

White Paper

The Right Tools for the Job: Simplifying Network Transformation for Midsize Organizations

Sponsored by: Aruba, a Hewlett Packard Enterprise company

Brandon Butler
January 2019

EXECUTIVE SUMMARY

Midsize organizations (those with 100-999 employees) are just as eager as larger enterprises to take advantage of the benefits that come with digitally transforming their businesses. Doing so allows them to access new technologies, enable new application use cases, and gain new insights about their business and customers. But organizations of this size face unique challenges when pursuing digital transformation (DX) given their resources compared with larger enterprises. Too often, solutions available to the midmarket either are lower-end products geared at small businesses that don't have the business-class capabilities that midsize organizations require or are targeted at large enterprises, making the solutions prohibitively expensive, and require specialized expertise to operate. This white paper examines the challenges faced by midsize organizations, explores what networking features and functionality are important for these businesses, and analyzes how solutions from Aruba, a Hewlett Packard Enterprise company, provide business-class benefits rightsized for the midmarket.

Today's Midsize Organizations: A Desire for Digital Transformation

A defining characterization of technology innovation over the past decade has been the rise of what IDC calls 3rd Platform technologies. These are centered around the advent and mainstream adoption of cloud computing, pervasive mobile usage, and advanced automation platforms that leverage artificial intelligence. 3rd Platform technologies have graduated from being tested and piloted to now being relied upon to drive business growth around the globe. Organizations of all sizes are looking to embrace DX to advance their businesses, keep pace with and overtake competition, and excite and delight their workforce, customers, and partners. Efficient adoption and use of 3rd Platform technologies enable DX to occur faster and the results to be more fruitful.

The network is a key enabler of 3rd Platform technologies. It is the connectivity layer that facilitates use of 3rd Platform technologies and optimizes their performance. But given the swift rise in demand for these technologies, too often the network has had trouble keeping up with the speed of DX and the rest of the business.

Midsize organizations have unique opportunities and challenges in this environment. They are interested in advancing their digital capabilities in an effort to compete with larger firms and create new business opportunities. As smaller organizations compared with large global enterprises, midsize organizations should be nimbler and more forward leaning in their technology usage. But midsize organizations have distinct difficulties when transforming their networks compared with larger enterprises. There are powerful tools available on the market for enabling digital and network transformation. But like many other 3rd Platform technologies, these tools can be challenging to

deploy and manage. While larger firms may have resources to invest in IT specialists, midsize organizations often prefer to rely on platforms that do the heavy lifting of enabling DX. For many midsize organizations, the right network management platform can become an enabler for 3rd Platform technologies, DX, and business growth and opportunity.

IT Challenges for Midsize Organizations

New technology investments are critically important for this market. The ability to leverage technologies can turn an IT department from operating in a break/fix mentality to becoming a business enabler. There are a handful of challenges that are specific to midsize organizations when it comes to deploying new network technologies:

- **Pervasive mobile devices and increased demand for access technology.** Users within the organization rely on mobile devices more than ever to conduct business-critical tasks, and they each have multiple devices that connect to the network. It's not uncommon for employees to each have a laptop, smartphone, and tablet, for example. WiFi networks and related campus Ethernet technologies are critical components of enabling mobile productivity.
- **Managing geographic sprawl.** Midsize organizations with multiple sites or locations can benefit greatly from centralized IT support and automated management. Relying on manual processes for spinning up and managing day-to-day operations at multiple sites not only is inefficient but also can present security risks. As sites become geographically dispersed or grow in number, these challenges become exponentially more difficult.
- **Organizations relying on cloud-based apps for mission-critical functions more than ever.** Both software-as-a-service (SaaS) and infrastructure-as-a-service (IaaS) platforms have risen in popularity for a range of use cases, from outsourcing IT or colocation facilities to standardizing on customer relationship management (CRM) or enterprise resource planning (ERP) platforms. These technologies have enabled workers to access business apps anytime from wherever they are, but they've also increased pressure for IT departments to supply reliable and secure networks.
- **Devices flooding the networks of midsize organizations.** This includes the proliferation of not just myriad client devices but also video surveillance systems, motion sensors, utility systems, IoT devices, and so forth. These all rely on the network and require organizations to ensure they are properly onboarded, managed, and secured. Doing this manually is untenable for an IT organization already stretched thin.
- **IT staff sizes and budgets under pressure.** In many cases when a business grows, the IT department's budget and staffing remain at the same percentage size of the overall business. This creates a requirement for IT teams to do more with the same or fewer resources as demands for their services increase. Furthermore, traditional network management platforms are not designed to easily scale up in size, functionality, and geographic diversity.
- **Complex, modern systems requiring specialization in products and platforms.** Network management platforms for large enterprises sometimes expect that there are dedicated and trained IT staff managing them, but midsize businesses don't typically have the capacity to employ IT specialists. More likely, midsize IT shops want to use platforms that are easy to deploy and use but that don't sacrifice business-class capabilities.

Goals of a Midsize Organization's Network Management Platform

There is a clear need for network management platforms that meet the specific needs of midsize organizations. They require a network management platform that enables them to support digital transformation efforts while being simple to use for an IT department that may be stretched thin. This simplicity and scalability can't sacrifice business-class features though.

Midsize organizations realize the importance of these technology buying decisions. A recent IDC survey of small and medium-sized businesses found that midsize organizations prioritize hardware purchases as an enabler of their business, with network management tools being among the biggest areas of investment in IT budgets (see Table 1).

TABLE 1

Midsize Organizations' IT Spending Share by Type

	%
Hardware (including network equipment, devices, storage, etc.)	30.7
Software (including applications, PC and OS licenses, app development, excluding salaries)	26.4
IT services (third-party services, maintenance, support, hosting)	22.5
Cloud services (SaaS, IaaS, and PaaS)	20.4

Note: Midsize organizations are those with 100-999 employees.

Source: IDC's *U.S. SMB Survey*, 2018

When making these purchasing decisions for network equipment, midsize organizations have priorities across a handful of key areas, which are discussed in the sections that follow.

Planning and Deployment

An important priority for network management platforms should be ease of use. IT departments of midsize organizations are forced to be generalists who need to manage many technologies simultaneously. For the access layer of the network, including access points (APs) and wired switching, there should be a management platform that is easy to set up and intuitive to use while still having the features and functionality critical for running a business.

Flexibility is a key consideration here. Not all midsize organizations are the same. Some are digital disruptors, eager to invest in and take advantage of 3rd Platform technologies. Other organizations are conservative in their IT management and technology acquisition approach. IT and network management systems should give organizations choices that match their needs, including cloud or on-premises management, controller or controller-less architectures, single-vendor or multivendor infrastructure support, and the ability to be managed independently or by a partner. And an ideal midsize network solution would give businesses the flexibility and investment protection of moving from one topology to another if requirements warrant it, without needing to start from scratch (rip and replace).

From a deployment standpoint, near-zero-touch provisioning of some network equipment is a reality today. Infrastructure such as APs can be unpacked, plugged in, and automatically connected to a cloud-based management platform where all the policy and management settings are configured and centrally managed regardless of office location. This enables nontechnical staff to deploy in remote locations without the need for onsite IT support.

This ease of deployment and management also makes scalability simple. As more resources are needed, capacity can be added by simply installing more APs or switches. Because they're all managed the same way, the same tools can be used for existing and new infrastructure.

Cloud-based network management systems have emerged in the past half a decade to ease management burdens on organizations even as demands on the network grow. These systems provide the ability to easily scale up and have instant access to new features and functionality. IDC data shows that the rate of adoption of cloud-managed wireless LAN (WLAN) systems is growing at more than double that of traditionally managed systems, driven by the ease of use of deploying and managing the network from a cloud-based system.

Management and Automation

One of the greatest advancements in network management functionality in recent years has been the substantial gains in the ability to replace manual tasks with automated processes. While the technology to do so has been around for years, organizations are only now starting to truly embrace the power of automation to manage their networks. For midsize organizations, this can be a game changer. Automation can enable a midsize organization to have the same IT and network capacity of a much larger organization while still staying within the means of the organization. Automation allows midsize organizations to grow and scale as needed and do so in a more predictable and secure way.

Another advantage of automation is the ability to manage multiple networks distributed across different sites from a central location. APs can be spun up with a simple MAC and IP address linking them to a cloud-based platform. Once turned on, the APs automatically receive preconfigured settings related to access policies and firewall rules and reporting.

Meanwhile, network management platforms should also be able to act autonomously if the connection to the cloud fails. Backup management systems within the APs and switches allow users to use the network even if the connection to the cloud-based management platform is severed.

Automation enables the ability to manage multiple networks distributed across different sites from a central location.

Proximity analytics can be very helpful for certain verticals such as the retail sector, allowing businesses to measure foot traffic and guest behavior, plus track those metrics over time for historical analysis. These features can be used to prioritize the layout of a store, analyze conversion rates, plan for staffing levels, and offer customized offers to valued customers.

Optimized Performance

A network is only as good as how it performs. Organizations can spend a large amount of time and resources planning a deployment, configuring optimal settings, and managing operations. But if end users experience inconsistent performance, traffic bottlenecks, or outages, all that planning can be wasted. Network platforms should be able to automatically ensure certain levels of performance and be programmed to dynamically modify the infrastructure settings to ensure all users are getting consistent high-level performance. This can be done in a handful of ways:

- **Matching clients to the best APs.** Smart network systems should automatically send clients' traffic to the best connection point, which may not always be the closest AP. The system should also steer clients to the best band to use (2.4GHz or 5GHz) based on environmental conditions and the applications being used.
- **Auto load balancing across APs.** Similarly, if one AP is experiencing too much of a load, traffic should automatically be directed to other APs for backup before users experience the bottleneck.
- **Providing user- and application-based quality of service (QoS).** APs should be able to ensure a prescribed quality-of-service level for specific users or applications, such as voice, video, or point-of-sale processing.
- **Advanced troubleshooting.** The advent of advanced machine learning tools allows management platforms to learn what normal behavior on the network is, recognize when a problem is happening, and identify the root cause so that the administrator is relieved of the time-consuming task of recreating issues in ever-changing radio frequency (RF) environments. This closed-loop management brings the network one step closer to becoming an autonomous, self-driving network.

Security and Protection

The most important and basic security function is the knowledge of what is happening on your network. With visibility of what's happening, nefarious activity can be spotted and mitigated. Thanks to technology developments from recent years, combined with advanced automation platforms, midsize organizations can have access to the same quality of tools that large global enterprises have access to, with a fraction of the investment.

The key to security visibility is having a platform that is both able to monitor real-time, high-level trends of what's happening and able to have deep, granular insights and historical logs on network vulnerabilities.

The system should be able to identify and mitigate any malware, unauthorized users, or online threats in the network, across both infrastructure and client devices. If a rogue device is detected, it should automatically be quarantined to ensure any nefarious actions do not spread. Two-factor authentication should be standard for client devices.

These rules apply for all organizations, no matter the size. But various industries have specific security issues that are important. For example, any company dealing with consumer payment processing may need a system that adheres to Payment Card Industry (PCI) standards. Healthcare organizations may be required to ensure compliance with HIPAA regulations. Advanced Encryption Standards (AES) may be required for certain government networks or those in finance and public safety deployments.

That visibility must be coupled with best-in-class security features that allow access policies to be created and enforced across the network; URL, content, and web filtering and intrusion prevention, firewall, and deep packet inspection services should be integrated directly into the service to ease operational concerns. Without this integration, midsize organizations must bolt on additional security platforms atop their network management tools, which creates new complexity and performance challenges.

Benefits of a Cloud-Managed System

One of the most important trends in the networking industry in recent years has been the popularity of cloud-based network management systems for wired and wireless LANs, as well as for the wide area network (WAN). IDC estimates that the total number of WLAN deployments that are managed from the cloud will grow from 26% in 2017 to 38% in 2021. While this would still represent a minority of total WLAN deployments, the number could be even higher for midsize organizations, where the advantages of a cloud-managed system could be especially beneficial. Some of the advantages of a cloud-managed network management system are:

IDC estimates that the total number of WLAN deployments that are managed from the cloud will grow from 26% in 2017 to 38% in 2021.

- **Ability to shift from capex to opex.** Cloud-based management platforms allow organizations to shift licensing from a one-time, up-front payment to a recurring monthly, yearly, or multiyear model.
- **Reduced management of on-premises hardware.** By using a cloud-based system, a business no longer has to purchase, deploy, and manage hardware the management software runs on; instead, the network management software is delivered as a service from the cloud.
- **Ease of deployment and day 2 management.** Cloud-based network management systems can be spun up and managed through online portals, helping IT teams shift from focusing on tactical, mundane tasks to focusing on strategic business enablement projects.
- **Integrated management of campus and branch.** Centrally managing the campus network and connections to branch offices provides advantages around centralized visibility, policy setting, monitoring, and security across the LAN and WAN.
- **Faster access to new features and functionality.** New features are accessible from cloud-based management systems as soon as the service provider or networking vendor makes them available to customers. This is opposed to an on-premises platform where IT must allocate time multiple times per year to apply updates.
- **Centralized control and visibility.** An inherent benefit of cloud-based management platforms is that network infrastructure is centrally controlled, creating an aggregation point for visibility and analytics.
- **Dynamic scalability.** Adding capacity to this system becomes as simple as adding infrastructure components, such as APs, without having to worry about scaling the back-end management system.

ADVICE FOR TECHNOLOGY BUYERS

Midsize organizations should strongly consider the ways in which 3rd Platform technologies can help digitally transform their business, if they haven't yet done so. A critical enabler of these DX initiatives is having a network that can execute and optimize these efforts. The fruits of these efforts can be seen in multiple ways:

- **Improved customer experience.** Customers and partners expect a certain level of network performance when they interact with the business. A reliable and secure WiFi environment that provides consistent performance is a baseline. Promotional campaigns based off location services can be used to target customers who return to retail stores, for example. Digital signage can be used to customize messaging to customers or partners.

- **Improved workforce performance and pride.** It's not just customers who can be delighted by technology. Workers within an organization don't just rely on reliable network connections to do their jobs, but they can be delighted by the ease of use and simplicity of the system. Network management and security software that automatically identifies, authenticates, and enables user-based access policies is intuitive to use and provides a frictionless experience for employees.
- **Growing with the business.** As small companies grow into midsize organizations and midmarket groups transition to larger enterprises, the demands on the IT team will only continue to grow. This requires IT teams to rely more on automation practices to provide the same or better levels of service. A cloud-based network management platform provides opportunities to easily scale up and add resources and centrally manage a distributed environment, and it future proofs the network for whatever changes may come.
- **Increased revenue opportunities.** These advancements can be beneficial to teams beyond just IT. Think about marketing departments that can use targeted campaigns using WiFi location apps to impress guests. Operations teams can track assets using Bluetooth to ensure no lost orders or inventory. Finance teams can use IoT services to dynamically modify pricing to link supply with demand. Having a network management platform that enables mobile workforces, provides connectivity to cloud-based applications, and can be managed in less time than traditional systems frees up time for the IT department to focus on higher-value tasks, as opposed to just struggling to keep up with the basic technology demands of the business.

ARUBA'S CLOUD-MANAGED NETWORKING FOR MIDSIZE ORGANIZATIONS

Aruba has a range of offerings optimized for midsize organizations. The company offers both infrastructure and management tools, including integrated wired and wireless LAN and WAN controls and a series of value-added services that run atop them.

Aruba switches, SD-WAN gateways, and Instant APs at any location can be managed centrally through the company's Aruba Central cloud-based management platform. In addition, Aruba Central provides Guest WiFi, Presence Analytics, and Connectivity Analytics designed to customize, automate, and secure guest onboarding; quickly resolve client connectivity issues; and track valuable user behavior. Instant APs are capable of streamlined zero-touch provisioning and come with a built-in redundant architecture to provide continuous operation and management despite WAN or service provider link failure. ArubaOS and the infrastructure and management systems include built-in security, wireless intrusion detection, and application and web filtering, along with built-in firewalls and role-based access. They include REST APIs for integrating the system with third-party monitoring systems, customer-specific applications, CRM databases, and so forth. Further, Aruba's flexible architecture allows organizations to easily shift from cloud-based to on-premises-based management without the need to replace APs or switches.

Aruba's full range of infrastructure hardware is performance optimized with options that meet varying budgetary requirements. Aruba's customers are able to leverage the company's extensive network of partners to assist with the planning, implementation, and ongoing management of their networks.

CUSTOMER CASE STUDY

During the past five years, a midsize retail fitness business in the Tri-state area of New York has decided to embrace new technologies in order to enable growth of the company, more easily manage distributed operations, and improve the security footprint of the company. This technology-first attitude resulted in this company using cloud computing services wherever possible. This includes not only outsourcing away from a managed service infrastructure environment to the infrastructure-as-a-service public cloud but also upgrading its network management to the cloud. The business operates in more than 75 locations, all managed from the company's moderate, but growing, corporate headquarters, which is where a lean but efficient centralized IT staff controls all IT operations.

Each site has somewhere from 5 to 12 Aruba Instant APs, each one connected to the cloud-based Aruba Central management platform. For IT personnel who are overseeing multiple IT projects and sites, this has been a game changer. In the past, rolling out new sites used to take weeks of planning and involve onsite IT staff to configure. With Instant APs, however, setting up a new site is as easy as shipping APs to the site and plugging them in. New APs automatically receive preconfigured settings from the cloud-based platform and are linked with the rest of the distributed system. With the new site onboarded, the IT staff is now able to manage all the APs across the company's entire distributed network from the Aruba Central platform. Whereas in the past firmware and software updates required logging in to each site individually to push the new features, Aruba Central now centrally manages automatic updates across all sites.

With this network management platform, new features and functionality are available as soon as Aruba makes them available, and they can be automatically pushed to devices across the company's many sites. Meanwhile, the APs integrate with the company's multivendor IT environment in other aspects of the shop: Switches are combined from Aruba and other vendors, the website membership platform is hosted in the cloud, and a PBX system is under IT control too.

The decision to embrace new technology is one that was made by this forward-leaning firm at a corporate level. Technology is seen as a way to not only improve operations management but also to allow the network to keep up with the speed of the business' growth. Aruba Central is designed for organizations that may not have IT staff dedicated to managing wireless networks but still want business-class features.

The decision to embrace new technology is one that was made by this forward-leaning midsize business at a corporate level.

CHALLENGES AND OPPORTUNITIES FOR ARUBA

Like many vendors that target midsize businesses, Aruba needs to educate customer prospects about its products. Often midsize organizations are confused as to whether a simple system aimed at the lower end of the market will fit their needs or are perplexed by the challenges of deploying systems meant for organizations with much larger IT staff with distinct specializations. While Aruba is a leading player in the WLAN and wired markets with solutions specifically tailored to the needs of midsize businesses, it does face challenges from a range of other vendors that also target the midmarket. Aruba's opportunity lies in highlighting the distinct advantages of the company's network management and security platforms for this critical segment of the market.

CONCLUSION

Network transformation is a key priority for organizations of all sizes. But midsize organizations have unique challenges in terms of what they need from their network and how they manage it. Network platforms and management solutions that not only are easy to deploy for midsize IT organizations but also provide the business-class features of higher-end solutions can be a key enabler of digital transformation efforts and create new opportunities.

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

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 2019 IDC. Reproduction without written permission is completely forbidden.

