3 Research from Gartner Survey Analysis: Address Security and Digital Concerns to Maintain Rapid SD-WAN Growth

12 About Fortinet

Fortinet Secure SD-WAN: Best-of-Breed NGFW and SD-WAN in a Single Offering

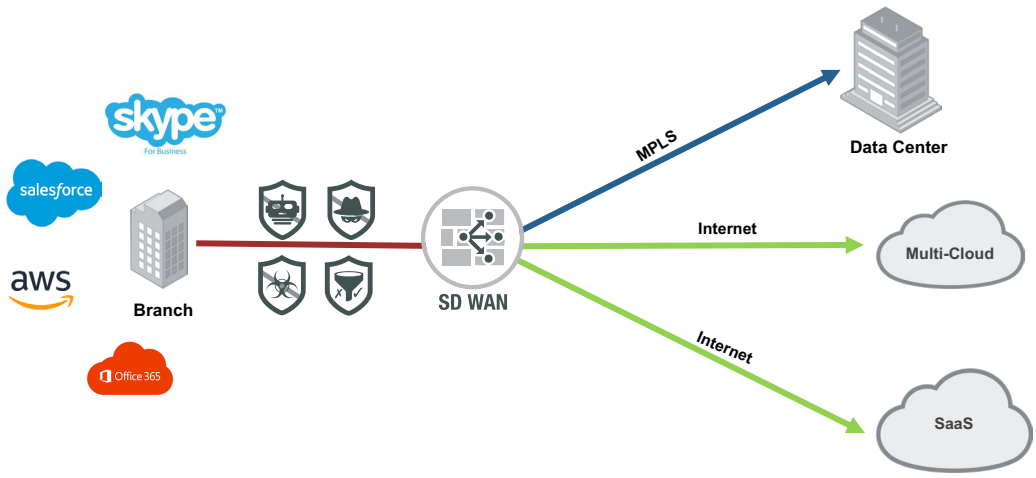
Digital Transformation at Enterprise Branches

Most organizations are in the midst of some form of digital transformation—which includes adopting more cloud services to deliver better value to customers. But digital initiatives without WAN transformation also bring complexity. This can lead to potential performance issues, especially at enterprise branch locations. Given these realities, it is no wonder that software-defined wide-area network (SD-WAN) technology is rapidly becoming a mainstream solution.

Why Integrated NGFW Is Critical for SD-WAN

SD-WAN technology enables direct internet connectivity from the branch for more efficient access to the cloud and Software-as-a-Service (SaaS) applications. Though it helps to move the business to the next level, SD-WAN also expands the network attack surface and exposes enterprise branches to significant risk. This is why every SD-WAN offering must include next-generation firewall (NGFW) protection for successful WAN edge transformation.

In a recent Fortinet Threat Landscape Report, the typical organization saw 20 cyberattack-related intrusions, with four of those resulting in breaches that caused damage (data loss, downtime, or a compliance issue).[1] The majority of these were advanced threats, designed to bypass conventional security measures. In these instances, a stateful firewall cannot provide sufficient protection.



[1] "Quarterly Threat Landscape Report: Q3 2018," Fortinet, November 2018.

Fortinet Secure SD-WAN

Fortinet is the first NGFW vendor to provide native SD-WAN capabilities, which include an application-aware WAN path controller. Over 360,000 customers have already deployed FortiGate NGFWs. With a simple software upgrade, these solutions can leverage best-of-breed SD-WAN capabilities. In the same offering, customers can now enable advanced security features such as intrusion prevention (IPS), web filtering, SSL inspection, anti-malware, and many more features—all of which are organically developed and validated.

Gartner Survey: Security Is the Biggest WAN Concern

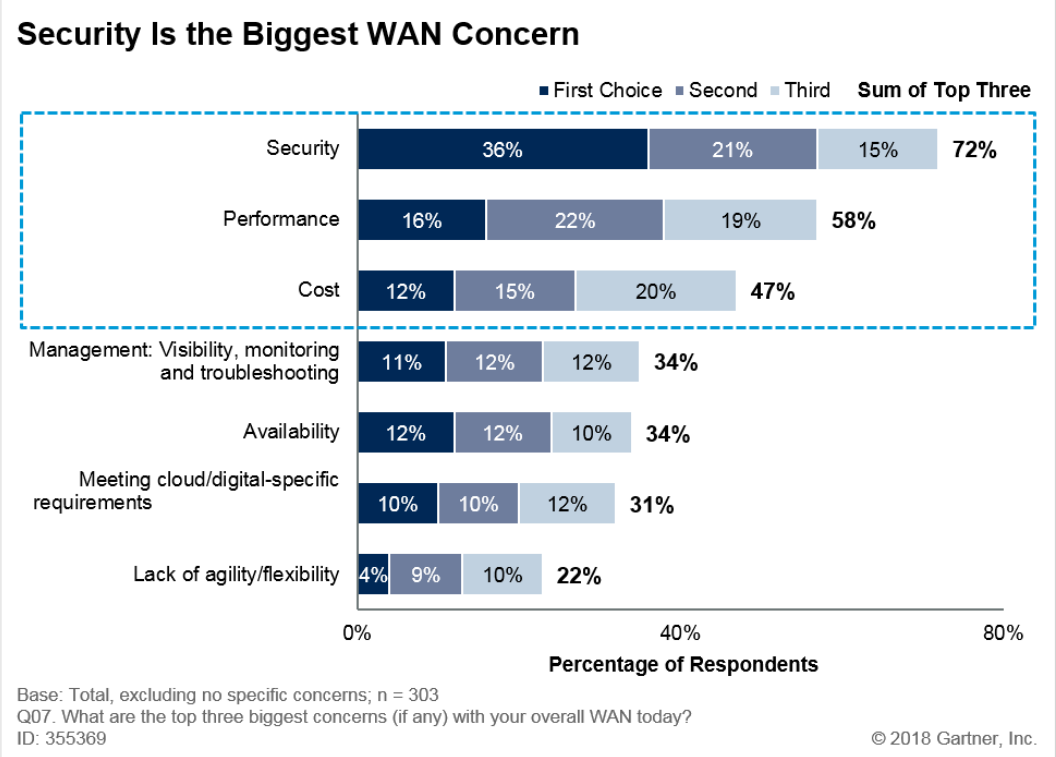
In the following Gartner research note, results presented are based on a Gartner study conducted to further understand the changing trends and adoption behavior of new disruptive technologies that are impacting WAN vendors and customers. The research was conducted from 31 October through 11 December 2017 among 305 respondents located in the U.S., the U.K., Germany, China, India, Colombia and Argentina. The interviews were conducted both online in a native language.

Qualified respondents participate in strategic decisions in WAN at their organizations and have 25 or more WAN locations globally.

The survey was developed collaboratively by a team of Gartner analysts who follow enterprise networking. The survey focused on data center networking, Ethernet fabric, software-defined networking, white-box and brite-box Ethernet switches, and other emerging data networking technologies for the data center and enterprise market and management group. It was reviewed, tested and administered by Gartner's Research Data and Analytics team.

Source: Fortinet

FIGURE 2 Security Is the Biggest WAN Concern



Source: Gartner (November 2018)

Research from Gartner

Survey Analysis: Address Security and Digital Concerns to Maintain Rapid SD-WAN Growth

As users transform their WAN, there are significant opportunities for equipment providers. However, SD-WAN technology product managers are challenged to deliver offerings that address buyer concerns with secure, cost-effective cloud connectivity and alignment with digital applications such as IoT.

Key Findings

- Security is users' top concern about their wide-area networks (WANs). This is followed by network performance and increasing costs.
- Digital business applications are bringing into the limelight requirements such as hybrid security architecture and more versatile wireless capabilities.
- WAN optimization remains not only relevant, but very important for customers as they transform their WAN. It not only can mitigate WAN performance challenges, but also help contain bandwidth growth and, hence, costs.

Recommendations

WAN technology product managers looking to take share in these high-growth agile infrastructure opportunities must:

- Differentiate from the fragmented security vendor landscape by delivering cost-effective, integrated dynamic threat protection across cloud connections at various points of aggregation, access and gateways.
- Attract enterprise buyers by aligning the network automation, and application-level security and quality of service (QoS) capabilities of their WAN edge solution to the specific needs of business-critical cloud and digital applications, including industrial Internet of Things (IoT) use cases.
- Address the WAN optimization needs of an increasingly hybrid data center environment by offering a suitable combination of software-defined (SD)-WAN and targeted simple WAN optimization functionalities in their WAN-edge platform.

Survey Objective

The key objective of this survey[1] was to track and assess how trends, including web 2.0, IoT and big data, are impacting adoption of new disruptive WAN technologies and, consequently, the supporting ecosystem.

Data Insights

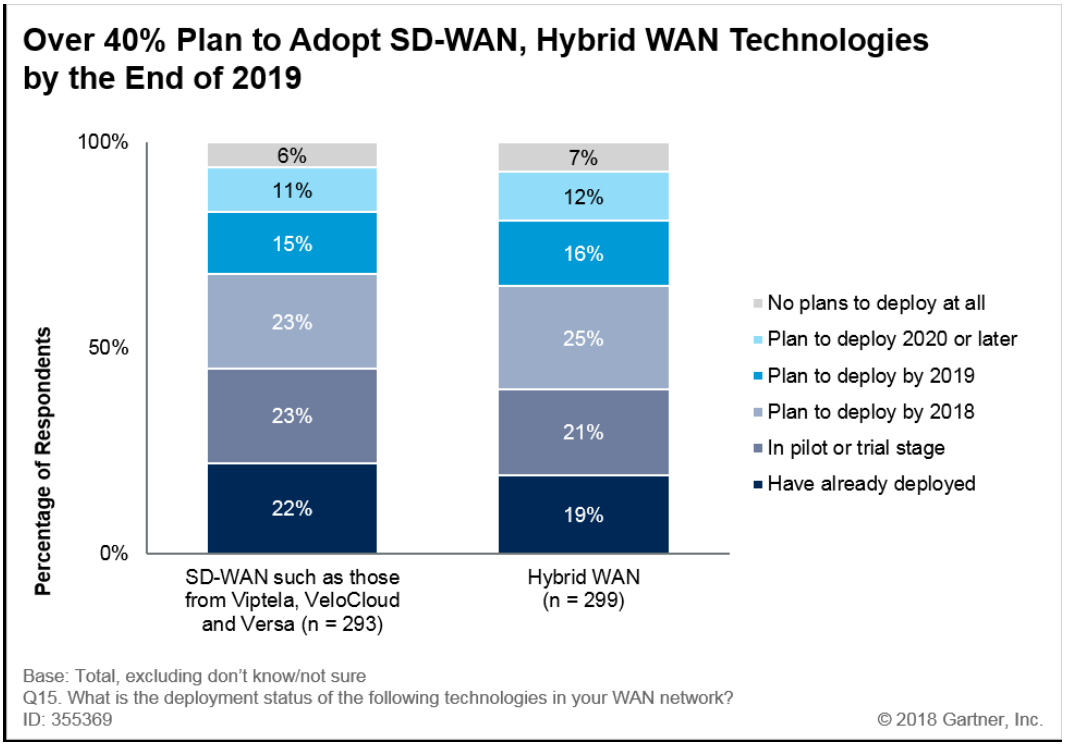
Introduction

Gartner has received over 1,400 client inquiries on the topic of SD-WAN alone in the last 12 months. From this number, and the market trends we see in the WAN equipment market, it is evident there has been a striking increase in adoption and expansion of usage of new WAN technologies disrupting legacy routers and WAN optimization.

Figure 1 depicts the adoption stage and plans for different, relatively new WAN technologies that the WAN managers indicated in their survey response. Clearly, there is significant latent demand for transforming their existing WAN.

According to our latest forecast, end-user spending on SD-WAN is expected to grow from $475 million in 2017 to $2.32 billion by 2022, at a five-year compound annual growth rate of 37.4%. The demand for hybrid WAN and SD-WAN has already been anticipated for some time, which also explains the crowded vendor landscape trying to compete in this space today. New offerings that focus on these new capabilities threaten to replace the lion's share of the router installed base. Existing router vendors (for example, Cisco and Juniper Networks) have already been pushed to acquire such products and also upgrade their existing router platforms incorporating some or most of the new requirements. Meanwhile, incumbent vendors from adjacent markets such as unified threat management (for example, Fortinet and Forcepoint), WAN optimization (for example, Riverbed and Silver Peak) and network virtualization (for example, VMware) have entered the market through internal development and

FIGURE 1 Over 40% Plan to Adopt SD-WAN, Hybrid WAN Technologies by the End of 2019



Source: Gartner (November 2018)

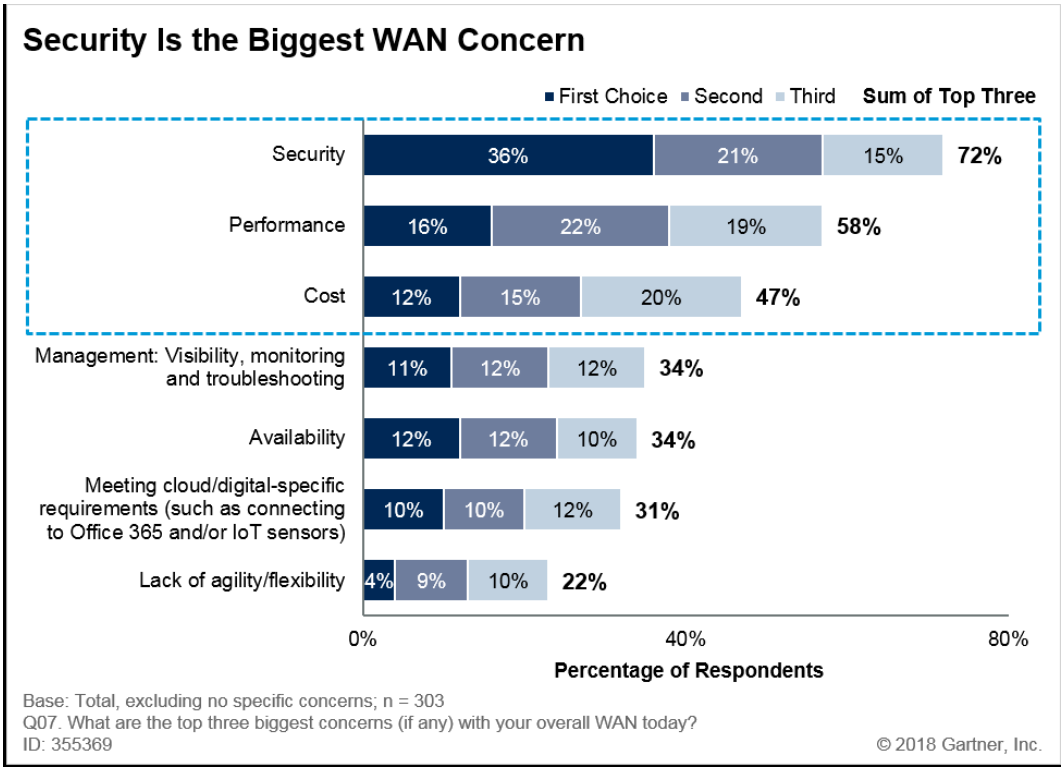
acquisition. Additionally, there are pure-play startups such as CloudGenix. However, technology providers need to better understand the user challenges and requirements to plan their products to differentiate themselves in this highly competitive market. This research provides some key insights that will help technology product managers to do so.

Security Is the Top WAN Concern

Customers continue to strive for better WAN performance and visibility, but security now tops their priorities when it comes to the challenges with their WAN. In fact, 72% of the respondents said that security was their topmost concern when it comes to their WAN (see Figure 1). Customers are increasingly breaking out their internet direct from the branch to have more efficient connections to the cloud. While this improves performance by reducing network latencies and traffic congestion, it also raises security concerns and the chief information security officer has to be involved for a smooth transition from centralized security gateways.

As enterprises try to address the security concerns, while moving to internet breakouts in the branches, technology and service provider (TSP) product managers have to make sure that they include the capabilities to address users' key WAN security concerns. The growing importance of security in WAN considerations also points to the urgency required by WAN equipment vendors to increase their security capabilities and features. Either they have to add more advanced security capabilities, or forge strong partnerships with well-known security vendors to address the customer requirements. Currently, most SD-WAN vendors support basic capabilities such as stateful firewalling and VPN; however, they lack and, hence, depend on security partners for, advanced functionalities such as, intrusion prevention system, malware analysis and sandboxing. The move by security vendors such as Fortinet to

FIGURE 2 Security Is the Biggest WAN Concern



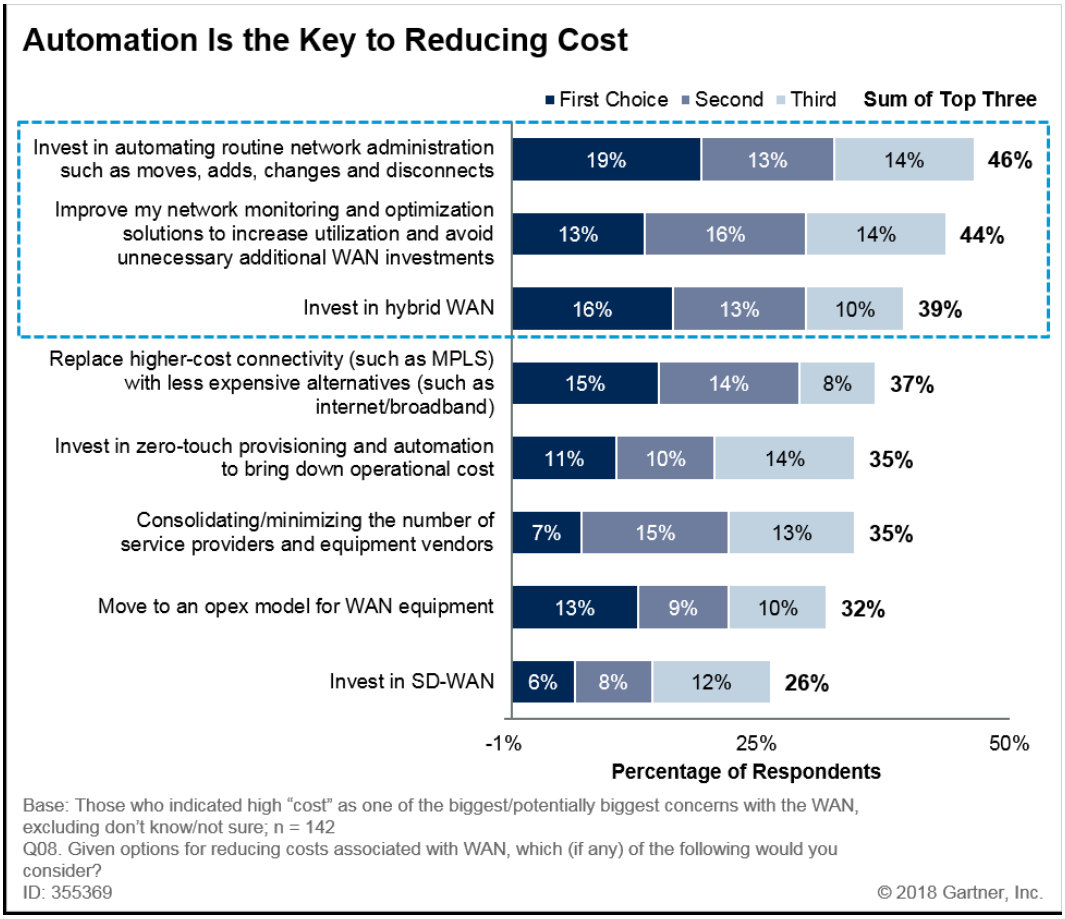
Source: Gartner (November 2018)

address the SD-WAN requirements also indicates the threat from security vendors. On the other hand, security vendors such as Fortinet that are increasingly interested in the WAN opportunity must understand that network performance and costs also still remain users' top concerns. This means that users also need uncompromised WAN capabilities and advanced SD-WAN functionalities that are critical for network agility and cost optimization. So, security vendors will need to greatly enhance their routing and other WAN functionalities to compete in the market.

One of the key propositions of SD-WAN has been to reduce the overall WAN costs by Multiprotocol Label Switching (MPLS) substitution with internet. Although this may be a valid justification in several cases, the equation is not so straightforward, and the discussion needs to shift from tactical to the strategic. This is borne out by the changing perception of users as depicted in Figure 3 — Users are looking for other options than just bandwidth savings for their cost-reduction goals. It is imperative that technology product managers put more focus on the operational cost savings and the far-reaching business benefits that automation and WAN performance optimization can bring to the organization.

As suggested in Figure 4, users intend to invest most significantly on strengthening their advanced threat protection capabilities in both their data centers and branch internet breakout points. However, it is interesting that 34% would also consider using a cloud-based security solution (for example, Zscaler) or a hybrid mix of on-premises and cloud implementation (for example, Palo Alto Networks) as an option for addressing their branch security requirements. This means that customers are increasingly willing to look at alternative options rather than using traditional firewalls and unified threat management.

FIGURE 3 Automation Is the Key to Reducing Cost



opex = operating expenditure
Source: Gartner (November 2018)

Recommendations

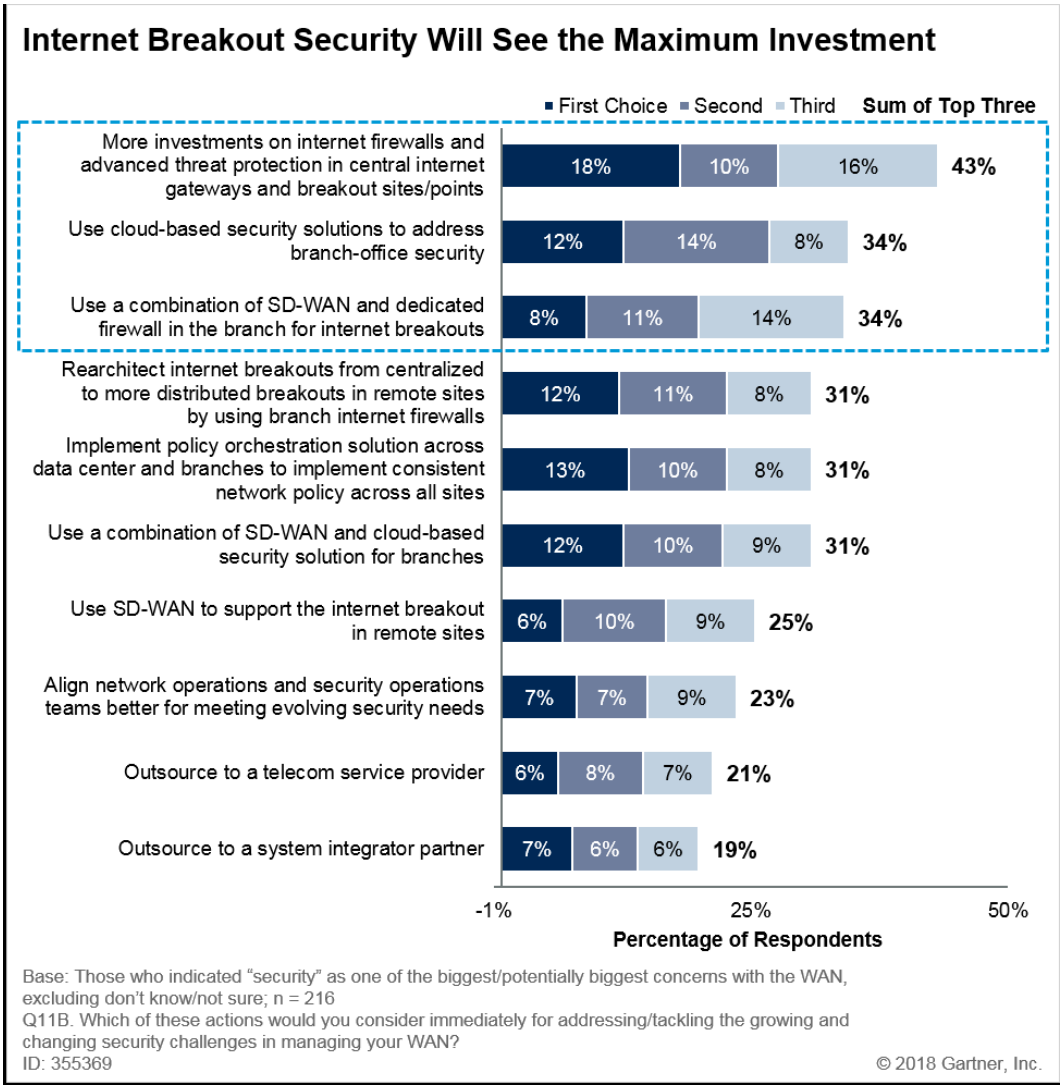
Technology product managers of TSP organizations in the WAN space must:

- Differentiate from the fragmented security vendor landscape by delivering integrated and dynamic threat protection for multiple cloud connections at both the cloud's edge and the customer's internet/WAN gateway points. This could also help to address customer concerns about growing security budgets.
- Enable ease of use and greater choice by providing a full range of flexible deployment models, including both cloud-based and on-premises controllers, remotely accessible management platform and managed/as-a-service offerings.
- Shift the discussion about cost reduction from MPLS substitution, to the network team's greater agility and the operational cost savings that automation can bring.

Cloud and Digital Initiatives Bring New Challenges and Opportunities

As organizations embrace cloud and look to implement multiple digital applications using technologies such as artificial intelligence (AI) and IoT, it is becoming clear that they need a hybrid strategy involving services executed in the cloud and at the edge. From a WAN perspective, customers anticipate several upcoming challenges.

FIGURE 4 Internet Breakout Security Will See the Maximum Investment

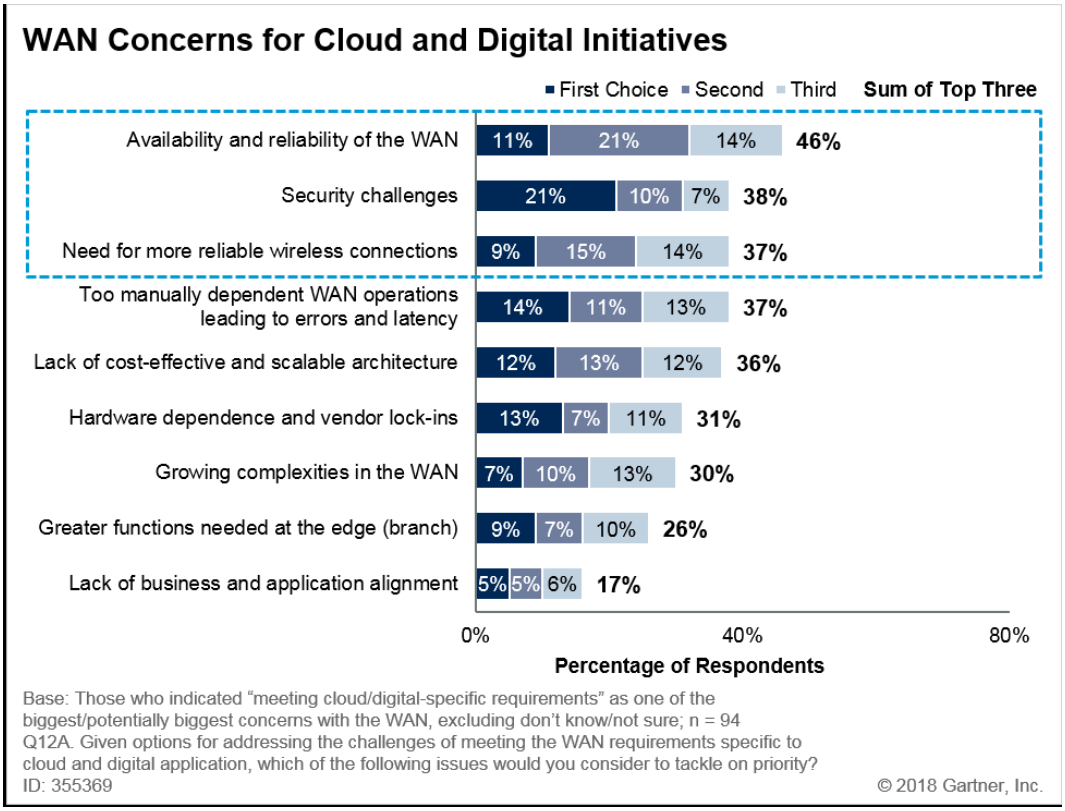


Source: Gartner (November 2018)

Their top concern about connectivity for digital applications is the availability and reliability of the WAN (see Figure 5). This is followed by the security challenges involved in protecting the information and other assets in multiple locations — which, increasingly, will be significantly distributed in some very physical remote locations as well. Wireless connectivity is, obviously, in major demand as a result, and in far, remote locations even satellite links are common. Here, users are very concerned about the reliability of the wireless connectivity to meet the operational requirements of the digital applications — not to mention the heightened security threat perception in that context.

It is not surprising that WAN availability and reliability are a big concern for digital applications, as these involve edge locations where WAN connectivity options may be limited and the WAN performance in those connections is often challenged. This challenge is only likely to increase as users look to internet connectivity in remote sites involving not just 4G, but also 3G mobile

FIGURE 5 WAN Concerns About Cloud and Digital Initiatives

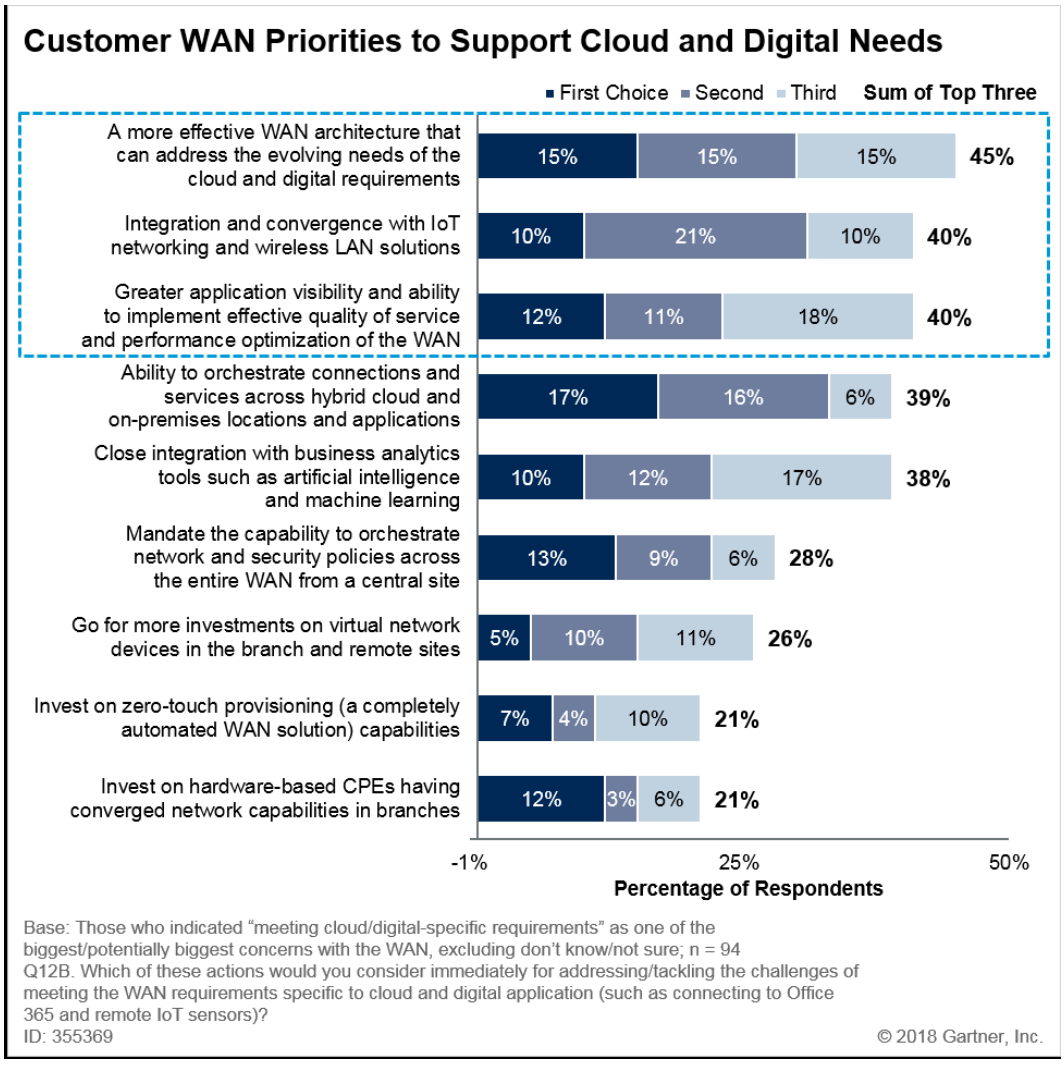


Source: Gartner (November 2018)

connections. Poor internet, especially wireless, typically leads to higher packet loss, and poor latency and jitter conditions, something any WAN solution needs to correct with techniques such as forwarding error correction and packet replication. Lack of SLAs provided by internet service providers in such remote internet connections is a big challenge as well. In such situations, SD-WAN can help in achieving better experience through its hybrid WAN architecture and dynamic path selection. Over-the-top backbone networks such as Aryaka and Cato Networks, and virtualized services such as VeloCloud gateways can help improve the cloud connectivity, too. Also, by operating the network based on business-aligned policies, SD-WAN can effectively support the implementation of cloud and digital applications. This is apart from enhanced security that they provide in the case of local internet breakouts.

WAN equipment providers that do not yet have a wireless WAN option in their WAN equipment must urgently address this requirement. Apart from having wireless access options on their customer premises equipment (CPE), they must ensure a well-integrated wireless functionality that is highly secured. It also requires deep level access to live conditions of multiple radio frequency links to effectively steer traffic between wired and wireless, and also between varying radio links. And the wireless options could be from a wide range of wireless technologies, including 3G/4G/5G cellular wireless connections, Wi-Fi, LoRa, and even point-to-point wireless technologies running on licensed private frequencies. Providing a consistent experience despite such variance in network connection characteristics of the different media used will be a key criteria.

FIGURE 6 Customer WAN Priorities to Support Cloud and Digital Needs



Source: Gartner (November 2018)

Figure 6 shows the actions that users anticipate they will take in their WAN to address their digital needs. Foremost of all, it is becoming clear that traditional WAN architectures are not good for the new traffic patterns involved, and the complex connectivity and network services required by digital applications. Although such applications most often reside in the cloud, many of them also need access to compute and store data at the edge. Securing the edge location becomes paramount as well. This is only possible by evolving to a more distributed WAN architecture that can dynamically orchestrate connectivity and services effectively across multiple locations, and using multiple connectivity options and different types of CPEs (both physical and virtual).

Users also see a need for WAN solutions that effectively integrate with local wireless LANs in the branch and IoT applications being deployed. This means an opportunity of convergence and deeper integration between the WAN and LAN platforms used in the branches. Some vendors such as Cisco and Hewlett Packard Enterprise (Aruba) already offer wireless LAN interfaces; however, truly unified functionalities and "single plane of glass" for management are still lacking. The current converged solutions are typically to meet

tactical needs of specific customers, including small and midsize businesses. However, a larger and more strategic approach is needed to address customers' digital requirements. Hence, it is imperative for technology product managers to push for closer integrations that can offer easier management, which could be internal or third-party-based.

Recommendations

Technology product managers of TSP organizations in the WAN space must:

- Attract C-level and business interest for their solution by aligning their functionalities such as WAN automation and dynamic QoS to successfully embed into relevant digital solutions such as specific vertical IoT solutions or customer engagement machine learning (ML) use case.
- Differentiate their solutions by providing both technically and commercially easy and effective migration roadmaps to their customers as they start embracing new WAN architectures to address the distributed compute and data needs of new digital applications.
- Enable greater agility, flexibility and closer business alignment by providing service chaining capabilities and integration with other external and third-party automation tools. Such tools include software-defined network controllers, cloud management platforms, service integration/assurance platforms, intent-based network platforms and network orchestrators.
- Combine with data center microsegmentation and network policy orchestration platforms to deliver the strict network isolation and zoning that is critically required as the IT and operational technology platforms increasingly converge at the edge.
- Incorporate advanced analytics using AI and ML to enhance the automation functionalities and troubleshooting capabilities.

WAN Optimization Still Important for Customers Looking to Improve Network Performance

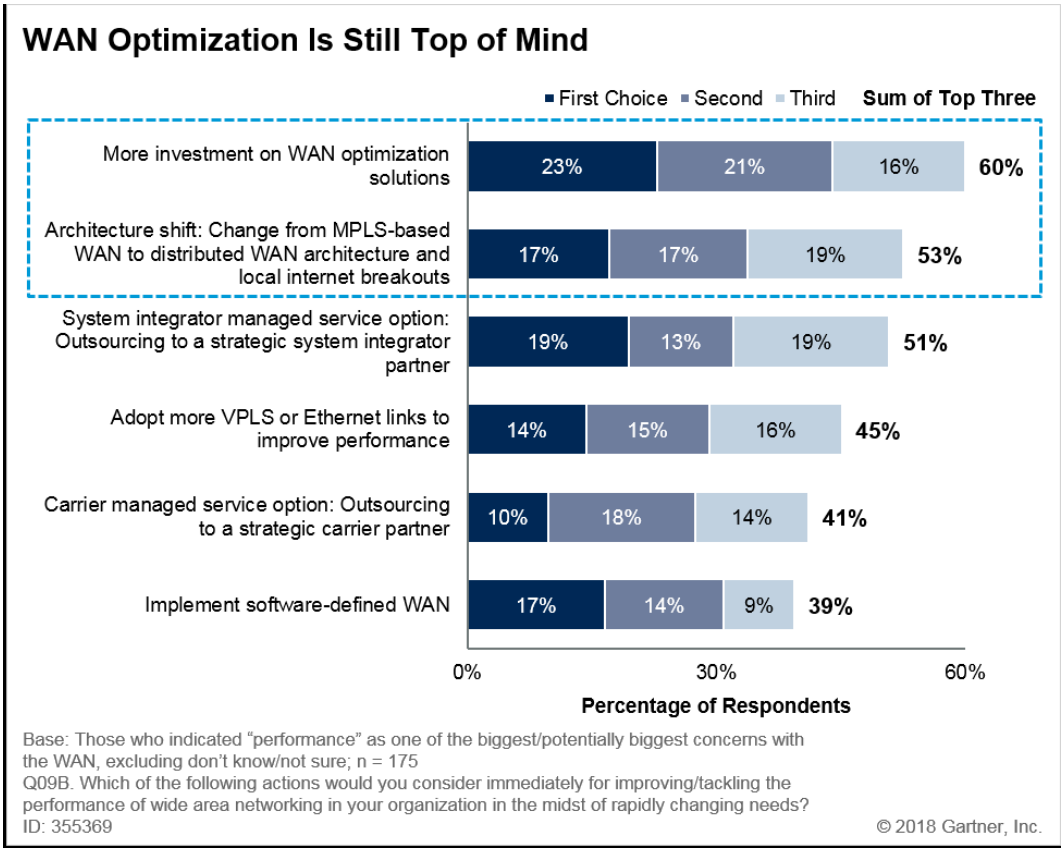
As enterprises increase their adoption of public-cloud-based software-as-a-service applications such as Office 365 and Force.com, many customers reported mixed results from employing traditional WAN optimization technologies from vendors such as Riverbed and Silver Peak. However, our survey indicates that WAN optimization capabilities are still very important for customers. The response in our survey (see Figure 7) points to a strong need felt for WAN optimization technologies. Customers still see network performance as a major concern, coming in at No. 2 in the top WAN concerns (as shown in Figure 2). However, the new application architectures and deployment models will require different techniques and deployment options of their WAN optimization solution to address the new optimization needs. Also, we see the need for tight integration with other WAN edge solutions such as SD-WAN to jointly process the traffic, and implement rules and share information. Based on inquiries, it is important to point out that SD-WAN users often go for higher bandwidth to address the inherent network issues of the internet such as packet loss. But, where affordable internet is not available, it is worth pointing out that users do not need all of the WAN optimization functionalities. They typically need specific, but relevant, WAN optimization capabilities such as HTTP/Secure Sockets Layer optimization, compression and deduplication.

Recommendations

Technology product managers of TSP organizations in the WAN space must:

- Revitalize the important role and relevance of WAN optimization functionality by bringing innovations that align with the specific needs of cloud applications. This can be, for example, by looking at techniques that use asymmetric deployment options. Or it could be via API integration with the cloud-based application or platform.
- Leverage WAN optimization capabilities as a key differentiator for their offerings, while competing with vendors that lack functionalities or/and experience in WAN optimization.
- Fill their functionality gap by quickly acquiring WAN optimization capabilities or establishing deep integration with WAN optimization controllers from partners that still do not have SD-WAN.

FIGURE 7 WAN Optimization Is Still Top of Mind



Source: Gartner (November 2018)

Methodology

Results presented are based on a Gartner study conducted to further understand the changing trends and adoption behavior of new disruptive technologies that are impacting WAN vendors and customers. The research was conducted from 31 October through 11 December 2017 among 305 respondents located in the U.S., the U.K., Germany, China, India, Colombia and Argentina. The interviews were conducted both online in a native language.

Qualified respondents participate in strategic decisions in WAN at their organizations and have 25 or more WAN locations globally.

The survey was developed collaboratively by a team of Gartner analysts who follow enterprise networking. The survey focused on data center networking, Ethernet fabric, software-defined networking, white-box and brite-box Ethernet switches, and other emerging data networking technologies for the data center and enterprise market and management group. It was reviewed, tested and administered by Gartner's Research Data and Analytics team.

Additional Research Contribution and Review

Kanwarpreet Oberoi

Evidence

[1] WAN Disruption and Transformation Survey conducted by Gartner in December 2017 to January 2018.

[2] Customer inquiries received by the author and his co-analysts of the networking and communications team in 2017 and 2018.

Source: Gartner Research Note G00355369, Naresh Singh, 12 November 2018

About Fortinet

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network - today and into the future. Only the Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud or mobile environments. Fortinet ranks #1 in the most security appliances shipped worldwide and more than 375,000 customers trust Fortinet to protect their businesses. Learn more at http://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

Share your thoughts with us and others about the report on social media. Use the hashtags #SDWAN, #Fortinet or connect with us online at Fortinet Twitter, Fortinet LinkedIn, Fortinet Facebook.

US Headquarters
899 Kifer Road
Sunnyvale, CA 94086
USA

Tel: +1-408-235-7700
Fax: +1-408-235-7737

www.fortinet.com