IDC TECHNOLOGY SPOTLIGHT

A Unified View of the Enterprise Network for Proactive Security

March 2016

Adapted from *IT's 3rd Platform Drives Need for Network Innovation by* Nolan Greene and Rohit Mehra,
IDC #259317

Sponsored by Fortinet

The 3rd Platform (cloud, mobility, big data/analytics, and social business) has transformed the network's importance to the enterprise, with IT enabling new opportunities for operational transformation and customer engagement. This transformation can result in meaningful cost savings and new revenue streams. At the same time, the proliferation of mobile devices and applications, along with the increased interconnectedness created, opens up organizations to ever more security threats. 3rd Platform accelerators such as Internet of Things (IoT) and cognitive computing will only intensify these trends. New technologies bring new threat vectors onto the network, and IT may be stuck in a cycle of merely reacting to the latest trends. This Technology Spotlight examines the need for an enterprise network infrastructure with deeply embedded security for more proactive threat prevention. It also looks at the role of Fortinet in addressing this need.

Introduction

The growing popularity of mobile devices and cloud-hosted enterprise applications is prompting organizations to reconsider how they deploy enterprise networks. The myriad traffic flows among private datacenters, public clouds, and the mixture of personal and corporate-owned devices have led to the need for more advanced management, policy setting, and security capabilities for wired and wireless networks. Many organizations are now seeing IoT devices access the enterprise network. These trends are leading to a seamlessly mobile workforce that can create value without regard to time and place. However, with these tremendous benefits come risks, especially with regard to security.

Network managers have a wide variety of security threats to worry about in today's enterprise. The rise in mobility is due in large part to the proliferation of bring your own device (BYOD), introducing risks around data exposure and threat vectors brought in from the outside. However, BYOD is not the only factor extending the borders of the enterprise. The network access needs of third-party business partners and their applications are also adding complexity.

Public-facing organizations increasingly offer guest WiFi access, which leads to many of the same risk factors as employee BYOD, but with fewer protections from any number of security technologies. Furthermore, the introduction of IoT in the enterprise multiplies the number of attack surfaces, and many IoT devices lack intuitive security interfaces.

Given these recent trends, the need for a proactive and unified approach to network access and security infrastructure is greater than ever. As workloads migrate back and forth between wired and wireless access (with many permanently migrating to wireless), it is important to be able to enforce consistent policies and security regardless of whether the application is being accessed on the wired network or the wireless network.

Similarly, it is imperative to have consistent deployment mechanisms for necessary security tools and industry-specific protocols. Perhaps overlooked are the efficiencies that can arise from having unified wired and wireless access, along with security management, on a single-pane-of-glass platform. A unified system increases visibility and reduces "swivel-chair management," allowing enterprise IT to make changes, respond to problems, and mitigate threats more quickly and thoroughly.

The Benefits of Unified Visibility and Integrated Security

The ability to have a unified view of the network and its security can lead to tremendous efficiencies for today's enterprise. As mentioned, single-pane-of-glass management visibility allows network administrators to work more efficiently on one platform. This can reduce the time to response for problem identification and troubleshooting on the network.

When security is baked into a unified platform, there is complete visibility from the wired switch to the wireless edge, accompanied by the corresponding ability to enforce security from end to end. This allows the enterprise to apply the same security policies across both wired and wireless aspects of the network for consistent end-user experience and security enforcement, regardless of whether the user is using a mobile or nonmobile device. Furthermore, a unified networking platform with integrated security can mitigate the lateral movement of threats on the network through internal segmentation and micro-segmentation.

Better visibility, integrated tools, and granular segmentation ultimately allow the enterprise to more proactively manage security. In today's cyberthreat environment, it is critically important that an organization's network security infrastructure remains one step ahead of emerging threats. When a threat emerges, the network must be quickly fortified to protect and remediate. To this end, a unified platform allows security updates to be pushed out uniformly across both the wired side and the wireless side of the network.

Unified Network and Security Visibility Trending in the Enterprise

At the macrolevel, IT convergence has been a hot topic for the past several years, and this has naturally extended into the network. Unified wired and wireless network access has become a fairly common offering as IT decision makers look to streamline network operations.

According to a 2015 IDC survey of United States–based organizations that have implemented some form of unified networking, 71% cited improved security visibility as a key benefit, with 66% citing the "ability to enforce the same user and application policies across wired and wireless networks." Other commonly cited benefits included reduction in staff needed to manage the network (59%) and reduction in time spent toggling among separate management platforms (58%). (Source: IDC's *Campus Network Innovation Survey,* October 2015.)

It is not surprising how top of mind network security is for enterprise IT. High-profile security breaches in 2015 at the Office of Personnel Management (OPM), the Internal Revenue Service (IRS), TalkTalk, and Hello Kitty, as well as in many other organizations, demonstrate the devastation caused by cybercrime in terms of both exposure of private data and the aftermath for customers whose credit card information was compromised. Given that mobility and IoT are introducing many new potential attack surfaces onto the network and that cloud applications make network traffic patterns more complex, enterprises are implementing tools that improve security enforcement.

Considering Fortinet's Secure Access Architecture

Fortinet's Secure Access Architecture (SAA) encompasses a wide range of technologies designed to meet the challenges associated with the growth of wireless technology in the enterprise. SAA is centered on the FortiGate Enterprise Firewall, which has supported secure unified access for a number of years.

The secure wireless capability of FortiGate is available in two different form factors: FortiWiFi, which features an integrated wireless access point (AP), and FortiAP, which connects via Ethernet to FortiGate's integrated wireless controller. Ethernet connectivity has been supported through a reasonably high Ethernet port density. This consolidation of access technologies into a single platform supported by the authentication capabilities of FortiAuthenticator has been positioned in several key markets such as the distributed enterprise.

SAA is the natural evolution of the initial FortiGate solution. Increased port density has been achieved with the addition of FortiSwitch Ethernet switches. Through an integrated switch controller, FortiSwitch is an extension managed through FortiGate. Wireless capability has also been expanded through the acquisition of Meru Networks, with the intention of offering a high-performance, controller-based WiFi capability for environments with requirements greater than the capability of FortiGate.

SAA also includes FortiAP-S, Fortinet's smart AP, where certain security services such as antivirus, IPS, URL filtering, and application control reside on the AP itself. FortiAP-S is a controller-less solution and fully managed via the Fortinet FortiCloud service.

The intent of SAA is to provide customers with choices so that they can select the unified access solution that best meets their needs without compromising security.

Challenges

Although many enterprises recognize the benefit of unified networking and integrated security, there can be challenges adjusting from the status quo. In some organizations, responsibilities for networking and for security fall into distinct silos, and this may inadvertently inhibit tighter integration. Similarly, wired networking and wireless networking exist as separate skill sets in some organizations.

In any case, unification and rationalization of these different functions can create momentary disruption. Furthermore, the move to unified networking could prompt a complete technology migration, resulting in a learning curve for all stakeholders. Proper demonstration of end-user benefits along with proactive training can go a long way in mitigating these challenges.

The principal challenge for a company such as Fortinet is the lack of mindshare as an access company. Incumbent competitors in the unified access market leverage their positions to convince customers that they have integrated sufficient security into their products, in contrast to Fortinet's "security first" messaging. The company's primary competitors have also made strategic acquisitions to bolster their wireless offerings.

Conclusion

IDC believes that a unified wired and wireless networking platform with integrated security, including internal segmentation and micro-segmentation, and locally securing devices on the switch or AP, can allow organizations to stay ahead of the challenges of cloud, mobility, big data, and social technologies.

Single-platform management, end-to-end security visibility, and the ability to standardize security and policy enforcement across the network enable IT to stay a step ahead of security threats, proactively guarding against emerging threats while more efficiently troubleshooting those that may find their way onto the network. Fortinet offers wired and wireless networking solutions with tightly integrated security addressing many of these capabilities. To the extent that Fortinet can address the challenges described in this paper, IDC believes the company is well positioned for success.

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