RESEARCH
Influence and insight through social media

September 2018

DYNAMIC NETWORK SEGMENTATION

Is a Must-Have for Digital Businesses

WHITE PAPER

Prepared by
Zeus Kerravala

ZK Research
A Division of
Kerravala Consulting

INTRODUCTION: DIGITAL TRANSFORMATION MANDATES A SECURITY RETHINK

The world is quickly becoming digitized, and the IT landscape is rapidly evolving to meet the needs of the new business environment. Client/server computing has given way to the disruption of traditional business and ownership models by private and public cloud services, "bring your own device" (BYOD) and mobility. This shift has provided new opportunities for businesses and their users, but it also has created unique security challenges for IT that traditional security solutions were never designed to address. Adding to this is the onslaught of Internet of Things (IoT) devices, which are growing at an increasing pace. By 2020, there will be more than 20 billion IoT devices in addition to corporate endpoints connected to the network.

Today, business leaders are expecting more agility from IT, but technology leaders must ensure that applications, data and users are protected within an evolving threat landscape. However, traditional security architectures were designed for the client/server computing era, when there was only a single ingress point from the outside, and all applications, infrastructure and endpoints were owned and controlled by the IT department. The security architecture was very rigid in design, which was sufficient to enable classic business models with IT infrastructure changes only once every few years. The traditional security architectures have a number of limitations, including the following:

Lack of agility: Businesses need to move quickly, which means IT must be highly agile. Traditional security is built on the concept of deploying best-of-breed point products at specific points in the network. In this model, each security tool must be configured individually, meaning changes could often take months to implement. Additionally, businesses are having to rely on more point products, adding to the complexity and the lack of agility. The ZK Research 2017 Security Survey found that large enterprises have an average of 32 different solution tools in their organizations.

Challenges in meeting compliance requirements: Regulated industries such as retail and healthcare need to comply with mandated regulations including the Payment Card Industry Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA), respectively. This means protecting their data from outside threats as well as those within the internal network.

Complexity of securing the data center: The benefits of software-defined data centers are undeniable, but so are their inherent security challenges. The dynamic aspect of virtualization provides speed, agility and cost efficiencies, but it also creates challenges for security teams, who are using unfamiliar and siloed security tools that allow attackers to take advantage of non-compliant and vulnerable endpoints. With about 70% of traffic in data centers moving

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.

Businesses spend 90% of their security budgets on protecting the perimeter, yet only 24% of attacks are aimed there.

east–west, this requires a new approach to protect such environments and ensure that they are compliant with company security policies.

Increased threat complexity: Persistent threats (i.e., attacks that get past existing defenses, go undetected and continue to cause damage) are difficult to detect. Taking the first step to combat such advanced threats entails companies obtaining up-to-date information about all the physical and virtual endpoints across the network, their function, how they are connecting, their security posture, etc. Armed with this granular information, businesses can build a "defense-in-depth" security approach—one that involves diligent separation of assets based on their function to minimize the lateral spread of malware across the network. It's unrealistic to expect traditional silo security products to proactively identify all physical and virtual assets, separate them based on the business function, and identify and stop the lateral movement of threats.

New security threats created by IoT: The IoT era has arrived and is bringing with it new challenges for today's security teams. The rise of IoT will see billions more devices connected to corporate networks over the next five years. Many of these headless devices have no inherent security capabilities, and if they are breached and are not compartmentalized within their sphere, they can create back doors into a company's network. Also, as identified by the ZK Research 2017 IT Priorities Survey, in 60% of the cases, IoT devices are deployed by the operational technology (OT) team, so IT is unaware of their existence. Also, a lack of visibility into these devices combined with the inability to detect the type of device being used creates enormous challenges for IT and security teams, who are tasked with monitoring and segmenting these devices.

According to the ZK Research 2017 Security Survey, businesses spend 90% of their security budgets on protecting the perimeter, yet only 24% of attacks are aimed there. Businesses need to complement investments made at the perimeter with technologies that can protect the internal network.

Traditional perimeter security alone is not sufficient in a world where everything is connected and more threats are coming from the inside of the network. Protecting the perimeter is certainly critical to security success, but this approach cannot be relied upon to provide all-inclusive protection—similar to the way a castle was protected by a moat but also employed internal guards. Simplified network segmentation can facilitate comprehensive security and ensure the business is in alignment with the next era of IT.

SECTION II: DYNAMIC NETWORK SEGMENTATION DEFINED

Network segmentation is a technology that enables organizations to logically separate the network into secure zones. Each of these zones is compartmentalized and isolated from the other segments. Traditional methods such as virtual local-area networks (VLANs) and access control lists

By 2020, 50 billion devices will be connected to the network, many of them driven by IoT initiatives.

(ACLs) have been used for decades. But as the network continues to expand, these methods can be easily complemented with a more dynamic form of segmentation.

Dynamic network segmentation works on the guiding principle that security must be ubiquitous and transparent to the network, allowing organizations to segment their network in an effective and meaningful manner across the campus, data center and cloud. It involves discovery and precise classification of users as well as different types of network-connected physical and virtual endpoints, their security postures, levels of compliance, etc., to enable next-generation firewalls to enforce granular identity and context-aware security policies and allow network access, regardless of location.

Dynamic network segmentation operates on a white list model, where no device or user can see any other unless it is explicitly enabled to do so. Once the white list is established, endpoints are confined to their groups. For example, a security policy could be set up that states "medical devices can connect only to the medical records server" or "a security camera (which can be an IoT device) can only connect to the video server." This approach dynamically prevents devices in a guest network from having access to these endpoints and limits access to their functions without connecting outside to the internet. This prevents an unauthorized user from having access to devices in the other zones. If a medical device moves within the network, for example, no reprogramming of the network is required, as the policy follows the endpoint. Similarly, in retail, separate secure zones could be created for the point-of-sale (POS) equipment, guest network and accounting department. This would ensure that people connected to the guest network cannot access separate segments that are designated only for POS devices.

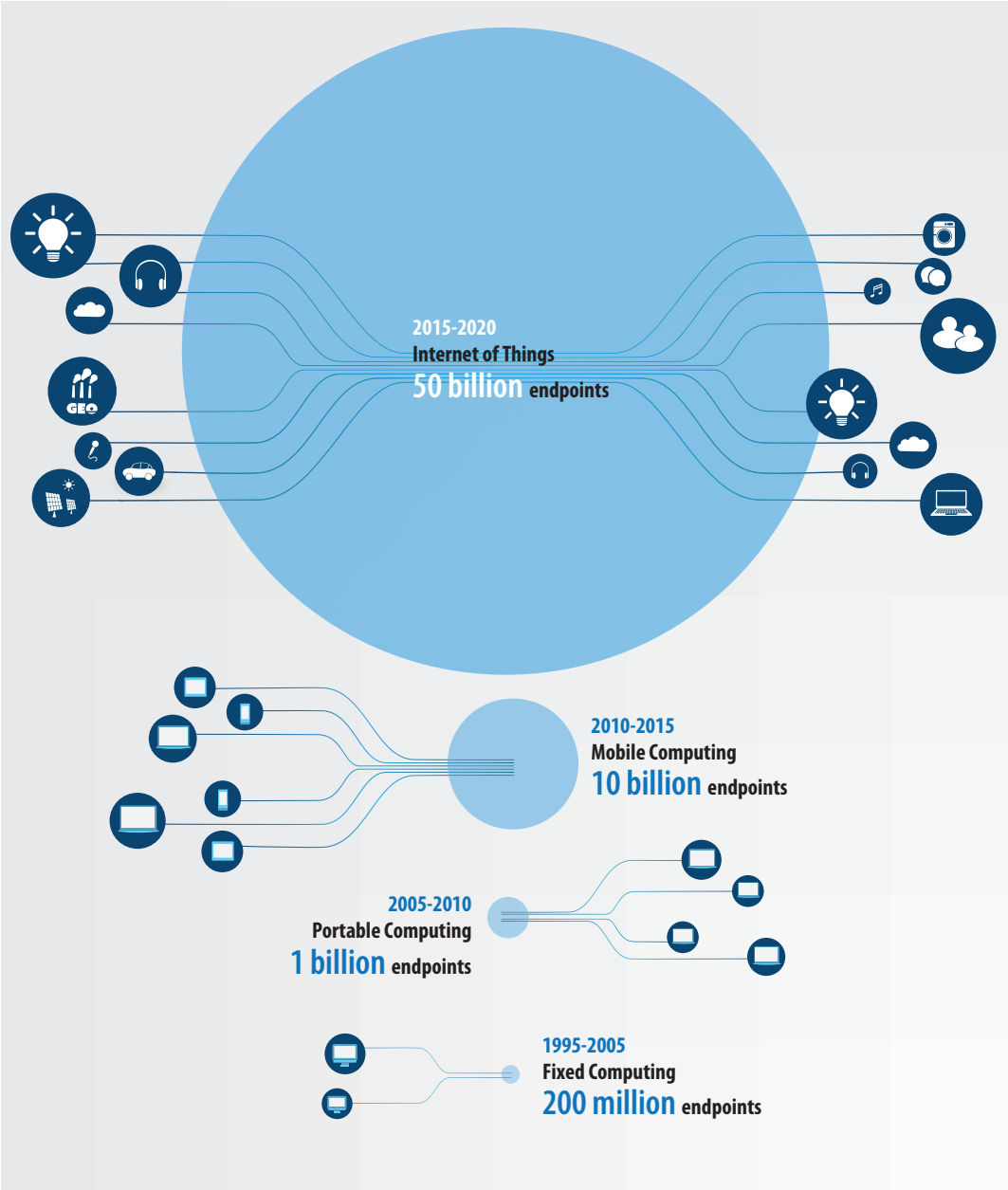
Dynamic network segmentation reduces the degree of human element involved when changes occur in the network and provides security for heterogeneous networks, allowing businesses the flexibility to choose diverse network infrastructure. ZK Research has forecast that by 2020, 50 billion devices (Exhibit 1) will be connected to the network, many of them driven by IoT initiatives. With this many connected devices, dynamic network segmentation can play a critical role in ensuring that the "blast radius" of a breach is limited.

SECTION III: BUSINESS BENEFITS OF DYNAMIC NETWORK SEGMENTATION

Dynamic network segmentation brings a level of agility to network security that is in line with business needs. The technology is an important enabler of a digital strategy and should be at the top of every business and IT leader's priority list. Organizations that embrace dynamic network segmentation will realize the following benefits:

IT as a business enabler: Typically, when security technology is deployed, there is some disruption to the business as the solutions are deployed. Dynamic network segmentation does not require a complete redesign of the network, so there is reduced complexity and minimal

Exhibit 1: 50 Billion Devices Will Be Connected to the Network by 2020



ZK Research 2017 IoT Forecast

impact to the business. In 2016, an IDC study on network segmentation found that the value of higher productivity created by network segmentation was $1,094 per device per year over a five-year period.

Simplified security architecture: Security has evolved, with new point products being developed to solve specific problems. All of the new appliances have created "security sprawl,"

Businesses will save an average of $2,058 per IoT device per year by using network segmentation.

where security professionals need to continually configure and update a wide variety of network and security infrastructure every time a change is made. Because dynamic network segmentation provides access regardless of user or device location on the network, it acts as an enabler for IT and security teams by greatly reducing their administrative tasks.

Improved productivity of IT staff: One of the biggest challenges with managing traditional firewalls is the need to constantly add, change and delete rules. In fact, the process can be so onerous that the task of deleting old rules often gets ignored, which results in critical firewall resources being unnecessarily consumed. Dynamic segmentation can greatly reduce the needless IT overhead associated with having to identify, classify and onboard traditional and IoT devices manually and include them in policies for network access. The previously mentioned 2016 IDC study calculated that businesses will save an average of $2,058 per IoT device per year by using network segmentation.

Dynamic security policies: Businesses can create policies that automatically adapt to changes, such as the addition or movement of servers or devices, without manually modifying each firewall rule, providing unhindered network access.

Meeting compliance requirements: Segmentation can help regulated verticals meet regulatory demands. For example, network segmentation can be used in healthcare to establish zones for medical devices and servers. In this case, patient records are stored in their respective compartments in order to secure patient information, records of procedures and doctors' notes while restricting the access of medical devices within their zones—making them unreachable from any other network or device.

SECTION IV: FORESCOUT ENABLES DYNAMIC NETWORK SEGMENTATION WITH NEXT-GENERATION FIREWALLS USING AGENTLESS VISIBILITY

Next-generation firewalls (NGFWs) deliver effective network segmentation by ensuring appropriate application and user access, along with inspection for all traffic crossing the segments.

ForeScout CounterACT® integrates with existing network infrastructure across the campus, data center and cloud to discover, profile and classify traditional and non-traditional devices (such as laptops, PCs, tablets, smartphones, BYOD and IoT endpoints, servers, cloud instances, virtual machines and applications) without the involvement of agents, and it assigns them to predefined groups/roles within the NGFW. This enables IT organizations to implement dynamic segmentation using granular access policies within NGFWs based on user identity and device context from CounterACT, regardless of device or user location on the network. This helps to provide secure access to critical applications, prevent unauthorized access to sensitive resources and minimize data breaches. In addition,

this improved visibility lets businesses true-up existing asset inventory tools such as configuration management databases (CMDBs) with up-to-date information about network-connected devices and their security contexts.

SECTION V: CONCLUSION AND RECOMMENDATIONS

In today's fast-moving digital business environment, it's imperative that organizations rethink their security strategies and implement a solution that can bring the same level of agility to security that other areas of IT have today. Security must act as an enabler and support organizations' digital transformations.

Dynamic network segmentation solutions, such as ForeScout CounterACT and NGFWs from Palo Alto Networks and Check Point Software, complement existing infrastructure and maximize a company's investments. Because of this, ZK Research believes that dynamic network segmentation needs to be a top initiative for all organizations today and makes the following recommendations to business and IT leaders:

Start with visibility. It's impossible to build an effective security strategy without having a good understanding of network-connected physical or virtual endpoints. The process of securing the network needs to begin with gaining complete visibility and taking inventory of network-connected devices, which will provide the information for businesses to make the right business decisions.

Implement dynamic network segmentation. Many network segmentation solutions are available to buyers today. Manually provisioning networks has limited value, as the continual reconfiguring of networks creates blind spots that can leave security teams in the dark. A better alternative is to implement best practices such as dynamic network segmentation and allow the network to dynamically adapt to changes or the movement of resources.

Maintain continuous compliance. With real-time and agentless visibility into the network, compliance can be enforced at the moment of device connection, and remediation actions can be taken when necessary.

CONTACT

zeus@zkresearch.com

Cell: 301-775-7447

Office: 978-252-5314