IDC ANALYST CONNECTION

Robert Ayoub

Program Director, Security Products

The Need for an Integrated Security Strategy

June 2018

Enterprise chief information security officers (CISOs) are seeking ways to leverage existing security investments to bridge the divide between largely siloed security systems. The focus is on reducing the number of consoles needed to manage the security infrastructure. Network security vendors have a significant role to play in bridging the communication gap between these systems. The creation of a unified defense architecture enables threat data exchange between existing security systems. It helps automate the process of raising an organization's security posture when a security infrastructure component detects a threat.

The following questions were posed by Fortinet to Robert Ayoub, program director in IDC's Security Products program, on behalf of Fortinet's customers.

Q. Why is a broad security architecture and partner ecosystem important for protecting critical systems and data during a time when the attack surface is quickly evolving?

A. Security is critically important to enterprises, especially as they pursue digital transformation initiatives such as the Internet of Things (IoT) and cloud. These pursuits introduce new challenges, complexities, and risks that require a greater degree of spending and attention to thwart sophisticated cyberattackers. In this battle, the jobs of CISOs, chief security officers (CSOs), chief information officers (CIOs), and even chief executive officers (CEOs) are at stake.

That said, there are numerous reasons why a broad security architecture and partner ecosystem should be more important to customers than ever before. In fact, the rapid evolution of the attack surface should drive customers to a broad, yet interoperable security architecture. Successful attacks are coming from many directions. IDC's Cloud Security Pulse Survey, 2017 showed that the top attacks organizations experienced include ransomware, data loss, targeted phishing attacks, and DDoS attacks. No one vendor has both the breadth and the depth to protect an organization against every attack vector. By implementing a security infrastructure that allows partners to interoperate efficiently, customers can still choose solutions that best fit their needs while ensuring that those solutions interoperate.

Q. What advantages should users expect to gain from a tightly integrated security framework?

A. Beyond "plug and play" interoperability and ease of deployment, a tightly integrated framework provides greater contextual richness, allowing the integrated systems to better differentiate among events to reduce false positives and give focused alerts to customers that are likely understaffed. Additionally, customers should see overall improvements in efficacy due to the sharing of real-time threat intelligence across the entire infrastructure.

Q. What capabilities should customers evaluate as they look for a security solution to protect their digital transformation strategies?

A. The security efficacy of any solution is key, but automation and interoperability with other systems should be top of mind. The ability to consolidate information from a wide variety of security systems under a single management platform and then manipulate that same information using a common interface is crucial.

Q. How important is automation as a component of the security architecture today?

A. Automation is quickly becoming a critical component of a security architecture. The ability for attackers to leverage distributed resources allows for attacks to occur much faster than ever before. That trend, coupled with the lack of information security talent, means that security analysts need help managing the vast amount of information coming into their security systems. While most organizations are uncomfortable automating security responses, automated information gathering is gaining wide acceptance.

Q. There are many security vendors in the market today. What criteria should customers use to evaluate them?

A. While of the utmost importance, security is hard. Too many enterprise leaders believe they've got it covered, but in reality, they are struggling to keep up with constantly changing architectural demands and a daunting threat environment. This struggle is due not only to the shortage of qualified in-house staff but also to the challenges of defining a security strategy, implementing the necessary technology, and maintaining a security solution.

There are an overwhelming number of security vendors in the marketplace. Each vendor has something unique to offer customers, whether a specialization in specific detection techniques or industry-specific security products. Most organizations today still purchase security solutions based on solving a single problem at a time. Anytime that customers are evaluating a security vendor, they should consider the impact of that vendor on their overall architecture. Customers should question not just the effectiveness of a product but also how the product will impact their environment. In addition, they should consider how a product fits within their existing workflow and how well the product interoperates with existing products in the network. The answer to all these questions should supersede hype around a vendor or loyalty to an existing vendor.

ABOUT THIS ANALYST

Robert Ayoub is a program director in IDC's Security Products program. In this role, he provides thought leadership and guidance for clients on a wide range of security products including traditional network security products such as firewall, IPS, and UTM and emerging products designed to protect the cloud and the Internet of Things (IoT). He is also responsible for research and analysis around a wide range of evolving security markets, including forensics and security and vulnerability management (SVM).

ABOUT THIS PUBLICATION

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

COPYRIGHT AND RESTRICTIONS

For more information on IDC, visit www.idc.com. For more information on IDC Custom Solutions, visit http://www.idc.com/prodserv/custom_solutions/index.jsp.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com