RESEARCH
Influence and insight
through social media

March 2020

A Unified Wired and Wireless Access Edge Is

BUSINESS CRITICAL

WHITE PAPER

Prepared by
Zeus Kerravala

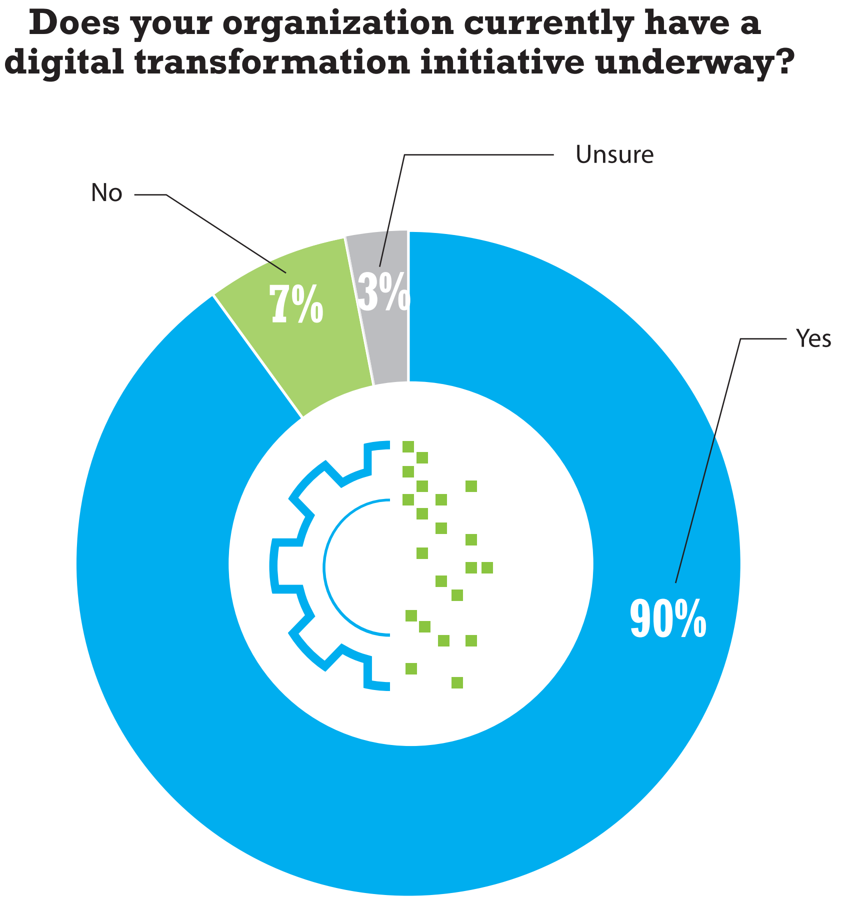
ZK Research
A Division of
Kerravala Consulting

INTRODUCTION: THE ACCESS EDGE IS KEY TO DIGITAL SUCCESS

The digital business era is here, and it's changing the business landscape faster than ever. Businesses that embrace digital transformation are more profitable and quickly become market leaders, while those that don't risk falling behind and becoming irrelevant. This is why digital transformation has become a top mandate for almost every IT and business leader. The ZK Research 2019 IT Priorities Survey found that 90% 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 their ability to understand market transitions and capitalize on them faster than the competition.

Exhibit 1: Digital Transformation Has Reached Near Ubiquity



ZK Research, 2019 IT Priorities Study

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.

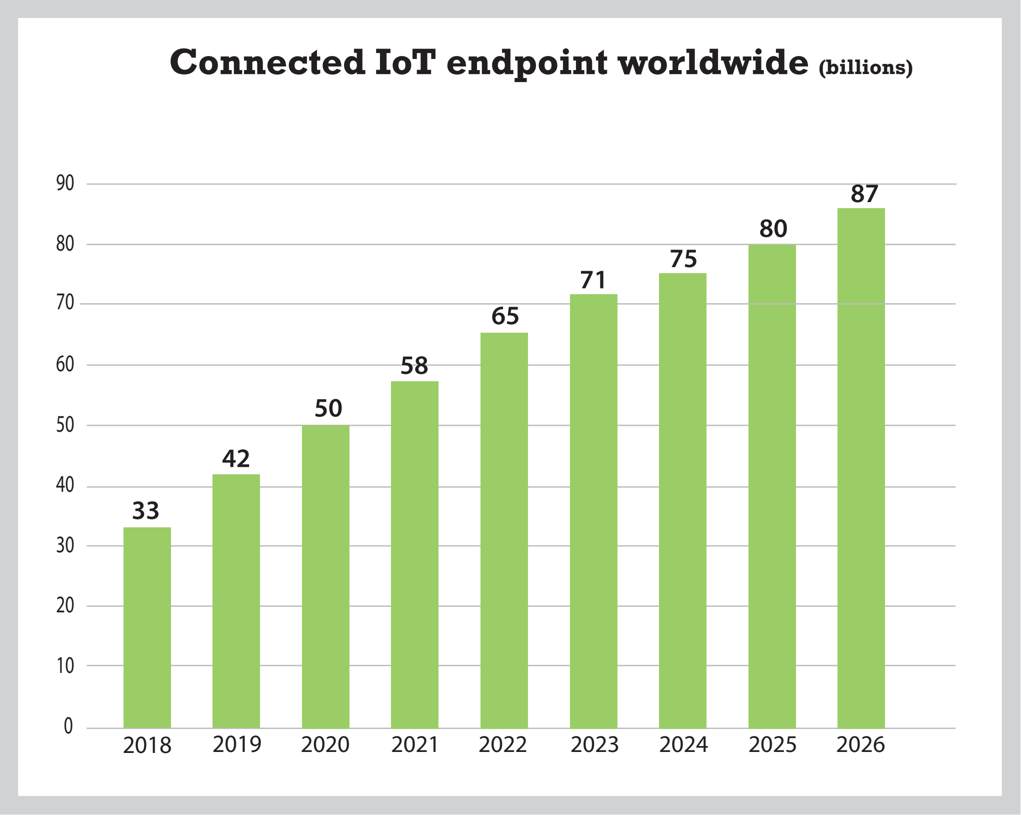
The network edge should now be considered the foundation of a digital business.

A critical step in the journey to becoming a digital business is becoming an agile organization. Doing so requires the IT infrastructure to be dynamic and able to adapt when required. The challenge is that an organization can only be as agile as its least agile IT component, which today is the network—particularly the access edge. Software-defined networks (SDNs) have transformed the data center, and software-defined wide-area networks (SD-WANs) have modernized the WAN, but the access edge remains as it did decades ago.

Historically, the network edge has been considered of low importance. It connected workers' computers, printers and a few other devices to the main network, but most user data and applications resided on computers. The network was used to periodically fetch new information or to support "best effort" services, such as email. In this scenario, the access edge played a role of base connectivity and was considered to be of low value. Today, the role of the access edge is completely different and should be considered mission critical. These are the top factors driving up the value of the access edge:

- **Almost all applications are networked.** When applications and data resided on a user's workstation, a poorly performing network had no impact on productivity. Today, increasingly more applications have moved to the data center, into a private cloud, out to a public cloud and to other places. This means the quality and reliability of the network edge have a direct impact on application performance. ZK Research predicts that within three years, 74% of business applications will reside in public or private clouds, further increasing the value of the network edge.
- **The Internet of Things (IoT) is now mainstream.** IoT has moved out of the operational technology (OT) shadows of a handful of verticals and has become a core component of most businesses' digital transformation strategies across all industries. As IoT adoption increases, so will the number of connected endpoints. The ZK Research 2019 IoT Device Forecast predicts that by 2026, there will be 87 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.
- **WiFi has become pervasive.** In the past, workers had to choose between high-speed wired connectivity or the convenience of WiFi. The Wi-Fi 5 and Wi-Fi 6 standards removed that decision, 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. Many businesses have expanded the scope of WiFi from the carpeted offices to everywhere including lobbies, cafeterias, outdoor locations and every other place the organization spans. 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

Exhibit 2: The Growth of IoT Connected Endpoints



ZK Research 2019 IoT Device Forecast

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 access 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 access edge. Network security also must shift to the edge to maximize its effectiveness.

Digital transformation has escalated the value of the access edge, as it's the first point of connection of users, applications, the cloud and IoT endpoints. The network edge should now be considered the foundation of a digital business. In fact, one could argue that for most companies, the access edge is the business. The legacy, static and non-differentiated access edge of years past is no longer sufficient. Businesses and IT leaders must focus on building an intelligent access edge, and doing so requires unification of the wired and wireless networks.

SECTION II: CHALLENGES WITH THE LEGACY ACCESS EDGE

The current architecture and operational models for the access edge have been in place for more than three decades. This design was sufficient when best-effort traffic and "good enough" were the norm and the network had little to do with application performance. Today, that's not the case, as the network has a direct impact on the performance and availability of applications—which, in turn, have a direct impact on worker productivity.

A poorly performing network leads to less productive workers. ZK Research quantified just how much less productive in its 2019 Network Purchase Intention Study, which found that workers are 16% less productive than they could be because of poorly performing applications. IT and business leaders should consider this factor—as organizations spend millions of dollars annually 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.

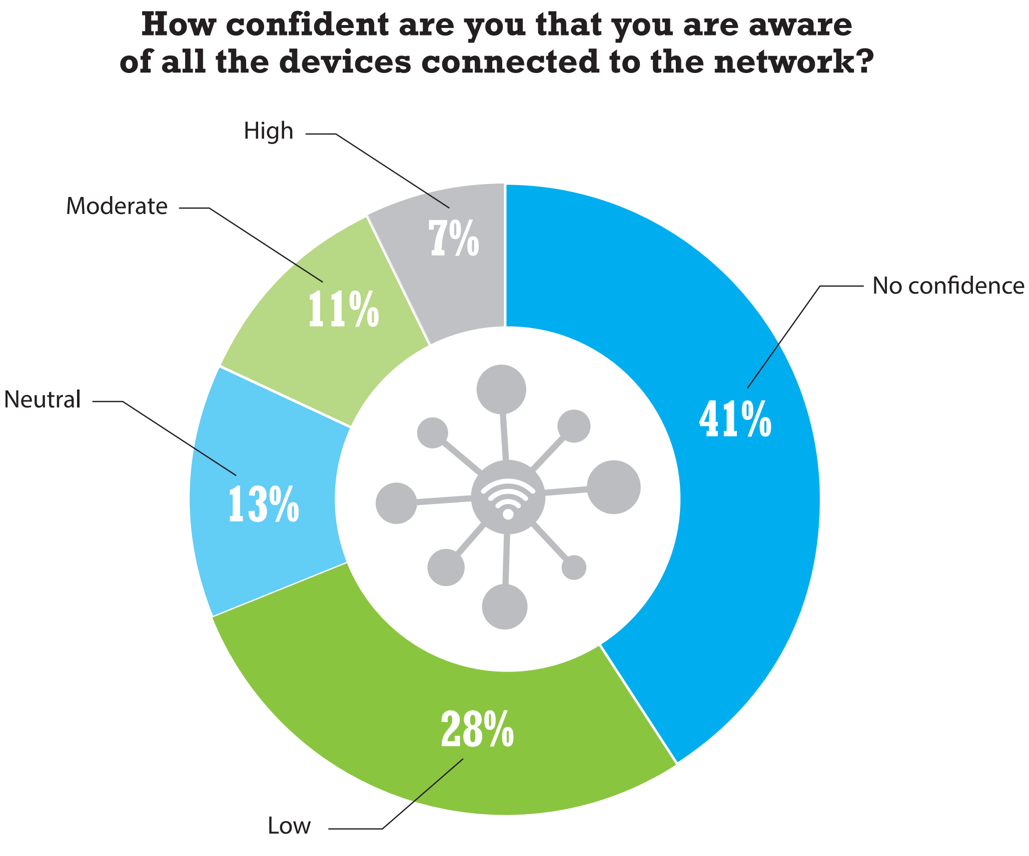
The legacy access edge is plagued with several issues that if not addressed will hold businesses back and costthem money.

The legacy access edge is plagued with several issues that if not addressed will hold businesses back and cost them money. These are the top issues that inhibit the access edge from becoming a digital enabler:

- **Lack of innovation:** Over the past 30 years, there has been very little innovation at the access edge. There have been advancements in speed and the introduction of Power over Ethernet (PoE) but nothing that transformed the operational model of the access edge.
- **Non-programmable infrastructure:** Traditional network infrastructure lacks programmable application programming interfaces (APIs), so the only way applications can interface with the networks is through custom scripts or the infusion of command line interface (CLI) commands. Application deployments and challenges need to be coordinated with network changes. Programmable infrastructure enables greater orchestration.
- **No automation capabilities:** With legacy edge infrastructure, network switches, access points or other edge devices were designed to be configured manually, one device at a time. Even simple changes could take a very long time to implement. The ZK Research 2019 Network Purchase Intention Study found that it takes companies an average of 110 days to implement a change network wide, which is far too slow for the digital era. Better automation capabilities can offload many of the mundane and repetitive tasks associated with running a network.
- **Independent security for wired and wireless networks:** In legacy networks, the wired and wireless networks are secured independently. This can create some significant security problems, as it's difficult to keep policies aligned across the two networks. In many businesses, the wireless network is locked down so non-credentialed individuals cannot access it. However, the wired network hasn't been secured, meaning anyone can unplug an Ethernet cable from the back of an IP phone and have network-wide access.
- **Inadequate visibility:** Traditional management was device specific and focused primarily on the state of an individual device. With this model, there is no way to get an

end-to-end view of how the network is functioning, making understanding application performance very difficult. Also, network management tools used data sources that were sampled roughly every 30 seconds instead of in real time. This was sufficient to study long-term trends, but the gaps in data left significant blind spots. Another issue with a lack of visibility is that it's difficult to understand what devices are connected to the network. Years ago, IT owned every device connected to the company network. With the rise of bring your own device (BYOD) and IoT, many IT pros struggle to understand what's connected. In the ZK Research 2019 Network Purchase Intention Study, 69% of respondents had no or little confidence about all the devices on the network (Exhibit 3). There's an axiom in IT circles that states, "You can't manage or secure what you can't see." Therefore, understanding what's connected is crucial to managing ongoing operations.

Exhibit 3: A Lack of Visibility Plagues Businesses



ZK Research 2018 Network Purchase Intention Study

- **Unreliability of WiFi:** For most businesses, the WiFi network is mission critical. This is problematic, as WiFi has historically been unreliable at best. It's common for connections to drop, networks to get saturated and applications to perform poorly when used over WiFi. This frustrates users and hurts both the bottom line and the top line. Also, in the digital era, many companies are mining customer data from the WiFi network, such as social information, or providing location-based services; therefore, unreliable WiFi could drive customers away. The technology available is great, but the problem lies in poor design and planning—partially due to a lack of awareness regarding how WiFi is being used. WiFi is also notoriously difficult to troubleshoot because many of the issues are intermittent. In fact, the ZK Research 2019 WiFi Troubleshooting Survey found that about 22% of all engineers spend at least one day a week doing nothing but WiFi troubleshooting.
- **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 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 2019 Security Survey, which found that 71% of security spend is focused at the traditional perimeter even though only 29% of breaches emanate from that point. It's clear that the entire security model requires a rethink and that security needs to be applied at the access edge first.
- **Lack of agility:** The infrastructure used to power the access edge is hardware centric, making it very rigid. In most cases, there is very little in the way of options as to how the equipment is deployed or how it's managed. Legacy infrastructure has not benefited from software innovation or the cloud. This lack of agility makes it very difficult for network professionals to keep up with the rapid changes in the area of application development.

The access edge has grown in importance and is now mission critical. The legacy access edge is too rigid, slow and insecure for digital businesses. Sticking with the status quo will certainly put businesses at risk. Therefore, transforming the access edge to a software-centric model with unified management needs to be a top priority for IT and business leaders.

Transforming the access edge to a software-centric model with unified management needs to be a top priority for IT and business leaders.

SECTION III: DEFINING THE NEW ACCESS EDGE

The evolution of the access edge is the single biggest change in networking in decades, as it is an entirely new operational and architectural model. An access edge is designed specifically for digital businesses and will bring a level of dynamism never seen before to the edge as well as 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.

Unified access requires automating all of the mundane and repetitive processes that plague network operations today.

Key criteria for the new access edge include the following:

- **Unified management of wired and wireless:** Businesses need to stop thinking of the wired and wireless networks as distinct entities. Instead, there should be a single access edge with policies that can be pushed across the network. This will ensure consistent performance and security across the unified edge.
- **Software-centric solution:** Digital businesses need to be agile, and legacy, hardware-centric infrastructure is very rigid and brittle. Software-based solutions enable companies to centralize control, automate management tasks and use APIs to interface with applications. Lastly, software-based solutions can be run on an appliance, in a virtual machine or in the cloud for maximum flexibility.
- **Segmentation everywhere:** One of the easiest ways to limit the damage from breaches is to separate critical assets. This is done through network segmentation, which is similar to virtual LANs (VLANs) but offers greater agility. Today's highly dynamic edge requires a segmentation solution that spans the entire network—from the campus core to the edge, including IoT devices.
- **Integrated threat defense:** Security needs to be tightly coupled with the network instead of deployed as an overlay. The network should act as a security platform that can integrate a broad ecosystem of security tools to deliver integrated and automated compliance checks, threat detection and mitigation. Integrated security protects a network from the moment a new device is onboarded until its session is terminated. It's critical that the security be consistent across the wired and wireless networks. It's also important that the solutions be trustworthy, which requires a process to ensure the hardware and software are from a legitimate vendor.
- **Automatable network:** Digital businesses need to move with speed. Therefore, waiting for network operations to update VLANs or access control lists (ACLs) delays innovation. Unified access requires automating all of the mundane and repetitive processes that plague network operations today. Although some may view automation as a threat, it should instead 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.
- **Single pane of glass management:** Network operations functions on the concept of "swivel chair management," where an engineer sits in the middle of multiple consoles and tries to correlate the data manually. Effectively managing a unified access edge requires a single management console where the network administrator can see everything but also execute configuration changes and updates.
- **Standards-based solution:** Many endpoints interoperate with the network and the access edge. A standards-based solution ensures maximum flexibility and interoperability with a broad ecosystem.
- **Machine learning (ML)–based intelligence:** Troubleshooting network problems is

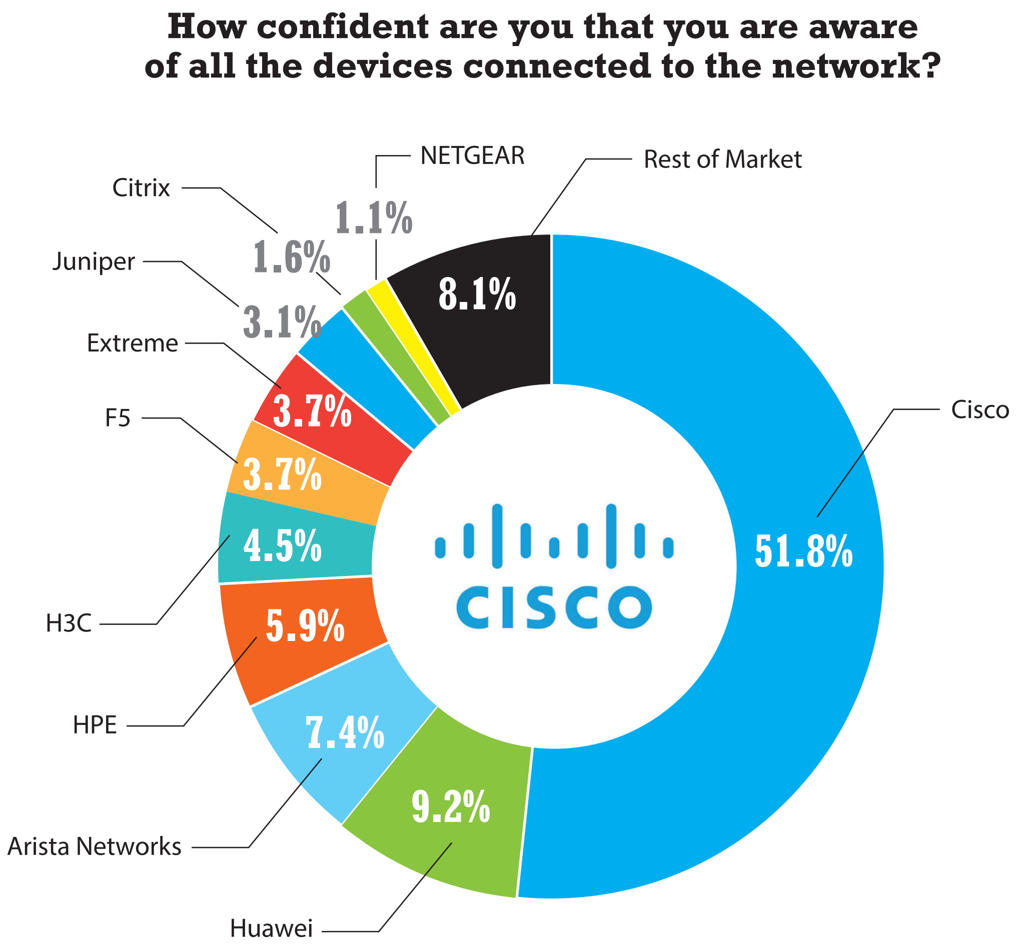
primarily a reactive process. The majority of problems are reported by workers and not the IT department, meaning network engineers are always in "firefighting" mode. In fact, many engineers spend the majority of their time doing nothing but troubleshooting problems. A modernized solution should use machine learning to continually analyze network information and proactively report anomalies that can be remedied before they cause problems for workers.

- **Intent-based networking (IBN):** IBN is a completely new paradigm in networking where the network develops autonomous capabilities. It uses a closed-loop model in which the network continually analyzes the end-to-end state to ensure the business intent is always being met.

SECTION IV: CISCO CATALYST 9000 FAMILY TRANSFORMS THE ACCESS EDGE

San Jose–based Cisco has been the market leader in networking for decades. According to Synergy Research Group, Cisco currently holds a little over 52% share in Ethernet switching (Exhibit 4), giving

Exhibit 4: Cisco Catalyst 9000 Family Transforms the Access Edge



Synergy Research Group and ZK Research, 2019 it deep experience in the changing dynamics of the access edge.

Recently, Cisco upgraded its widely deployed Catalyst line of access switches and added new line of Catalyst Access Points and Wireless Controllers. The new Catalyst 9000 family delivers on the vision of intent-based networking with some advanced features today, but it also provides a path to a fully autonomous network in the future. The series includes the following products:

- **Catalyst 9100:** High capacity WiFi6 access points (APS) with a form factor for companies of all sizes
- **Catalyst 9200:** Stackable form factor designed for branch offices and small to medium businesses
- **Catalyst 9300:** Stackable form factor fixed for branches and mid-size to large campuses
- **Catalyst 9400, 9500 and 9600:** Fixed and modular campus core and distribution
- **Catalyst 9800 Wireless LAN Controller (WLC):** Highly reliable and secure controller for Catalyst 9100 APs. Supports flexible deployment models, including the clould.
- **Catalyst Embedded Wireless Controller (EWC):** An embedded controller on Catalyst Access Points that makes it fast and easy to deploy WiFi without the need for a physical controller
- **Catalyst 90 Watt UPoE+:** Extends the IEE Power over Ethernet plus (PoE+) standard to double the power at 90w enabling a broader range of devices to be powered via an Ethernet cable available on the entire Catalyst 9000 series switches.

Product highlights include the following:

- All of the Catalyst products run Cisco's latest operating system, Cisco IOS XE, on its programmable unified access data plane application-specific integrated circuit (UADP ASIC). This chip was specifically designed by Cisco to meet the demands of a unified access edge. Cisco IOS XE is an open and programmable network operating system that has become an industry de facto standard.
- The products offer flexibility of management, as they can be managed through the Cisco DNA Center single pane of management tool, the local web user interface (UI) or the traditional command line interface.
- Always-on capabilities are provided via stacking and stateful switchover, along with cold patching for minimal downtime and PoE when rebooting.
- Integrated threat defense capabilities include the following:

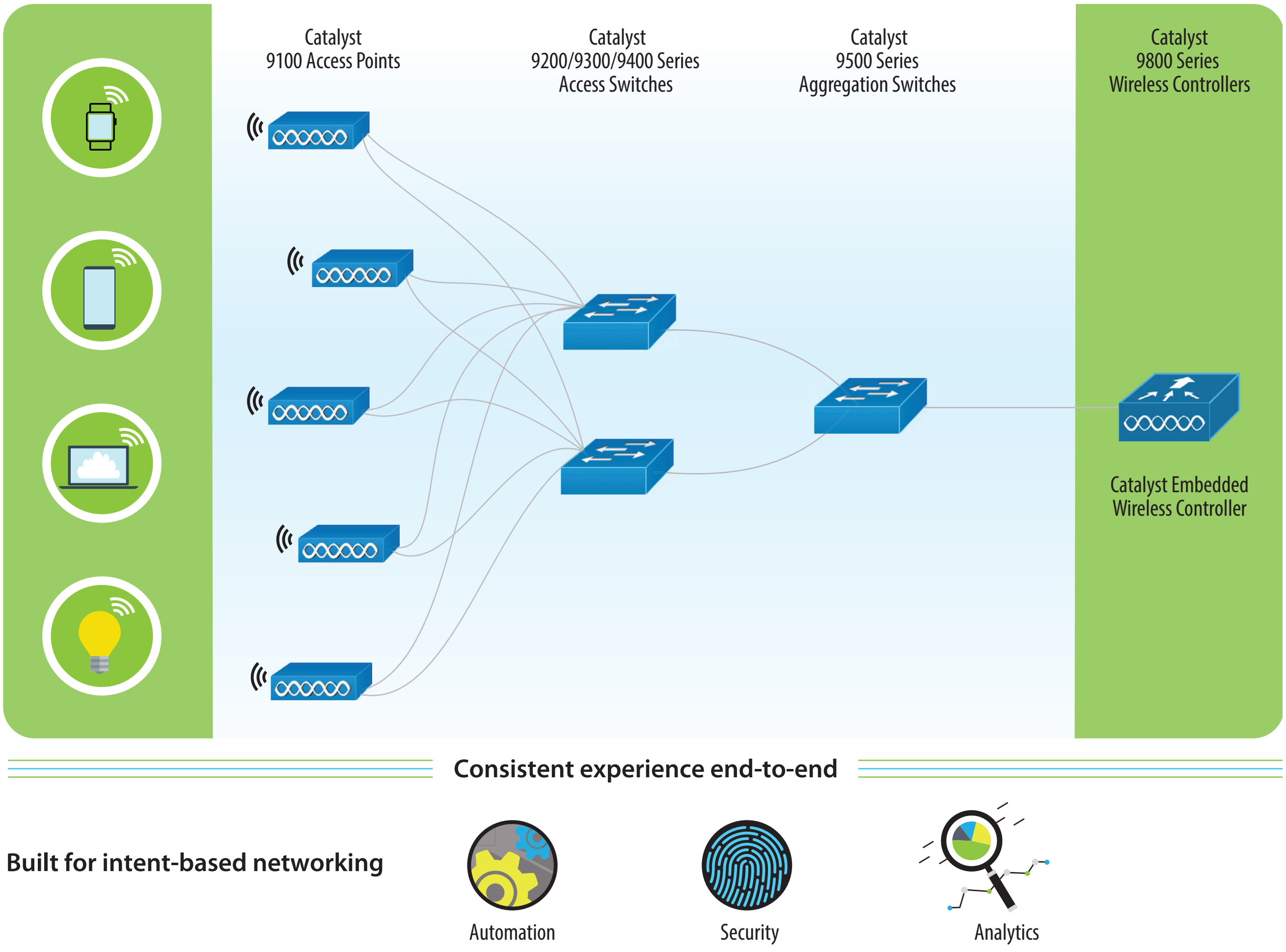
  > Policy-based micro and macro segmentation
  > Software-defined access
  > MACsec link encryption
  > Anomaly detection using Flexible NetFlow
  > Trustworthy solutions

- The Catalyst products offer application recognition (500+ apps) and assurance.

- The products are IoT-ready solutions offering the following capabilities:
  > Uninterrupted fast PoE, PoE+ and Universal POE+ (UPOE+)
  > IEEE 1588 Audio Video Bridging
  > Support for IoT-specific protocols

The family also includes the Catalyst 9800 wireless controller, which is Cisco's first controller to be powered by the same Cisco IOS XE operating system as in the Ethernet switches. The benefit of this is that it provides a consistent, end-to-end experience from the wireless edge to the campus core (Exhibit 5).

Exhibit 5: Digital Transformation Requires a Unified Access Edge



Cisco and ZK Research, 2020

Shifting to a unified access network needs to be top of mind for CIOs today, as it is the foundation for digital transformation.

As the demands on WiFi have grown, so has the need to raise the bar on what enterprise-class WiFi is. To accomplish this, Cisco designed the Catalyst 9800 controller with the following three tenets in mind:

- **Always on to eliminate downtime:** The controller can do software updates without having to be turned off or rebooted, which eliminates planned downtime. Also, access points (APs) can be upgraded or added without having to restart the system.
- **Secure solution:** Cisco recently announced a feature called Encrypted Traffic Analytics (ETA) that can find malware in encrypted traffic. This feature is now available on the WiFi network via the Catalyst 9800 controller. Also, micro and macro segmentation has been automated to keep wireless assets separated.
- **Deployment flexibility:** Businesses are constantly changing, and customers need choice and flexibility. The Catalyst 9800 controller offers that, as it can be deployed on premises, in a private cloud, in a public cloud service such as Amazon Web Services or embedded in a Cisco Ethernet switch. Whatever the customer preference, Cisco can support it.

The Catalyst 9800 Controller is also highly scalable and can support up to 6,000 APs so that customers can start with a small deployment but then scale as required.

Customers that choose to leverage the new Catalyst 9000 family will realize several business and technical benefits, including the following:

- **Simplification of security policies:** Security policies can be created once and pushed across the wired and wireless networks.
- **Policy extension to the data center:** Through the use of Cisco's ACI controller, security policies can be extended to the data center for "core to hand" protection.
- **Segmentation of the network everywhere:** Businesses can leverage both micro and macro segmentation across the entire network, including the data center, by utilizing ACI.
- **Faster operations across the wired and wireless network through automation** ensure an optimal application experience.
- **Single pane of glass management across wired and wireless with DNA Center** ensures there are no management or security blind spots.
- **Platform for IoT:** Any type of IoT device can be connected and secured, regardless of protocol.
- **Automation and assurance** will result in reduced operational time and faster issue remediation time. In addition, the lower amount of downtime will have a direct impact on improving the productivity of the IT department and workers.
- **Programmable network** allows for integration into systems and enables new features and functions to be quickly added after deployment.
- **Path to intent-based networking:** Cisco delivers many IBN features today such as automated segmentation, ETA and automated operations. Over the next several years,

Cisco will deliver more intelligence with the end goal of enabling customers to shift to a fully autonomous network when they are ready.

SECTION V: CONCLUSION AND RECOMMENDATIONS

The digital transformation era is here, and businesses need to adapt to survive. Today, competitive advantage is based on a company's ability to be agile, adapt to changes and make rapid shifts to capture market transitions. Most of the digital-enabling technologies—such as IoT, cloud and mobility—are network centric, which raises the value of the network, particularly the access edge. If the business is to harness the full potential of these technologies, the access edge must evolve, with the first step being implementing a unified edge. Shifting to a unified access network needs to be top of mind for CIOs today, as it is the foundation for digital transformation.

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

- **Focus on first evolving the access edge.** For most businesses, the edge is where both the action and the complexity are. 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 first invest in a unified access network to enable a higher level of network agility; it's important to note that the rest of the network will need to be upgraded after. The Wi-Fi 5 and 6 standards will have a cascading effect where a campus core refresh and possibly a data center refresh will be needed, but the edge is the starting point.
- **Ruthlessly automate network processes.** 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 artificial intelligence (AI)– and machine learning–based automation tools to streamline network operations and move to a predictive management model that is self-healing and offers better security. The more automation that is in place, the more IT can focus on strategic initiatives.
- **Plot a course to an intent-based network.** Automation is the first step in network transformation but not the end goal. IT leaders should focus on evolving toward an intent-based network in which security and management policies are constantly being checked to ensure the goals of the business are being met. Start modestly with high-impact features, such as Cisco's ETA, that can deliver value today, and then use that as a springboard to a broader IBN deployment.

CONTACT

zeus@zkresearch.com

Cell: 301-775-7447

Office: 978-252-5314