RESEARCH

Influence and insight
through social media

Businesses Can Gain a Competitive Edge with a

HIGH-POWERED NETWORK EDGE

WHITE PAPER

Prepared by
Zeus Kerravala

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.

INTRODUCTION: BUSINESSES ARE NOW NETWORK CENTRIC

Digital transformation is reshaping the business landscape faster than ever before. Companies that have embraced digital have quickly become leaders in their respective markets, and those that have not done so have fallen farther behind. ZK Research studies have found that digital organizations are 64% more profitable than ones that have not embraced this shift. It's for this reason that digitization is a top initiative for IT and business leaders.

The evolution to digital, like other major shifts before it, requires new technologies. The last major business transition—the Internet era—was fueled by the convergence of low-cost PC computing, the Windows operating system, the creation of the browser and the rise of home broadband.

The digital era will be led by a number of emerging technologies such as cloud computing, mobility, the Internet of Things (IoT), big data and collaboration. All of these technologies may seem like unrelated components, but they do have one point of commonality—they are all network centric, meaning the network plays a key role in the success of deployment. For example, cloud services are exploding (Exhibit 1), but users require high-quality network service to have a good cloud experience.

Over the years, many experts have predicted that the network would become a commodity. In this scenario, the best choice would be to purchase the lowest-cost product, as the choice of vendor would make little difference. This trend happened in other areas of IT such as personal computing, so there was some speculation that the network industry would head down the same path.

It's true that commodity switches are lower cost than leading-edge ones, which are often sold at a premium, but the cost of one switch versus another should not solely be made on the price of one

Exhibit 1: **Cloud Services Are on the Rise**
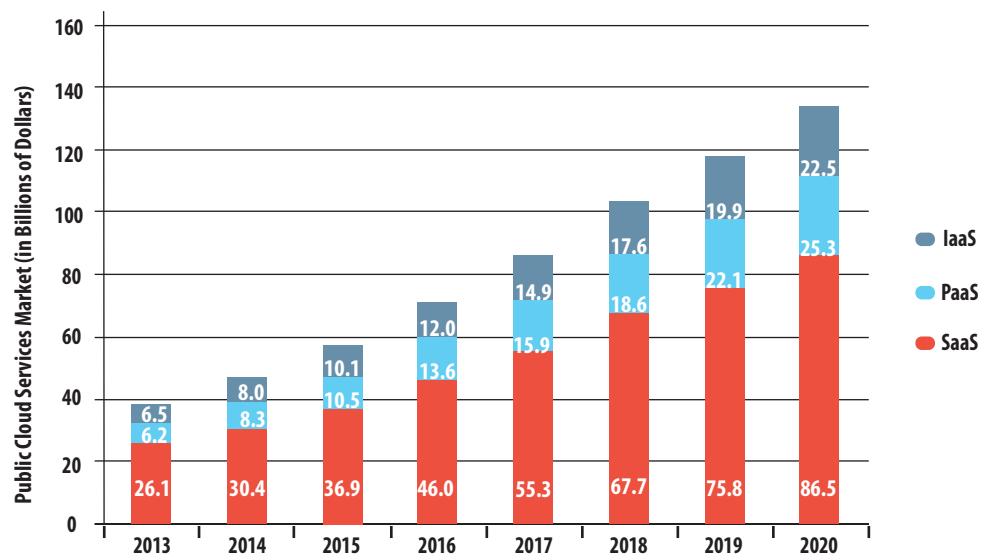
ZK Research 2016 Global Cloud Forecast

device versus another. In fact, ZK Research believes that a commodity switch will eventually cost an organization more for the following reasons:

Security risks: All of a company's valuable data can be accessed over a network. This makes it vulnerable to hackers if the proper precautions are not taken. Every device that attaches to the network today can be infiltrated. Historically, security teams would put agents on company-owned PCs to protect the endpoints. Today, IT needs to deal with the influx of personal mobile devices and IoT endpoints, which are much harder to secure using agents. IoT devices pose a significant challenge, as most IoT endpoints have no ability to run agents. Also, the ZK Research 2016 IoT Survey found that 78% of IT individuals polled are not confident in their ability to know whether IoT devices have been connected to the network. This is why security ranks number one among the top concerns for IoT deployment (Exhibit 2).

The cost of downtime: Commodity switches are generally built more cheaply than premium ones and do not have the same levels of resiliency. In today's digital world, where everything

Exhibit 2: IoT Deployment Concerns

What are the biggest IT challenges with respect to IoT?
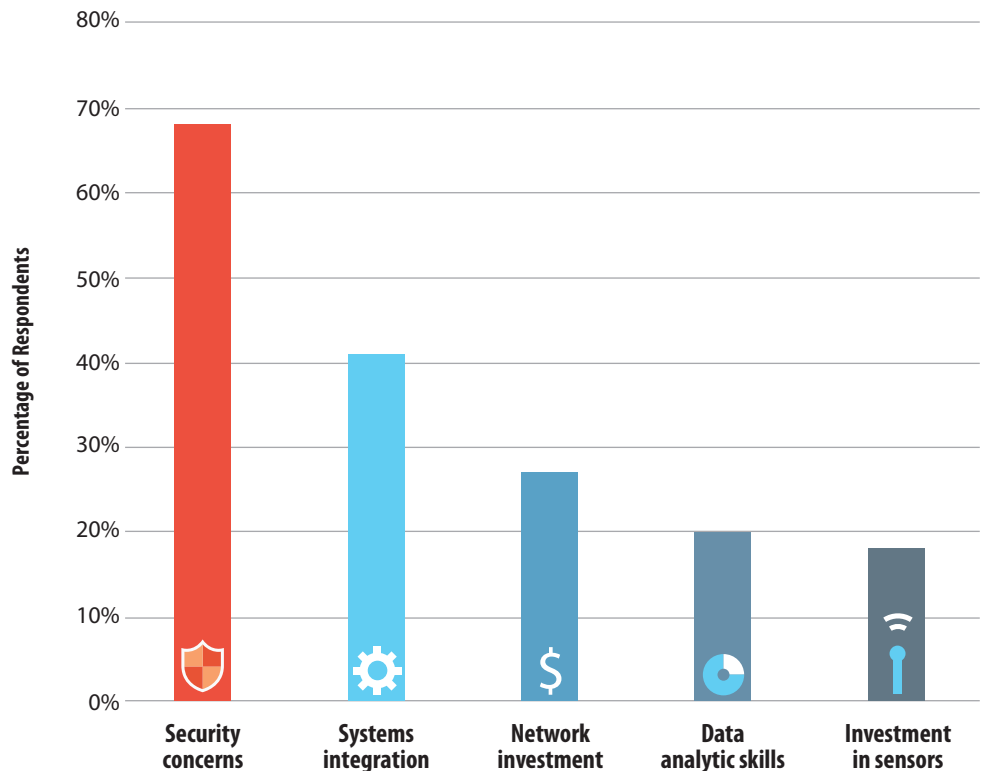
ZK Research 2016 Network Purchase Intention Study

IT leaders must consider the network edge to be a strategic asset, not a commodity, and use a vendor that drives innovation rather than one that drives down cost.

is connected, downtime costs companies money. ZK Research calculates the average cost of downtime across all verticals to be $1.7 million per hour. Even a small variance in uptime can quickly wipe out any savings from using a commodity switch.

The cost of a bad user experience: Businesses spend billions on new technology to make users more productive. ZK Research has calculated that users are on average 14% less productive because of poor application performance. A commodity switch will not perform as well under high loads and will have a direct impact on user productivity.

The cost of missing opportunities: Digital transformation is not a one-time event. Businesses must continually gather data and analyze it to gain new insights as to how to stay ahead of competitors. The network edge can provide a wealth of data regarding users, devices, applications and other contextual information. Commodity network devices do not have the same level of instrumentation and visibility to provide relevant insights to the business.

Also, commoditizing the network will stifle innovation over time. Manufacturers of network products will use the lowest-cost, off-the-shelf components and cut engineering costs. Theoretically, if all products are the same, then the only competitive advantage will be based on price, which will slow down innovation even more.

However, this thesis has proven to be incorrect, and now more than ever, the choice of network matters, particularly at the edge—as this is the point of connection for users, applications and devices. IT leaders must consider the network edge to be a strategic asset, not a commodity, and use a vendor that drives innovation rather than one that drives down cost.
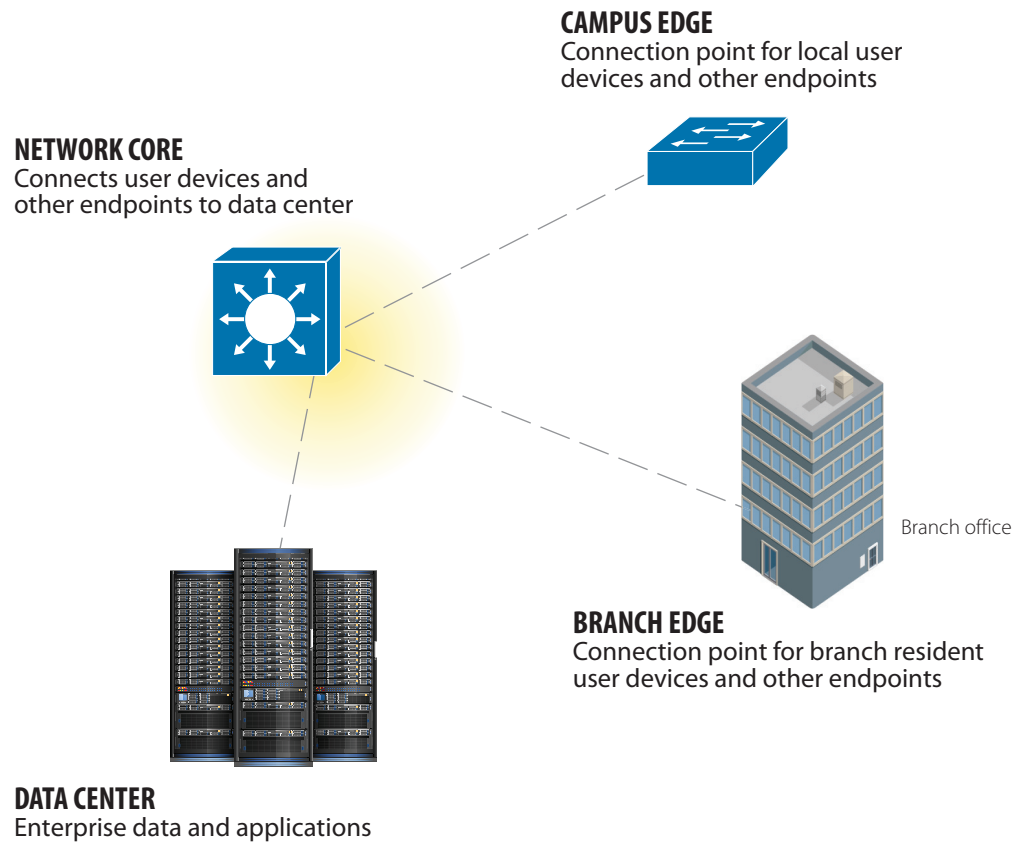
SECTION II: UNDERSTANDING THE ROLE OF THE NETWORK EDGE

Non-network engineers often struggle to understand how networks operate. A network may act like a single entity, but the network is actually composed of several tiers or layers with specific functions (Exhibit 3).

The data center and the network core are critically important but are built primarily to move traffic from one location to another as fast as possible. A decade ago, the network edge connected primarily PCs and printers to the company network. But digital transformation has made the network edge, which is composed of the campus edge and the branch edge, more important than ever. Below are all the functions that happen at the network edge today:

The first security enforcement point: According to the ZK Research 2016 Security Survey, 80% of security breaches occur inside the perimeter. This has a profound impact on security strategy, as the enterprise firewall cannot protect against security threats. The edge of the network is the best place to apply and validate policies, as this will not limit access to resources to

Exhibit 3: The Role of Network Layers

CAMPUS EDGE
Connection point for local user
devices and other endpoints

NETWORK CORE
Connects user devices and
other endpoints to data center

Branch office

BRANCH EDGE
Connection point for branch resident
user devices and other endpoints
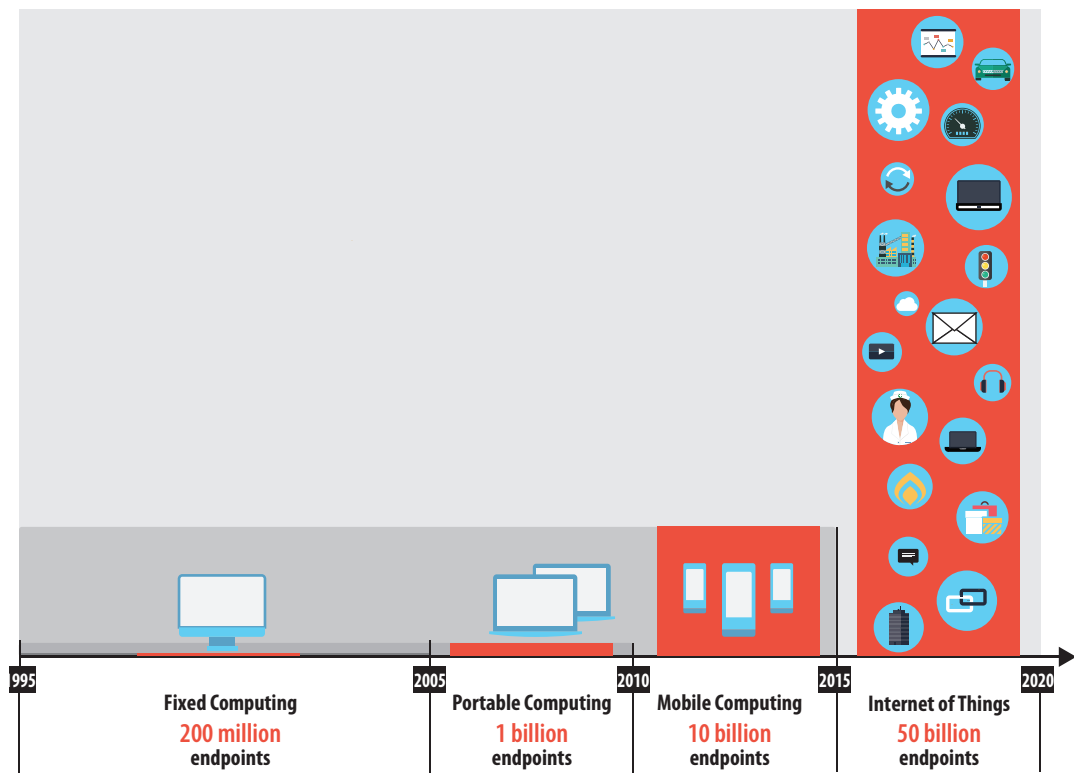
DATA CENTER
Enterprise data and applications

ZK Research, 2016

which users need to connect. Security policies set at the edge can stop most internal threats as well as prevent them from spreading laterally if a breach occurs.

Foundation for IoT: ZK Research predicts that the number of connected endpoints will explode between now and 2020 (Exhibit 4). As IoT connectivity coalesces around IP, the network edge is where devices such as healthcare systems and LED lighting systems will connect. In addition to being connected, many of these devices will be powered by the network using power over Ethernet (PoE). If the right functionality is not at the edge, businesses may not maximize their IoT investment.

Optimization of application performance: All business applications must pass through the network edge regardless of whether they are located in the company's data center or in the cloud. The network edge is where prioritization of applications occurs, preventing real-time or mission-critical applications from running slowly.

Exhibit 4: IoT Creates Tens of Billions of Network Edge Connections

995		2005	2010	2015	2020
	Fixed Computing 200 million endpoints	**Portable Computing** 1 billion endpoints	**Mobile Computing** 10 billion endpoints	**Internet of Things** 50 billion endpoints	

ZK Research, 2016

Improved customer experience: One of the top digital initiatives for businesses is creating a differentiated customer experience. Digital technology can change the way customers shop, students learn and doctors practice medicine. However, a poor-performing edge can significantly impact customer-facing services, which can cause customers to change their loyalties. A recent ZK Research study found that two-thirds of millennials have switched providers in the past 12 months because of a poor experience.

Added business value: The network edge is the best place to gain new insights as to what is happening with the business. All data traffic passes through the network edge, making it easy for organizations to capture and analyze the traffic. Information regarding users, devices, applications and threats can be used to make better decisions faster than the competition and put the organization in a sustainable leadership position.

SECTION III: QUESTIONS TO CONSIDER WHEN ENABLING A HIGH-PERFORMANCE NETWORK EDGE

When it comes to choosing a network vendor, many options are available ranging from low-cost, commodity products to higher-value, full-featured ones. Evaluating these products can be

difficult because the price, range of features, manageability and security implications can be quite varied. Below are the key questions that companies should ask when enabling a high-performance network edge.

What is the total cost of ownership (TCO) over a five-year period?

As companies continue to deploy digital technologies, organizations should shift their thinking about the network and view it as the digital foundation. If deployed correctly, networks can deliver rich services to the network edge. However, this cannot be done at the expense of easily adapting to changing business climates and supporting integrated advanced features without business interruption, which can have tremendous long-term TCO benefits.

When evaluating the products at the network edge, organizations should look ahead five years or more to calculate TCO—the equivalent of one replacement cycle. As Exhibit 5 shows, commodity products may appear to have a lower TCO early in the life cycle. However, as companies need new services and perform incremental upgrades, a commodity switch choice can quickly lead to a skyrocketing TCO, as it needs to be replaced more often. In addition, the implications of choosing the wrong long-term products can lead to unnecessary downtime, lost opportunities and inconsistent device manageability. One CTO described a full-featured switch to ZK Research as a Swiss Army knife: He wasn't sure when he'd need the additional features, but he knew they'd be there when he needed them.

Exhibit 5: Full-Featured Network Switches Provide a Significant TCO Advantage over Commodity Products
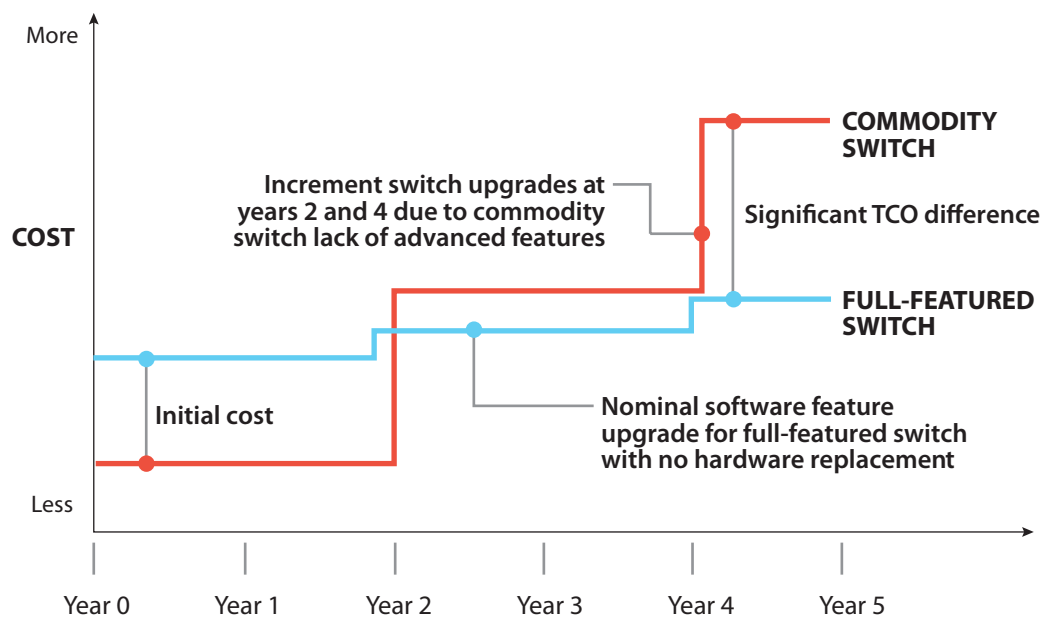
ZK Research, 2016

Digital transformation requires constant change, so it's important to understand the role the network can play in innovation.

Digital transformation requires constant change, so it's important to understand the role the network can play in innovation regardless of whether it is deployed in a greenfield location or as a refresh of an existing network. The question can be divided into three major categories: innovation, security and agility.

How does the network drive innovation?

The network does more than provide connectivity; it also needs to enable digital activities, which raises the following questions related to innovation:

1. **Can the solution assure availability and consistent service delivery?** Gone are the days of catastrophic network failures. Keeping the network up and running is fairly easy to do; what is difficult is making sure the end-user experience is not affected if a network component fails. Networks today need to automatically adapt to these failures and assure the same level of perceived performance. IT also needs a view of network anomalies and trends to identify their potential impact. Telemetry data can be used to quickly find and remediate application issues. The ZK Research 2016 WiFi Operations Survey found that almost 50% of respondents spend at least 25% of their time troubleshooting WiFi issues. Organizations need to look at how they can dramatically cut this time.

2. **Can the solution quickly adapt to new and unforeseen demand?** The demand on the network can change in an instant. Therefore, companies need to be diligent in deploying a solution that can automatically adapt WiFi networks to account for the rapid scale-up of clients and changes in signal quality.

3. **Can the solution improve device performance and battery life?** Mobile devices are the primary way in which users access information, and the network must have built-in intelligence that understands the devices connecting to it and adjusts to provide an optimal experience in the new mobile world. Being able to optimize roaming will reduce battery drain and keep users connected on the move.

4. **Can the network provide accurate insight about internal and external elements?** Data is king. The network is a valuable source, providing an understanding of users, devices, applications and even threats. However, that data is only as valuable as it is accurate—and accuracy comes from granularity. A one-meter view with more data points will provide a more realistic view of what is truly going on than a five-meter view with periodic data points. New customer use cases and experiences are being created through advanced network services such as 360-degree triangulation of a client, network or application. It is this view that can help IT gain a seat at the table by providing actionable, business-relevant data.

Digital businesses require an agile IT foundation so they can respond to market dynamics faster than their peers.

5. Is the solution ready to support new IoT devices that are not constantly interfaced by a user? The network edge can improve the availability of the endpoint. Many devices connecting to the network, such as the ones used with IoT, do so with a single power over Ethernet (PoE)–enabled connection, making it a single point of failure if the switch fails. The switches to which these devices connect need to have resiliency features to minimize downtime. Also, the requirement to power devices through switches is increasing, and the switch needs to provide enough wattage to meet this demand.

Does the network provide the level of agility required for the digital era?

Digital businesses require an agile IT foundation so they can respond to market dynamics faster than their peers. However, IT is only as agile as the least dynamic component, which is often the network. The network edge must be as agile as the rest of IT but without increasing cost and complexity. To understand if this is the case, companies must ask the following questions:

1. Can the solution consistently prioritize applications from cloud to end user? Having a siloed approach to defining the quality of service for applications delivers diminishing returns. Organizations are finding that addressing applications consistently from cloud, private or public networks to the end-user device is critical to maintaining a consistent, high-quality user experience.

2. Can the solution help turn up new branches or segments with little local support? Having to perform a "truck roll" to turn up a network in a remote location is an expensive and time-consuming proposition. Digital businesses operate fast—too fast to wait for new branches, network segments or functionality to be enabled by an engineer who must physically be on site to plug in a box and configure it. Plug-and-play capabilities and zero-day provisioning are critical to speed deployment and lower costs.

3. Can new functionality and standards be added without a "forklift" upgrade? Being able to add functionality without constantly having to replace old infrastructure with new devices minimizes business disruption and can save a significant amount of money. Also, network managers need to be able to deliver software updates without disrupting users, as this will impact productivity. Investing in solutions that can expand functionality quickly and easily is paramount to meeting new business demands.

4. Can licenses be easily transferred? Organizations need the ability to refresh hardware without incurring additional costs from having to purchase new software licenses. Decoupling the software license from the hardware is critical, as organizations will refresh their network infrastructure more often due to faster growing demand.

Threat detection remains a significant challenge for organizations.

Can the network be leveraged to increase security and minimize risk?

The network can serve as a valuable vantage point to not only grant user access but also validate user activity based on deeper context. Threat detection remains a significant challenge for organizations. The ZK Research 2016 Security Survey found that the average time to locate a breach is well over 100 days. Organizations need to find ways to detect threats in hours instead of days by asking the following questions:

1. **Can the solution logically segment traffic using a software-based approach and automatically adapt and scale when new risks are identified?** Network segmentation has been on the rise as customers look to isolate user and application traffic in secure zones. Assuring employees, guests, contractors and IoT have access to the things they require is straightforward when dealing with access control lists and radius in small deployments. But as the user and device counts expand, managing these lists becomes untenable. New digital organizations are looking to logically segment traffic based on user type and role. This allows them to quickly adapt their access policy and potentially automatically adapt based on the risk level.

2. **Does the solution embed security within the network infrastructure to detect internal and external threats at the access, core, WAN and branch?** The ZK Research 2016 Network Purchase Intention Study found that 78% of respondents were not confident that the IT organization is fully aware of all the IoT devices connected to the network. The network is a valuable asset in terms of automating IoT endpoint discovery, and it can leverage traffic analysis to monitor user and IoT activity. Any changes in normal behavior can indicate malicious activity or a possible breach.

3. **Can the solution remediate the impact of threats by analyzing traffic flows?** Every organization will have to deal with threats at one point or another, but the impact these threats can have in a small amount of time can cripple a business. Organizations need to look beyond conventional threat detection and analysis. Leveraging data from the network allows organizations to identify the root cause of an infiltration and where it resides to quickly remediate it. The edge can quickly mirror traffic for further inspection if a breach occurs.

4. **Can the solution consistently update information regarding new threats before they are seen on the network?** Having a reactive approach to reducing risk means there is no notification until malicious activity is occurring on the network. Organizations can stay ahead of new threats by constantly learning about them from outside the organization and automatically updating the system to prevent a breach. Network and security professionals need to shift security strategy from being reactive to being proactive to reduce the risk of a breach occurring. If one occurs, tools that collect data and perform analytics can find the malware quickly and automate network changes to minimize the effective blast radius.

Hardware only accounts for about 20% of the total cost of running a network, whereas operational costs constitute 50% or more.

How should the network be managed?

This question is often overlooked by many organizations but is one of the most important to ask. There is a tremendous amount of focus on the cost of network devices, but hardware only accounts for about 20% of the total cost of running a network, whereas operational costs constitute 50% or more.

Historically, networks were managed one device at a time through a command-line interface. The process of making changes across the network was long and laborious. ZK Research studies have shown that the average time to implement a change network wide is four months—far too slow for digital businesses. Also, human error accounts for 35% of network downtime, making it the largest cause of outages. Network management must change in the digital era. Network managers should seek out a solution that offers the following capabilities:

Unified wired and wireless management

Network-wide versus device-centric provisioning

Rich graphical interface so lower-level engineers can make basic configuration changes

Ability to roll back configuration changes if required

Both on-premises and cloud-based management capabilities, giving customers a choice of management models

SECTION IV: CONCLUSION AND RECOMMENDATIONS

Digital trends have raised the value of the network. It should no longer be considered a low-value resource or a "commodity." Instead, the network edge is where users connect to applications and content, making it highly strategic and a point of competitive advantage. IT and business leaders must consider all the activity that happens at the network edge and consider commodity infrastructure versus premium networks from vendors such as Cisco.

Low-cost network devices may seem attractive at first, but over time they will create greater security risk, reduce the organization's ability to monitor and optimize application performance, and have very little ability to automate processes. These are all critical to success in the digital era, so it's imperative that organizations make the right choice at the network edge and use it as the foundation for digital transformation. Consequently, ZK Research makes the following recommendations:

Consider TCO, not acquisition cost, when purchasing network devices. ZK Research data shows that network hardware only accounts for about 20% of the overall cost of running a network, whereas 50% is from operational costs. Saving a few percentage points on hardware could dramatically increase operational issues, driving up overall TCO.

Analyze the network's impact on your business. To properly understand the impact of the network edge, a clear understanding of the organization's planned and unplanned downtime costs is needed. Any downtime or performance issues will cause workers to be less productive and cause customers to go elsewhere. A security breach can cause significant brand damage and lead to potential lawsuits.

Make a future-proof network edge decision. Understand what applications and communications services you are using today and what your company will use in the future (video, IP voice, messaging, mobile, IoT, etc.), and choose the vendor that provides you with the best overall solution. This will establish the foundation on which digital services and applications will be built.

CONTACT

zeus@zkresearch.com
Cell: 301-775-7447
Office: 978-252-5314