IDC TECHNOLOGY SPOTLIGHT

Rethinking the Network as a Security Sensor and Enforcer

October 2015

Adapted from *Worldwide Enterprise Network Infrastructure Forecast*, 2015–2019, by Nolan Greene, Rohit Mehra, Rich Costello, et al., IDC #258012

Sponsored by Cisco

Today's corporate networks are more important to business objectives than ever before. Consequently, greater amounts of sensitive data traverse both wired and wireless networks. This plethora of valuable data in today's enterprise attracts an increasing number of hackers and malware applications. However, the inherent connected intelligence and distributed nature that makes the network a treasure trove for cybercriminals can also empower the network to be a proactive security tool. Through traffic visibility, and segmentation, today's enterprise network can prove itself to be a sensor and enforcer for security.

Introduction

With the rise of what IDC has termed "the 3rd platform", a new paradigm of technology and applications built around cloud, mobility, Big Data, and social business is emerging. The network has moved to a strategic function enabling innovation. Among the reasons for this transition is that the 3rd Platform has enabled 24/7 access to critical applications- promoting collaboration, removing barriers with regard to time and place, and hastening innovation. With an explosion of new devices and applications in the enterprise, more sensitive data than ever before traverses the network, heightening security needs from core to edge. In fact, 80% of companies will experience at least one successfully executed security breach- and even excluding major breaches, the average enterprises loses $1.3 million per year to security threats and attacks.

To put it succinctly, enterprise networks have never been as complex as they are now. Every node, app, certificate, cloud, device, and user accessing today's network has the potential to be infected or compromised. If not detected and remediated immediately, every piece of malware or other attack vector entering any surface can quickly spread through the network. However, the intelligently connected nature of networked resources that presents an opportunity to attackers can also serve as one of its greatest assets. That is to say, intelligence on the network can be used to proactively detect and remediate many different types of attacks and breaches. With advances in network intelligence, the network can be used as a sensor to provide rapid insights to network threats. The network can be used to "know your normal" and rapidly identify anomalous activity. This bolsters the network's role as a security asset as the network further transforms into an enforcer to implement network access control across the network to contain attacks.

The Moving Security Target

In many organizations, BYOD and the mainstreaming of enterprise mobility continues to bring an onslaught of devices onto the corporate network. BYOD devices add complexity to securing the network and may even bring greater amounts of sensitive data onto the network. Moreover, adding

more devices onto a corporate network means there are more endpoints to protect. Concurrently, employees exercising their desire to use mobile devices for mission-critical tasks has led to a burgeoning ecosystem of mobile-enabled cloud applications. These applications add more complexity to network traffic flows as applications and the associated data can be housed in-house or off-premises, in public or private/hosted cloud. These are then delivered to various points in the enterprise network, from headquarters to branch offices, and even out to remote workers connected via mobile devices. The applications are not only new attack surfaces containing large amounts of potentially sensitive data, but have the potential to open up pathways for breaches to enter the network.

Adding yet another layer is the emergence of Internet of Things (IoT) in the enterprise. IoT is a network of networks of uniquely identifiable endpoints (or "things") that communicate without human interaction using IP connectivity — whether locally or globally. IDC estimates that by 2020, nearly 30 billion IoT devices will be in deployment. These endpoints, or sensors, add a bevy of new attack surfaces to the network. In this early stage of evolution of IoT, security interfaces may not be intuitive to configure, and may even have difficulty integrating with the overall security infrastructure. The uncertainty around IoT security is especially concerning. Much of the value of IoT lies in the data that IoT devices/sensors can collect. The volume, breadth, and depth of this data is astounding. Already in many of today's production environments, IoT devices are collecting a mass of both valuable structured and unstructured data, much of it highly sensitive to security and privacy concerns. Realizing the greatest benefit from IoT hinges upon tight network security integration.

With the constant evolution of mobility in the enterprise, the addition of productivity-enhancing public cloud-hosted business applications, and the rapid emergence of IoT, enterprise IT must re-evaluate its approach to network security- and this is well understood by network security decision makers. In fact, a recent IDC survey of security professionals revealed that 52% were concerned about employees underestimating the importance of following security policies. Nearly as many (45%) worried about increasing complexity of attacks. All the while, a significant portion (38%) believed their budgets may be too small to respond appropriately to shifting challenges.

These intensifying challenges, along with problems in garnering appropriate levels of funding and support for network security, can seriously slow down enterprise IT in detecting breaches and subsequently resolving them, as well as putting measures in place to prevent similar breaches in the future. IDC has found that 3rd platform security infrastructure updates such as endpoint hardening and user management can take more than a year to become mainstream across an organization. In the 3rd Platform era, it has become more important to deploy a responsive, intelligent, and scalable network security architecture that is platform-based and fully integrated within the network infrastructure. This type of delivery model for network security leverages the network's inherent distributed intelligence, enabling the network to be a defender against breaches rather than a readily susceptible attack surface. Network attackers move quickly, thus network security needs every advantage in order to respond in kind.

The Network as a Security Resource

As management of networks becomes more standardized, enterprises have unprecedented visibility of their networks from datacenter to edge and across widely dispersed locations. This applies to visibility of devices, users, and applications. Given the ability to collect all of this data, and the increasing ability to analyze it, networks today have previously unseen ability to detect irregular and suspicious activity. Abuses of the network involving malware, anomalous traffic flows, unauthorized app usage and other user policy violations, rogue devices and wireless access points (APs), and others are more easily identified, quarantined, and remediated through network intelligence.

Effectively leveraging the network for security involves seeing and using the network as a sensor and enforcer across all points in the network - including the datacenter, branch, and campus along with

every endpoint and application that touches it. Using the network infrastructure as a security tool does not replace, but rather, reinforces traditional network security tools such as firewalls and advanced malware protection. The following section will examine how Cisco's end-to-end solution set can be used to accomplish this.

Considering Cisco

Cisco's network security portfolio is built on the concept that security should be embedded everywhere in the network. Using NetFlow, which allows the network to function as a sensor, integrating with Identity Services Engine (ISE) for granular policy control, TrustSec for enforcing network segmentation, network security can extend seamlessly from the infrastructure down to the end-user. The following tools support the end-to-end implementation of using the network for security:

NetFlow and Lancope

At the heart of "network as a sensor" is NetFlow. NetFlow is a feature on Cisco routers, switches, and some wireless equipment that is able to create continuous records of all conversations that travel through a NetFlow enabled switch or router. Each communication session on a NetFlow-enabled device provides rich visibility and insight, including these seven that are often of elevated importance: network scanning, botnet detection, denial of service, fragmentation attack, host reputation change, and worm propogation.

Data can be stored for future use, empowering NetFlow to be a critical tool for identifying security breaches. Detailed forensics, and end-to-end communication logs give full details as to suspicious activity on the network, allowing better detection and more focused remediation. Working in tandem with Lancope StealthWatch, greater network visibility is provided along with real-time alerting to identify security threats. Integration of Lancope StealthWatch with Cisco ISE further provides correlation of context of a device (who, what, where, when and how) with network traffic, and provides an ability to rapidly isolate infected devices from the network.

Identity Services Engine

The Identity Services Engine (ISE) is Cisco's security policy management platform that streamlines the delivery of consistent secure access controls across wired and wireless networks and VPN connections. Secure user access through ISE begins with user authentication and device classification, which ISE augments with rich contextual information for better decision making to ensure that the right level of access control is assigned at any given moment. Using more granular contextual information such as role, location, and time, ISE can decide to grant more restricted access to the network ensuring very comprehensive secure access, both in terms of depth and breadth. Depending on the policy criteria, ISE can allow a range of selected access based on the user and device. One policy woven throughout the network increases operational efficiencies—by avoiding separate and individual policies to manage and enforce, and by integrating policy enforcement visibility.

TrustSec Software-Defined Segmentation

Cisco TrustSec is embedded technology in Cisco switches, routers, and wireless and security devices that allows enterprises to implement software-defined network segmentation. TrustSec enforces role-based access controls, created in Cisco ISE, for secure access to highly sensitive network resources based on identity and role. TrustSec aims to simplify the setting and management of whom can talk to whom (or what) on the network, who has access to resources, and how systems can communicate with other systems. TrustSec enforcement begins in the datacenter and reaches out to the access edge as well as remote VPNs.

Benefits of Using the Network as a Security Tool

In a time when all capital and operating expenses are subject to scrutiny, it is critically important for enterprise IT to justify investment decisions and find ways to generate additional value from the network. Using the network infrastructure as a security sensor and enforcer is a way to leverage what is already in-house to protect against security breaches that can disrupt the business and result in lost revenues. An end-to-end embedded network security infrastructure such as the one offered by Cisco leverages valuable metadata to allow faster time to insights on network traffic. Using TrustSec and ISE together allows for granular policy-based network access control with software-defined segmentation that can contain threats and prevents their lateral movement across the network. This type of security paradigm is also highly scalable, as NetFlow, ISE, and TrustSec can be enabled across the network to protect the resources that the network connects.

Challenges and Opportunities

Rethinking and fully realizing the security power of the enterprise network represents a fairly significant paradigm shift, considering the conventional wisdom is that protection comes from outside resources rather than from within the network itself. As with any radically different way of thinking about IT infrastructure, there needs to be an educational effort involved in bringing about an understanding of this new paradigm and cultural shift to organizational decision makers. Moreover, for organizations that have already built out complex network security infrastructures, stakeholders may be hesitant to re-imagine today's systems (especially when they appear to be working). Enterprise IT often walks a tightrope between maximizing pre-existing investments while making sure current infrastructure can withstand tomorrow's challenges, and this situation is no different.

However, as with most challenges, there are tremendous opportunities on the other side of the coin. As mentioned, implementing a network architecture with tightly integrated security components may represent a more efficient investment that can eliminate the redundancies of more piecemeal network security implementations. Being able to demonstrate operational efficiencies and return on investment from the network that acts as a security sensor and enforcer is possibly the greatest tool in demonstrating why it is a worthwhile opportunity.

Conclusion

In the era of the 3rd Platform, the enterprise network plays an unprecedented role in day-to-day operations, customer and employee engagement, competitive differentiation, and innovation. However, given the vast amounts of sensitive data traveling across enterprise networks, a variety of hackers and cybercriminals will look to use networks to accomplish their goal of data breach, potentially causing significant damage and disruption to the lives of customers and employees, while also impacting the reputation of the organization. The good news is that today's networks have the ability, from end to end, to have security tools deeply embedded in their infrastructure, giving the network never-seen-before abilities to protect and defend against future attacks. Considering a network infrastructure with tightly integrated security features is highly recommended in this era of IT, and a solution set such as the one offered by Cisco may be a viable solution for organizations.

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.

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