behind. They identified customer data as the most common kind of data attacked, followed by financial data and corporate intellectual property. Targeted spam was experienced by 77 percent of respondents at least once a week, and phishing and concealed malicious applications were experienced at least once a week by 69 percent and 54 percent of respondents respectively.

More than a third of respondents say they have observed an increase in the number of attacks stemming from user activity in the network. And among those who spend more on network security, more than 40 percent have observed an increase in these attacks.

Techniques used Respondents detailed techniques they use to identify the "patient zero"—the first case of a virus or breach. Intrusion prevention systems (IPS) far outstripped other techniques, and just under one-third use security information and event management (SIEM) solutions.

IPS needs When asked what features on an IPS are most important to them, 94 percent identified security effectiveness as the key attribute they look for. Network performance and reliability were also important to 85 percent and 79 percent of respondents respectively. More than 45 percent of those surveyed believe IPS will be consolidated into next-generation firewalls (NGFW) in the future, although one in five continues to see next-generation IPS (NGIPS) as a standalone security function blocking inbound and outbound threats.

Concerns when migrating to SDN As organizations begin to plan for software-defined networks (SDN), they are also beginning to consider the security of these future networks. The concern about SDN most named by respondents was manageability (54 percent). But 45 percent of those surveyed also expressed concern that attackers could compromise SDN controllers.

HPE recommendations

The survey reinforces other findings that cyber attacks are on the increase and security-conscious organizations are stepping up defenses. But security organizations must look carefully at their investments to ensure they are spending on the right things. Defenses must provide protection against attacks targeting zero-day vulnerabilities. They should use website reputation data to block unfiltered spam and phishing attacks. Security technology must be able to detect and block the command and control traffic malware generates when communicating with hackers' systems. NGFWs must implement application controls. And organizations must use software security assurance programs and tools to find and fix vulnerabilities in the software they develop.

No single security solution can detect and block all attacks. What companies need is a layered security approach—from perimeter firewalls, to IPS in the core network, to application security testing and remediation. Smart security managers are layering NGIPS, NGFW, sandboxing, and SIEM solutions to disrupt every phase of a cyber attack.

Learn more at
hpe.com/go/tippingpoint

Hewlett Packard Enterprise

4AA5-5732ENN, November 2015, Rev. 1