IDC

SPOTLIGHT

Sponsored by: Cambium Networks

Midmarket organizations are looking to transform their networks to meet the needs of their digital businesses. As they do so, they're increasingly realizing the importance of integrated and cloud-managed networking and security.

How Integration and Cloud Management Help Optimize Networks for the Midmarket

November 2022

Written by: Brandon Butler, Research Manager, Enterprise Networks

Introduction

Organizations around the globe are increasingly realizing the importance of delivering high-quality and reliable network connections to the digital applications on which they rely. The need for predictable and secure connectivity has been driven in part by the significant adoption of cloud-based applications for mission-critical business use cases. The increased reliance on distributed applications not only places greater emphasis on the network but also requires organizations to ensure secure connectivity of their networks.

For smaller organizations in the midmarket (compared with large enterprises), there are unique challenges in transforming their networks to meet the needs of their digital business. These challenges include a lack of IT skills to implement advanced technologies, a need for solutions that integrate multiple functions in one (e.g., networking and security, LAN and WAN, wired and wireless), and a need for simplicity in deployment, operation, and ongoing management.

AT A GLANCE

KEY TAKEAWAYS

A converged, cloud-managed network generates myriad benefits, including:

» Integrated management of network and security policies

» Predictable and secure access to distributed applications

» Simplicity across the full network life cycle, from initial deployment to ongoing management

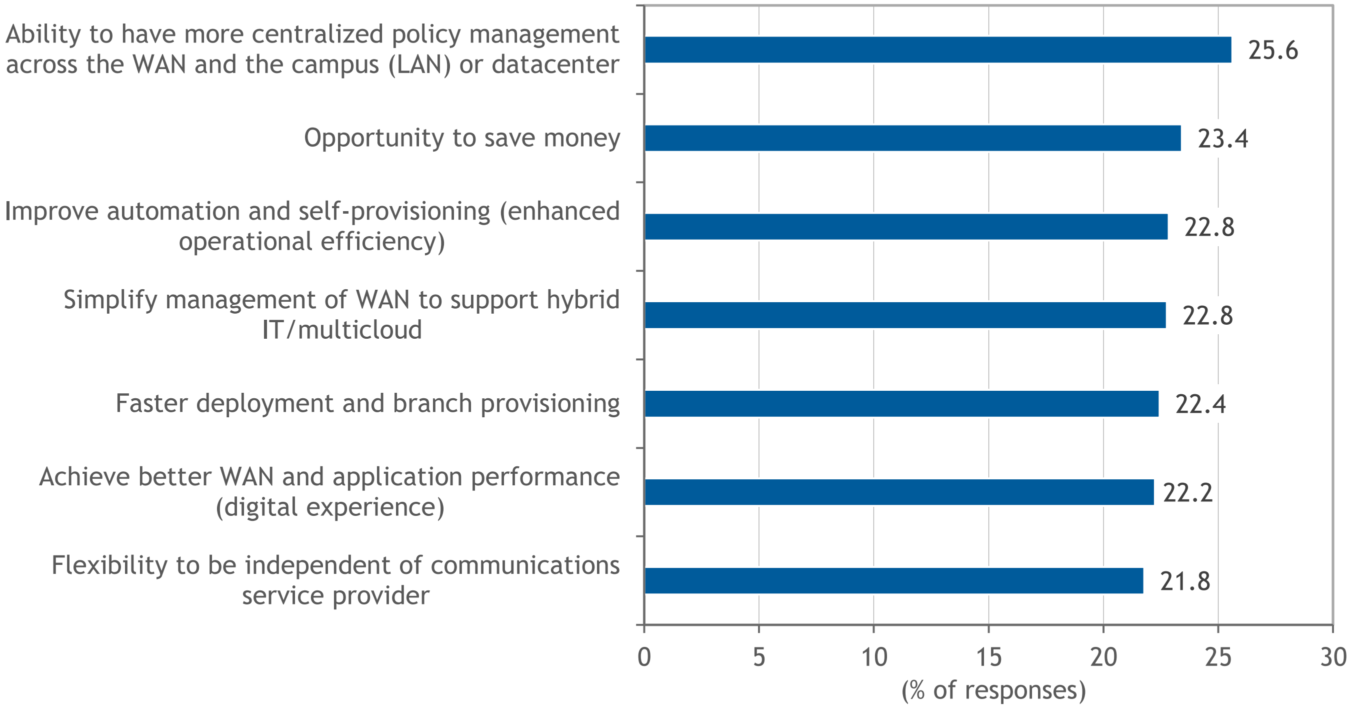
There are a variety of ways in which organizations can transform their networks to overcome these challenges. This paper outlines the value of cloud-based management and the power of integrated network and security offerings. It showcases the benefits of converged management in helping accelerate the network transformation goals of midmarket customers.

Network, Security, and Cloud Challenges in the Midmarket

Enterprise networking today is a complex environment. The past decade has seen a dramatic shift by companies to embrace cloud-based applications for mission-critical workloads. Organizations are fundamentally re-architecting their networks — particularly their WANs — to optimize connectivity to the cloud. A global IDC survey on WAN trends asked respondents what their top motivations are for considering SD-WAN, a technology that applies software-defined networking principles to the WAN. Figure 1 shows the top drivers for SD-WAN deployments, including more centralized policy management across the WAN and campus or datacenter.

FIGURE 1: ***Top SD-WAN Motivations***

Q *Which of the following are the top 3 motivations for considering a SD-WAN deployment? (Select up to three.)*



n = 375

Source: IDC's Software-Defined WAN (SD-WAN) Survey, June 2021

Meanwhile, businesses in the midmarket face additional challenges, including:

- **Lack of IT skills.** Compared with large enterprises, smaller organizations are typically less likely to have dedicated IT workers in multiple domains (i.e., across LAN, WAN, cloud, and security). Instead, it's more typical to see a lean IT group where one person or team is managing multiple domains.
- **Fragmented and heterogeneous tools.** It's not uncommon to have a fragmented set of multiple tools for managing network and security policies. This "swivel chair" syndrome leads to management inefficiencies while adding complexity, which can impact the performance of the network.
- **Need to simplify.** Compared with larger organizations, midsize enterprises prioritize simplicity in deployment and ongoing management. Investing in a platform approach that can consolidate management across domains can help achieve these goals while aiding in reducing total cost of ownership.
- **Ever-expanding threat landscape.** As organizations look to secure their corporate assets, there are more threats than ever. Challenges range from bad actors infiltrating the network to getting a handle on Internet of Things (IoT) devices and the security vulnerabilities associated with them. Securing the network and the company's corporate assets requires a multipronged approach. One key to success is having natively integrated security capabilities in crucial parts of the network infrastructure.

Trends in Network Transformation

Organizations face numerous challenges in managing a network for a modern, digital business. Fortunately, there are a variety of trends coalescing in the market to help achieve network and digital transformation goals. Key trends include:

- **Embrace of cloud-managed networking.** Managing the network from the cloud has myriad benefits, including being able to centrally manage geographically disparate locations, gaining fast access to new features and functions of the network management software in real time, and eliminating the need to dedicate on-premises infrastructure resources for the management software. As organizations consider a converged approach of centralized management of network and security policies, unified policies across the wired and wireless LAN, or integrated management of the LAN and WAN, a cloud-based platform becomes an ideal deployment method compared with on-premises management.

- **Integration of network and security.** One of the most significant recent trends in networking has been the integration of security capabilities into networking products, particularly in SD-WAN. Having integrated security capabilities in SD-WAN products helps improve the security posture of traffic to and from the cloud while giving customers an opportunity to manage networking and security policies more cohesively. Common security capabilities that are integrated with SD-WAN include threat management, firewall, VPN services, intrusion detection/prevention, and DNS-based filters.

- **Machine learning (ML)- and artificial intelligence (AI)- enhanced automation.** One way to counteract the growing complexity of network operations is to rely on automation platforms that simplify network management. As ML and AI algorithms become integrated in the management plane, network and security policies go from being reactive to proactive, alerting customers about security or performance degradations before they impact users. Advanced automation can also help with simplifying the initial deployment and ongoing optimization of the network using zero touch provisioning (ZTP) principles and self-optimizing capabilities.

- **Convergence across LAN and WAN.** Increasingly, organizations of all sizes are looking for a common network management platform that can span multiple parts of the network stack. Common integrations include across the wired and wireless LAN (e.g., Wi-Fi and access switching) as well as across the LAN and WAN (e.g., campus and branch networks). Having a common management platform that can span these aspects of the network will lead to more efficient operations.

Goals of Network Transformation Initiatives

A primary goal of midmarket companies should be to prioritize a cloud-based management platform so they can address challenges such as the lack of dedicated IT skills, the need to manage fragmented and heterogeneous IT tools, and the need for management efficiencies. Cloud-based platforms are the simplest way to manage policies across multiple domains, such as across the LAN and WAN or across networking and security.

The convergence of networking and security is driving other trends. In *IDC FutureScape: Worldwide Future of Trust 2022 Predictions,* IDC's security research team noted that by 2023, 20% of IT buyers with IT environments that span disparate locations, clouds, remote workers, and devices will have turned to network security as a service to ensure consistent protection. Another prediction noted that by 2023, 55% of organizations will have allocated half of their security budgets to cross-technology ecosystems/platforms designed for rapid consumption and unified security capabilities to drive agile innovation.

By 2023, 20% of IT buyers with IT environments that span disparate locations, clouds, remote workers, and devices will have turned to network security as a service to ensure consistent protection.

The Power of Integrated Network and Security Management

As organizations look to transform their networks to provide secure, predictable access to distributed applications, the need for more integration across networking and security becomes clear. The network is an ideal place to set and enforce security policies, and having converged network and security management facilitates better enforcement of integrated network and security policies.

Integrated networking and security policies are especially important in controlling IoT deployments in the access layer of the LAN and in supporting connectivity to cloud-based resources. From an IoT perspective, integrated management of network and security policies can help organizations understand all the users and devices on the network and provide fine-grained access controls that set which IoT devices and communicate with other devices on the network. Having a centralized, cloud-based platform to inventory devices, set security policies, and alert when policies are broken can become a key strategic benefit.

In the campus and branch, integrated network and security policy management can ensure a zero trust network access (ZTNA) approach, which can be based on user identity. By using LAN device vulnerability scans, DNS-based filtering, and identity-based policy enforcement, users and devices can be set up to have white-list access to business resources. Similarly, in the WAN, converged management of networking and security policies provides centralized, secure access to cloud-based and distributed applications from multiple geographically dispersed sites. Components such as an integrated firewall along with intrusion detection and prevention services and application visibility and control ensure that any traffic going between a business location and the cloud is authorized.

Organizations can achieve other benefits from converged management across the LAN and WAN too. Another recent IDC survey asked organizations what advantages they received from integrated management across SD-WAN and the LAN access layer. Top responses included having centralized creation and enforcement of policies across the LAN and WAN; providing optimized application experiences regardless of device location; and easier deployment and management of the WAN because of integrations with the LAN.

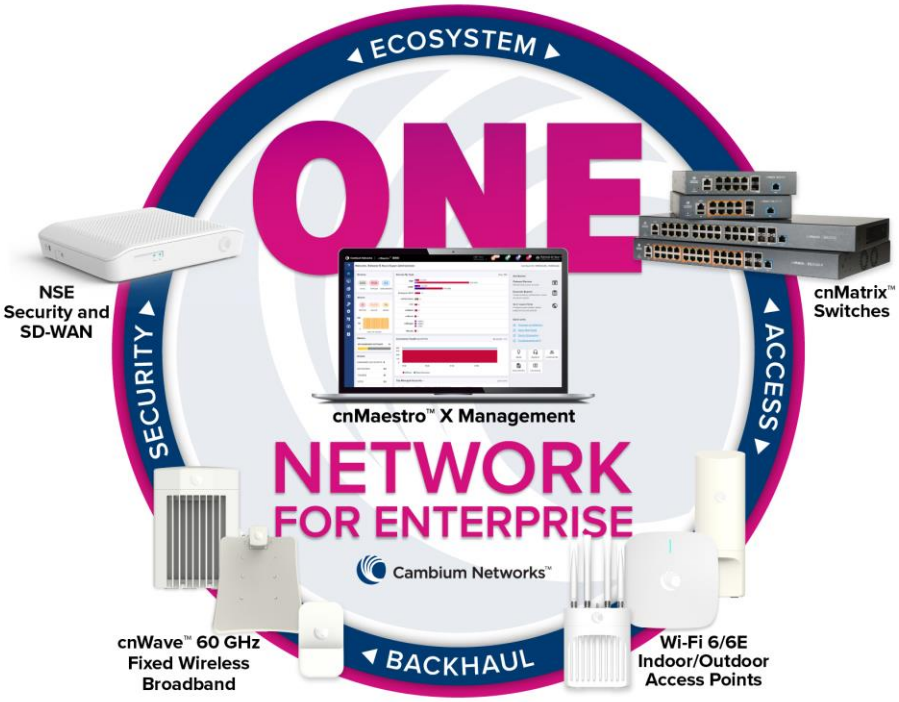
Having converged management across multiple layers of the network and security stack enables many benefits for organizations. It can help improve the security posture of the organization while enabling management efficiencies.

Considering Cambium Networks

Cambium Networks is a network infrastructure vendor with enterprise networking, fixed wireless broadband, outdoor wireless, and small cell backhaul solutions, among others. Within enterprise networking, the company has a robust portfolio of wired and wireless LAN offerings across Wi-Fi and Ethernet switching as well as fixed wireless access. The company also has a cloud-based management platform, cnMaestro X, which provides full life-cycle services, AI-driven automation, and open APIs. New to the company's portfolio is the Network Service Edge (NSE), which combines centralized management of WAN and security functions.

The Network Service Edge is a next-generation SD-WAN and security solution that provides network threat protection via firewall and DNS-based filters, along with VPN services, intrusion detection/prevention, WAN load balancing, and failover. NSE extends Cambium's portfolio across wired and wireless LAN as well as LAN and WAN and networking and security domains (see Figure 2).

FIGURE 2: ***Cambium Secure Converged Network***



Source: Cambium Networks, 2022

Challenges

As organizations look to transform their networks, they will have a range of partners to work with, including Cambium Networks. It will be critical for Cambium to prove the value of its offering in a field of competitive vendors that offer a variety of networking and security services. It's also important for Cambium and its customers to focus on the broader business goals of technology deployments. In many ways, deploying the technology is the easy part; aligning the technology investment with digital transformation goals to ensure value is the hard part.

Conclusion

Digital transformation is causing organizations around the world to understand the need to transform their networks to meet the needs of their digital businesses. IDC recommends midmarket organizations focus on platforms that help converge management of disparate parts of the enterprise network and security policies and ensure consistent and high-quality performance of the network. Doing so will position the network as an enabler rather than an inhibitor of organizational digital transformation goals.

About the Analyst

Brandon Butler, *Research Manager, Enterprise Networks*

Brandon Butler is a Research Manager with IDC's Network Infrastructure group covering Enterprise Networks. His research focuses on market and technology trends, forecasts, and competitive analysis in enterprise campus and branch networks. His coverage includes technologies used in local and wide area networking such as Ethernet switching, routing/SD-WAN, wireless LAN, and enterprise network management platforms.

MESSAGE FROM THE SPONSOR

More About Cambium Networks

There is clear evidence that a converged infrastructure provides tangible benefits for customers deploying networks in support of today's applications and services. Agility, efficiency, and consistency are key buzzwords we hear in working with our customers who are often grappling with limited resources to execute their projects. In practice, these higher level goals translate to capabilities such as automated discovery and configuration during installation, common definition and deployment of policy across a network, consistent reporting of system health and utilization, and coordinated workflows for troubleshooting. Cambium's ONE Network is a platform designed to bring these types of capabilities together in a single framework to more efficiently address the dynamic requirements faced by today's IT teams in supporting their organizations. For more information, visit our web site at www.cambiumnetworks.com.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

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

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.