FROST & SULLIVAN

October 2013

The Market Has Spoken:
Provide Better Visibility and Manageability across Network Security Tools

Frost & Sullivan Analysis by
Frank Dickson

The Market Has Spoken: Provide Better Visibility and Manageability across Network Security Tools

Introduction

The Internet as a communication medium has been evolving. This evolution, unfortunately, has brought with it growth in Internet-based attacks and corresponding growth in the tools to fight those attacks. But with this growth in security technologies, unintended complexity for security professionals has intensified. Described in this article are the factors contributing to security management complexity and why enhanced visibility and manageability across security technologies is the right remedy.

A Richer World of Internet-Based Communication

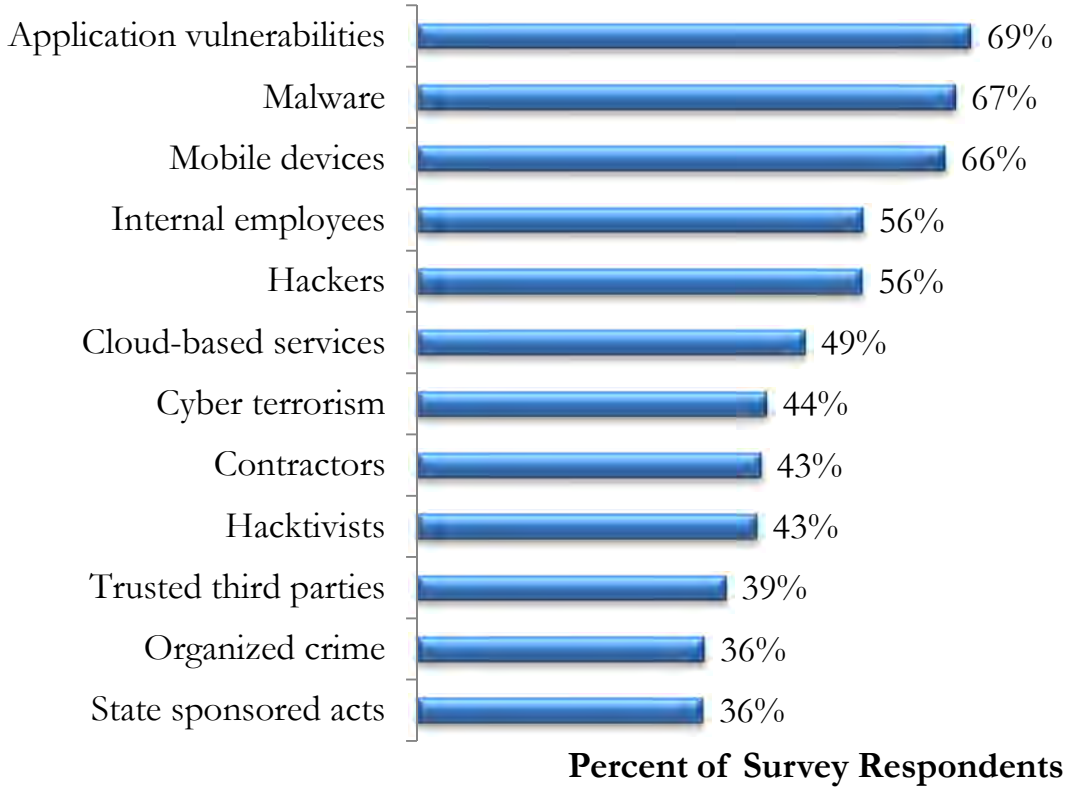
It is not a secret that the manner in which people interact and communicate via the Internet has changed with social media and other forms of communication, computing, and collaboration. Gone are the days in which a Web browser was used as one-way tool to obtain information from the Internet and interactive information was only exchanged via e-mail. Web browsers are now the interface for a number of communication channels including Facebook, LinkedIn, Twitter, Skype, and many others.

Increasingly Worrisome Vulnerabilities, Threats, and Attacks

This new world of rich and dynamic Internet-based communication channels has brought with it a host of new vulnerabilities. While each vulnerability is a cause for concern, that concern is higher when the intent of malicious actors is financial gain. Furthermore, with profit as a motive, the actors have become more sophisticated (multi-variable exploits) and stealthier than the first wave of malicious activity which was driven by the quest for notoriety.

No surprise, information security professionals are feeling the impact. Figure 1 highlights the lengthy list of security concerns they face.

Figure 1: Top and High Threats and Vulnerability Concerns Voiced by Information Security Processionals



N = 12,396 Information Security Professionals

Source: Frost & Sullivan

An Increasing Complexity Created by a Multitude of Security Technologies

The increasing sophistication and breadth of threats has driven an evolution in the type and number of security technologies.

- **Anti-virus** software is used to prevent, detect, and remove malware from client devices such as PCs or mobile phones.
- **Web content security** protects users and their organizations from Web-based malware and malicious URLs.
- **E-mail content security** filters and strips e-mail of phishing schemes, spam, malicious links, inappropriate images or content, and malware.
- **Intrusion prevention systems** (IPS) monitor network traffic for malicious activity and provide security professionals with the tools to block.
- **Data loss prevention** (DLP) detects and lessens instances of nefarious and unintended outward flow of sensitive data.
- **Distributed denial of service (DDoS) identification and mitigation technologies** provide protection against resource-robbing and Web site-disrupting attacks.
- **Stateful inspection and next generation, context-aware firewalls** create a barrier between trusted, secure internal network and the Internet.

Network and Information Security Professionals Need Help

The security industry has been commendable in creating new point solutions to address the evolving threat landscape. However, an unforeseen consequence has developed. As the complexity of the threats being combatted increased, the complexity of the tools used to combat the threats also increased. Additionally, as the number of security technologies grew, so did management complexity. This problem of complexity is further exacerbated by an expanding universe that security professionals are tasked to secure as more organizations supplement their IT resources with cloud services and employees increasingly access corporate resources through their personal mobile devices, a trend often referred to as BYOD (bring your own device).

The increasing complexity of network and information security is being addressed by security teams that are already overtaxed. In a recent survey conducted by Frost & Sullivan of over 12,000 information security professionals, 56 percent report that their organizations have too few information security workers. The reasons for the understaffing include "business conditions can't support additional personnel at this time" (57 percent), "leadership in our organization has insufficient understanding of the requirement for information security" (45 percent) and "it is difficult to find qualified personnel" (37 percent).

The result of increased security complexity and understaffed security departments is that the quality of security is suffering. According to the IBM X-Force 2013 Mid-Year Trend and Risk Report, "Many of the breaches reported in the last year were a result of poorly applied security fundamentals and policies and could have been mitigated by putting some basic security hygiene into practice. Attackers seem to be capitalizing on this 'lack of security basics' by using a model of operational sophistication that allows them to increase their return on exploit. The idea that even basic security hygiene is not upheld in organizations, leads us to believe that, for a variety of reasons, companies are struggling with a commitment to apply basic security fundamentals."[1]

56 percent of security professionals in a recent Frost & Sullivan survey report that their organization currently has too few information security workers.

[1] *IBM X-Force 2013: Mid-Year Trend and Risk Report*, September 2013

Clear Message: Richer Tools to Manage across Security Technologies

The message from the marketplace is clear: administrators of security technologies need tools that simplify the task of managing security. These tools need to go beyond just using, managing, and maintaining an individual solution, but also provide visibility and consolidated management functionality across multiple security technologies.

Customers of networking security solutions need tools that simplify the task of managing network security. These tools need to go beyond just using, managing and maintaining a stand-alone solution, but also provide greater visibility and consolidated management functionality across network security tools.

Frost & Sullivan makes the following recommendations to network security vendors:

1. Security professionals should not need to manually log into several individual security systems to compile a security status of the network. Integrated views across systems and technologies need to be provided in a singular easy to use view to alleviate the burden of diagnosis and allow security professionals to implement solutions more expeditious.
2. Management tools need to integrate across solutions to further alleviate the burden of manually jumping from system to system, and to reduce the requirement of being proficient in multiple individual systems (which often are delivered by multiple different vendors).
3. Cross-platform management tools should allow a security professional to establish one set of policies that are automatically implemented across multiple network security services. As security professionals remediate security breaches, they need to be able to implement solutions across several security technologies without the need of operating multiple management consoles.
4. Finally, reporting tools need to aggregate information across multiple security services to enable a singular view, allowing for ease in management and greater effectiveness of network security problem diagnosis.

Security professionals are resource constrained and time poor. Vendors need to proactively respond to address this need.

Frank Dickson

Industry Principal – Network Security

Frost & Sullivan

Frank.Dickson@frost.com

FROST & SULLIVAN

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? For more information about Frost & Sullivan's Growth Partnership Services, visit http://www.frost.com.

CONTACT US

For more information, visit www.frost.com, dial 877-463-7678, or e-mail inquiries@frost.com.