A Custom Technology Adoption Profile Commissioned By Cisco Systems And Lancope

Responding To New Threats Requires A New Approach

August 2012

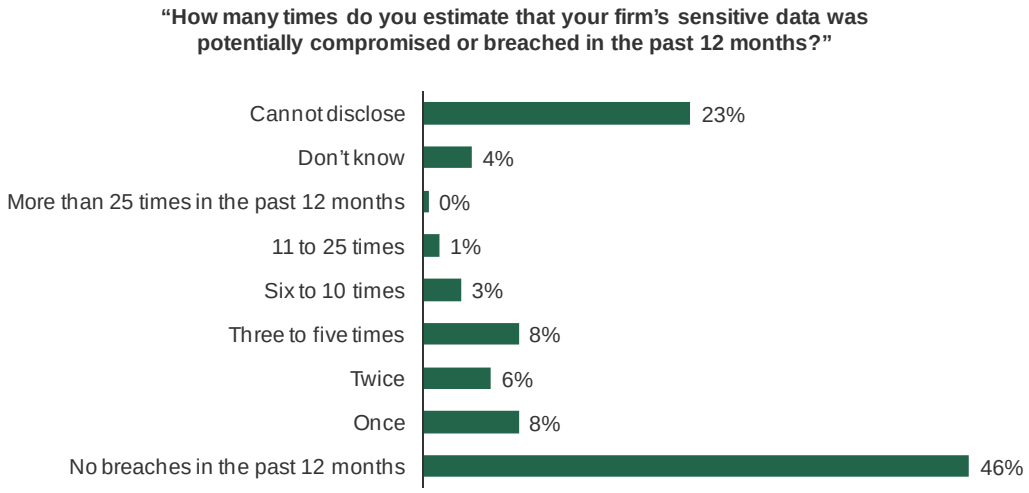
Introduction

Today, information security success is no longer defined by preventing attacks, but instead by how quickly organizations can detect and contain breaches. Many enterprises fail to recognize this important shift, overestimating their ability to stop attackers and focusing on traditional preventative controls as the anchor of their defensive strategy. But these controls have proven ever less effective over time with the advent of new, stealthy, and evasive attack vectors. Enlightened organizations have adopted network flow analysis capabilities to augment their preventive controls, but fail to include the additional context necessary to truly identify malicious activity within their networks. To be successful in this advanced threat environment, organizations must adopt new robust detection and analysis capabilities.

Many Organizations Don't Realize That They Have Been Breached

2011 was commonly known as the year of the breach, and thus far, 2012 is continuing the trend. Numerous high-profile companies have suffered from embarrassing headlines this year. The FBI's former head of cyber investigations, Shawn Henry, recently painted a bleak picture of the threat landscape: "The current public and private approach to fending off hackers is unsustainable. Computer criminals are simply too talented and defensive measures too weak to stop them."[1] Despite the headlines and comments from experts such as Mr. Henry, enterprises still have a false sense of security about the integrity of their networks. Only 26% of organizations surveyed admitted being compromised in the past year, while 23% of respondents wouldn't disclose any information on compromises. A shocking 46% claimed to have had no breaches in the past 12 months. A significant portion of this group has no doubt experienced a breach, but lacked the necessary tools to identify the compromise (see Figure 1).

Figure 1
Enterprises Underestimate Data Breaches

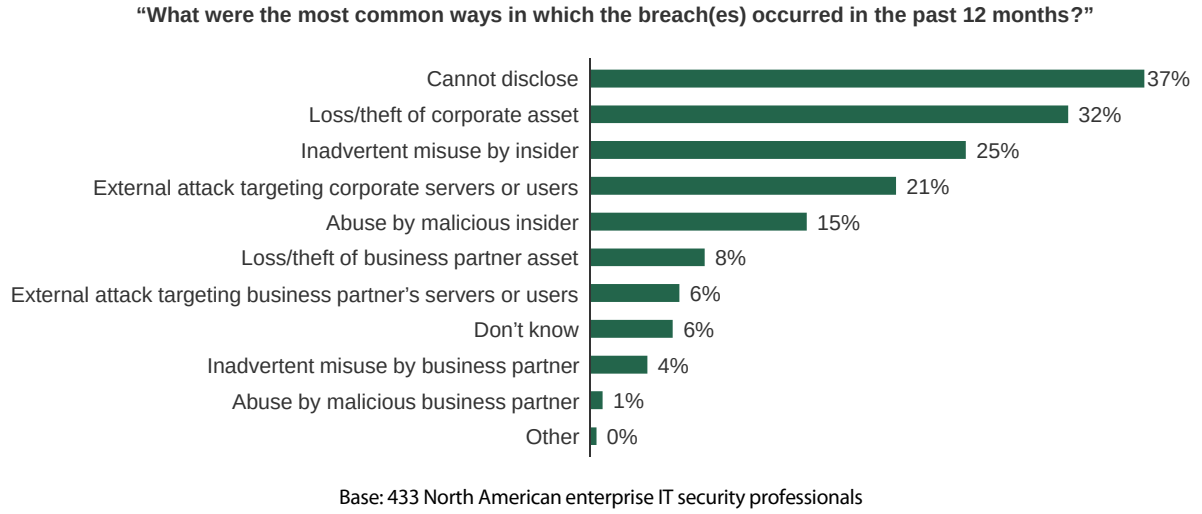


Base: 433 North American enterprise IT security professionals
Source: Forrsights Security Survey, Q2 2012

The loss or theft of corporate assets led the most common disclosed method organizations have been breached by in the past 12 months (see Figure 2). The loss of a corporate physical asset is almost always reported. If an employee wants to be able to continue to work, he or she must inform the information technology department in order to get a new laptop. The loss of a physical asset is much more apparent than the loss of a digital asset. It is easy to know when a laptop disappears, but it can be much more difficult to know when data has left your control.

Additionally, insider misuse and abuse remain a significant concern. As demonstrated by the Bradley Manning/WikiLeaks breach, the insider threat is serious that even a highly classified "secure" government network was victimized. The survey data confirms that the insider threat remains a significant concern. "Inadvertent misuse by insider" and "Abuse by malicious insider" made up 40% of the breach methods (see Figure 2). If a firm doesn't have the necessary tools, attacks from within the organization will go unnoticed.

Figure 2
Physical Asset Loss Leads Reported Breach Methods

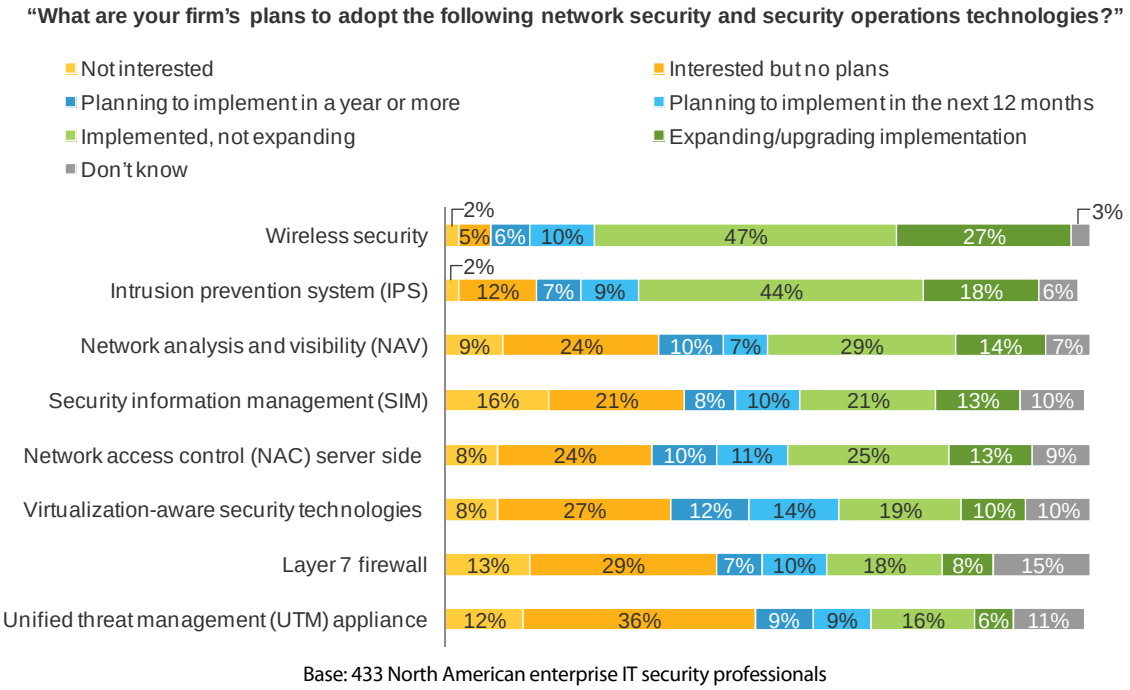


Base: 433 North American enterprise IT security professionals
Source: Forrsights Security Survey, Q2 2012

Prevention Drives Security Investment

Prevention has long been a cornerstone of defense in depth and continues to drive security investment. Prevention technologies such as IPS are widely deployed within companies. Sixty-two percent of respondents have implemented intrusion prevention systems (see Figure 3). Faith in prevention solutions contributes to the false sense of security that some organizations have regarding data breaches. Contrast this investment in prevention technologies with the 43% of respondents who have adopted network analysis and visibility (NAV) solutions. These tools look at various types of traffic generated by networks to find anomalous behaviors and potential threats unseen by perimeter controls. Enterprise investment in innovative detection capabilities needs to increase.

Figure 3
IPS Is The Limited Cornerstone Of Defense



Base: 433 North American enterprise IT security professionals

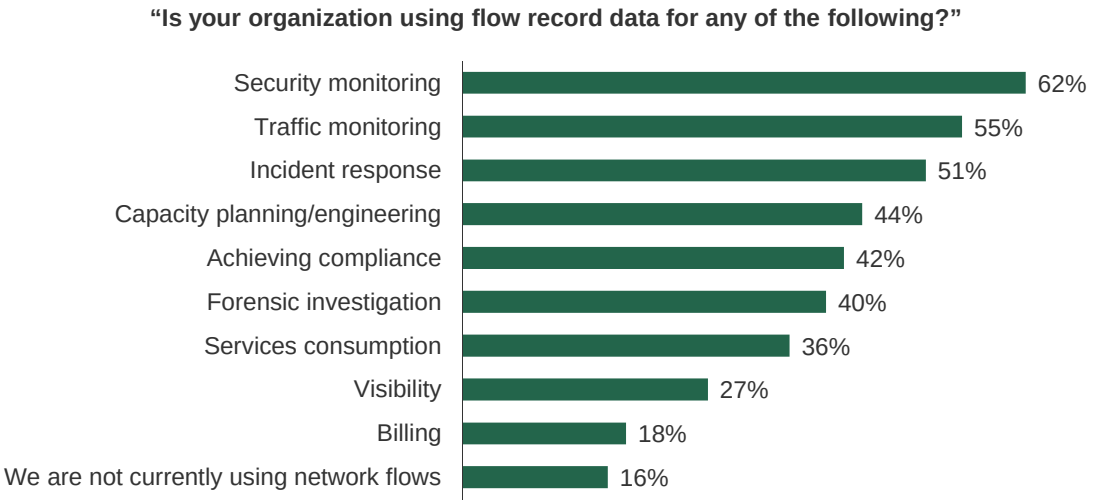
Source: Forrsights Security Survey, Q2 2012

Effective Use Of Network Flow Data Enhances Security

Network flow is built into the DNA of networks and has a long history of use within enterprises. Traditionally rooted in network operations, information security teams now leverage the same data for detecting anomalous behavior. Cisco and Lancope commissioned Forrester to survey IT security professionals further on the topic. Forrester found that security teams that utilize network flow data are able to identify and respond to incidents much faster and that today; only 16% of respondent organizations aren't utilizing network flow data. The survey data indicates that while IT teams may use NAV tools such as network flow analysis systems, there is still a need for more adoption of these tools by security teams. Security monitoring without contextual information does not provide the insight necessary to detect advanced modern threats. A comprehensive strategy leveraging flow analysis with contextual data is imperative in today's enterprise.

Security monitoring, traffic monitoring, and incident response are the most common uses for network flow data for security professionals (see Figure 4). Monitoring network flows can help enterprises reduce the time it takes to identify the root cause of many types of incidents. This applies to both security and non-security incidents that an operations team would investigate. In these days of limited budgets, the high level of adoption is no surprise. Any solution that can leverage existing router and switch infrastructure and be utilized by multiple groups within an organization is easier to justify.

Figure 4
Flow Record Data Use



Base: 55 North American enterprise IT security professionals
Source: A commissioned study conducted by Forrester Consulting on behalf of Lancope and Cisco, July 2012

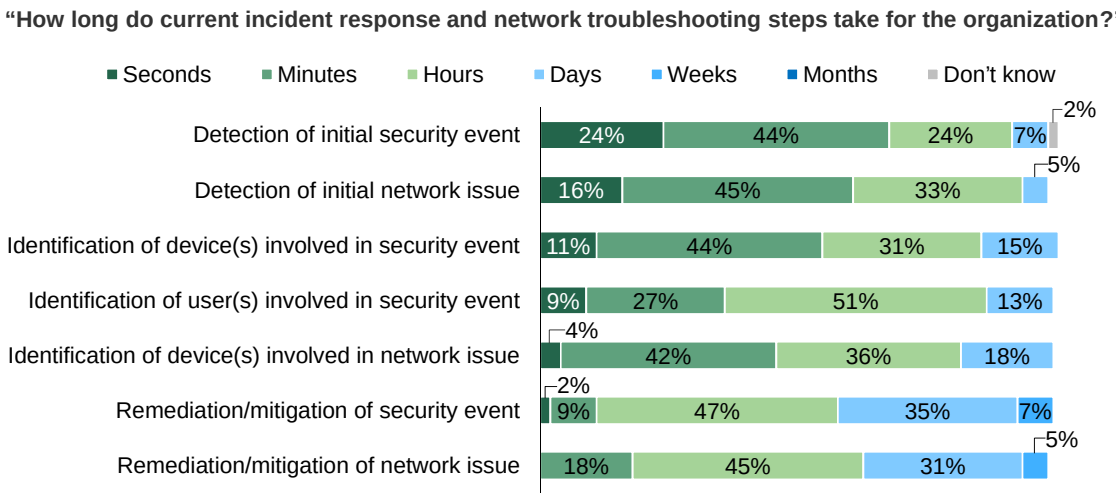
Network Flow Analysis Is Powerful, But Additional Context Is Critical

Security teams are using network flows for analysis, yet with adoption so high, why do we continue to see so many network breaches? Sixty-eight percent of survey respondents reported that they were able to detect security incidents within seconds or minutes (see Figure 5). It is very unlikely, however, that these organizations truly have the necessary capabilities to detect malicious activities. As a result, incident response capabilities may be overstated, while data breaches may be understated.

In addition to network flow data, organizations need additional context to identify threats. Attackers are encrypting traffic and exfiltrating data over common communication ports. Without additional context, only reviewing layer 3/4 packet data and flow size may not necessarily reveal malicious activity. When intellectual property is leaving an environment, seconds count and the faster an organization is able to identify and contain a security incident the better.

Figure 5

Breaches Are Prevalent Despite Respondent Confidence In Detection Capabilities



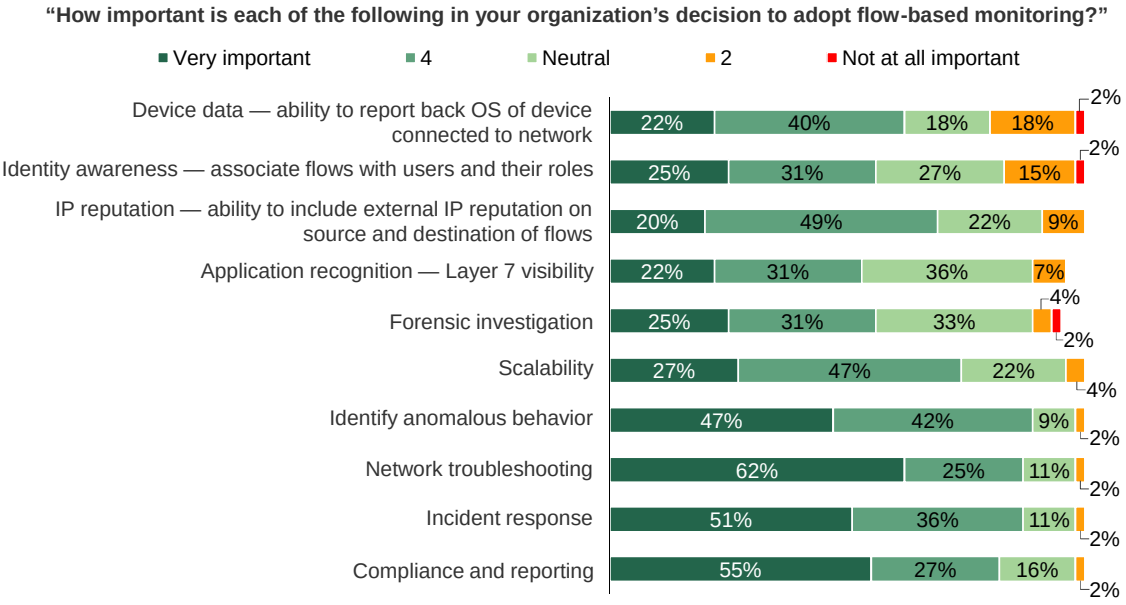
Base: 55 North American enterprise IT security professionals

Source: A commissioned study conducted by Forrester Consulting on behalf of Lancope and Cisco, July 2012

There are several key flow monitoring capabilities that organizations don't consider important, but should. IP reputation, device data, identity awareness, and application recognition should all have a higher importance (see Figure 6). First, automatically associating a user with an IP address can save time by eliminating the need to manually correlate data from server logs. Is the person associated with the IP an executive, an R&D staff member, or an employee who routinely uses P2P applications? The response will vary greatly depending on the identity. Next, reputation is another key contextual component. The solution must be able to leverage the vendor's threat intelligence network so that an analyst can quickly identify an IP address as malicious or potentially malicious is very important. Data can be overwhelming and reputation data can be leveraged to highlight anomalous behavior. Reputation data uses a scoring system to granularly identify potential threat traffic. Details regarding the device are another important piece of context. What type of device is an analyst looking at and what is its disposition? Finally, having layer 7 visibility into packets is critical. An analyst needs the ability to identify masquerading traffic and malicious applications tunneling through HTTP.

A security analyst that is armed with network flow data enriched with context is well positioned to detect the attack precursors from threats. The ability to detect data reconnaissance activity or covert channel communications prior to data exfiltration is key.

Figure 6
Context Is Critical, And Deserves Increased Focus



Base: 55 North American enterprise IT security professionals
Source: A commissioned study conducted by Forrester Consulting on behalf of Lancope and Cisco, July 2012

Conclusion: Continued Breaches Offer Organizations No Option But To Deploy Robust NAV Solutions

To evolve with the threat landscape, organizations will shift focus from relying upon prevention technologies and instead invest in robust anomalous behavior detection beyond traditional network flow analysis. Solutions that offer enhanced visibility and the context necessary to quickly identify and respond to incidents will become strategic investments for enterprises.

Endnotes

[1] Source: "U.S. Outgunned in Hacker War," *The Wall Street Journal*, March 28, 2012.

About Forrester Consulting
Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit www.forrester.com/consulting.