White Paper

The Intelligent Edge Era Requires a Secure, Scalable, and Automated Enterprise Network

Sponsored by: Aruba, an HPE Company

Brandon Butler
May 2020

THE RISE OF THE INTELLIGENT EDGE

Enterprise IT is entering a new frontier: the era of the intelligent edge. The intelligent edge is where people, devices, and things connect to the digital world. In the intelligent edge era, data is processed close to where it is generated to ensure real-time analysis drives new business outcomes. The emergence of the intelligent edge era is being driven by a handful of factors. First, the amount of data generated in the world continues to expand exponentially. In the coming years, the amount of global data created by connected Internet of Things (IoT) devices will be in the scores of zettabytes (ZB). There has been a fundamental realization among enterprises that data of all types can be leveraged to improve internal operations, weather economic downturns, enhance customer experiences (CXs), and expand business opportunities. Data doesn't reside solely in centralized datacenters though, it is being created, and must be processed in real time, at the edge. Enterprises have significant opportunity to benefit from the intelligent edge, but there is one central, key component that enables this new era: the network.

Key Statistics

- By 2023, over 50% of new enterprise IT infrastructure deployed will be at the edge rather than corporate datacenters, up from less than 10% today
- By 2024, the number of apps at the edge will increase 800% above 2019 levels
- By 2025, there will be 41.6 billion connected IoT devices generating 79.4ZB of data

The opportunity to leverage the intelligent edge has led organizations across the globe to reassess their network constructs. Enterprise networks are being re-architected from a datacenter-focused hub-and-spoke model to a distributed design that embraces the edge and the cloud.

Today, internal and external data is created from a dizzying array of connected devices. Enterprises are building new analytics models to gain value from their enterprise data, leading to new performance metrics upon which businesses operate. Compute resources are being distributed, extending from public cloud resources to the edge of the enterprise network.

To gain value from the intelligent edge, data and processing capabilities from the edge must be connected to both the cloud and the rest of the enterprise. This requirement makes the enterprise network a critical component of the intelligent edge era. The network must be optimized for the

intelligent edge; it must be secure, scalable, and automated. Organizations that embrace a modern network to support the intelligent edge will be the winners in this data-driven era.

Data as the New Currency for Digital Business

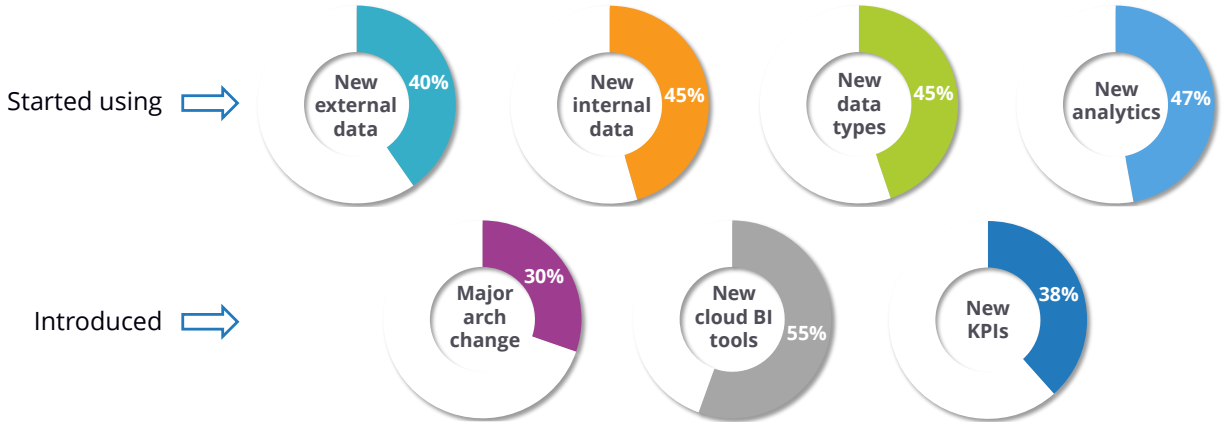
Businesses around the globe are being disrupted by digital-native and digital-savvy companies. In response, organizations are looking to digitally transform themselves to keep pace with competition, win new business, and provide high-quality digital customer experiences. Data has become the new currency for digitally transforming businesses.

A recent IDC study of 310 large and midsize enterprises in the United States found a significant portion of the participants beginning to use data to influence business operations (see Figure 1). The survey found that 40% of enterprises were using new external data sources, while another 45% have begun using new internal data sources. This has led to 38% of companies creating new key performance indicators (KPIs) within their business and 55% of organizations reporting the use of new cloud-based business intelligence tools. The data assets that enterprises are increasingly relying on for their business operations are more detailed, more diverse, and spread out across more locations.

FIGURE 1

Data and Analytics Changing How Enterprises Operate

Q. In the past 12-18 months has your organization done any of the following?



n = 310

Note: For more information, see *Agility Needed More than Ever to Respond to Ongoing Data and Analytics Changes* (IDC #US46105220, March 2020).

Source: IDC's *Business Intelligence End User Survey,* February 2020

Gaining insights and taking action from the troves of internal and external data have become a key priority for savvy businesses. Enterprises are realizing that business intelligence data can be used to improve operations, provide high-quality customer experiences, and increase revenues. Data on the current and past operations of the business can help predict and plan for future events, improving operations to keep the business functioning in the face of significant economic challenges. From a customer experience perspective, this ensures businesses have the right resources ready to deliver to customers at the right time and place. Taken together, intelligence plus customer focus leads to

increased business opportunities and revenues for enterprises. The challenge is having a platform that can enable the efficient and secure transfer of that data from where it is generated and collected to where it will be processed.

Challenges of Existing Platforms and Processes

Enterprises are experiencing a number of challenges as they attempt to fully leverage data available to them. This is natural because the realization of how powerful data can be has just recently become clear. Now, enterprises are feverishly updating their platforms and processes to ensure they can benefit from the intelligent edge era. Some challenges enterprises face are:

- Existing systems have been built on a legacy model of datacenter-focused networks. The rise and mainstream adoption of cloud services, edge data sources, and IoT device proliferation require a new architecture that enables an efficient and secure connection between the source of data generation and processing.
- Manual, reactive, ad hoc, and/or siloed management of these systems in a distributed environment is untenable given the volume, velocity, and variety of data being processed. Organizations can no longer rely on fixing issues when they become broken: they must be able to predict when systems will fail to prevent any impact to customers, users, or the business.
- The pervasive network administration culture is conservative, which inhibits adoption of innovations such as machine learning (ML) and artificial intelligence (AI); these enhanced automation tools benefit organizations greatly in recognizing trends, identifying issues, and making changes quickly.
- Security must evolve in this new paradigm as well. Having perimeter-based security policies does not work in a highly distributed system. Security should be based on a zero-trust system that enforces security dynamically at the per-user and per-device level, at all points of the network.

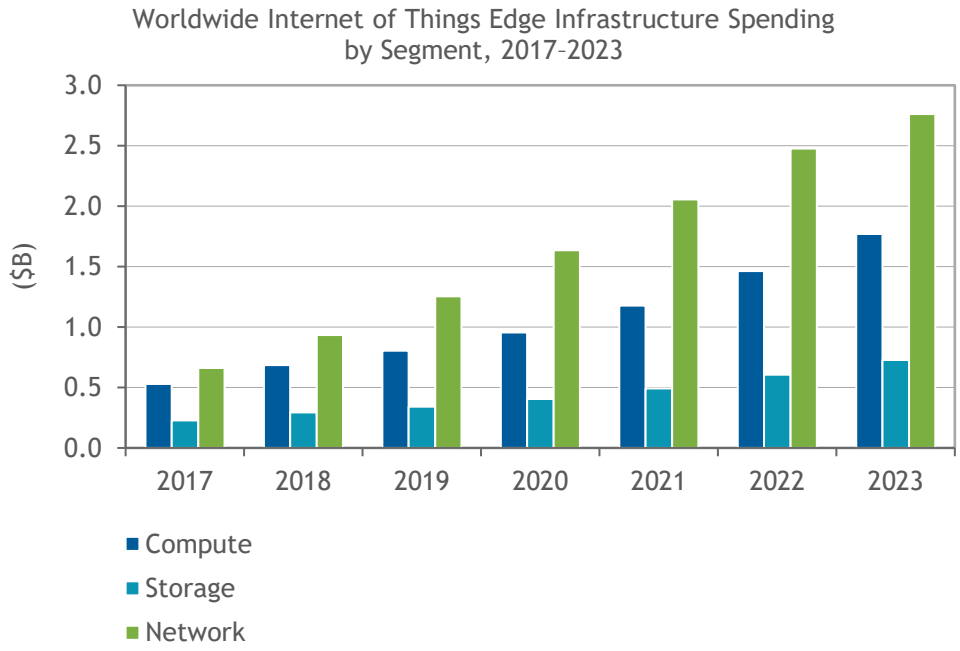
The Importance of the Network in Accessing the Intelligent Edge

As enterprises look to overcome the aforementioned challenges, they will seek new platforms and processes that allow for the secure and efficient collection and processing of data from the edge of their networks. In this new era, the network becomes a critical layer for connectivity, bringing data from the edge to where it needs to be stored, processed, analyzed, and acted upon. This requires a strong and robust network connection and unified infrastructure across all domains of the network. In the coming years, network spending is set to make up the largest share of worldwide Internet of Things infrastructure spending compared with compute and storage (see Figure 2).

The volume, velocity, and variety of data being created will require organizations to graduate from manual, reactive, and siloed processes for managing network connections and data flows and evolve into relying on ML/AI-powered platforms that automatically establish, scale, and secure connections and manage the infrastructure.

FIGURE 2

Network Spending Makes Up Largest Share of Intelligent Edge Infrastructure Spending



Note: See *Worldwide Internet of Things Infrastructure Forecast, 2019-2023: IoT Edge Growth Spurred by Stronger Expectation of Efficiency and Cost Reduction Benefits* (IDC #US45371818, July 2019).

Source: IDC, 2019

KEY TENETS OF AN INTELLIGENT EDGE PLATFORM

The intelligent edge represents a tremendous business opportunity for enterprises. To efficiently and securely access, manage, and leverage data from the intelligent edge requires a new platform. There are a handful of key tenets that are required of this platform.

Artificial Intelligence-Enhanced Operations

One of the most significant advancements in the past handful of years has been the advent and maturation of machine learning and artificial intelligence platforms to aid in data analysis. This megatrend has far-ranging impacts across multiple areas of the economy. Within networking, one of the most promising implementations of ML and AI technology is enhancing management platforms to improve operations. ML/AI algorithms integrated with advanced management platforms yield a range of benefits, including:

- ML- and AI-enhanced network management platforms can nonintrusively learn what normal and abnormal behaviors are in a network. Abnormal activity is a harbinger for either a security event or a performance degradation. ML and AI platforms can alert administrators to events before any harmful action can be taken by nefarious actors, before any users notice a

performance degradation issue, and perhaps, most importantly, before any business operations are negatively impacted.

- The key to successfully mitigating issues is to quickly identify the root cause and execute proven steps to remediate the issue. Management platforms enhanced with ML and AI can be programmed to keep a historical record of normal network operations, so when an abnormality is observed, the ML/AI platform is able to quickly identify the issue and work to reset the network to normal operations, before any issue impacts the business.
- AI-enhanced operations can help validate changes to networking equipment before they're implemented to ensure performance is not degraded. By crowdsourcing anonymized network operations data, organizations can optimize their networks based on results from operations of peer organizations.
- Automated management and response to network issues is a requirement of the new era of the intelligent edge. Relying on manual processes to monitor, analyze, remediate, and validate security or performance issues is not just inefficient – it is unsustainable and is an insecure way to run a network. Given the massive increases in the number of devices and amount of data at the intelligent edge, automated management, enhanced by ML and AI, is quickly moving from a nice-to-have to a must-have requirement of enterprise networks.

Unified Infrastructure

Having AI-enhanced operations is just one piece of the puzzle. To get the full value from advanced management, the management plane must extend across all areas of the enterprise network, from the datacenter to the enterprise campus to remote worker locations and branch offices, out to IoT edge locations and into the cloud. A centralized management console is needed to unify infrastructure across the various domains of the network. Important qualities of a centralized dashboard include:

- Ability to provide a single pane of glass management and unified views of operations and performance across all domains of the enterprise network
- A cloud-managed system built using modern-day web-scale best practices that provides centralized visibility and management (A key advantage of cloud-managed platforms is that enterprises do not need to devote on-premises resources to run the management system, organizations get faster access to new features and enhancements, and the management platform can extend to anywhere on the network.)
- Creating common user, device, and application access and usage policies from the campus out to the branch and into the intelligent edge simplifies operations, ensures security, and eases management

Zero-Trust Security

A third critically important tenet of a platform for the intelligent edge is security. Security must be at the forefront of any architecture discussion, but as IoT devices proliferate and enterprise networks expand from being centralized to becoming distributed across multiple domains (datacenter, campus, cloud, and IoT), securing that environment becomes increasingly challenging. The key is building in security from the ground up and ensuring it extends across all areas of the network. There are a handful of architectural practices that can be put in place to ensure security across the intelligent edge. The most critical is a zero-trust network that contains the following capabilities:

- By default, every user, device, traffic flow, and "thing" on the network should be authenticated. Doing so requires an AI-enhanced platform with the ability to automatically detect, profile, and segment devices.

- Role-based policies should be created centrally and then implemented across all aspects of the intelligent edge, from the core datacenter out to every IoT device.
- A zero-trust system should dynamically segment users and devices and their traffic, no matter where they enter the network. The access and usage policies should follow users, devices, and data flows, no matter where on the network they traverse.
- The zero-trust system should be based on ML/AI-enhanced management processes that allow enterprises to manage policies through an intuitive dashboard, eliminating the need to use command-line interfaces and set up complicated webs of VLANs and ACLs.

Connecting to Internal and External Apps and Services

An enterprise network has many components, existing systems and new external services that users must access. The network should be an enabler of those systems rather than a roadblock of the business benefitting from them. The network should be extensible to be able to support integrations with existing applications and systems. Perhaps there are financial, human resource, or enterprise management systems that must be supported, or a range of third-party SaaS applications that must be spun up and supported on short notice. The network should be a fabric that enables seamless flows of information while ensuring secure usage of each of these types of systems. Achieving fluid connectivity to a variety of internal and external resources requires a network that is built from the ground up to be secure and is extensible to support the distribution of workflows wherever they need to go.

An Architectural Approach to Building an Intelligent Edge Platform

Enterprises should consider a network architecture based on the key tenets of: AI-enhanced operations, unified infrastructure, and zero-trust security. Enterprises shouldn't have to make revolutionary changes that are typically required of enterprises to enable value from the intelligent edge era though. Instead, enterprises should look to familiar architectural patterns that have been relied on for years. A simple way to think about enabling this architecture is to consider the components of how enterprise networks are built and ensure each one is optimized for the intelligent edge era based on the key tenets described previously. These include:

- **Underlay:** This layer provides the connectivity across all areas of the network, from wireless access to wired Ethernet switching, out across the WAN and inclusive of 5G. These underlay connectivity methods should be comanaged, allowing for integrated policy controls no matter the underlay connectivity method.
- **Overlay:** Management of the aforementioned underlying connectivity platforms should be done through a software-defined overlay platform that runs atop. This is where user and device access and usage policies are created and dynamically enforced.
- **Apps and services:** Atop the underlay and overlay components are applications and services that optimize the system. This is where provisioning, orchestration, analytics, and location-based services run that add value to the business.

ARUBA EDGE SERVICES PLATFORM

Aruba, an HPE company, has recently launched its Edge Services Platform (ESP), which is built upon a series of enhancements to its product lines across the datacenter, campus, branch, remote worker, and edge to offer a unified infrastructure across key enterprise domains and with machine learning- and AI-enhanced management to simplify network operations and ensure zero-trust security.

Aruba's ESP spans multiple layers of the networking stack: for connectivity, it enables unified management of wired and wireless as well as WAN and IoT components, with integrations for 5G networks in the future. Atop the infrastructure components sits a software-defined policy layer inclusive of dynamic segmentation capabilities, managed by ClearPass Policy Manager and enhanced by ClearPass Device Insight for automatically recognizing and classifying devices on a network. ESP also encompasses a series of applications and services that run natively within the platform, including those for onboarding users and devices, provisioning and orchestrating resources, and generating detailed analytics through Aruba's Network Analytics Engine (NAE).

From an infrastructure component perspective, ESP integrates a handful of key technologies, including the company's CX switching line, full lineup of Aruba access points for WLAN, and SD-Branch gateways for WAN connectivity. Aruba Central is the company's cloud-based centralized interface for managing this unified infrastructure and the software-defined policies and apps and services that run atop them with a single pane of glass and common data lake.

As part of the enhancements to the products, Aruba Central and infrastructure products are available through a variety of financing and consumption models. All Aruba infrastructure components can be purchased outright or financed through HPE Financial Services. Aruba Central is now available in a variety of consumption models ranging from on-premises deployed and managed, to SaaS delivered, to being delivered as a managed service, and now as part of HPE GreenLake for Aruba, a completely managed network-as-a-service (NaaS) offering. A new aspect of ESP is Aruba's Developer Hub, which is a central repository for APIs across the portfolio along with developer documentation.

Challenges

As enterprises explore new ways to enable connectivity in the era of the intelligent edge, they will deal with a variety of challenges. First and foremost is finding the leadership and motivation for action. Too often, new initiatives that can add value to an organization are put off in lieu of just maintaining the status quo. Aruba must work with its customers and partners to ensure enterprises understand the value of embracing the intelligent edge and help them execute a plan to capitalize on it. Aruba will be doing so in a competitive field of networking vendors enabling connectivity in the intelligent edge era.

CONCLUSION

Enterprises are operating in a new world today, one that is driven by data and won by organizations that understand how to process that data for their benefit. Key to this era is having a network that enables organizations to collect data and process and act upon it. Doing so requires a network that is secure, scalable, and automated. Organizations that embrace these trends will be the ones that will succeed in the next era of the intelligent edge.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com