IDC DICKER DATA

ANALYST CONNECTION

Sponsored by: HPE (Aruba)

As organizations modernize their SD-WANs, they must also consider new networking security requirements.

Meeting Cloud-First Requirements for WAN and Edge Security Modernization

November 2022

Questions posed by: HPE (Aruba)

Answers by: Christopher Rodriguez, Research Director, and Brad Casemore, Research Vice President

Q. Why is WAN modernization necessary in a cloud-first environment?

A. The ongoing migration of workloads to clouds has had a profound effect on network architectures, infrastructure, and operating models. This impact is perhaps felt most acutely by the WAN, as enterprises adopting hybrid IT must modernize their networks to accommodate and optimize the delivery and experiences associated with increasingly distributed application environments while meeting the business need for agility and flexibility. Not only are the applications more distributed than ever before, but the users of applications, whether employees or customers, are also increasingly distributed, with hybrid workforces and the rise of work-from-home scenarios in the wake of the pandemic.

SD-WAN emerged as a direct response to the cloud-driven requirement for WAN modernization. Most SD-WAN infrastructure on the market today addresses, to varying degrees, the limitations of traditional enterprise WANs in areas such as support for cloud applications (SaaS and IaaS), simplified deployment and management, cost-effective bandwidth utilization, greater overall WAN flexibility and efficiency, and improved WAN security.

Q. What are the most important/critical networking requirements?

A. SD-WAN has evolved considerably since its inception nearly a decade ago. Back then, SD-WAN infrastructure generally looked similar architecturally. SD-WAN offerings typically included a centralized, application-based policy controller; a software overlay to abstract underlying networks; analytics and/or telemetry for application and network visibility; and an optional SD-WAN forwarder (routing capability). Together, these components provided an intelligent path selection across WAN links based on the application policies defined on the controller.

Now, as SD-WAN evolves and customers make greater use of internet breakout at the branch office, edge security is seen as integral to cloud-first requirements. Intelligent application-based steering is another critical requirement, especially as enterprises adopt more IaaS and SaaS applications, which need to be optimized differently from traditional on-premises applications. According to IDC's surveys and customer interactions, enterprises are prioritizing solutions that integrate networking and security yet also offer choice and flexibility between how each is delivered and sourced. Enterprises are seeking greater simplicity in the procurement, deployment, and management of modern WAN infrastructure, especially given the added complexity that accompanies hybrid and multicloud environments. Cloud and multicloud also are driving a growing

interest in how SD-WAN infrastructure integrates seamlessly with cloud interconnects and direct connects, which can improve the delivery and performance of cloud-based applications. In addition, we see a growing use of wireless (4G/5G) for both primary and backup WAN connectivity, especially in certain industries. Last but certainly not least, there's a growing cloud-driven requirement for pervasive telemetry, analytics, and observability as the importance of digital experiences comes to the fore.

Q. What new network security requirements should IT organizations consider in their WAN modernization strategy?

A. The transformation of the enterprise network has been driven by pressing business needs such as a workforce that migrated from corporate offices to home offices or hybrid work models. Similarly, while the complexion of the enterprise cloud environment continues to change, the scalability and flexibility of the cloud ensure its lasting relevance in future IT plans. WAN modernization offers key benefits, but the enterprise network is now highly distributed and complex and will become only more so as businesses continue to invest in emerging technologies. The IT organization is challenged to regain control over cloud applications, protect valuable data as users continue to utilize their preferred devices and applications, and detect and secure IoT devices.

Attempts to extend perimeter-based approaches to the modern enterprise WAN are proving to be incomplete. Security architecture has traditionally focused on several specialized solutions tasked with defending a particular environment or specific technology. The approach leads to unmanageable numbers of security tools, gaps in protection, and security silos that allow advanced threats to evade perimeter defenses and persist undetected. Naturally, integration has been a top priority in security modernization efforts. A modern security architecture requires the integration of multiple network security technologies to ensure a security posture through universal policy enforcement and consistent protections. Workers require secure, performant access, regardless of location. Policies must be applied at the network edge in order to enable secure cloud access and direct internet access. SOC teams require complete and deep security observability to correlate indicators of compromise.

In this way, security and SD-WAN modernization are both equal and indispensable infrastructure pillars for enterprises as they devise and implement converged security at the WAN edge.

Q. Do the network and security requirements of large enterprises differ from those of midsize and smaller organizations?

A. In some ways, enterprises and organizations all need similar capabilities, and there definitely are more commonalities than differences. We see differences in requirements in certain vertical industries, where "thin branches," which have personnel and real estate constraints, are prioritized and tend to proliferate. Think of service stations, real estate or branch financial offices, fast-food outlets, and other "fast-service" facilities. These sites, which often have no IT personnel in them, benefit enormously from intelligent automation throughout the life cycle not only to get them provisioned effectively but also to keep them running optimally.

At the other end of the spectrum, large multinational corporations tend to want seamless interconnections with globe-girding cloud networks, which provide for greater digital resiliency and improve the performance attributes and service quality of cloud applications.

A similar dynamic occurs in security, where most organizations regularly face a deluge of opportunistic, untargeted threats. As a result, businesses of all sizes require a common set of core security functionality such as firewall, VPN or zero trust network access, secure web gateway, and cloud access security broker. However, large enterprises are high-value targets for skilled, persistent cybercriminals and require advanced protection. These organizations will require the aforementioned security stack, plus deep security visibility across the WAN, including edge and cloud. Telemetry from across the WAN, cloud, and edge is required to help security analytics tools identify elusive attacks and zero-day exploits. Of course, the challenge is to do this at enterprise scale and complexity.

Q. How can organizations ensure that their SD-WAN and edge security solutions deliver investment protection and ROI?

A. It's important to not make compromises in either the quality of SD-WAN technology or the selection of security technologies. The siren song of consolidation and integration of SD-WAN and edge security can be tempting because it promises to provide the simplicity that should derive from an integrated single vendor offering. That said, it usually does involve compromises in one area or the other, and it can lock customers into an architectural model that limits choice and flexibility as their needs and distributed application environment evolve.

A key to achieving investment protection and to optimizing ROI is maintaining as much choice and flexibility as possible in both your SD-WAN infrastructure and your edge security posture. Security is challenged to be everywhere at once throughout this process, without slowing down traffic or breaking applications. The ultimate characteristic of a modern security architecture is flexibility, with multiple options for deployment across various environments, applications, user locations, and device types. Organizations should focus instead on solutions that deliver integrated network QoS and security policy and comprehensive threat protection.

Further, IDC always recommends that enterprises be application driven in their network architectures, infrastructure, and operating models. Applications are the lifeblood of digital business, and cloud — as a destination for workloads, but even more as an operating model — is predominating. Organizations need to ensure that they have a modern network and security infrastructure that aligns with and fully supports a modern, distributed application landscape.

About the Analysts

Christopher Rodriguez, *Research Director, Security and Trust*

Christopher Rodriguez is a Research Director in IDC's Security and Trust research practice focused on the products designed to protect critical enterprise applications and network infrastructure. IDC's Security and Trust research services to which Chris contributes include Network Security Products and Strategies and Active Application Security and Fraud.

Brad Casemore, *Research Vice President, Datacenter and Multicloud Networks*

Brad Casemore is IDC's Research Vice President, Datacenter and Multicloud Networks. He covers datacenter network hardware, software, IaaS cloud-delivered network services, and related technologies, including hybrid and multicloud networking software, cloud networking, and cloud WANs. Mr. Casemore also works closely with IDC's Enterprise Networking, Server, Storage, Cloud, and Security research analysts to assess the impact of emerging IT and converged and hyperconverged infrastructure.

MESSAGE FROM THE SPONSOR

Aruba's EdgeConnect SD-WAN platform, built for today's edge-to-cloud enterprise, delivers the highest quality of experience for users and IT, no matter where applications reside.

EdgeConnect SD-WAN supports:

- Business-driven application routing that automates network, security, and application policies
- Highest quality of experience for voice and video over any broadband
- Increased SaaS and IaaS performance with continuous real-time network monitoring
- Unified SD-WAN, routing, NGFW, segmentation, and WAN optimization in a single platform

Aruba EdgeConnect SD-WAN provides comprehensive security services at campus, branch, data center, and cloud locations including next-generation firewall, IDS/IPS, and DDoS detection and remediation. EdgeConnect replaces outdated, difficult to manage physical firewalls at branch locations while delivering consistent security for all users, from any network location, from any device -- wherever applications are hosted.

EdgeConnect SD-WAN provides an enhanced, comprehensive security offering for enterprises that need consistent, secure, and predictable experiences across multiple locations over the WAN.

IDC Custom Solutions

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com