RESEARCH
Influence and insight
through social media

December 2019

New Security Realities Demand

NEXT-GENERATION VISIBILITY

WHITE PAPER

Prepared by
Zeus Kerravala

ZK Research
A Division of
Kerravala Consulting

© 2019 ZK Research

INTRODUCTION: THE EVOLVING COMPLEXITY OF CYBER SECURITY AND NETWORKS DEMANDS THE ABILITY TO CHANGE QUICKLY

The job of today's security professional is markedly more difficult than at any time in history. The closed and controlled nature of the IT environment has given way to an open one where users come and go on personal devices and connect to applications that exist only in the cloud. The current environment is highly dynamic, creating a huge headache for security professionals as complexity has gone through the roof. Adding to the challenge is the fact that the nature of attacks has changed as businesses have moved from closed to open environments.

For most organizations, it's very difficult to deploy new security technologies or rip and replace older ones. Doing so potentially disrupts the current environment and requires extensive steps and approvals. However, maintaining the status quo can also have detrimental effects, particularly when there is such a heavy emphasis on cyber security all the way up to a company's C-level. The current state of security forces the organization to engage in a balancing act between security and control by using the latest technologies and practices while ensuring network availability, reliability, flexibility, performance and adherence to budgeted expenditures—they all matter.

Combatting this dilemma requires thinking differently about how to deploy network security solutions. The combination of an ever-changing network, constantly evolving security threats and new technologies geared to meet current or anticipated threats and challenges suggests that organizations must adopt new tools and systems faster. Typical approval cycles and quasi-political negotiations regarding adherence to networking and security goals need to change. There should be a way to easily deploy a necessary security or networking solution in the network while still upholding requirements for both.

There has certainly been a flurry of innovation in the area of cyber security, where new tools are being developed seemingly weekly. A decade ago, good security involved firewalls, intrusion prevention systems (IPSs) and anti-malware on user endpoints. Today, security professionals are deploying things such as user and entity behavior analytics (UEBA), endpoint detection and response (EDR), network traffic analysis (NTA), x detection and response (XDR), decoy systems, email security and a never-ending list of security tools. ZK Research has found that the average number of security tools in use at large enterprises is a whopping 72 and that it now takes 103 days to find a breach once it has occurred—which is more than double the 45 days it took five years ago. The shocking reality is that despite spending a record amount on security—about an aggregate of $75 billion today, according to ZK Research estimates, based on ongoing research—businesses are falling farther behind, and the trend will not change unless security architectures change.

One challenge is that getting the right traffic to the security tools has been difficult, particularly for in-line but also for out-of-band monitoring. Adding a solution to the network for hosting and in-line or out-of-band traffic is easier said than done. There has been and continues to be a turf war between security and networking. Historically, hardware-based network packet brokers have

ABOUT THE AUTHOR

Zeus Kerravala is the founder and principal analyst with ZK Research. Kerravala provides tactical advice and strategic guidance to help his clients in both the current business climate and the long term. He delivers research and insight to the following constituents: end-user IT and network managers; vendors of IT hardware, software and services; and members of the financial community looking to invest in the companies that he covers.

A new style of network packet broker or visibility platform is emerging: an open platform that can host and manage the security solutions that run on it.

provided traffic delivery for solutions, but their closed, restricted nature has failed to bring the flexibility or speed required to address current challenges.

A new style of network packet broker or visibility platform is emerging: an open platform that can host and manage the security solutions that run on it. Network and security professionals should seek out this type of platform, such as the Open Visibility Platform offered by Niagara Networks, as a way of bringing a higher level of agility to security. Doing so will eliminate the struggle between agility and new technology adoption and remove the constraints related to deploying new technologies into the network.

SECTION II: CHOOSING THE RIGHT PLATFORM FOR NETWORK VISIBILITY AND OPERATIONAL AGILITY

A handful of visibility platforms are available today. As companies navigate the evaluation process, the following attributes are those that ZK Research deems to be the most important in these platforms:

Hosts any virtualized solution: Historically, packet brokers or visibility platforms have maintained a list of approved applications that they support, and non-approved applications cannot be supported unless or until the manufacturer approves them. This limits choice and could hold organizations back, as they can't always use the tools they want to use. Also, with new security solutions, organizations must wait until the visibility platform vendor sanctions them and assures support for the appliance. Buyers should seek out a solution that works with any and all solutions, even those that are brand new. Ideally, the platform will also accommodate proprietary or homegrown solutions as well as on-demand or ad hoc solutions used on a temporary basis by hired testing or certification professionals.

Enables intelligent tool chaining: The messy quagmire of security tools makes establishing a logical flow of network security very difficult, as the order of security operations matters. A web or application firewall should be in a path before an intrusion detection system (IDS) or IPS, and each should be treated differently if a failure affects either solution. The visibility platform will ideally have intelligent tool chaining capabilities for proper logical sequencing and management.

Provides core traffic processing utility functions: Handling core utility tasks, such as deduplication and decryption, can greatly degrade the performance of security applications or devices. When such tasks are offloaded and performed centrally on a visibility platform that specializes in such workloads, individual security applications can achieve higher performance and focus on areas of core competence. A centrally performed process may be able to serve multiple tools.

Today's visibility platforms must be built with the principles of digital transformation in mind.

Meets network requirements for robust, reliable infrastructure: Visibility platforms are not just for security operations. The intelligent network traffic data can be used to deliver new functionality for network and performance tools to ensure the network runs better and trouble-shooting time is minimized.

Ensures policy-based compliance: Core utility tasks should be handled according to policy so that compliance and overall security rules can be maintained. For example, the way European Union (EU) data is handled is unique, as are the requirements for the Health Insurance Portability and Accountability Act (HIPAA). The way logging, data storage, transit, decryption and other functions are handled must be based on compliance policies.

Several vendors claim to play in the visibility platform space. After considering the requirement for openness and the ability to support any and all third-party solutions, ZK Research believes that Niagara Networks most closely fits these criteria. For those who aren't familiar with Niagara Networks, the company provides high-performance network visibility solutions that can be used for both security and network management and monitoring. Niagara Networks provides all the building blocks for a visibility platform at data rates up to 100 Gbps.

SECTION III: CONCLUSION AND RECOMMENDATIONS

Many visibility platforms are available today, but most are built on older architectures from a time when network and security tools were deployed in silos. Digital transformation has created a need for businesses to adopt a number of new technologies such as mobility, the cloud and the Internet of Things (IoT). These bring a wealth of new functionality to companies but create some new security risks, causing companies to invest in new security tools. Therefore, today's visibility platforms must be built with the principles of digital transformation in mind. Instead of being closed, proprietary solutions, they must be open in nature. ZK Research has evaluated many platforms and believes the Open Visibility Platform from Niagara Networks meets all of the above requirements.

Selecting the right visibility platform is critical to simplifying security architectures and providing streamlined operations while increasing the level of threat protection. To help security professionals along this journey, ZK Research makes the following recommendations:

Bring security and network operations together. Historically, security and networking teams have operated independently, as their goals were at odds. Security teams are concerned about protection, but this can impede network performance or compromise reliability. Visibility platforms can act as a catalyst, enabling security and network teams to have common goals and finally work in harmony instead of against one another.

Choose a vendor based on modern criteria. There are several packet brokers on the market, many of which claim to be visibility platforms. Other low-cost vendors claim that their "good enough" solutions are sufficient. Make a decision based on today's needs, and enable security teams the freedom to deploy what they want, where they need to, without getting in the way of network operations.

Collect and analyze visibility data for best results. IT departments should continually analyze the data generated by a visibility platform. Doing so can help them understand exactly what is happening today, who is accessing what information, where apps reside and other critical information. As the environment changes, visibility platforms can shine a light on blind spots and points of risk while enabling IT to move to a predictive model.

CONTACT

zeus@zkresearch.com

Cell: 301-775-7447

Office: 978-252-5314

© 2019 ZK Research:
A Division of Kerravala Consulting
All rights reserved. Reproduction or redistribution in any form without the express prior permission of ZK Research is expressly prohibited. For questions, comments or further information, email zeus@zkresearch.com.