RESEARCH
Influence and insight through social media

June 2018

Digital Transformation Success Requires a

SMART NETWORK EDGE

WHITE PAPER

Prepared by
Zeus Kerravala

ZK Research
A Division of
Kerravala Consulting

ABOUT THE AUTHOR

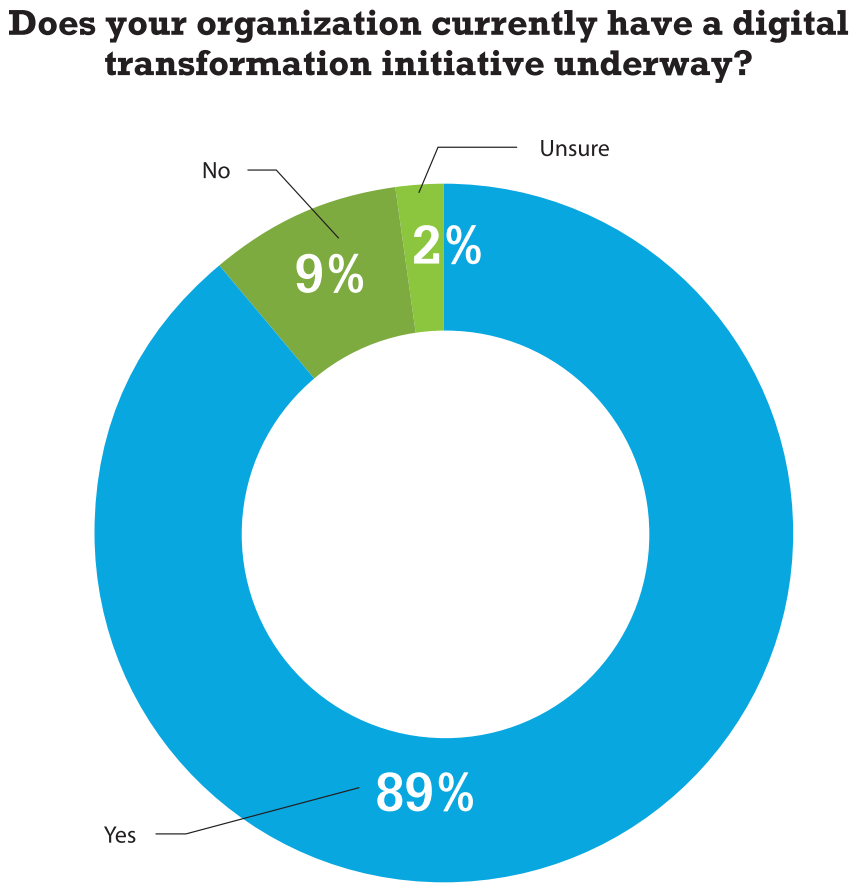
Zeus Kerravala is the founder and principal analyst with ZK Research. Kerravala provides tactical advice and strategic guidance to help his clients in both the current business climate and the long term. He delivers research and insight to the following constituents: end-user IT and network managers;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

INTRODUCTION: THE RISE OF THE NETWORK EDGE

The digital era has arrived and is changing the business landscape faster than ever. This is why digital transformation has become a top mandate for almost every IT and business leader. The ZK Research 2018 IT Priorities Survey found that 89% of businesses currently have digital transformation initiatives underway (Exhibit 1), up from 84% in 2017. In the digital business era, sustaining market leadership is no longer about having the best products, the lowest prices or the best people. Rather, the industry leaders will be determined by an organization's ability to understand market transitions and capitalize on them faster than the competition.

A critical step in the journey to becoming a digital organization is transforming into an agile business. Doing so requires the business's IT infrastructure to be dynamic and able to adapt when required. However, an organization can only be as agile as its least agile IT component, which today is the network—particularly the network edge. The rise of software-defined networks (SDNs) has transformed the data center, and software-defined wide-area networks (SD-WANs) have modernized the WAN, but the edge largely has stood still.

Exhibit 1: Digital Transformation Is Well Underway



ZK Research 2018 IT Priorities Survey

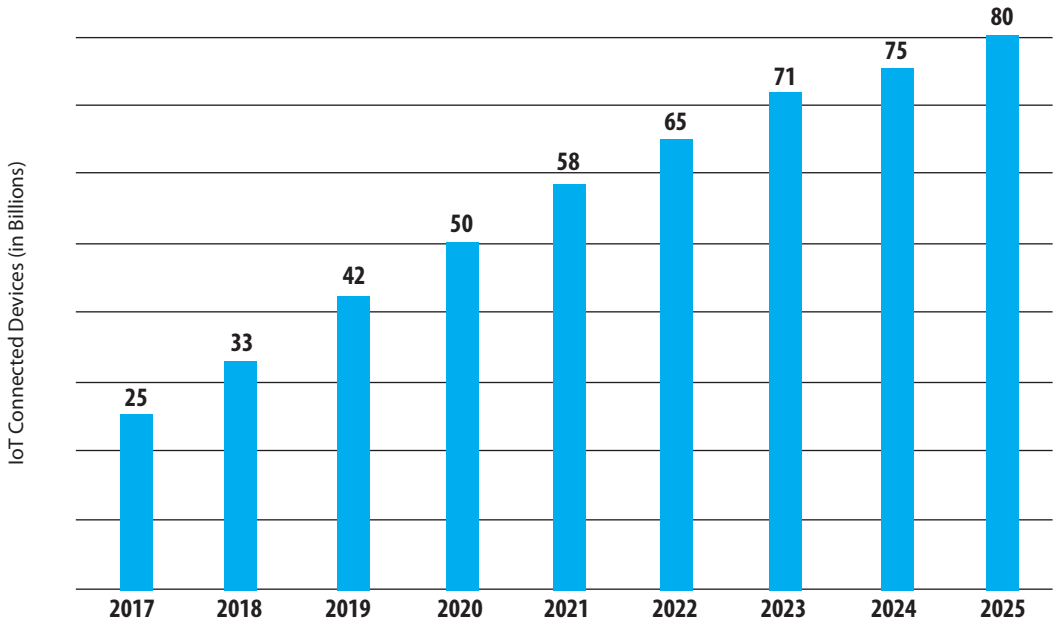
A decade ago, the network edge was considered of low importance. It connected workers' computers to the network, but most content and applications resided on computers. The network was used to periodically fetch new information or to support "best effort" services, such as internet browsing. Today, the network edge has become mission critical, and it has never been more important.

The following are the top five reasons why the network edge has increased in criticality:

Applications are now networked. When applications and data resided on a user's computer, a poorly performing network had no impact on productivity. Today, increasingly more applications are moving to public and private clouds, and the quality of the network has a direct impact on application performance. ZK Research predicts that within three years, 70% of business applications will reside in public or private clouds. This will continue to increase the value of the network edge.

The Internet of Things (IoT) is now mainstream. IoT has moved out of the operational technology (OT) shadows and has become a core component of most businesses' digital transformation strategies. As IoT adoption increases, so will the number of connected endpoints. The ZK Research 2017 IoT Device Forecast predicts that by 2025, there will be 80 billion connected IoT endpoints (Exhibit 2). Almost all of these devices connect at the network edge—therefore, problems at the edge could significantly impair IoT applications.

Exhibit 2: IoT Devices Are Set to Explode



ZK Research 2017 IoT Device Forecast

Businesses and IT leaders must focus on building a smart network edge.

WiFi has become pervasive. In the past, workers had to choose between high-speed wired connectivity or convenient wireless access. The 802.11ac standard for WiFi removed that choice, as WiFi speeds are now at parity with those of wired connections, giving workers the best of both wired and wireless. Also, many mobile and IoT devices are wireless only, meaning they have no wired interface. The combination of these trends has made WiFi now the primary access network, with the edge being the point at which all of these devices connect with the company network.

The use of sensors and beacons has grown. Retailers, entertainment facilities, airports, hospitals and other venues with a significant number of transient individuals have been building mobile applications to provide differentiated services. Bluetooth Low Energy (BLE) beacons and other types of sensors can be used to improve the accuracy of location-based services from 30 feet using WiFi triangulation to less than 3 feet. These connect into the WiFi access point, increasing the importance of the network edge.

Security is shifting to the network edge. Legacy networks had a single ingress/egress point for network traffic. Securing the environment meant putting a massive firewall at that single point and scanning all traffic coming into or leaving the network. Today, mobile devices, IoT endpoints and cloud computing have created many new entry points and shifted them to the network edge. Network security also must shift to the edge to maximize its effectiveness.

As the expression goes, for most businesses, this isn't your father's—or even your older brother's—network edge. Today's network edge should be thought of as the foundation for the digital enterprise, as it's the place users, cloud applications and IoT devices connect to an organization. For most businesses, the network edge *is* the business. The legacy, static and non-differentiated network edge of years past is no longer sufficient. Businesses and IT leaders must focus on building a smart network edge.

SECTION II: CHALLENGES WITH THE LEGACY NETWORK EDGE

The current architecture and operational model for the network edge have been in place for the better part of 30 years. The legacy design was fine when best-effort traffic was the norm and the network had little to do with the user experience. But change is needed in the digital era—or businesses will suffer. For example, a poorly designed network edge can significantly degrade the performance of applications. The ZK Research 2017 Network Purchase Intention Study found that on average, workers are 14% less productive than they could be because of poorly performing applications. Businesses spend billions of dollars on IT projects to improve worker productivity, but a double-digit improvement in productivity could be achieved by ensuring the applications already in use are always performing optimally. The legacy edge is plagued with several issues that if not addressed will hold businesses back and cost them money.

During the past few decades, very little innovation has occurred at the edge outside of gigabit speeds and Power over Ethernet (PoE).

The following are the top issues that hold the network edge back from being a business enabler:

Lack of innovation: During the past few decades, very little innovation has occurred at the edge outside of gigabit speeds and Power over Ethernet (PoE). These advances have increased connection speeds and enabled devices to connect more easily, but very little has been done to address things like operational issues.

Complicated and slow network operations: With legacy edge infrastructure, the management and data-forwarding planes are tightly coupled together. This meant that each switch, access point or other edge device needed to be configured one at a time. Businesses would often need to send network engineers on the road to visit remote locations to configure edge infrastructure in branch offices.

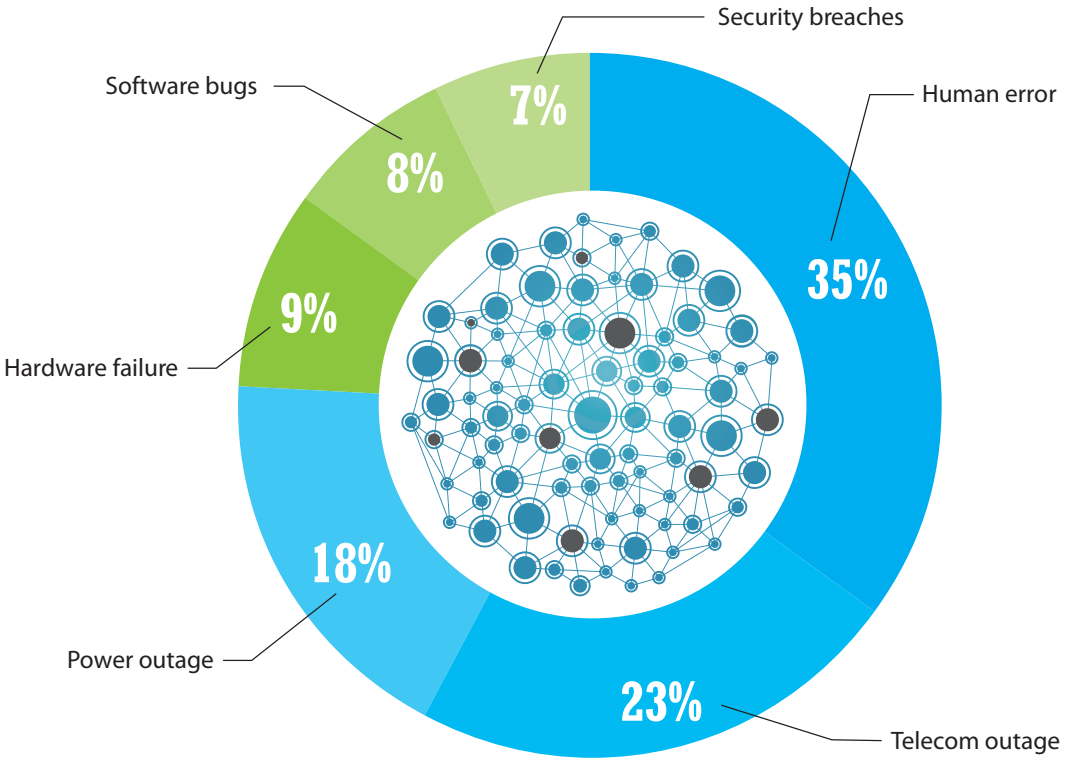
The manual nature of operations causes long lead times for network changes. ZK Research found that the average time for an enterprise to implement a change network wide is four months—far too long for a digital business. Adding to the complexity is the fact that network infrastructure needs to be configured through a cryptic command line interface (CLI) that only high-cost network engineers are proficient in using. In addition, managing a network device through a CLI leads to high amounts of human error. In fact, the ZK Research 2017 Network Purchase Intention Study found that the top cause for unplanned network downtime was human error (Exhibit 3).

Lack of programmability: The current infrastructure in place lacks application programming interfaces (APIs), so the only way applications and networks can interact is through custom scripts. As businesses embrace the concept of DevOps, infrastructure must become programmable to enable it to adapt to the needs of applications.

Poor visibility and analytics: Legacy management was device specific and focused primarily on the state of a particular switch or router. With this model, there was no way to get an end-to-end view of how the network was functioning, making troubleshooting very difficult. Also, the only way to analyze data to improve the network was through manual analysis. This was possible a decade ago, when traffic volumes were low. But networks create orders of magnitude more data today—far too much for even the most experienced engineer to keep up with. The lack of visibility also leads to several "blind spots," such as IoT devices that are primarily deployed by non-IT individuals.

Security challenges: Legacy networks have been secured by placing overlay devices at specific points in the network, such as the demilitarized zone (DMZ). This was effective when all traffic

Exhibit 3: Human Error Is the Leading Cause of Network Downtime



ZK Research 2017 Network Purchase Intention Study

was coming into and out of an organization through a single point. Today, cloud applications, IoT devices, mobile users and other factors have increased the network attack surface by orders of magnitude. One related and compelling data point comes from the ZK Research 2017 Security Survey, which found that 75% of security spend is focused at the traditional perimeter even though only 27% of breaches emanate from that point. It's clear that the entire security model requires a rethink.

SECTION III: INTRODUCING THE SMART NETWORK EDGE

The smart network edge is the single biggest change in networking in decades, as it is an entirely new operational and architectural model. A smart edge is designed specifically for digital businesses. It will bring a level of dynamism never seen before to the network and enable it to have the same level of agility as other areas of IT. Consequently, the network will no longer be the bottleneck that holds organizations back.

A smart network edge is built on the following principles:

Pervasive intelligence: A smart network edge enables greater intelligence across the business. The network is the one resource in every business that reaches every point, sees every

Digital businesses need to move with speed.

device and connects every user. The data it handles can be used to fuel digital transformation efforts, such as personalizing a customer's or worker's experience, or to acquire business insights that can lead to capturing market transitions faster.

Intrinsic security: This type of security is tightly coupled with the network instead of as an overlay. With a smart edge, the network acts as a security platform that can integrate a broad ecosystem of best-of-breed security tools to deliver integrated and automated compliance checks, threat detection and mitigation. Intrinsic security protects a network from the moment a new device is onboarded until its session is terminated.

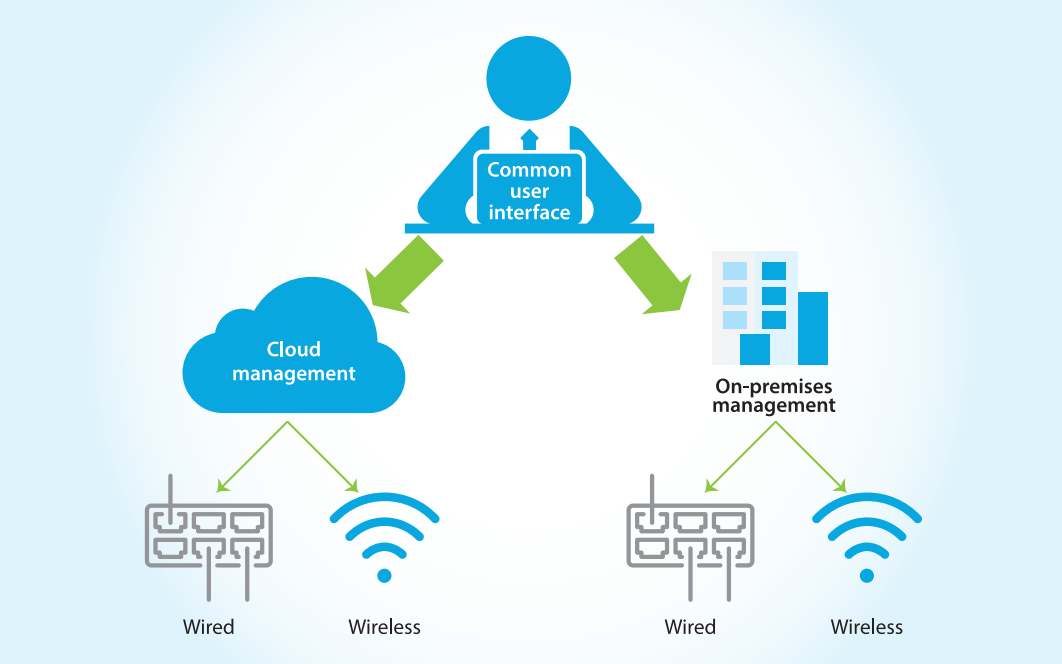
Automation of operations: Digital businesses need to move with speed. Therefore, waiting for network operations to update virtual LAN (VLANs) or access control lists (ACLs) delays innovation. A smart edge automates all of the mundane and repetitive processes that plague network operations today. Although some may view automation as a threat, it should be viewed as a key tool in the network professional's tool kit, as it eliminates human error and frees up valuable time that can be used to drive innovation.

Management options: The separation of the control and data-forwarding planes in network devices has enabled configuration and management to be abstracted away from the hardware and exist purely as software. Network management can now be centralized so an administrator can make a single change and propagate it across the entire network at once. Also, by putting the control functionality in software, it can be centralized and placed in an on-premises controller or located in the cloud.

Common configuration interface and workflows: Vendors often have different configuration tools for different product lines. This can happen when acquisitions are used to fuel innovation or when product teams operate in silos. A smart edge requires a single management tool across all products, regardless of whether the management is handled in the cloud or on premises, or whether the network being configured is wired or wireless (Exhibit 4). This arrangement also ensures that policies are consistent across the wired and wireless networks.

Architectural choice: Historically, network engineers had limited architectural choices when designing the network edge. The typical centralized campus model is still viable; but in many organizations, such as retail and education, a distributed architecture makes more sense. There's no correct decision between centralized and distributed architecture. Network professionals need a choice of architectures to meet the specific needs of their organizations.

Exhibit 4: A Smart Edge Needs Consistent Configuration Interfaces



ZK Research, 2018

Licensing options: Historically, businesses procuring network infrastructure had only one option available, and that was to purchase the equipment up front. This perpetual model has been in place as long as networks have existed. Recently, many organizations have preferred to purchase infrastructure using a subscription model as a way of budgeting more efficiently. Businesses looking to invest in a smart edge should have the choice of procuring the network infrastructure using a traditional perpetual model or a subscription model.

Programmable network: A smart edge should expose APIs that application developers can use to interface with the network. For example, a video application could dynamically reserve bandwidth for the duration of a call and then release it when the call ends. Without APIs, developers would need to use vendor-specific scripts that invoke CLI commands, requiring a deep understanding of that vendor's network commands—something that most application developers do not have. Developers can access the programmable network directly via APIs or via automation by their cloud tools.

Proactive intelligence: Troubleshooting network problems is primarily a reactive process. The majority of problems are reported by workers and not the IT department, meaning network engineers are always in "firefighting" mode. In fact, many engineers spend the majority of their time doing nothing but troubleshooting problems. The ZK Research 2017 WiFi Troubleshooting Survey found that 60% of network engineers spend at least 25% of

Deploying a smart network edge offers several significant business benefits.

their time fixing WiFi problems. A smart edge should continuously analyze network information and proactively report anomalies that can be remedied before they cause problems for workers.

Businesses that adopt a smart edge will realize many IT operations benefits such as faster provisioning time, lower operations cost, less downtime related to human error and proactive management to identify problems before workers are impacted—keeping IT operations out of constant troubleshooting mode. However, deploying a smart network edge also offers several significant business benefits, including the following:

Empowers digital transformation: Legacy networks were never considered strategic assets capable of creating a competitive advantage. A smart edge is an agile fabric that can deliver new services and applications faster, while continuously optimizing service delivery so businesses can stay ahead of their competition.

Enables personalized services: Improving the customer experience is a key tenet of digital transformation. In fact, many research studies have shown that by 2020, businesses will compete on the basis of the customer experience. For digital enterprises to succeed today, they must differentiate themselves through personalized services in order to meet the needs of today's wide range of customers. A smart network edge provides application optimization, mobile services and other technology required to enable the creation of differentiated services.

Ensures budget effectiveness: Every business needs to watch its bottom line. Purchasing network equipment with traditional perpetual pricing creates big spikes in spending every few years when the network needs refreshing. This might be fine for some businesses, but others may need to delay the upgrade—which can put them at a strategic disadvantage. The licensing flexibility of a smart edge enables companies to shift to a subscription model, which creates a more flexible spending model and ensures the business always has the latest features.

Improves security: There isn't a CEO, CFO or CIO who isn't worried about securing his or her organization. The penalties for a breach can include hefty fines, lawsuits and brand damage, and can often cripple a company. A smart network edge is built on the principle of intrinsic security, enabling companies to deploy the right security technology where and when they need it.

SECTION IV: EXTREME NETWORKS—A COMPLETE SMART EDGE SOLUTION PROVIDER

Extreme Networks has been an innovator in networking for well over two decades. In June 2018, the company announced its Smart OmniEdge solution that transforms and modernizes the network

edge. Many vendors, including Extreme, have advanced data center offerings, but Extreme is one of the few that have focused on innovation at the network edge.

Extreme's Smart OmniEdge is a network edge solution that is designed to provide the intelligence, agility and security required for businesses to meet the challenges of digital competition both now and into the foreseeable future. Smart OmniEdge is designed to let enterprises quickly and easily acquire and provision edge services with a choice of consumption models (hardware, software or "as a service") to meet the specific needs of each company. The solution enables businesses to create a consistent, personalized experience across both wired and wireless networks.

Smart OmniEdge is a fundamental change in network operations. Rather than focusing on maintaining the status quo, its management model uses the network to transform the business—leading to sustainable market leadership.

The following are the top five core components of Extreme's Smart OmniEdge solution:

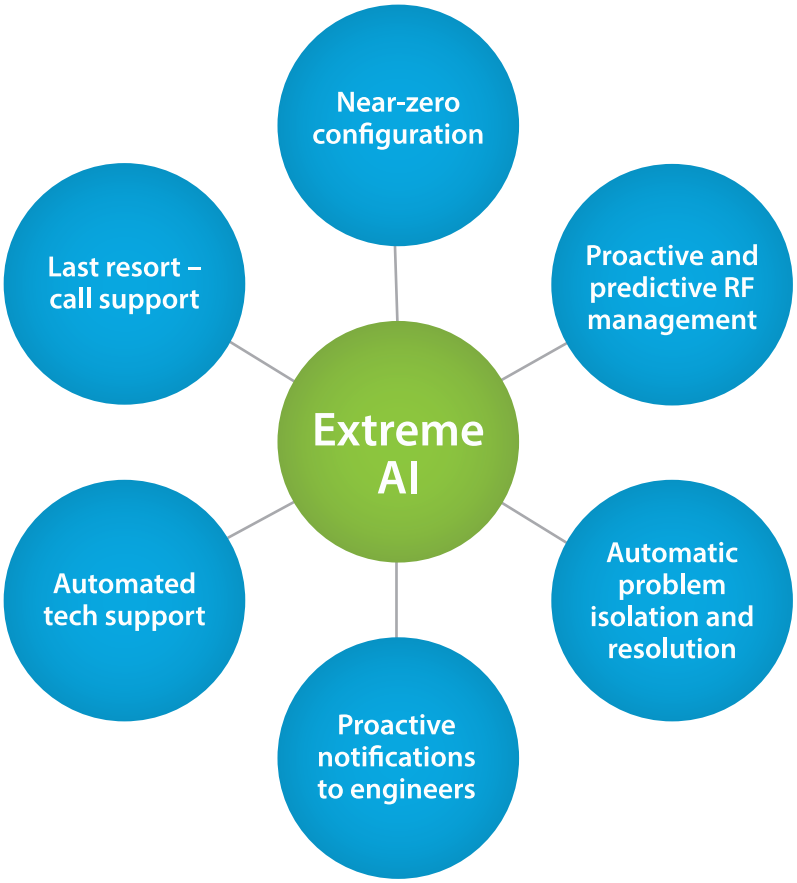
Extreme AI (Exhibit 5) is a machine learning (ML)– and artificial intelligence (AI)–based solution that is used to deliver an enhanced edge experience. Through AL and ML, it facilitates self-optimization and automated correction of the radio frequency (RF) issues from learned history, events, users and devices. The solution also provides a wide range of key performance indicators (KPIs) to validate and ensure performance.

ExtremeCloud Appliance is designed for customers that want to take advantage of the simplicity of the cloud to manage the network edge but want to keep the infrastructure on premises. Extreme's software-as-a-service (SaaS)–based management tool, ExtremeCloud, enables organizations to manage the network via an intuitive portal. The ExtremeCloud

Why use ML and AI for networks, and why now?

Machine learning is an emerging field of computer science that enables machines to "learn" based on the data used as inputs. Artificial intelligence enables computers to analyze the data and make inferences. Historically, in networking, the data collection, analysis and inferences were done by highly skilled engineers. Today, the volume of data, number of conditions and required analytics have grown by orders of magnitude and are too complex for even the most skilled engineer to "connect the dots." Also, humans can only react to problems that are observed in situations where machines can continually run simulations and predict when problems will occur. In particular, RF issues with WiFi are some of the most complex and chaotic that IT encounters. AI and ML can bring order to networking, including RF, enabling applications and IoT devices to perform optimally.

Exhibit 5: Extreme Networks Brings AI and ML to Networking



Extreme Networks and ZK Research, 2018

Appliance gives customers the same capabilities, but the appliance is deployed in the customer's data center. The ExtremeCloud Appliance is available as a physical appliance or as a virtual machine for customers that have their own private cloud infrastructure.

Advanced IoT features: Extreme Smart OmniEdge includes several IoT capabilities enabled by the IoT thread support on the Extreme WiFi access points. These advanced capabilities make it easier to onboard and secure IoT devices. For endpoints with no native networking capabilities, Extreme offers its Defender for IoT and its Defender Adapter that connects devices that were previously unconnectable. The ExtremeCloud Appliance services a centralized IoT controller that manages the security and policies of IoT devices.

The **Extreme Extended Edge Switching** portfolio has been made more intelligent with the addition of the 802.1BR features. Extreme's Extended Edge Switching technology collapses multiple network tiers into a single, logical tier, which increases the intelligence at the edge

while flattening the network and cutting deployment costs. The new architecture leads to a much simpler operational model that costs less to procure and is easier to manage.

Pervasive APIs across the entire networking portfolio connect applications to the network. This enables new business insights to be discovered and customer engagements to be personalized, and it also enables the network to be programmable. In addition, the APIs support third-party applications and services to extend business insights.

Exhibit 6 highlights other key attributes of the Extreme Networks Smart OmniEdge solution that align with ZK Research's discussion of the concept in Section III.

Exhibit 6: The Extreme Networks Smart OmniEdge Solution

Extreme Networks and ZK Research, 2018

SECTION V: CONCLUSION AND RECOMMENDATIONS

The digital era has arrived, and it's here to stay. Today, competitive advantage is based on an organization's ability to be agile, adapt to changes and make rapid shifts to capture market transitions. Several digital-enabling technologies—such as IoT, cloud and mobility—have been introduced into businesses in the past several years, and they are all network centric. If the business is to harness the full potential of these technologies, the network—particularly the access network—must evolve into a smart edge. Shifting to a smart network edge must be at the top of every IT leader's priority list.

To help businesses get started, ZK Research makes the following recommendations:

Focus on transforming the network edge. For most businesses, the edge is where the action is. It's where IoT devices connect and where the cloud interfaces with a business, and it's the source of the data pulled from mobile clients. The inflexible, rigid architecture of the legacy network edge is holding organizations back from becoming digital organizations. Businesses must invest in the network edge to enable a higher level of network agility.

Automate as much as possible. Automation is not the enemy of the network engineer; rather, it should be viewed as a strategic tool that can eliminate many mundane tasks, such as WiFi troubleshooting, that network professionals are burdened with today. Businesses should use AI- and ML-based automation tools to streamline network operations and move to a predictive management model that is self-healing and offers better security.

Evaluate a wide range of vendors for a new network edge. When refreshing the network, it's easy to choose the incumbent or the market leader. However, at moments of market transition, the market leaders are often hesitant to move the industry in a new direction because it disrupts their own businesses. Therefore, companies should evaluate at least three vendors as part of their evaluation process. ZK Research believes that Extreme's Smart OmniEdge aligns closest to the ZK Research definition of this technology and that Smart OmniEdge should be one of the solutions considered by businesses today.

CONTACT

zeus@zkresearch.com

Cell: 301-775-7447

Office: 978-252-5314