

White Paper

Transforming the Enterprise Network: How a Software-Defined Branch Enables Cohesive WLAN, LAN, and WAN Management with Integrated Security, Managed from the Cloud and Enhanced by AI

Sponsored by: Juniper Networks

Brandon Butler
February 2023

EXECUTIVE SUMMARY

Enterprise networking is at an inflection point. A variety of trends are converging to bring about new ways that enterprises are thinking about architecting, deploying, and managing the access and wide area layers of the network. Some of these changes have been more than a decade in the making – such as the rise and mainstream adoption of cloud-based services. Others are more recent shifts, such as leveraging machine learning (ML) and artificial intelligence (AI) algorithms to enhance the management of the network. Taken together, enterprises across the globe are exploring ways to transform their network to improve their business.

Enterprises have myriad goals when considering a reimagined enterprise network. They're looking to be more efficient in network management – meaning network management platforms that break down silos across the networking stack. They're looking for security to be natively built into networking platforms and for ways to ensure exceptional user experiences. Enterprises are looking for ways to consume network infrastructure that meet organizational sustainability goals.

Overall, organizations are evolving their connectivity strategy to ensure the enterprise network is an accelerator, rather than an inhibitor, of broader business goals. A key architecture to help transform enterprise campus and branch networks is the software-defined branch (SD-Branch). SD-Branch architectures enable integrated management across local area network (LAN), wireless local area network (WLAN), and software-defined wide area network (SD-WAN) networks, managed from the cloud, with native security and enhanced by ML/AI operations.

This paper outlines the drivers behind SD-Branch, the benefits this modern enterprise network architecture enables, and the key components that make up a modern and successful SD-Branch deployment. The paper outlines recent important developments in SD-Branch that have emerged to help transform the enterprise campus and branch and deliver on the full promise of this architecture. The paper also explores the critical role service provider partners can play in accelerating enterprise network transformation.

THE CHANGING ENTERPRISE NETWORK

Drivers of Change

The enterprise network has changed significantly in recent years. Some of these changes have been more than a decade in the making. For example, enterprises have been steadily increasing their reliance on the cloud. Enterprises rely on the cloud not just as a destination for hosting applications – within the context of enterprise networking, the cloud has emerged as a powerful platform for managing the access and wide area networks.

There are other changes in the ways devices and end users access the enterprise network. Notably, since the COVID-19 pandemic, users and devices are more distributed than ever. Enterprises also rely more heavily today on Internet of Things (IoT)-connected devices for mission-critical and business-advancing capabilities.

These changes have created significant shifts in the enterprise network. Users and devices – including a growing cadre of Internet of Things devices – are more distributed than ever. Meanwhile, those distributed users and devices are accessing applications that are distributed across multiple clouds. This creates hyper-distribution of both users and the applications they're accessing. Fundamentally, the enterprise network must transform to reflect this new reality.

IDC forecasts that the number of IoT-connected devices is set to continue to grow rapidly in the coming years. IDC expects there to be 51.9 billion connected devices by 2025 (growing from 44.7 billion devices in 2021); 75% of connected devices in 2025 (39.3 billion) will be IoT-connected devices.

Challenges of Legacy Network Architectures

Legacy enterprise campus and branch network architectures have a variety of challenges that do not reflect the recent advances in the needs of a modern enterprise network. Some of the key challenges of legacy architectures are:

- **On-premises/controller-based architectures:** In the past, the standard architectural model for an enterprise access network was to leverage a controller that is managed on premises. While this architecture has been suitable for many organizations, controller-based architectures do not lend enterprises to taking advantage of all the benefits of cloud-managed networking.
- **Lack of visibility/analytics:** Traditional legacy architectures focused on enabling connectivity, but less so on ensuring user experiences. Enterprise networking today is about not just providing connectivity but ensuring the high-quality nature of the connected experience for end users. That means metrics regarding the uptime and availability of the network and any network performance degradations or security incidents being identified rapidly and resolved quickly.
- **Not harnessing management efficiency opportunities:** Having siloed management across various parts of the enterprise network leads to management inefficiencies. For example, having separate management tools across the wired and wireless local area network or separate management tools for the local and wide area network leads to inefficiencies in network management.

SD-Branch as an Architectural Solution for the Modern Enterprise Network

In recent years, advancements have emerged for the enterprise network that address the challenges of legacy network LAN and WAN designs. The software-defined branch is an enterprise network architecture that provides integrated management of the LAN, WAN, and security.

SD-Branch architectures enable more cohesive management across the wired and wireless local area network, as well as across the campus (LAN) and branch (WAN) networks. SD-Branch architectures can vary (e.g., enterprises can manage an SD-Branch on premises), but cloud-managed SD-Branch has myriad benefits for organizations. Furthermore, when SD-Branch management tools are enhanced by ML and AI algorithms, enabling AI operations (AIOps), the benefits of an SD-Branch approach expand.

THE POWER OF CONNECTIVITY TO ACCELERATE BUSINESS TRANSFORMATION

Enterprises have an imperative to ensure their enterprise access and wide area networks are meeting the needs of their business. The enterprise access and wide area network is essential for ensuring that employees, customers, partners, and others can access critical enterprise applications, with secure privileges. Meanwhile, the wide area network provides connectivity to applications users and devices are accessing.

Enterprises today have a variety of goals for their overall business. These goals may change from industry to industry, but IDC research has found that a handful of goals apply across different organizational types. Some top goals of enterprises are improving customer experience/satisfaction, focusing on sustainability, improving operational efficiency, and enhancing employee productivity (see Figure 1).

FIGURE 1

Customer Satisfaction the Top Priority for Enterprises, But Sustainability Gaining Significant Traction

Q. What are your organization's top 3 business priorities?



Source: IDC's *Future of Connectedness Survey*, August 2022

Connectivity can play a vital role in enabling these goals. Technology should not just meet the needs of the business and users, but it should be operationally efficient to deploy, manage, and optimize on an ongoing basis. A key to enabling this is relying on AI-driven automation. SD-Branch architectures can play a significant role in enabling improved operational efficiency within the enterprise network. SD-Branch designs allow for more cohesive management across the wired and wireless LAN, as well as integrated management across the LAN and WAN, and tighter integration across networking and security.

Having more integrated management across these domains allows IT organizations to break down siloed management of the network and apply consistent policies across different parts of the network. Doing so has an added security benefit as well, as consistent policies that are hardened and securely enforced decrease the likelihood of inconsistent misconfigurations across the network.

SD-Branch architectures can also help organizations focus on sustainability and improve employee productivity. From a sustainability standpoint, new technologies like AI-driven radio resource management and power over Ethernet can reduce the amount of cabling that needs to be deployed and optimize connectivity – saving money and resources. Advanced infrastructure components that are power efficient can be deployed in SD-Branch architectures that can reduce energy consumption while improving the performance of the network. Zero-touch provisioning capabilities enable fewer onsite truck rolls for network deployments, while automation tools speed large deployments.

For employee productivity, AI-driven management of the network can ensure high service levels for user experience while reducing the operational burden on IT staff. This can be validated by integrated visibility and analytics tools and AIOps management that can recognize – and remediate – network performance degradations before they impact users. AIOps can help IT teams focus on business-enabling tasks with their valuable time rather than simply keeping the network up.

Another key to ensuring the enterprise network is meeting the needs of the business is to have security capabilities built directly into the network management platform. For example, having tools that enforce role-based network access controls or having integrated firewall capabilities are some examples of ways that security can be integrated directly into the enterprise network via an SD-Branch approach.

Overall, enterprises should have a handful of goals when considering a modern, enterprise-grade access and wide area networking platform. The platform should enable high-quality end-user experiences, should be secure and sustainable, and should improve operational efficiencies across the organization.

THE CRITICAL ROLE OF SERVICE PROVIDERS IN ENABLING ENTERPRISE NETWORK TRANSFORMATION

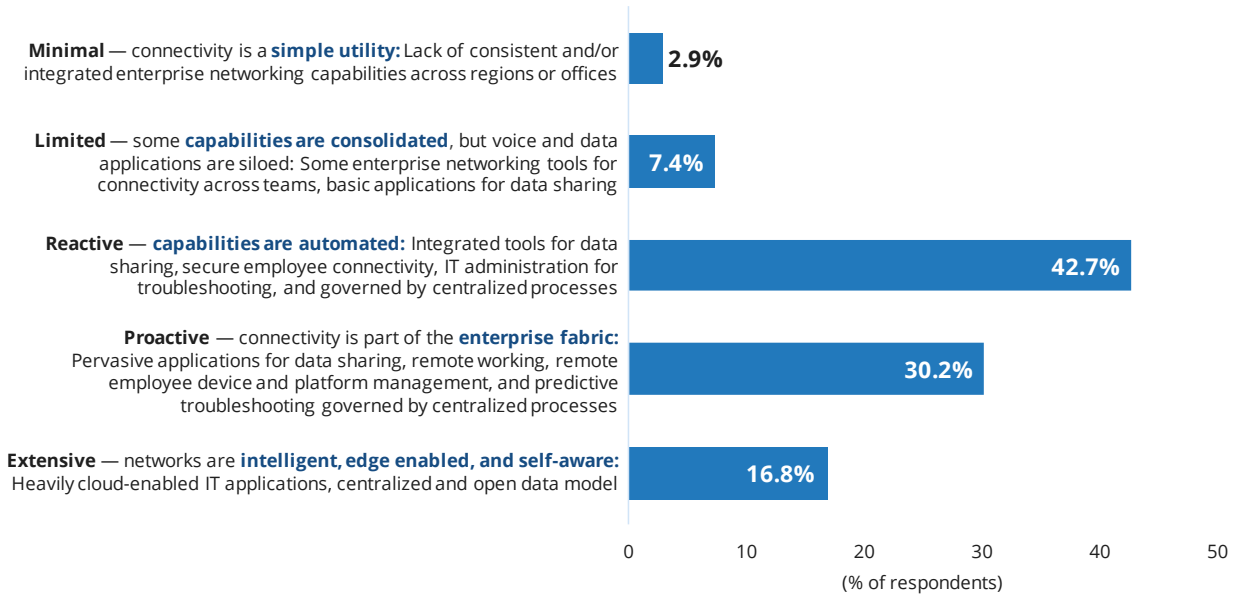
While there is a significant opportunity for enterprises to reconsider their enterprise network architectures, IDC research shows that enterprises are in the early stages of transforming their connectivity strategy.

An IDC survey in August 2022 asked enterprises to what extent their organization is currently connected digitally across their entire network footprint. Respondents were given a five-point scale, with "minimal" maturity being the lowest level and "extensive" maturity being the highest level of maturity. The most mature networks are defined as networks that are intelligent, edge enabled, self-aware, and heavily cloud based with a centralized and open data model. Of the respondents, more than half – 53% – said they were in one of the three lowest categories of maturity. Less than 17% said they were in the highest category of network maturity (see Figure 2).

FIGURE 2

Enterprise Connectedness Maturity Today

Q. To what extent is your organization currently connected digitally across your entire network footprint?



Source: IDC's *Future of Connectedness Survey*, August 2022

This data shows that enterprises are in the early stages of transforming their networks. There are a handful of keys that can help organizations achieve more advanced levels of network and connectivity maturity. First, embracing new enterprise network architectures – such as SD-Branch – can help modernize the enterprise network. Second, working with a trusted partner that can help organizations deploy, manage, and implement the modern enterprise network is another key too. Finally, ensuring that any network architecture design and choice of a partner meets the broader needs of the business is another way to ensure success.

Service providers play a critical role in enabling more advanced enterprise network transformation. Service providers bring a number of advantages to enterprises as they consider adopting an SD-Branch approach. For example, service providers have the expertise to be able to help execute the full life cycle of an SD-Branch deployment, from the initial day 0 planning to the day 1 implementation, all the way through the day n optimization and management of the network.

Second, enterprises working with a service provider are able to leverage integrated consumption of networking technologies, including via emerging consumption-based models. More specifically, enterprises are able to get a bundled offering of not just the components of an SD-Branch architecture (e.g., wireless access points [APs], Ethernet switches, and routers) but also the integrated connectivity. That could include broadband, fiber, MPLS, or cellular connectivity.

Service Providers and SD-Branch

For service providers to become a strategic partner of enterprises, they need a platform to be able to deliver a modern, enterprise-grade network. SD-Branch architectures can be managed by service providers and delivered to enterprise customers. Embracing an SD-Branch architecture has benefits for service providers too. It allows service providers to expand their strategic relationship with enterprise customers by helping enterprises with the full life cycle of the network deployment; it can improve response times via advanced automation capabilities and create an opportunity for more efficient management of multiple customer sites.

Here's an example of how a service provider could expand its strategic relationship with an enterprise client by leveraging an SD-Branch approach. Say, for example, that a telecommunications company sells WAN connectivity to an enterprise customer. The communication service provider could position an SD-Branch architecture as an expanded way to optimize the WAN connectivity by leveraging a hybrid WAN that includes not just broadband but also cellular connectivity, managed by a cloud-based SD-WAN platform. Then, as customers deploy the SD-WAN, they could upgrade to include LAN and WLAN management from the same cloud-based platform. Additional value-added features like security services (e.g., a firewall as a service or location-based asset tracking services) could be bundled in as well. SD-Branch is a flexible architecture that allows partners to work with enterprise customers to meet their digital and network transformation goals.

SD-Branch approaches are an ideal architecture for service providers to use with enterprises. SD-Branch approaches can include cloud-based management, enabling multitenant management of multiple enterprise accounts from a centralized platform. The cloud-based platform can also conduct advanced visibility and analytics, to be able to monitor network performance and security events. AIOps capabilities allow service providers to rely on advanced management capabilities and allow for self-identification and self-remediation of issues that arise. SD-Branch architectures allow for cohesive management across various parts of the network, creating management efficiencies for the service provider, and improved service levels for enterprises.

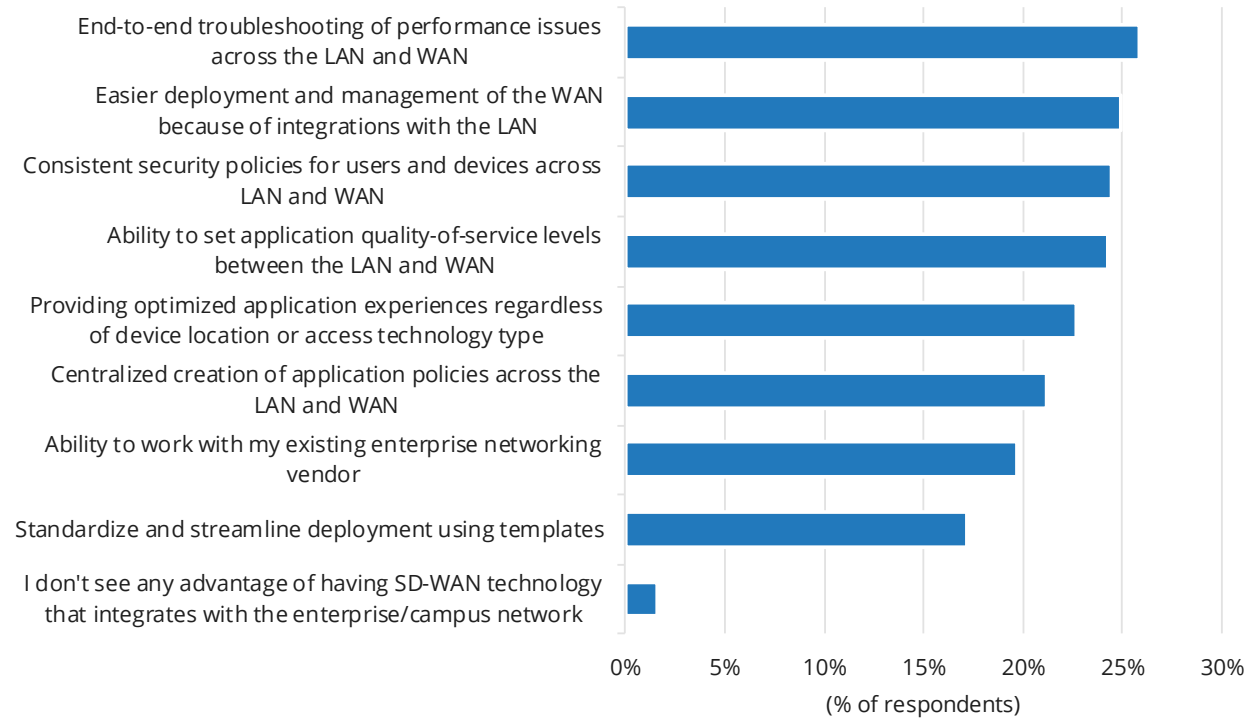
KEY SD-BRANCH CAPABILITIES

SD-Branch can be a powerful enterprise network architectural approach for both enterprises and service providers alike. Recent IDC survey data shows growing interest in SD-Branch approaches. Figure 3 shows two survey data points from an IDC survey conducted in November 2022. One of the questions asked respondents what advantages respondents see with SD-WAN technology that integrated with the enterprise network (e.g., wired and wireless). The top-rated responses included having end-to-end troubleshooting of performance issues across the LAN and WAN, having easier deployment of the WAN because of integrations with the LAN, having consistent security policies across the LAN and WAN, and the ability to set application quality-of-service levels between the LAN and WAN. This data points to the significant benefits enterprises achieve from an SD-Branch approach.

FIGURE 3

Top Advantages to an Integrated SD-WAN and LAN/WLAN: Troubleshooting, Easier Deployment, and Consistent Security Policies

Q. *What advantages, if any, do you see with SD-WAN technology that integrates with enterprise networking needs (wired and/or wireless)?*



n = 1,044

Notes: Data is not weighted.

Multiple responses were allowed.

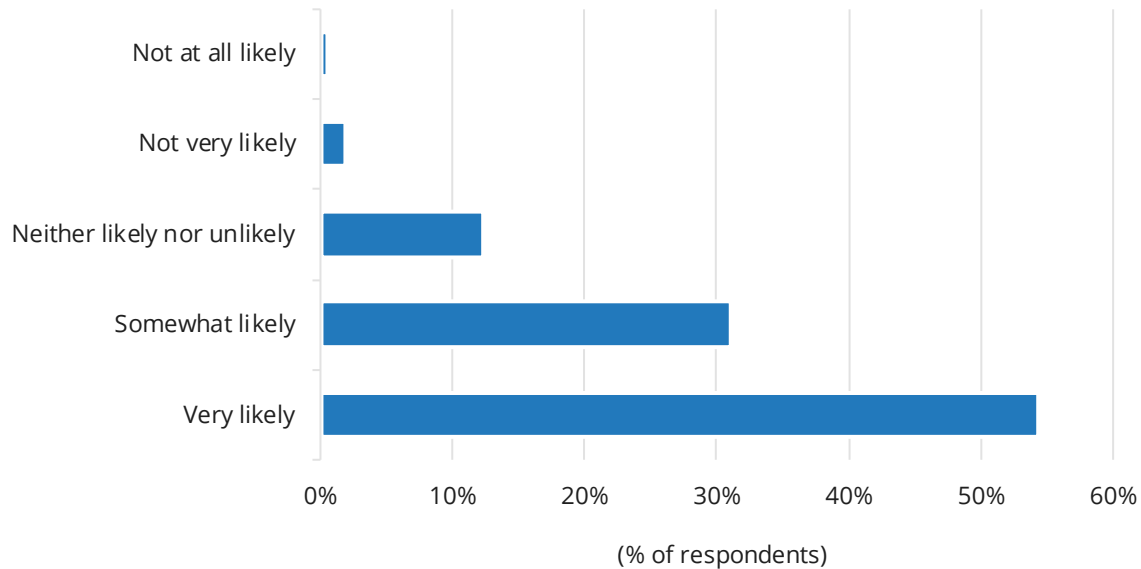
Source: IDC's *Software-Defined WAN (SD-WAN) Survey*, November 2022

These advantages of integrated management across the LAN and WAN are causing organizations to consider vendors that can provide SD-Branch architectures. Another survey data question asked – on a five-point scale – how likely respondents would be to work with their existing enterprise campus/local area networking vendor when deploying SD-WAN, with one being "not at all likely" and five being "very likely." Responses showed that 85% of those surveyed said they would be somewhat or very likely to work with their existing LAN vendor when deploying SD-WAN (see Figure 4).

FIGURE 4

Enterprises Overwhelmingly Wanting to Work with Existing LAN Vendor When Deploying SD-WAN

Q. How likely would you be to work with your existing enterprise/campus local area networking (LAN) vendor when deploying SD-WAN technology?



n = 1,044

Source: IDC's *Software-Defined WAN (SD-WAN) Survey*, November 2022

SD-Branch Components

As an architectural design, the specific components of an SD-Branch can vary, but IDC believes there are a variety of components that are important for an SD-Branch architecture to ensure it can enable maximum value for the service provider or enterprise. Among these key capabilities are:

- **An integrated platform for managing WLAN, switch, and SD-WAN:** As the previously mentioned survey data shows, enterprises see value in platforms that can provide integrated management across the LAN (wired and wireless) and WAN/SD-WAN. There are benefits related to the initial deployment, as well as the ongoing management, of a more cohesive enterprise network architecture.
- **Cloud-based management:** Managing an SD-Branch architecture from the cloud enables a variety of benefits. For service providers, the cloud-based platform enables centralized management of multiple enterprise networks. For enterprises, leveraging a cloud-based platform eliminates the need to devote on-premises resources to management tools or controllers. Furthermore, cloud-based platforms allow both service providers and enterprises to be able to get the fastest access to new features, functions, and capabilities enabled by the networking vendor; the cloud is constantly updated, ensuring that all network infrastructure is running the latest and most advanced software.

- **Visibility and analytics:** Observability is a foundational aspect of being able to efficiently manage an enterprise network. For service providers or enterprises to enable advanced automation, improve service levels, or ensure security, first there must be a base level of knowledge of the network. Visibility and analytics in the network performance, end-user experience, and overall health of the network allows enterprises and service providers to layer on advanced automation and security capabilities atop this information.
- **AI-enhanced automation:** One key to improving the operational efficiency of managing an enterprise network is to rely on automation platforms to do tasks that previously may have been done manually. From the initial deployment to ongoing management – including setting and enforcing role-based security policies – AI-based automation can be a significant key to helping run an enterprise network more efficiently. Leveraging natural language processing – including conversational AI-based platforms – can help organizations more efficiently manage all aspects of the enterprise network.
- **Integrated security:** Any technology buying decision includes an evaluation of the security of the offering. There are two fundamental categories of security as it relates to an SD-Branch architecture: the first is the native security capabilities of the SD-Branch design, meaning integrated security functions like a firewall as a service, cloud access security broker, or network access control. Another component of security is how the SD-Branch platform integrates with third-party security tools, those hosted both on premises and in the cloud. Having security be a part of the SD-Branch is critical, but equally important is having a platform that allows organizations to leverage existing security tools and investments.
- **Direct cloud and multicloud connectivity:** As enterprise applications have become increasingly distributed, an important function of SD-WAN platforms has become the direct cloud and multicloud connectivity capabilities. This includes having the ability to efficiently route traffic to – and in some cases through – cloud platforms and hosting virtualized or containerized versions of an SD-WAN management platform directly in the cloud.
- **Additional features/services – location-based services:** There are a variety of other services enterprises may be interested in deploying in conjunction with an SD-Branch architecture, for example location-based services that can provide asset tracking, wayfinding, and other Wi-Fi-enabled services. Integrated location technology can have a robust impact on business operations, allow for further consolidation of hardware platforms and, in the case of service providers, develop greater strategic relationships with end customers.
- **New flexible consumption models/network as a service (NaaS):** While the technology that is part of an SD-Branch architecture is important, there are also new ways that enterprises are considering consuming enterprise network infrastructure, including as consumption-based and enterprise network-as-a-service models. Comprising an opex, subscription-based licensing scheme, enterprise NaaS allows for increased financial flexibility while embracing cloudlike economics for network infrastructure.

JUNIPER NETWORKS'S AI-DRIVEN SD-BRANCH

Juniper Networks' AI-Driven SD-Branch portfolio is made up of a range of wireless, wired, and WAN/SD-WAN infrastructure, managed via the Juniper Mist Cloud. Juniper's cloud-based management platform is built on microservices and leverages ML- and AI-based automation. The SD-Branch portfolio includes a range of cloud-delivered services such as Wi-Fi, wired, WAN, user engagement, and IoT assurance tools for fine-grained observability and location-based asset tracking services. It also includes a virtual network assistant – named Marvis (which provides a conversational

assistant for AI-driven problem solving) and Marvis Actions (a proactive network insights and remediations platform powered by network visibility and analytics tools).

Network infrastructure components include a range of indoor and outdoor WLAN APs, including Wi-Fi 6 and 6E and BLE versions; the company's family of EX access, aggregation, and core switches; and a series of routers including the SRX and Session Smart Routers, the latter of which provides tunnel-free SD-WAN capabilities, zero trust, and improved performance and scale.

CONCLUSION

Enterprises around the globe are looking to digitally transform, and they're increasingly realizing the importance of networking and connectivity in not just enabling – but also accelerating – their organization's broader business goals. The enterprise network is where users and devices access mission-critical corporate resources. The enterprise network is also the gateway to access a broad and diverse array of enterprise applications that are hosted both within and outside of the enterprises' domain and, increasingly, across a multicloud landscape. In today's modern enterprise network, just simply providing connectivity is not enough. Enterprises are looking to ensure exceptional network experiences for all those people, things, and devices that require connectivity.

Achieving these goals cannot come at the expense of a complicated network architecture and management platform, however. Organizations are looking to optimize efficiencies in terms of managing technology – from the earliest days of considering and deploying a network to the ongoing management. There are a variety of new technologies that can help achieve these goals, such as cloud-based management, integrated platforms that stretch across multiple parts of the network, enhanced visibility, analytics and ML/AI operations, and security that is built into the network rather than bolted on. Partners play a particularly important role in enabling network transformation projects too. SD-Branch is a way to help services providers and enterprises alike adopt new architectures that can help advance their network transformation and ensure that connectivity is an enabler of the broader business goals.

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

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com

Copyright Notice

External Publication of IDC Information and Data – Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2023 IDC. Reproduction without written permission is completely forbidden.

