

## The Source Code

### V112 - SD-WAN Primer

There has been a lot of discussion about the emerging SD-WAN market and in particular how it is benefiting network security companies, including Fortinet, Palo Alto Networks, and Zscaler. We find that many investors struggle to understand exactly how the technology works, where it is deployed, and what the overall market opportunity is. This issue of The Source Code is aimed at framing out the market in an easy-to-understand manner.

- **What is SD-WAN?** It stands for software defined wide-area network, and it uses an intelligent software layer to control the routing of data across the internet.
- **Replacing \$25B of MPLS spend.** Today, companies spend upwards of \$25 billion on dedicated connections between locations called MPLS. Often they are used to route traffic back to the core data center before hitting the internet for security reasons. But the combination of cloud security offerings from companies like Zscaler is allowing much of that traffic to go directly to the internet, and what remains that must go back to headquarters can now utilize SD-WAN solutions. We do not expect SD-WAN to be a \$25B market, but even at a discount to that level it is a compelling market.
- **SD-WAN is still in the early stages.** Only 35% of enterprises have SD-WAN implementations currently, according to Gartner, and that is projected to grow to 60% by 2024 with tailwind from cloud applications. We see the rise in voice and video delivered content, MPLS costs, and potential for increasing company locations to support the desire for more socially distanced workforces, to all play into the hands of SD-WAN vendors.
- **Dedicated SD-WAN vs Network Security vs Cloud Vendors.** The market is unfolding along three lines. You have vendors like HPE (Silver Peak) and Citrix that offer standalone SD-WAN solutions versus network security companies like Fortinet (FTNT/N) and Palo Alto Networks (PANW/N) offering solutions that are either installed on their firewalls or offered in the cloud. Lastly, there are cloud vendors like Zscaler (ZS/OW) and Cloudflare (NET/OW) that can route customer traffic through their security clouds without the need to buy or manage on premise hardware.

#### Software Technology

##### Sterling Auty, CFA <sup>AC</sup>

(1-212) 622-6389

sterling.auty@jpmorgan.com

Bloomberg JPMA AUTY <GO>

##### Matthew Parron

(1-212) 622-0155

matthew.parron@jpmorgan.com

##### Jackson E Ader, CFA

(1-212) 622-4863

jackson.e.ader@jpmorgan.com

##### Drew E Glaeser

(1-212) 622-8020

drew.e.glaeser@jpmchase.com

J.P. Morgan Securities LLC



#### See page 26 for analyst certification and important disclosures.

J.P. Morgan does and seeks to do business with companies covered in its research reports. As a result, investors should be aware that the firm may have a conflict of interest that could affect the objectivity of this report. Investors should consider this report as only a single factor in making their investment decision.

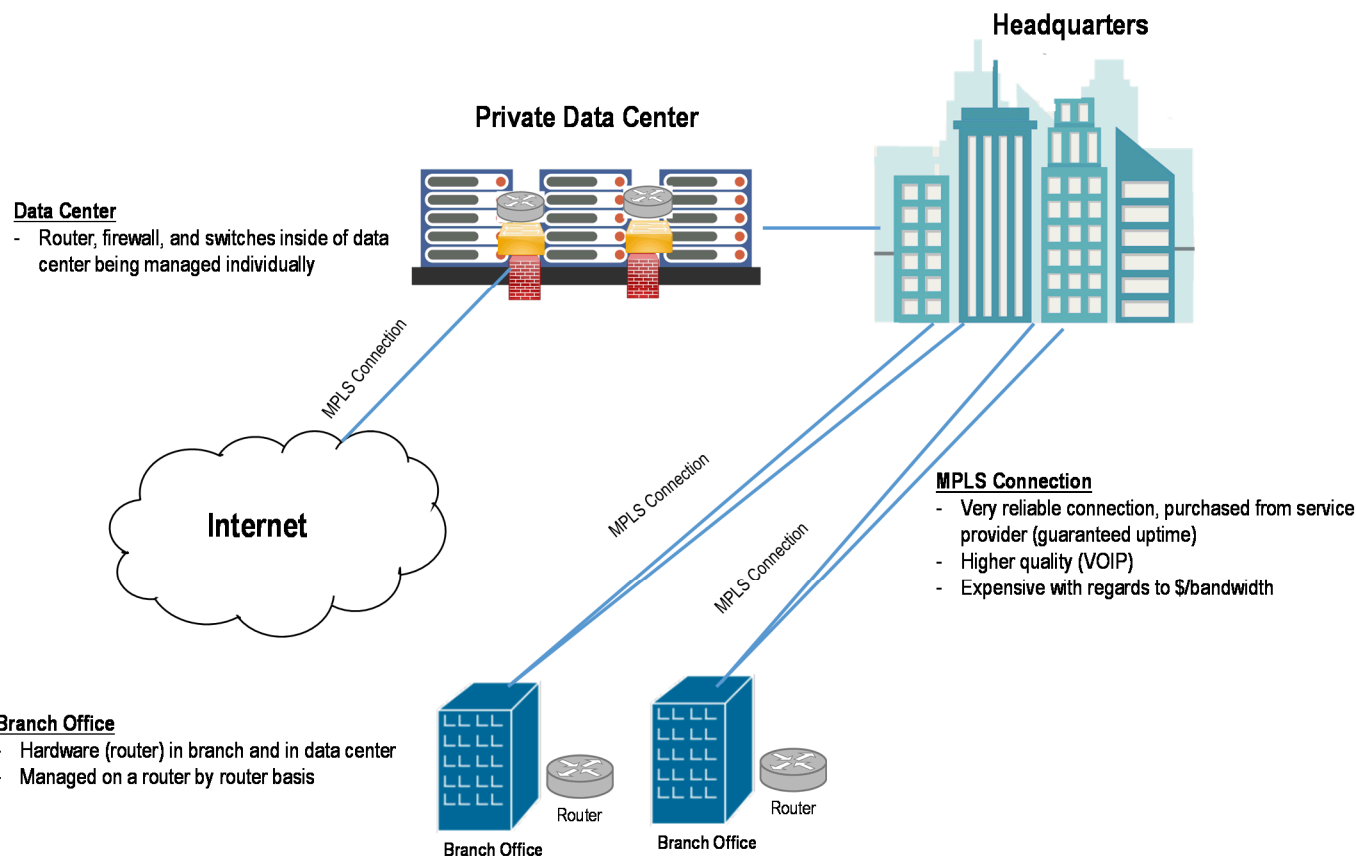
## Table of Contents

<b>Evolution of the Wide Area Network (WAN)</b>	<b>3</b>
A Closer Look at Multiprotocol Label Switching (MPLS)	3
<b>Introducing Software Defined Wide Area Networking (SD-WAN)</b>	<b>5</b>
Use Cases of SD-WAN Across Verticals	7
Why Security Matters with SDWAN? Public Internet and the Cloud	8
<b>SD-WAN vs Cloud Security – Is There a Winner?</b>	<b>8</b>
A Closer Look at the Cloud Security Providers	9
<b>How Large Is the Opportunity? \$25B in MPLS Spend, Cloud Communication Adoption</b>	<b>10</b>
Voice and Video Communications Delivered over the Cloud	12
COVID-19 Impact on SD-WAN – Acceleration Cloud Migration	14
<b>Mapping the SD-WAN Vendor Landscape</b>	<b>14</b>
Different SD-WAN Deployments from Different Vendors	16
Market Shares – Shifting Tides	16
Selected M&A Summary in SD-WAN	17
Palo Alto Networks – Newest to Enter the Market	18
Fortinet – Capturing More Market Share	18
Zscaler – Partnering with SDWAN Vendors	20
Cloudflare – Newest Disruptor in the Market	21
<b>Secure Access Service Edge (SASE) – Comparing and Contrasting to SD-WAN</b>	<b>23</b>
Understanding Where Cloud Providers Fit into SASE	24

## Evolution of the Wide Area Network (WAN)

Traditionally, enterprise network and security were based on a castle and moat architecture, where all security and networking flowed through HQ. Users that requested access to internal applications or websites were directed to HQ/private data centers via routers in a branch office that were pointed in that direction. Once the request came through, the traffic flowed through a private secure Multiprotocol Label Switching (MPLS) connection to HQ/Data Centers, where the security stack laid, and then granted access to applications or directed to public internet. This entire process was done through individual appliances like routers, switches, and firewalls, all of which had to be managed separately at each location.

Figure 1: Traditional Networking Model



Source: J.P. Morgan Research

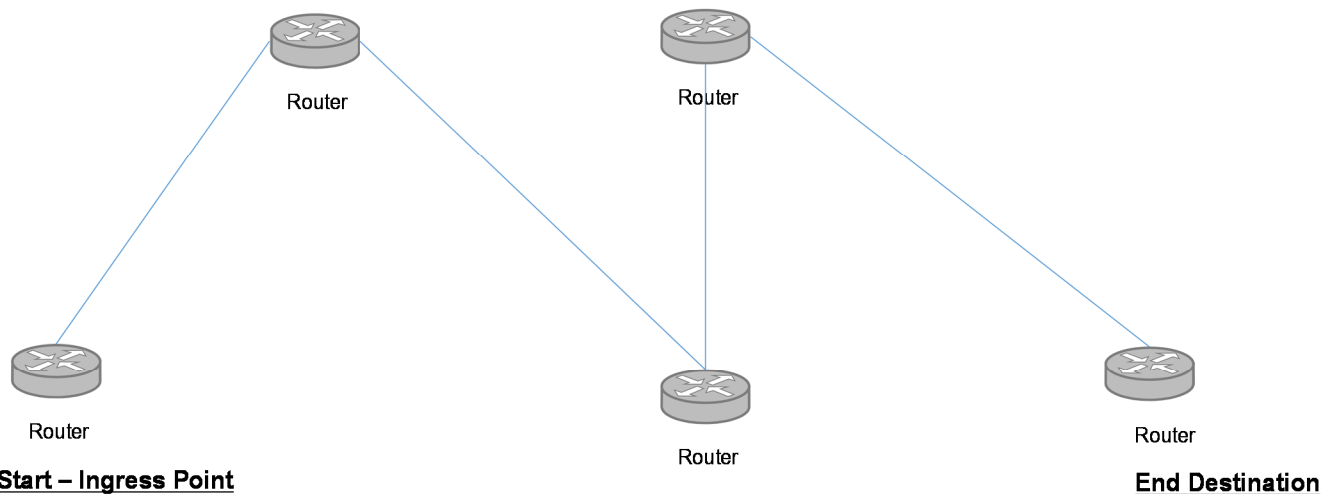
## A Closer Look at Multiprotocol Label Switching (MPLS)

In order to understand the use cases and reasons for the growing adoption of SD-WAN, let us take a closer look at what MPLS is, why was it used, and what the pros and cons of using MPLS in an enterprise environment are today. MPLS was introduced in the late 1990s and at its core is a private tunnel that secures connections, transporting data from and to routers in different locations. These connections are generally provided by an internet service provider (ISP). The diagram below shows at a basic level how the MPLS routes traffic from point A to

Point B by applying labels to packets based on a predetermined path to get from start to end destination inside a network.

**Figure 2: How MPLS Works**

Label information is used throughout at each stop, instead of looking for IP each time to get to final destination



1. At the ingress point, router does a lookup for end destination router to transport packet
2. Based on path that is determined, router applies a label to the packet being transported

Source: J.P. Morgan Research, North American Network Operators' Group

### What are the pros and cons of using MPLS?

MPLS connections tend to be more reliable and have a security layer on top given it is a private connection into Enterprise Data centers and not shared like broadband. However, these MPLS connections have been on the more expensive side compared to other alternatives that we explore further on in the report. In addition, the routers used for MPLS have to be managed on an individual basis, unable to do protocol uniformly, and as the footprint grows it becomes difficult for IT professionals to manage the network.

**Figure 3: Measuring the Pros and Cons of MPLS**

Pros	Cons
Reliability - connection has SLA with Internet Service provider	Cost - Expensive connection that is purchased from carrier
Security - Private tunnel between connections	Uniformity - Difficult to manage uniformly, service provider control priority traffic
Bandwidth - better experience for more bandwidth intensive activities like Voice Over IP, Video, etc	Scalability - Global footprint, becomes difficult to piece together international MPLS lines through different ISP's

Source: J.P. Morgan Research

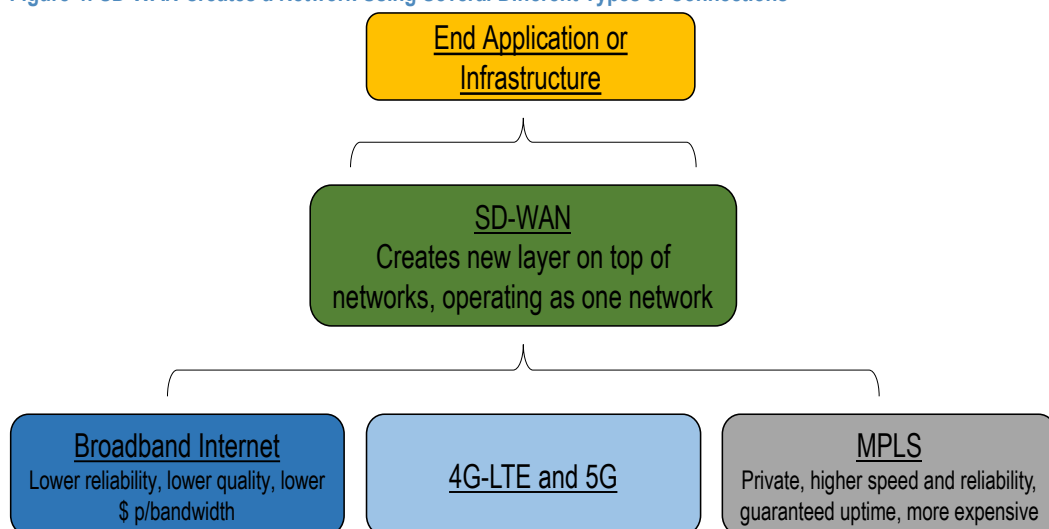
This model worked until the move to the cloud for both application/infrastructure and more remote usage came along. With that, SD-WAN has come to center stage.

## Introducing Software Defined Wide Area Networking (SD-WAN)

### What is SD-WAN?

SD-WAN, or Software Defined Wide Area Networking, creates a centralized network on top of connections like broadband, 4G/5G, and MPLS. The software portion is able to detect the type of application and destination for more intelligent routing of traffic. This allows for more granular policies on traffic and security, as well as a centralized place for control and orchestration. SD-WAN can be deployed through an appliance at the branch and at HQ and is available in virtual and cloud deployments as well.

Figure 4: SD-WAN Creates a Network Using Several Different Types of Connections



Source: J.P. Morgan Research

### Why is SD-WAN being used?

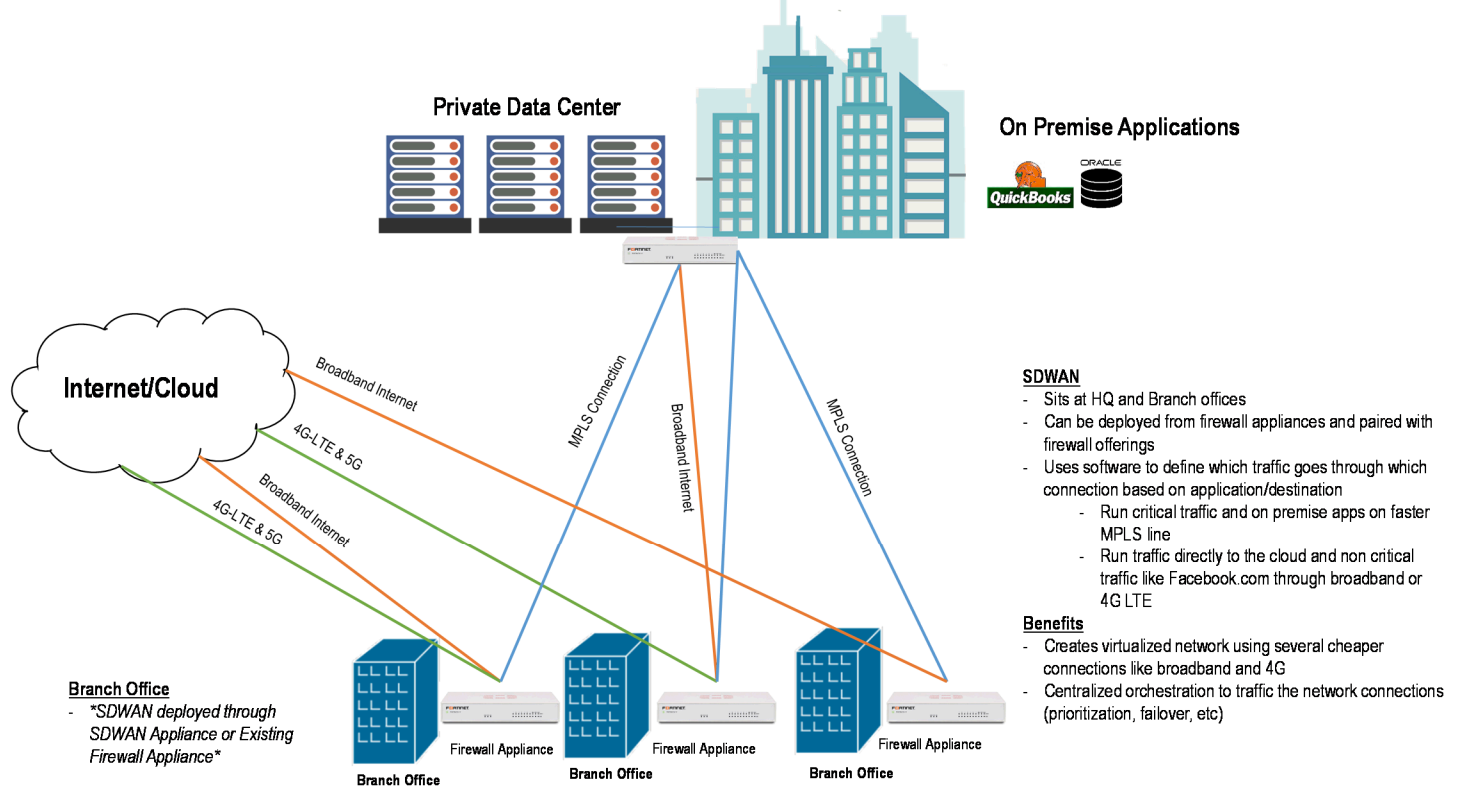
Enterprises have migrated from a hub and spoke model, where data/applications are held at HQ with traffic coming from within the network, to a branch model, where traffic requests are coming from outside the network as workers have become able to work remotely or while traveling. With the deployment of SD-WAN at the branch and at HQ, IT professionals are able to have better control over traffic and networking, allowing for cuts in spending in MPLS connections that were used to transport traffic. As mentioned above, MPLS connections are sold by ISPs and, given the SLA/reliability, tend to be much more expensive than other connections.

### How SD-WAN works

In the chart below, we show how the basic steps in what SD-WAN would look like hypothetically, where an appliance sits at HQ and branch offices, either be a thin client (SD-WAN appliance) or deployed inside of a next-generation firewall (NGFW). The software overlay directs traffic based on the criticality of the application/destination. Enterprises can send non-critical traffic, like accessing YouTube or Facebook, through less expensive public internet connections and send critical traffic, like VOIP traffic from RingCentral with the need for low latency,

through the faster more reliable MPLS lines. This allows enterprises to cut back on costs through more efficiently managing traffic, especially with the capability in SD-WAN to use, for example, three different broadband connections instead of one expensive MPLS line. In addition, if the SD-WAN is deployed with next generation firewall capabilities, it brings the security stack to the edge, instead of having to route the traffic to the datacenter just to run security filtering. The other capability in SD-WAN, is the ability to manage all the devices through software, instead of having to individually manage all the different appliances like routers, switches, and firewalls at the HQ.

Figure 5: How SD-WAN Functions From a Network Perspective – Saving Networking MPLS Costs

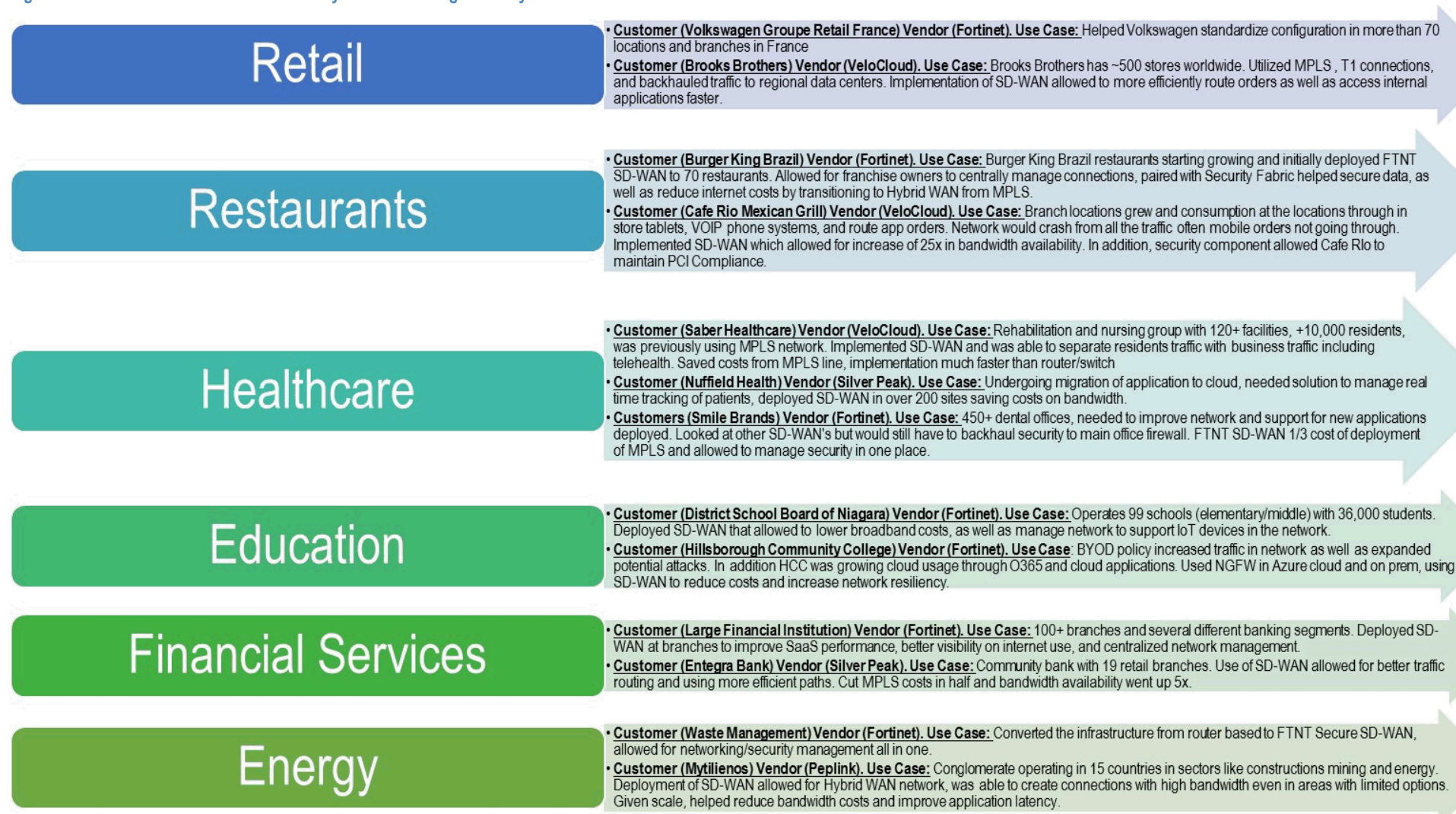


Source: J.P. Morgan Research



## Use Cases of SD-WAN Across Verticals

Figure 3: Consolidated SD-WAN Use Cases by Verticals through Primary and Case Studies



Source: J.P. Morgan Research, Company Websites, Customer case studies

## Why Security Matters with SDWAN? Public Internet and the Cloud

With rise of cloud computing, applications and infrastructure transitioned to the cloud, outside of the HQ. With the move to the cloud, there is no longer the need to always backhaul employee traffic from the branch to HQ. This has brought the focus on securing traffic to cloud applications. In addition, as mentioned above, while connections like broadband that can be used with SD-WAN to connect traffic are cheaper, they are also transported over the public internet, which can remain vulnerable to attacks. Vendors like Fortinet that have next gen firewalls have deployed SD-WAN capabilities to the appliances, combining security with networking. We would point out that not every SD-WAN vendor has an integrated security solutions like Fortinet (see section *Mapping the Vendor Landscape*) and instead are focused more on the networking side (VeloCloud, Citrix), partnering with other vendors like Zscaler for security.

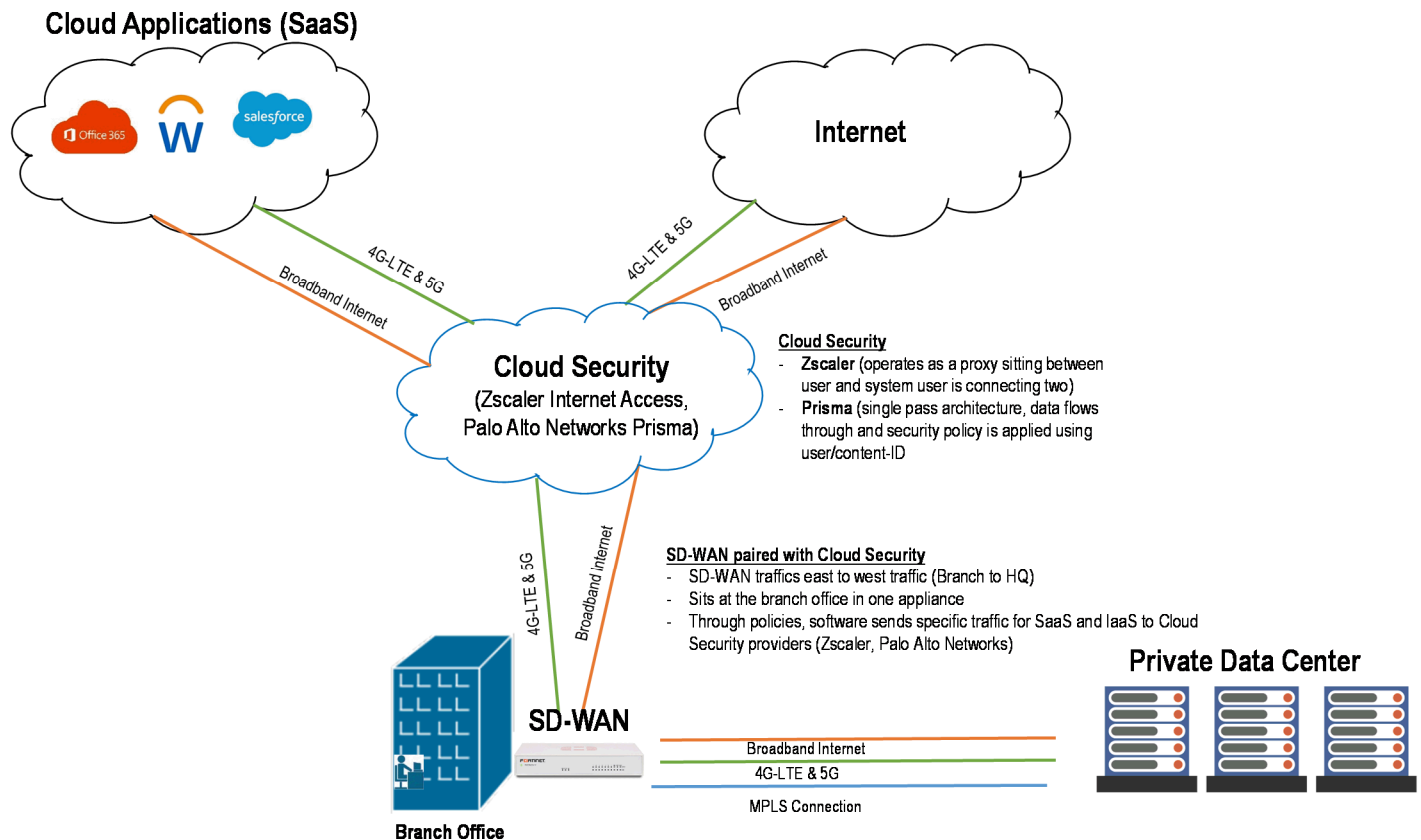
## SD-WAN vs Cloud Security – Is There a Winner?

As workloads have moved the cloud, there has been the emergence of cloud security vendors like Zscaler (ZS/OW) and Cloudflare (NET/OW), as well as Palo Alto Networks (PANW/N) through a series of acquisitions. In our conversations with investors we regularly found that there was some confusion around where players that have SD-WAN solutions like Fortinet (FTNT/N) fit compared to cloud players like Zscaler (ZS/OW).

We believe the role of SD-WAN is in securing and connecting east to west traffic, from branch to HQ, and using cloud security like ZIA or Prisma Access to secure north to south traffic from users to the cloud. In the chart below, we illustrate how SD-WAN and Cloud security go hand in hand, with the SD-WAN appliance sitting at the branch, and through policies set in the software, route specific traffic going cloud to specific cloud security solutions, and routing/securing traffic from and to the HQ.



Figure 6: SD-WAN Routes East to West Traffic to HQ, Routes Internet and Cloud Traffic to Cloud Security Providers



Source: J.P. Morgan Research

Our view is that there will still be a need to secure traffic to on-premise applications, which can be done through SD-WAN solutions from vendors like Fortinet or through cloud security vendor solutions like Zscaler. We note that firewall vendors like Fortinet have mentioned that they do partner with Zscaler in some deals, and Zscaler has partnerships with its ZIA product with several SD-WAN providers. Palo Alto's recent acquisition of CloudGenix, an SD-WAN provider, we believe positions PANW well for the opportunity to combine both SD-WAN and Cloud Security in one integrated platform.

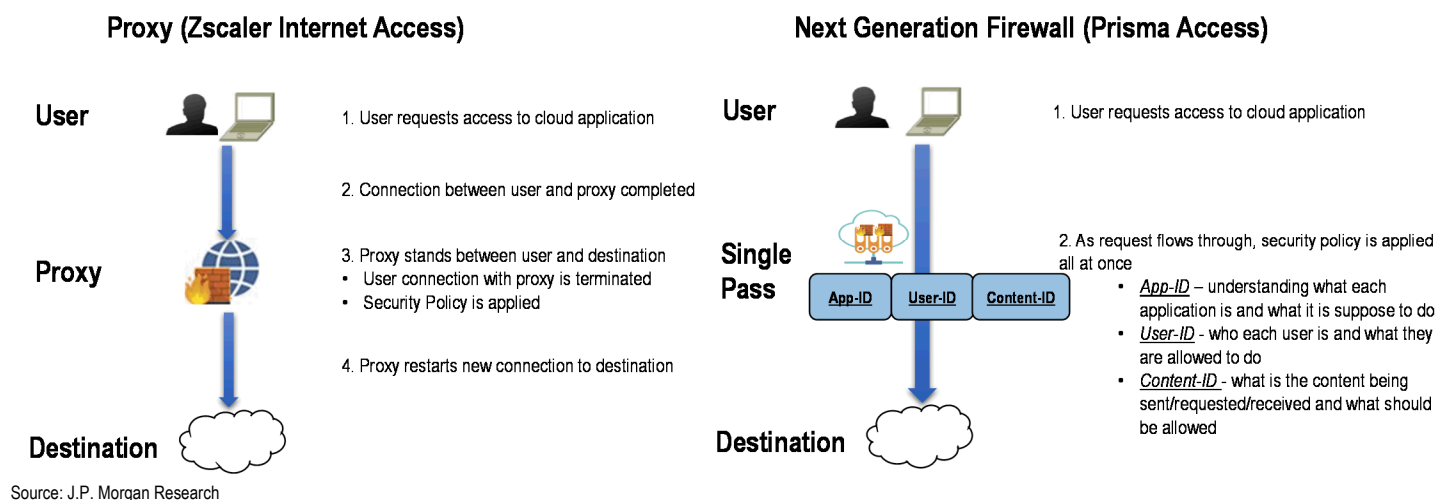
## A Closer Look at the Cloud Security Providers

The vendors we look at here are Zscaler (ZIA), which was founded in 2007, and Palo Alto, which introduced its Prisma Access solution in May of 2019. While both vendors are in essence trying to do the same thing, they are achieving that in two different ways.

Zscaler operates as a proxy and sits between the user and the system, creating a virtual gap between what the user is connecting to (application, website, etc.) and applies the security policy at that gap. When the user's connection meets the proxy, the connection is terminated at this point, and the proxy then reactivates the connection on behalf of the user.

Palo Alto Networks applies the security policy in a single pass architecture. Here, there is no gap where the security policy is applied, rather the security policy is applied all at once as the data flows past. PANW uses App-ID, User-ID, and content-ID to filter the data.

Figure 7: Zscaler vs Palo Alto Networks



Other vendors in the cloud security space include Menlo Security, iBoss, Forcepoint and Cloudflare. Here, NET has launched Cloudflare for Teams, which combines Cloudflare Gateway and Cloudflare Access, and Cloudflare One, which we see as a step in going after Zscaler with a product at an attractive price point.

## How Large Is the Opportunity? \$25B in MPLS Spend, Cloud Communication Adoption

While MPLS pricing has been on a steady decline between 5-20%, on average, in the last couple of years, the increased bandwidth consumption and amount of users connected to the internet have increased consumption costs for enterprises. Below we show the difference in MPLS and other internet connections that can be used with SD-WAN, which helps enterprises be more intelligent/efficient about their connection spend. Fortinet's own [case study](#) mentioned savings of ~\$400k in networking expenses per year for its enterprise after transitioning to SD-WAN. This calculation assumes ~50Mbps in each of FTNT's 28 sites as well as pricing of \$300/mbps for MPLS and \$15/mbps for broadband.

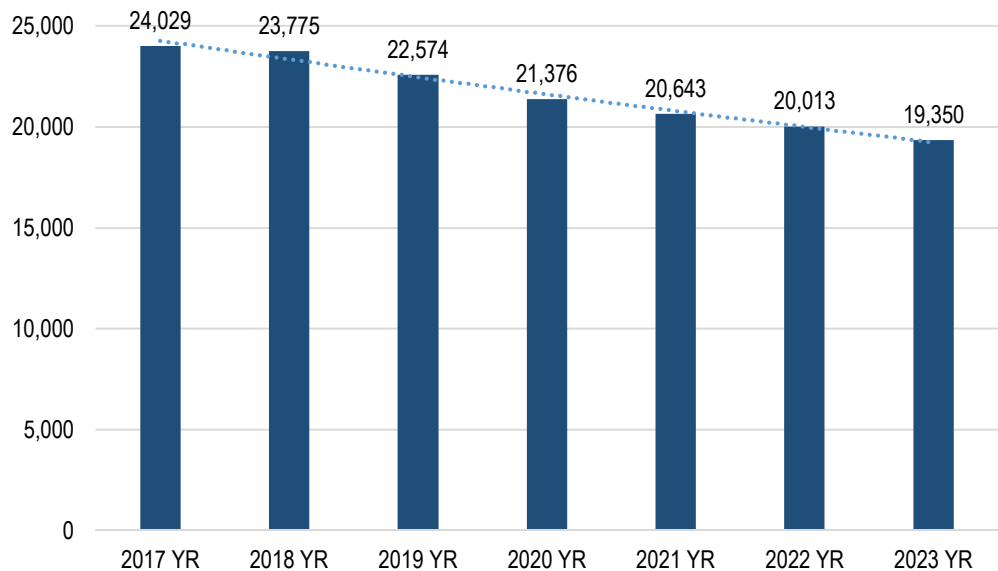
Table 1: MPLS Is ~23x More Expensive

Service Type	Mature Countries	Maturing Countries	Other Notes
10M Managed MPLS	\$500-\$1,100	\$1,000-\$1,600	Fully dedicated to enterprise
10M Managed Business Internet	\$300-800+	\$400-\$1,000+	Fully dedicated to enterprise
10M Unmanaged Consumer Internet	\$35	\$15-\$30	Shared bandwidth

Source: J.P. Morgan Research, Gartner

Gartner estimates there is currently ~\$23B in annual MPLS spend by enterprise worldwide. MPLS spend has declined ~5% in the last 3 years, with forecasts showing a 6% CAGR decline through 2023. The decline is largely because there is no longer a need to always backhaul traffic to the Enterprise via MPLS connections, with the shift in the workforce and shift of applications/infrastructure to the cloud. While we do not expect SD-WAN to completely wipe out the MPLS spend, our takeaway is that enterprises are spending huge amounts on MPLS, and part of that spend could shift towards SD-WAN vendors that provide cost benefits to enterprises.

Figure 8: +\$20B in Annual Spend in MPLS Connections



Source: Gartner Forecast: Communications Services, Worldwide, 2018-2023, 3Q20 Update

#### SD-WAN is the fastest growing segment within Enterprise Network Equipment

Spend on SD-WAN totaled ~\$2B in 2019, which represented only 3% of total \$75B Enterprise Network Equipment spend but is the fastest growing segment inside of Network Equipment. Part of the opportunity and growth in the segment can also be from the billions of dollars spent on router spend, which were used in the past to point traffic from branch to HQ through MPLS lines.

Table 2: SD-WAN Equipment Market Forecasted to Reach ~\$7B by 2024

	2018	2019	2020E	2021E	2022E	2023E	2024E	19-24E CAGR
Application Delivery Controllers	2,964.6	3,318.1	3,699.6	3,992.0	4,215.6	4,410.9	4,594.0	6.7%
Enterprise Branch Office Routers	4,171.3	4,525.4	3,165.5	2,493.5	1,856.5	1,362.0	963.8	-26.6%
Enterprise Core Routers	1,065.6	1,108.1	1,042.2	1,085.4	1,065.1	1,029.8	964.1	-2.7%
Enterprise Ethernet Switches - Campus	19,429.3	20,667.1	19,309.5	20,728.7	21,509.3	22,099.5	22,653.5	1.9%
Enterprise Ethernet Switches - Data Center	17,537.1	18,505.6	17,913.7	18,675.4	19,280.8	19,856.2	20,560.4	2.1%
Enterprise WLAN APs	5,545.5	5,650.9	5,300.8	6,158.2	6,831.0	7,443.8	8,068.5	7.4%
Enterprise WLAN Controllers	721.2	694.7	560.0	532.4	483.4	422.9	362.0	-12.2%
Firewall Equipment	11,692.9	13,243.2	14,311.7	15,458.5	16,279.3	17,013.7	17,693.6	6.0%
IDPS	1,407.0	1,534.6	1,254.1	1,209.0	1,148.7	1,087.4	1,025.0	-7.8%
Network Access Control	890.5	1,070.4	1,219.9	1,396.2	1,545.1	1,679.4	1,805.4	11.0%
Network Detection and Response	499.4	848.2	1,059.5	1,353.0	1,632.8	1,904.4	2,161.9	20.6%
SD-WAN Hardware	390.2	846.9	1,294.4	1,660.6	1,983.7	2,238.6	2,409.2	23.3%
SD-WAN Software	688.2	1,400.0	2,197.2	2,853.5	3,437.3	3,908.7	4,275.5	25.0%
<b>SD-WAN Total</b>	<b>1,078.4</b>	<b>2,246.9</b>	<b>3,491.6</b>	<b>4,514.1</b>	<b>5,421.0</b>	<b>6,147.3</b>	<b>6,684.7</b>	<b>24.4%</b>
Small-Business WLAN APs	998.6	1,161.8	1,124.8	1,316.2	1,407.0	1,500.2	1,583.2	6.4%
<b>Total</b>	<b>68,001.5</b>	<b>74,574.9</b>	<b>73,452.9</b>	<b>78,912.7</b>	<b>82,675.6</b>	<b>85,957.5</b>	<b>89,119.9</b>	<b>3.6%</b>
<b>Worldwide Growth Rate</b>		<b>9.7%</b>	<b>-1.5%</b>	<b>7.4%</b>	<b>4.8%</b>	<b>4.0%</b>	<b>3.7%</b>	
<b>SD WAN Growth Rate</b>		<b>108.4%</b>	<b>55.4%</b>	<b>29.3%</b>	<b>20.1%</b>	<b>13.4%</b>	<b>8.7%</b>	
<b>SD-WAN % of Total Network Equipment Spend</b>	<b>1.6%</b>	<b>3.0%</b>	<b>4.8%</b>	<b>5.7%</b>	<b>6.6%</b>	<b>7.2%</b>	<b>7.5%</b>	
<b>SD-WAN % of Enterprise WAN Edge</b>	<b>17.1%</b>	<b>28.5%</b>	<b>45.3%</b>	<b>55.8%</b>	<b>65.0%</b>	<b>72.0%</b>	<b>77.6%</b>	

Source: Gartner Forecast: Enterprise Network Equipment, Worldwide, 2018-2024, 3Q2020 Update. Sum of User Spend Constant Currency

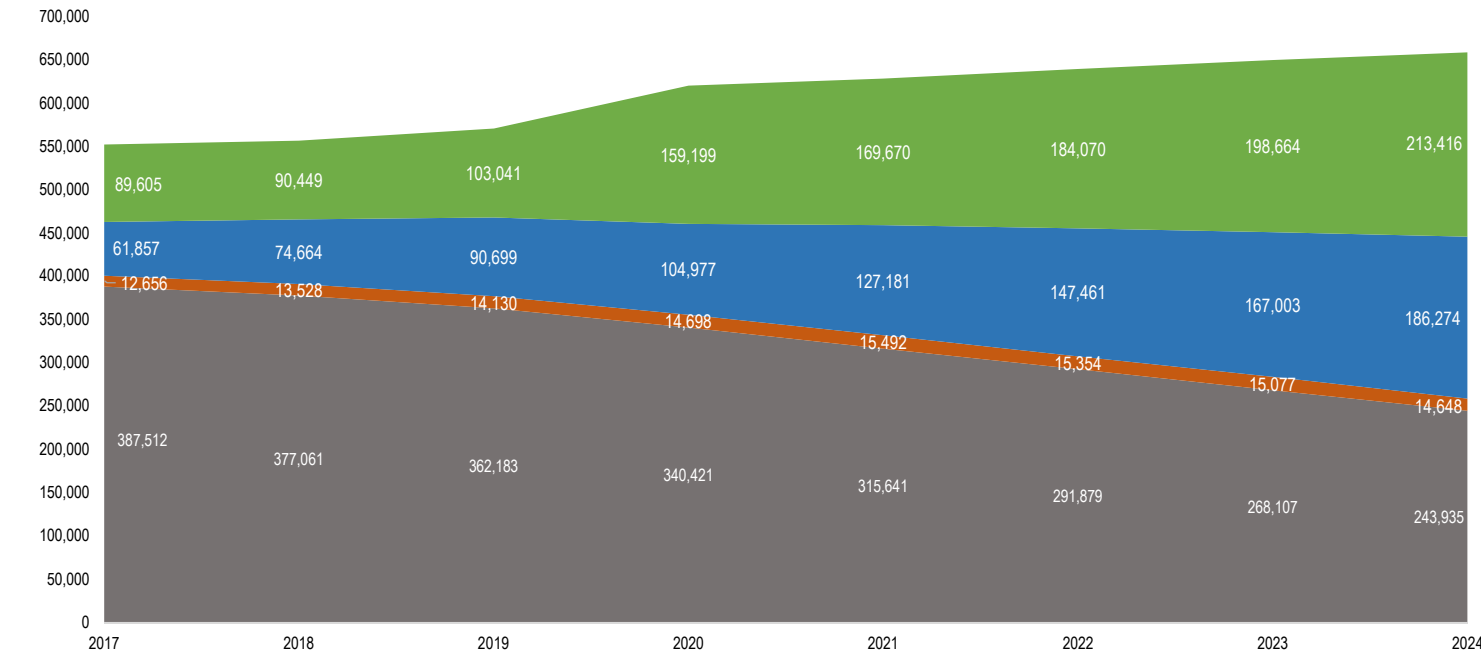
### What are the economics for SD-WAN deals

Through our conversations with vendors and customers in the SD-WAN space, we found that there is no one size fits all in terms of pricing/economics in SD-WAN deals. Some vendors have resorted to pairing the SD-WAN solutions for free as a bundle within firewall deals, while others have resorted to taking a percentage of the cost savings that SD-WAN brings from reduced MPLS spend. Therefore, while the SD-WAN solutions might not be generating substantial revenue right now, it has helped vendors in landing deals and in providing a tailwind for product growth.

### Voice and Video Communications Delivered over the Cloud

Companies have continued their digital transformations also in the voice space, using cloud solutions like Zoom and RingCentral to communicate. The COVID-19 pandemic has only accelerated the shift of communication and collaboration to the cloud, evidenced by the 300M daily participants in Zoom meetings, up from 10M at the start of 2020. According to Gartner, in 2019 there were approximately ~453M telephony users, ~91M of which were cloud based. Companies like ZM and RNG are providing cloud delivered telephony services that have better performance and are cheaper than maintaining legacy hardware. This is leading to forecasts of cloud-based telephony users growing to over 186M by 2024, as displayed in Figure 9 below.

Figure 9: Installed Base of Cloud Telephony and Conferencing Users Growing at a 15%+ CAGR Through FY24E



Source: Gartner Forecast Unified Communications, Worldwide, 2017-2024, 3Q20

In addition, with the move to a remote workforce due to COVID-19, there has been an increased focus on connecting student, health care workers and patients, and entire enterprise workforces. Voice and Video traffic tend to be more bandwidth heavy, and routing that cloud traffic back to the datacenter and to the cloud can cause latency issues and also clog up pipes for other internet traffic. With SD-WAN, companies are able to identify voice applications and prioritize certain types of traffic to direct important traffic through faster connections like 4G or an MPLS like while directing other internet traffic through broadband. In fact, our research indicates that some customers have migrated over to SD-WAN in order to cut on connection costs and improve the quality of voice/video services. This is leading to cloud-based unified communications spend growth to outpace the overall market as displayed in Table 3.

Table 3: Cloud-Based Communication Forecasted to Become the Majority of Communications Spend

	2017	2018	2019	2020	2021	2022	2023	2024	19-24 CAGR
<b>Total Telephony and Messaging</b>	<b>32,528</b>	<b>33,835</b>	<b>33,555</b>	<b>32,362</b>	<b>34,564</b>	<b>36,613</b>	<b>38,202</b>	<b>39,526</b>	<b>3.3%</b>
Premises-Based Telephony and Messaging	9,291	8,422	6,698	4,931	4,893	4,981	4,808	4,567	-7.4%
Telephony Product Support Services	11,906	11,958	11,444	10,542	10,127	9,692	9,212	8,734	-5.3%
Cloud-Based Telephony and Messaging	11,331	13,455	15,412	16,888	19,545	21,940	24,182	26,225	11.2%
<b>Total Conferencing</b>	<b>3,208</b>	<b>3,432</b>	<b>3,676</b>	<b>5,288</b>	<b>5,474</b>	<b>5,816</b>	<b>6,170</b>	<b>6,519</b>	<b>12.1%</b>
Premises-Based Conferencing	211	204	192	185	179	173	161	148	-5.1%
Conferencing Product Support Services	154	158	156	151	151	147	140	133	-3.1%
Cloud-Based Conferencing	2,843	3,069	3,329	4,953	5,144	5,496	5,868	6,238	13.4%
<b>Total Spend</b>	<b>35,736</b>	<b>37,267</b>	<b>37,231</b>	<b>37,650</b>	<b>40,039</b>	<b>42,429</b>	<b>44,372</b>	<b>46,045</b>	<b>4.3%</b>
<b>Total Cloud Based Spend</b>	<b>14,174</b>	<b>16,525</b>	<b>18,741</b>	<b>21,841</b>	<b>24,689</b>	<b>27,437</b>	<b>30,050</b>	<b>32,463</b>	<b>11.6%</b>
<b>Cloud as % of Total</b>	<b>40%</b>	<b>44%</b>	<b>50%</b>	<b>58%</b>	<b>62%</b>	<b>65%</b>	<b>68%</b>	<b>71%</b>	

Source: Gartner Forecast Unified Communications, Worldwide, 2017-2024, 3Q20

A [study](#) conducted jointly by Zoom and VeloCloud showed that implementing VMware's SD-WAN improved the packet loss that could occur and also doubled video quality to 720p HD. In the study linked, VMware provides a visualization of the improvement in both quality as well as decreased packet loss, both of which are critical to traffic like video communication and voice.

## COVID-19 Impact on SD-WAN – Acceleration Cloud Migration

### Initial IT focus was on expanding VPN capacity

In the beginning of the pandemic, enterprises shifted their focus to rapidly expanding capacity for remote workers through VPN purchases. However, VPNs are intended as a point-to-point communication between the end user and the network of that enterprise and do not provide direct access straight to cloud applications. In addition VPN's do not provide the ability to manage what applications get priority of the bandwidth, causing complexity and potentially slowing users connections for critical traffic.

### COVID-19 changing the way enterprises think

While a 100% remote workforce will likely not be permanent, we do believe the current environment will augment the percentage of permanent remote workers as companies realize cost savings and higher worker productivity. This is accelerating the transition to the cloud and forcing companies to accelerate their network transformations, which could be a boost to SD-WAN. This would allow for access to cloud applications, internet, and internal datacenter in a more bandwidth efficient and secure way. However, we believe in the current environment enterprises are rethinking their IT spending and network architecture. Some customers we have talked to have indicated that in smaller less internet intensive branches, they are thinking of not deploying SD-WAN and just having a local internet breakout linked to solutions like Zscaler.

## Mapping the SD-WAN Vendor Landscape

Only 35% of Enterprises have SD-WAN, and Gartner expects that number to reach 60% by 2024 as more enterprises look for lower-cost and effective ways to manage the complex network state. Potential customers have many SD-WAN vendors from which to choose, and through our research in the space, we came across over 50 different vendors. These range from more networking SD-WAN players like VMware, Silver Peak, and those with integrated security offerings bundled together like Palo Alto and Fortinet. Most of SD-WAN players have integrations with public cloud providers and partnerships with cloud security providers like Zscaler. In Table 4 below we aim to help investors understand the different main vendor offerings and how they differentiate.



Table 4: Understanding the Different SD-WAN Vendors' Approaches

## Networking Focused SD-WAN Vendors

VMware 

**Magic Quadrant Position:** Leader  
**SD-WAN Market Ranking, Market Share %:** #2, 13.8%  
**# of SD-WAN Customers:** 9,000  
**M&A:** Purchased VeloCloud for \$450M in Nov 2017

- Networking focus with WAN Edge
- Selling motion comes from leveraging MSP channel, as well as partnership with Zscaler to provide to provide cloud security for cloud transformations
- Provides datacenter security through NSX but lacks true cloud security

**Reference Customers:** Brooks Brothers, Lincoln Investment, Dell EMC

Cisco 

**Magic Quadrant Position:** Leader, up from Challenger in 2019  
**SD-WAN Market Ranking, Market Share %:** #1, 17.2%  
**# of SD-WAN Customers:** 30,000  
**M&A:** Purchased Viptela for \$610M in May 2017

- Offers SD-WAN through Meraki/Viptela, leverages large enterprise relationships
- Has made acquisitions in the security space, does have cloud security (Umbrella) and WAN Edge but portfolio needs to be pieced together
- Also partners with Zscaler in case that customers want best in class cloud security

**Reference Customers:** National Instruments, BBVA, Vodafone

## Networking/Security SD-WAN Vendors

Palo Alto Networks   
A PALO ALTO NETWORKS COMPANY

**Magic Quadrant Position:** Leader, up from Visionary in 2019  
**SD-WAN Market Ranking, Market Share %:** #7, 5.0%  
**# of SD-WAN Customers:** 1,000  
**M&A:** Purchased CloudGenix for \$420M in March 2020, \$99M raised prior

- 2 SD-WAN's: PANW solution released '19, acquisition of CloudGenix in '20
- Made \$1B+ in acquisition to form Prisma Access which combined with SD-WAN edge has the options for SASE platform
- Leverage channel relationships, and existing Prisma Access customers to upsell, without need for Zscaler for cloud security

**Reference Customers:** Chipotle, Coca Cola, Autodesk

Fortinet 

**Magic Quadrant Position:** Leader, up from Challenger in 2019  
**SD-WAN Market Ranking, Market Share %:** #3, 9.1%  
**# of SD-WAN Customers:** 30,000

- Went from no market share to #3 in one year, leveraging firewall install base to turn on SD-WAN functionality
- Product can scale from lower end model for DIY to the highest throughput deployments for enterprise
- Leveraging MSP for SASE offering, expect investment in cloud security





**Reference Customers:** Waste Management, Volkswagen, Alaska Airlines, Burger King

Source: J.P Morgan Research, Gartner, Company Websites, SDXCentral, Crunchbase

## Different SD-WAN Deployments from Different Vendors

Some players are purely networking vendors and need to partner with security vendors to deploy NGFW, which leads customers having to manage separate boxes and multiple vendors. One of the concepts in the market currently is in finding vendors with both SD-WAN and Cloud Security that we explore further on in the report when talking about SASE.

Table 5: The Different Deployments of SD-WAN

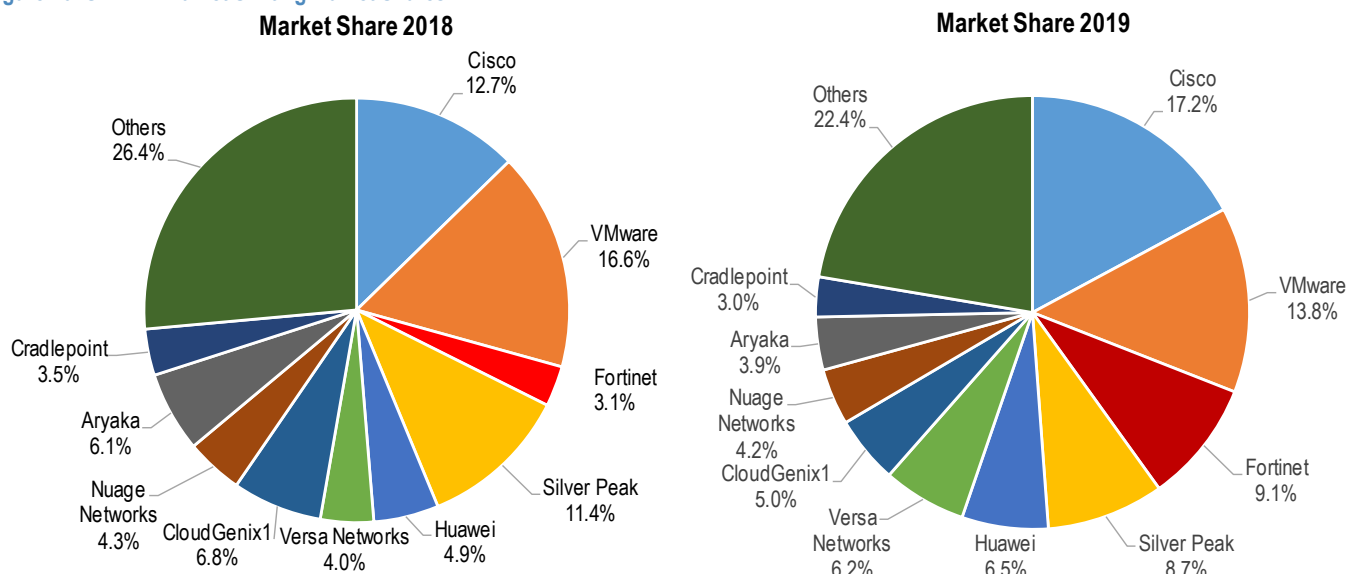
	SD-WAN	SD-WAN with NGFW	SD-WAN with SWG	SD-WAN with MSP
<b>Focus</b>	Networking	Networking w/ Security	Networking w/ Securing Internet Access	Outsourcing
<b>Description of Deployment</b>	Deployed in appliance which contains basic firewall features, solution where security is not a priority or where security will be deployed with another vendor. Least expensive deployment.	Deployed in appliance with NGFW. Can be deployed through one vendor with embedded NGFW. Can also be deployed through 2 vendors, one for SD-WAN and one for firewall security.	Deployed in partnership with a Secure Web Gateway vendor (i.e. Velocloud with Zscaler). Integration between the two providers is done where traffic aimed at internet is routed from SD-WAN to SWG.	Deployed by bundling together SD-WAN solutions, SWG solution, and carrier solution. An example of this would be Verizon pairing their carrier services with Citrix and zScaler in a bundle. Tends to be cheaper than SD-WAN with SWG or NGFW.
<b>Security Level</b>				
<b>Vendors</b>	Citrix, Silverpeak, VMware, Meraki	Fortinet, Palo Alto Networks, Cisco, Barracuda, Cato Networks, Forcepoint	Symantec, Zscaler, Forcepoint, Cato Networks, Cisco Secure Internet Gateway	Verizon, AT&T

Source: J.P Morgan Research, Gartner, Company Websites

## Market Shares – Shifting Tides

Looking at the market share for SD-WAN players, Cisco and VMware have been at the top, taking advantage of their large install bases and large acquisitions made in the SD-WAN space in 2017. Note the estimates for Cisco's revenue in SD-WAN may include other network spend, since SD-WAN can be bundled with routing. Silver Peak, which has been in the market since 2004, was in the top 3, but Fortinet has gone from no market share in 2018 to the third largest in 2019. The top 3 vendors (Cisco, VMware, Fortinet) control over 40% of the market, leading to fragmented market share among other smaller players. PANW entered the SD-WAN party late, announcing an internally developed solution in December 2019 and then acquiring CloudGenix, which held 5% of the market in 2019, according to Gartner estimates. We view this partially as an admission from the company that it was easier to buy vs build (i.e. Cisco and VMware acquisitions), which has been common among players trying to enter the space. We expect further consolidation from niche networking SD-WAN plays for offerings with both networking and security integrated in one solution.

Figure 10: SDWAN Market Shifting Market Shares



Source: Gartner Market Share: Enterprise Network Equipment by Market Segment, Worldwide, 1Q20 (June 2020)

Table 6: SDWAN Market Share FY18-FY19

	2018	2019	2018 Share	2019 Share	Growth 18-19
Cisco	110.0	302.9	12.7%	17.2%	175.5%
VMware	144.3	243.9	16.6%	13.8%	69.0%
Fortinet	26.6	161.3	3.1%	9.1%	510%
Silver Peak	99.0	154.0	11.4%	8.7%	55.6%
Huawei	42.8	114.0	4.9%	6.5%	166.3%
Versa Networks	35.0	109.6	4.0%	6.2%	213.3%
CloudGenix1	59.4	88.3	6.8%	5.0%	48.6%
Nuage Networks	37.7	74.3	4.3%	4.2%	97.3%
Aryaka	53.1	69.6	6.1%	3.9%	31.0%
Cradlepoint	30.5	52.8	3.5%	3.0%	73.3%
Others	229.4	395.0	26.4%	22.4%	72.2%
<b>Total</b>	<b>867.7</b>	<b>1,765.7</b>	<b>100.0%</b>	<b>100.0%</b>	<b>103.5%</b>

Source: Gartner Market Share: Enterprise Network Equipment by Market Segment, Worldwide, 2Q20 (September 2020)

## Selected M&A Summary in SD-WAN

Table 7: Selected SD-WAN M&A

Date	Acquirer	Target	Transaction Value	Transaction Multiple
10/19/2020	Juniper	128 Technology	\$450M	11x EV/NTM Revenue
9/17/2020	Ericsson	Cradlepoint	\$1.1B	8x TTM Revenue
7/13/2020	HPE	Silver Peak	\$925M	7x TTM Revenue
3/31/2020	Palo Alto	CloudGenix	\$420M	4.7x TTM Billings
11/15/2018	Oracle	Talaria Networks	Undisclosed	
11/2/2017	VMware	VeloCloud	\$450M	
5/1/2017	Cisco	Viptela	\$610M	6x TTM Revenue
3/2/2015	HP	Aruba Networks	\$3B	

Source: JP Morgan Estimates, Company Press Releases

## Palo Alto Networks – Newest to Enter the Market

Palo Alto launched its internally developed SD-WAN solution back in December 2019 and then in March 2020 bought CloudGenix, one of the main vendors in the space. Management has not commented on the revenue contribution from the \$420M purchase, though it did disclose that CloudGenix had 200 employees at the time of purchase. Palo Alto does have customers currently using its internally developed SD-WAN solution, and CloudGenix was founded in 2013 and brings over an estimated 800 customers with large reference customers like Chipotle.

Different from our initial expectations and from the integration commonly seen in the market, Palo Alto's first goal was to integrate CloudGenix into Prisma Access rather than into the NGFW. Our research indicates that since then, PANW has expanded deployment, which was initially limited to Series 800 and 3200, and we expect continued expansion of deployment options through software updates.

Table 8: Palo Alto's SD-WAN Deployment

Deployment	Series	Model	Deployment	Model
Hardware	PA-800	PA-220	Virtual	VM-300
		PA-220R		VM-500
		PA-820		VM-700
		PA-850		
	PA-3200	PA-3220		
		PA-3250		
		PA-3260		
		PA-5280		
	PA-5200	PA-5260		
		PA-5250		
		PA-5220		

Source: Company Website

Prior to being acquired, CloudGenix's ION appliances were used to deploy the SD-WAN solution and were available in public cloud marketplaces like Azure and AWS, as well as through hardware and virtual deployments. With the acquisition, CloudGenix SD-WAN boxes that sit at the branch can direct traffic to Prisma Access, which then determines which traffic is required to go back to datacenters/HQ or directed securely to a SaaS application like O365. This is the type of offering that we could see competing with what is often achieved with Zscaler for cloud security and a WAN Edge provider like VMware.

## Fortinet – Capturing More Market Share

As mentioned above, Fortinet has gone from no market share in beginning of 2018 to 9% at the end of FY19. Management talked about SD-WAN contributing 7% of the 17% product growth in FY19, which we estimate would equate to ~\$50M in revenue. Hence, we believe the Gartner data below represents billings numbers rather than straight revenue. This checks out when taking into account commentary that SD-WAN represented mid- to high-single-digit percentage of total billings (6% would equate to ~\$150-\$160M in SD-WAN billings in FY19).

Table 9: Fortinet Rising from No Market Share to Third Biggest Vendor

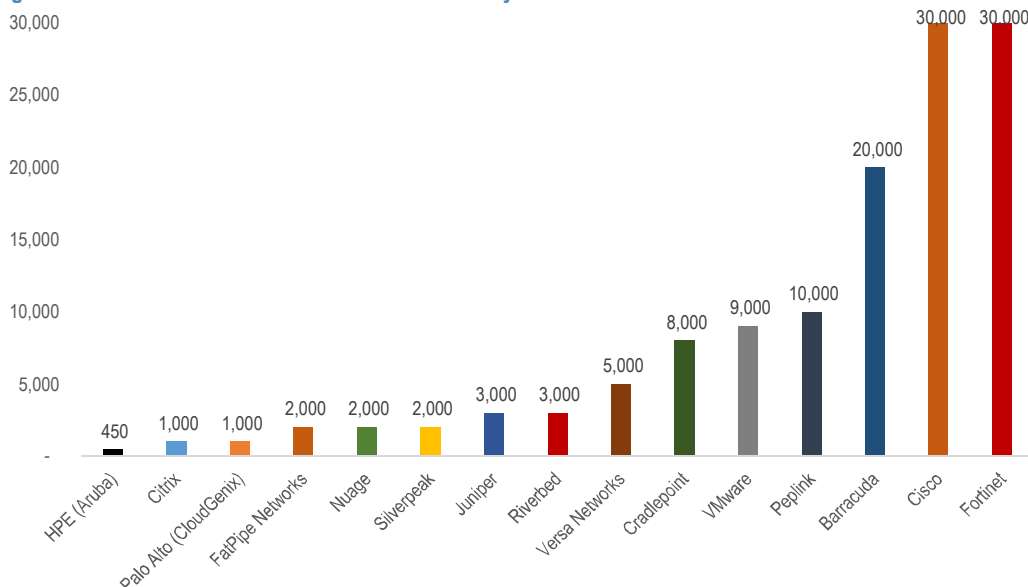
	1Q18	2Q18	3Q18	4Q18	1Q19	2Q19	3Q19	4Q19	1Q20	2Q20
Cisco	21.3	27.1	30.1	31.5	46.7	67.7	86.2	102.3	127.3	152.7
VMware	30.1	34.6	38.1	41.5	46.1	54.1	66.6	77.1	66.7	69.8
Fortinet	-	-	7.2	19.4	13.8	46.2	41.2	60.0	51.9	54.4
Silver Peak	20.0	24.0	26.0	29.0	33.0	37.0	40.0	44.0	46.0	45.7
Huawei	1.8	8.0	15.8	17.2	23.1	23.5	24.3	43.1	29.8	31.4
Versa Networks	5.3	6.7	8.9	14.1	13.5	18.9	28.5	48.7	29.5	41.4
Palo Alto										15.3
CloudGenix*	13.5	14.9	15.3	15.7	16.8	18.7	27.6	25.1	18.0	
Nuage Networks	7.2	8.3	9.6	12.5	11.3	17.5	20.5	25.1	20.7	20.0
Aryaka	12.0	12.9	13.6	14.6	15.9	16.8	17.9	18.9	18.2	
Barracuda Networks								12.1	14.5	14.1
Cradlepoint	6.4	5.3	10.6	8.3	6.2	15.4	11.5	N/A	N/A	13.8
Others	36.6	52.2	62.8	77.8	76.7	92.6	94.5	138.7	100.6	110.0
<b>Total</b>	<b>154.2</b>	<b>194.0</b>	<b>238.0</b>	<b>281.5</b>	<b>303.2</b>	<b>408.5</b>	<b>458.8</b>	<b>595.2</b>	<b>523.3</b>	<b>568.7</b>

Source: Gartner Market Share: Enterprise Network Equipment by Market Segment, Worldwide, 2Q20 (September 2020) \*Cloudgenix purchased by Palo Alto

### Fortinet surpasses Cisco in number of SD-WAN customers

Cisco is widely regarded as the #1 and largest player in the SD-WAN market, both in terms of customers and market share. This changed when Fortinet stated in December 2019 that it had over 21,000 SD-WAN customers, which was more than the 20,000 customers Cisco disclosed in November of the same year. The figure below consolidates estimates of current SD-WAN customers by vendor.

Figure 11: Estimated Number of SD-WAN Customers by Vendor



Source: J.P Morgan Research, Gartner, Company Website, SDXCentral

Fortinet's success in the SD-WAN space has relied on the large existing install base of FortiGates, which can use the Secure SD-WAN functionality in the same firewall appliance. The table below outlines the various deployment methods of SD-WAN through the Hardware, Virtual and Cloud, ranging from the newly launched SD-WAN FortiGate 40F SD-WAN specific appliance to the higher throughput enterprise firewalls.

**Table 10: Deployment of Fortinet's SD-WAN**

Deployment	Model	Deployment	Model	Deployment	Model
Hardware Appliances	FortiGate/FortiWiFi 30E	Virtual Appliances	FortiGate VM01/01V	Cloud	FortiGate on AWS
	FortiGate/FortiWiFi 40F		FortiGate VM02/02V		FortiGate on AWS (BYOL)*
	FortiGate/FortiWiFi 50E		FortiGate VM04/04V		FortiGate on Azure
	FortiGate/FortiGate 60F		FortiGate VM08/08V		
	FortiGate 60E		FortiGate VM16/16V		
	FortiGate 80F				
	FortiGate 80E				
	FortiGate 100E				
	FortiGate 100F				
	FortiGate 200E				
	FortiGate 300E				
	FortiGate 400E				
	FortiGate 500E				

Source: Company Website

### Why do customers choose Fortinet's SD-WAN? Cost and Security

As mentioned earlier in the report, SD-WAN technology helps companies cut costs through utilizing connections like broadband that go over public internet. However, that traffic needs to be secured, and this is where Fortinet sets itself apart from the other major SD-WAN players. Fortinet is approaching the convergence of security and networking from the security angle. Through company case studies and our conversations with existing customers, one of the most common reasons for going with Fortinet was the ability to integrate the SD-WAN solution with their Next Generation Firewall creating Secure SD-WAN. Customers frequently mentioned having a single pane of glass, using other Fortinet solutions like Forti Manger and Forti Analyzer, was something that stood out. Lastly, some customers did mention the throughput being a differentiator given that FTNT develops tis own ASIC chip, however this was not a big priority for all customers. In addition, the SD-WAN product has far reach with the multitude of deployment options, allowing the solution to help SMB customers but also scale up to larger enterprises.

### Future investments in MSP channel

An area of focus as of late for Fortinet has been in developing service provider partnerships, evidenced by announcements with Orange back in November of 2019. This can be an important channel, especially in SASE deployment. FTNT also recently purchased OPAQ, a cloud security and networking company to expand some of the SASE offerings by MSSP service providers ([See our takeaways here](#)). In terms of where FTNT can further develop its capabilities is in cloud security, where we believe Palo Alto through its acquisitions has a step ahead in being able to deliver a platform with SD-WAN and Cloud Security rivaling what Zscaler is doing in its partnerships with vendors like VeloCloud.

### Zscaler – Partnering with SDWAN Vendors

MPLS is expensive, and we believe Zscaler, though not an SD-WAN player, is also capturing part of the +\$20 billion in annual MPLS spend. Through our research we have found that Zscaler is commonly deployed in conjunction with an SD-WAN solution. Zscaler is integrated into the SD-WAN software, it recognizes the application/destination, and based on that can point the traffic to Zscaler. Zscaler has



integrations with all the major SD-WAN providers given the potential simultaneous rollout. Table 11, below, shows the SD-WAN partners for Zscaler.

**Table 11: Zscaler Partners with the Major SD-WAN Providers**

SD-WAN Vendor	SDWAN Market Share (2019)
Aruba	
Aryaka	#9
Citrix	
CloudGenix	#6
Cradlepoint	#9
FatPipe	
infovista	
Lancom	
ngena	
Nuage Networks (Nokia)	#7
Riverbed	
Silverpeak	#4
Talari Network (Oracle)	
VeloCloud (VMware)	#2
Viptela (Cisco)	#1
128 Technology	

Source: Company Website, Gartner

### **Telco service provider channel partners helping Zscaler adoption**

Service providers are the ones who provide the MPLS connections and, in recognition of the market declining, are providing managed security offerings with SD-WAN paired with Zscaler. This way, the service provider holds on (monetizes) as much of the original MPLS business as possible. We believe the opportunity for Zscaler is bigger than what the opportunity is for SD-WAN, given the opportunity to take share from spending on traditional firewalls vendors.

### **Watching to see if SD-WAN partners start to become competitive**

But we are watching what SD-WAN providers are doing in the development of their own security clouds. VMware is looking to roll out its own cloud security solution through a partnership with Menlo Security. In the very large enterprises, we have often found Zscaler deployed with Cisco's Viptela and VMware's VeloCloud, and that is thanks in part to Service providers.

### **Cloudflare – Newest Disruptor in the Market**

In our CDN and Cloud Security report ([here](#)), we mention how Cloudflare began in the mid-market and traditionally sought to challenge legacy vendors in Performance/Reliability (DNS, Load Balancing) and Security (DDOS, WAF, NGFW, Bot Management) segments. In January 2020, Cloudflare announced Cloudflare for Teams (Access + Gateway), an offering that extended its competition to vendors like Zscaler (vs the ZPA product). On October 12<sup>th</sup>, NET launched Cloudflare One, which integrated the different existing solutions into a platform and introduced new offerings like Magic WAN and Magic Firewall. This brings Cloudflare into competition with Zscaler ZIA and could offer opportunities to partner with SD-WAN vendors.

Figure 12: Cloudflare One Overview

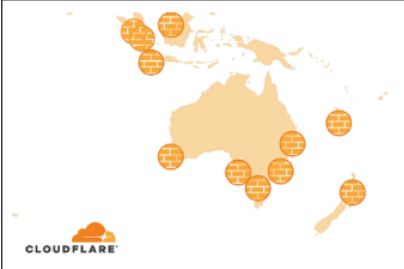

Problem	Band-aids	Cloudflare One
How teams connect trailed the move to the cloud	VPNs, expensive MPLS links, difficult SD-WAN deployments	<b>WARP</b> : Users and endpoints <b>Magic Transit</b> : offices and data centers <b>Magic WAN*</b> : accelerate and route
Defense-in-depth splintered	Point solutions, backhaul of traffic to centralized appliances	<b>Gateway</b> : threat filtering and DLP <b>Magic Firewall*</b> : network layer filtering <b>Access</b> : Zero trust rules for every app <b>Browser</b> : Zero day security for endpoints
High-visibility became high-effort	Data lakes and gaps in log visibility	<b>Cloudflare Logs</b> : capture and standardize <b>Analytics</b> : a single analytics view
Fixing issues relied on best guesses	Virtual appliances and manual configuration	<b>IDS*</b> : detect and stop intrusion attempts <b>EPP</b> : endpoint scanning integrations

\* Launching soon

Source: Company Website

This rollout of Magic Firewall extends the abilities from Magic Transit and, in our view, completes Cloudflare's platform to compete with basic ZIA and ZPA features, though these products are not all generally available yet. In the case of Magic Firewall, Cloudflare uses its extensive network of points of presence (PoPs) and pushes network security to the edge, applying NGFW capabilities at NET's datacenters all over the world, eliminating the need to route traffic back to headquarters where the hardware security stack lays. This is similar to Zscaler, which also leverages its extensive network infrastructure to push security closer to the end user and improves performance and does have some of the architecture attributes of Palo Alto Networks Prisma solution.

Figure 13: Magic Firewall Overview

	
Cloudflare applies firewall policies at every data center	Meaning you have firewalls applying policies across the globe

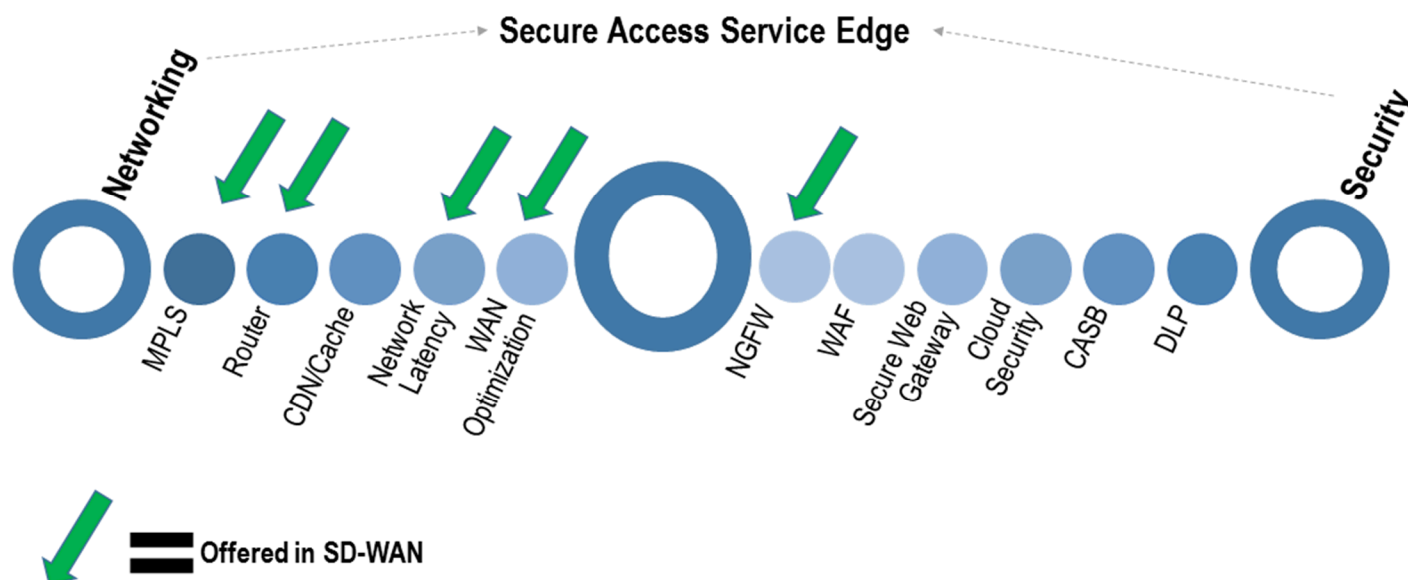
Source: Company Website

## Secure Access Service Edge (SASE) – Comparing and Contrasting to SD-WAN

### What is SASE?

In 2019 Gartner coined the term Secure Access Service Edge, or what is commonly referred to as SASE. The idea behind Gartner's new term was the convergence of security and networking into an integrated platform. Some service providers have tried to bundle different offerings from various vendors, but those are dependent on how smooth the integrations are and can be costly. In the SASE world, networking and security have equal weighting. One can attempt to piece together SASE through Cloud security technology from Zscaler, SD-WAN from VeloCloud, and a Global backbone. But the ability to have one platform that does this all and one management plane is the biggest difference. SD-WAN is a part of the SASE framework addressing some of the networking and security components.

Figure 14: SASE Is the Convergence of Networking and Security

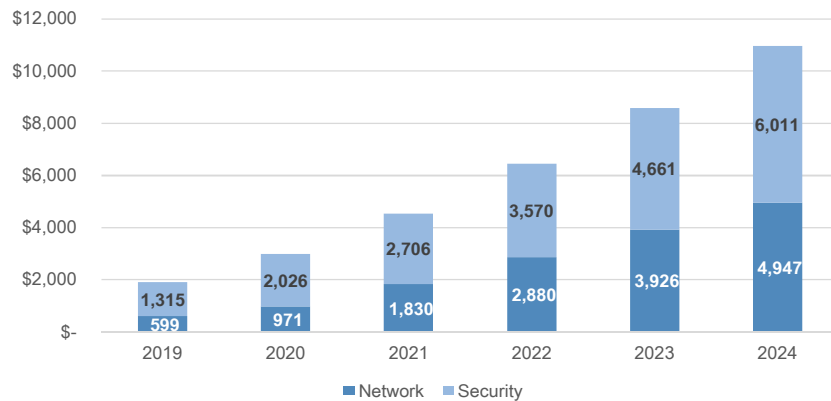


Source: J.P. Morgan Research, Gartner

### Understanding the different vendors in SASE

As mentioned above, some players have just the WAN EDGE and no cloud service (VMware), and some have cloud security service but no WAN edge. Given that SASE gives equal weighting to both, vendors that do not offer the full breadth of solutions will continue to rely on partnerships. We have seen Zscaler's success in this market, partnering with major SD-WAN providers, including situations where service providers have recommended pairing SD-WAN deployments with Zscaler's ZIA. Vendors in this market include PANW, with its cloud security portfolio (Prisma Access, Prisma Cloud) and the acquisition of CloudGenix for SD-WAN. One other player on the private side is Cato Networks, which has its own SD-WAN solution, and a network backbone, using its own PoPs to scale deployments. We see SASE as more of a concept of the further evolution of network and security consolidation, especially on the Enterprise side. We believe the approach will continue to be best of breed, in each segment piecing together the best solutions from vendors.

Figure 15: Gartner SASE +\$10B Forecast Across SD-WAN, Firewall, SWG, CASB, ZTNA

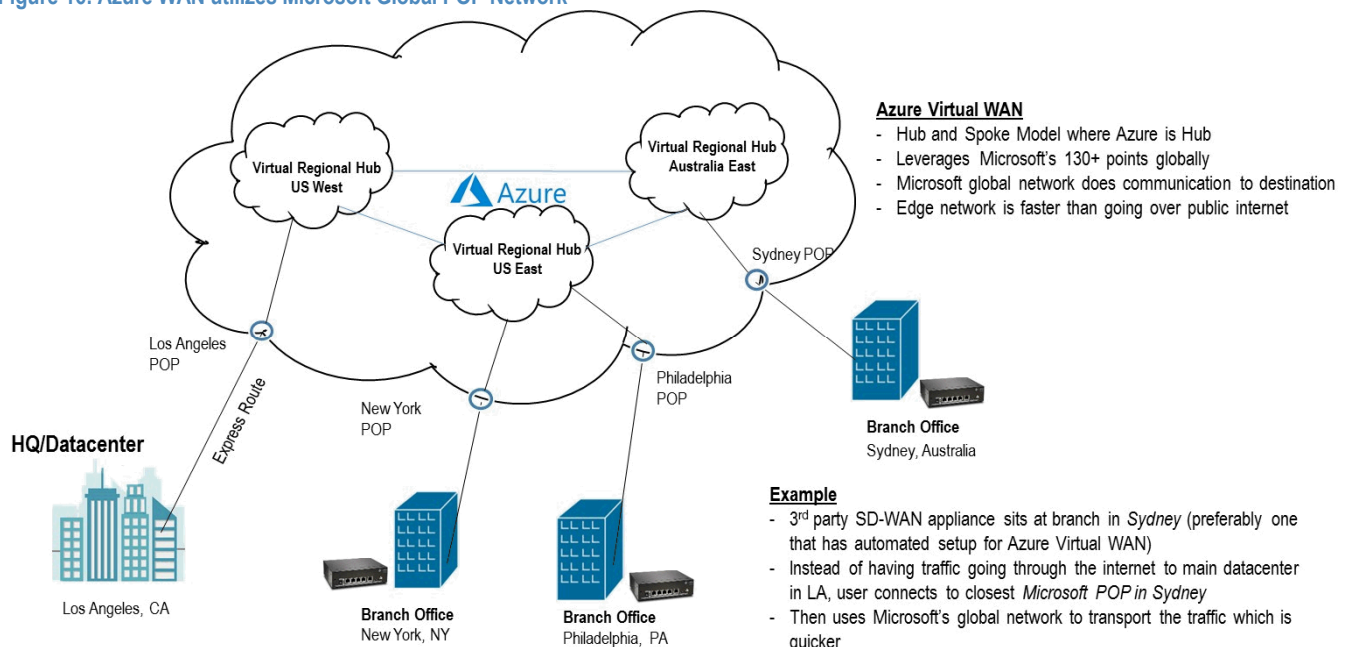


Source: Gartner's Initial Secure Access Service Edge Forecast

## Understanding Where Cloud Providers Fit into SASE

Cloud vendors like Azure offer Virtual WAN solutions that work to transport traffic leveraging the provider's points of presence instead of using internet for long distance transport. Azure Virtual WAN is an example of this, utilizing a hub and spoke model and leveraging the 130+ POPs located worldwide. The hub is Azure, and when a user requests access, it connects to the closest located POP, which is then connected to the Virtual Regional Hubs. The approach of transporting the traffic through the reach of POPs instead of over public internet can be faster.

Figure 16: Azure WAN utilizes Microsoft Global POP Network



Source: J.P. Morgan Research, Microsoft Azure

Cloud vendors do play in SD-WAN, however we do not see them taking over SD-WAN given that the edge appliance would need to be provided through partner devices that come pre-integrations from vendors like Cisco, Barracuda, CloudGenix, etc. In addition, while vendors like Azure do offer Firewall security, that would in most cases be different from what is used at the datacenter or other parts of the networks, creating another level of complexity in terms of orchestration and managing security politics. Lastly, given the use of multi public clouds, this would create a limitation for centralizing security and networking among different cloud vendor workloads.

**Analyst Certification:** The Research Analyst(s) denoted by an “AC” on the cover of this report certifies (or, where multiple Research Analysts are primarily responsible for this report, the Research Analyst denoted by an “AC” on the cover or within the document individually certifies, with respect to each security or issuer that the Research Analyst covers in this research) that: (1) all of the views expressed in this report accurately reflect the Research Analyst’s personal views about any and all of the subject securities or issuers; and (2) no part of any of the Research Analyst’s compensation was, is, or will be directly or indirectly related to the specific recommendations or views expressed by the Research Analyst(s) in this report. For all Korea-based Research Analysts listed on the front cover, if applicable, they also certify, as per KOFIA requirements, that the Research Analyst’s analysis was made in good faith and that the views reflect the Research Analyst’s own opinion, without undue influence or intervention.

All authors named within this report are Research Analysts unless otherwise specified. In Europe, Sector Specialists (Sales and Trading) may be shown on this report as contacts but are not authors of the report or part of the Research Department.

## Important Disclosures

- Gartner: All statements in this report attributable to Gartner represent J.P. Morgan’s interpretation of data opinion or viewpoints published as part of a syndicated subscription service by Gartner, Inc., and have not been reviewed by Gartner. Each Gartner publication speaks as of its original publication date (and not as of the date of this report). The opinions expressed in Gartner publications are not representations of fact, and are subject to change without notice.

**Company-Specific Disclosures:** Important disclosures, including price charts and credit opinion history tables, are available for compendium reports and all J.P. Morgan–covered companies by visiting <https://www.jpmm.com/research/disclosures>, calling 1-800-477-0406, or e-mailing [research.disclosure.inquiries@jpmorgan.com](mailto:research.disclosure.inquiries@jpmorgan.com) with your request. J.P. Morgan’s Strategy, Technical, and Quantitative Research teams may screen companies not covered by J.P. Morgan. For important disclosures for these companies, please call 1-800-477-0406 or e-mail [research.disclosure.inquiries@jpmorgan.com](mailto:research.disclosure.inquiries@jpmorgan.com).

## Explanation of Equity Research Ratings, Designations and Analyst(s) Coverage Universe:

J.P. Morgan uses the following rating system: Overweight [Over the next six to twelve months, we expect this stock will outperform the average total return of the stocks in the analyst’s (or the analyst’s team’s) coverage universe.] Neutral [Over the next six to twelve months, we expect this stock will perform in line with the average total return of the stocks in the analyst’s (or the analyst’s team’s) coverage universe.] Underweight [Over the next six to twelve months, we expect this stock will underperform the average total return of the stocks in the analyst’s (or the analyst’s team’s) coverage universe.] Not Rated (NR): J.P. Morgan has removed the rating and, if applicable, the price target, for this stock because of either a lack of a sufficient fundamental basis or for legal, regulatory or policy reasons. The previous rating and, if applicable, the price target, no longer should be relied upon. An NR designation is not a recommendation or a rating. In our Asia (ex-Australia and ex-India) and U.K. small- and mid-cap equity research, each stock’s expected total return is compared to the expected total return of a benchmark country market index, not to those analysts’ coverage universe. If it does not appear in the Important Disclosures section of this report, the certifying analyst’s coverage universe can be found on J.P. Morgan’s research website, [www.jpmorganmarkets.com](http://www.jpmorganmarkets.com).

**Coverage Universe: Auty, Sterling P:** Adobe Inc (ADBE), Akamai Technologies, Inc. (AKAM), Autodesk (ADSK), Avalara (AVLR), Check Point Software (CHKP), Cloudflare (NET), CoStar Group (CSGP), CrowdStrike (CRWD), CyberArk (CYBR), Datadog (DDOG), DocuSign (DOCU), Duck Creek (DCT), Dynatrace (DT), Everbridge (EVBG), FireEye (FEYE), Five9 (FIVN), Fortinet, Inc (FTNT), GoDaddy Inc (GDDY), Guidewire Software (GWRE), Intuit (INTU), JFrog (FROG), Jamf (JAMF), LivePerson (LPSN), Mimecast (MIME), New Relic (NEWR), Okta (OKTA), PTC Inc (PTC), PagerDuty (PD), Palo Alto Networks (PANW), Pluralsight (PS), Q2 Holdings Inc. (Q TWO), Qualys (QLYS), RealPage (RP), RingCentral (RNG), SecureWorks (SCWX), ServiceNow (NOW), SolarWinds (SWI), Tenable (TENB), Tufin Software (TUFN), Varonis Systems (VRNS), Veeva Systems (VEEV), VeriSign (VRSN), Vonage (VG), Wix.com (WIX), Zoom Video (ZM)

## J.P. Morgan Equity Research Ratings Distribution, as of October 10, 2020

	Overweight (buy)	Neutral (hold)	Underweight (sell)
J.P. Morgan Global Equity Research Coverage	47%	39%	14%
IB clients*	52%	49%	37%
JPMS Equity Research Coverage	46%	40%	14%
IB clients*	75%	70%	55%

\*Percentage of subject companies within each of the "buy," "hold" and "sell" categories for which J.P. Morgan has provided investment banking services within the previous 12 months. Please note that the percentages might not add to 100% because of rounding.

For purposes only of FINRA ratings distribution rules, our Overweight rating falls into a buy rating category; our Neutral rating falls into a hold rating category; and our Underweight rating falls into a sell rating category. Please note that stocks with an NR designation are not included in the table above. This information is current as of the end of the most recent calendar quarter.



**Equity Valuation and Risks:** For valuation methodology and risks associated with covered companies or price targets for covered companies, please see the most recent company-specific research report at <http://www.jpmorganmarkets.com>, contact the primary analyst or your J.P. Morgan representative, or email [research.disclosure.inquiries@jpmorgan.com](mailto:research.disclosure.inquiries@jpmorgan.com). For material information about the proprietary models used, please see the Summary of Financials in company-specific research reports and the Company Tearsheets, which are available to download on the company pages of our client website, <http://www.jpmorganmarkets.com>. This report also sets out within it the material underlying assumptions used.

**Analysts' Compensation:** The research analysts responsible for the preparation of this report receive compensation based upon various factors, including the quality and accuracy of research, client feedback, competitive factors, and overall firm revenues.

## Other Disclosures

J.P. Morgan is a marketing name for investment banking businesses of JPMorgan Chase & Co. and its subsidiaries and affiliates worldwide.

All research material made available to clients are simultaneously available on our client website, J.P. Morgan Markets, unless specifically permitted by relevant laws. Not all research content is redistributed, e-mailed or made available to third-party aggregators. For all research material available on a particular stock, please contact your sales representative.

Any long form nomenclature for references to China; Hong Kong; Taiwan; and Macau within this research material are Mainland China; Hong Kong SAR, China; Taiwan, China; and Macau SAR, China.

**Options and Futures related research:** If the information contained herein regards options- or futures-related research, such information is available only to persons who have received the proper options or futures risk disclosure documents. Please contact your J.P. Morgan Representative or visit <https://www.theocc.com/components/docs/riskstoc.pdf> for a copy of the Option Clearing Corporation's Characteristics and Risks of Standardized Options or [http://www.finra.org/sites/default/files/Security\\_Futures\\_Risk\\_Disclosure\\_Statement\\_2018.pdf](http://www.finra.org/sites/default/files/Security_Futures_Risk_Disclosure_Statement_2018.pdf) for a copy of the Security Futures Risk Disclosure Statement.

**Changes to Interbank Offered Rates (IBORs) and other benchmark rates:** Certain interest rate benchmarks are, or may in the future become, subject to ongoing international, national and other regulatory guidance, reform and proposals for reform. For more information, please consult: [https://www.jpmorgan.com/global/disclosures/interbank\\_offered\\_rates](https://www.jpmorgan.com/global/disclosures/interbank_offered_rates)

**Private Bank Clients:** Where you are receiving research as a client of the private banking businesses offered by JPMorgan Chase & Co. and its subsidiaries ("J.P. Morgan Private Bank"), research is provided to you by J.P. Morgan Private Bank and not by any other division of J.P. Morgan, including, but not limited to, the J.P. Morgan Corporate and Investment Bank and its Global Research division.

**Legal entity responsible for the production and distribution of research:** The legal entity identified below the name of the Reg AC Research Analyst who authored this material is the legal entity responsible for the production of this research. Where multiple Reg AC Research Analysts authored this material with different legal entities identified below their names, these legal entities are jointly responsible for the production of this research. Research Analysts from various J.P. Morgan affiliates may have contributed to the production of this material but may not be licensed to carry out regulated activities in your jurisdiction (and do not hold themselves out as being able to do so). Unless otherwise stated below, this material has been distributed by the legal entity responsible for production. If you have any queries, please contact the relevant Research Analyst in your jurisdiction or the entity in your jurisdiction that has distributed this research material.

## Legal Entities Disclosures and Country-/Region-Specific Disclosures:

**Argentina:** JPMorgan Chase Bank N.A Sucursal Buenos Aires is regulated by Banco Central de la República Argentina ("BCRA"- Central Bank of Argentina) and Comisión Nacional de Valores ("CNV"- Argentinian Securities Commission) - ALYC y AN Integral N°51). **Australia:** J.P. Morgan Securities Australia Limited ("JPMSAL") (ABN 61 003 245 234/AFS Licence No: 238066) is regulated by the Australian Securities and Investments Commission and is a Market, Clearing and Settlement Participant of ASX Limited and CHIX. This material is issued and distributed in Australia by or on behalf of JPMSAL only to "wholesale clients" (as defined in section 761G of the Corporations Act 2001). A list of all financial products covered can be found by visiting <https://www.jpmm.com/research/disclosures>. J.P. Morgan seeks to cover companies of relevance to the domestic and international investor base across all Global Industry Classification Standard (GICS) sectors, as well as across a range of market capitalisation sizes. If applicable, in the course of conducting public side due diligence on the subject company(ies), the Research Analyst team may at times perform such diligence through corporate engagements such as site visits, discussions with company representatives, management presentations, etc. Research issued by JPMSAL has been prepared in accordance with J.P. Morgan Australia's Research Independence Policy which can be found at the following link: [J.P. Morgan Australia - Research Independence Policy](#). **Brazil:** Banco J.P. Morgan S.A. is regulated by the Comissão de Valores Mobiliários (CVM) and by the Central Bank of Brazil. Ombudsman J.P. Morgan: 0800-7700847 / [ouvidoria.jp.morgan@jpmorgan.com](mailto:ouvidoria.jp.morgan@jpmorgan.com). **Canada:** J.P. Morgan Securities Canada Inc. is a registered investment dealer, regulated by the Investment Industry Regulatory Organization of Canada and the Ontario Securities Commission and is the participating member on

Canadian exchanges. This material is distributed in Canada by or on behalf of J.P.Morgan Securities Canada Inc. **China:** J.P. Morgan Securities (China) Company Limited has been approved by CSRC to conduct the securities investment consultancy business. **Dubai:** JPMorgan Chase Bank, N.A., Dubai Branch is regulated by the Dubai Financial Services Authority (DFSA) and its registered address is Dubai International Financial Centre - The Gate, West Wing, Level 3 and 9 PO Box 506551, Dubai, UAE. This material has been distributed to persons regarded as professional clients or market counterparties as defined under the DFSA rules. **Germany:** This material is distributed in Germany by J.P. Morgan Securities plc, Frankfurt Branch, which is regulated by the Bundesanstalt für Finanzdienstleistungsaufsicht and also by J.P. Morgan AG ("JPM AG"), which is a member of the Frankfurt Stock Exchange, is authorised by the European Central Bank ("ECB") and is regulated by the Federal Financial Supervisory Authority (BaFin), JPM AG is a company incorporated in the Federal Republic of Germany with a registered office at Taunustor 1, 60310 Frankfurt am Main, the Federal Republic of Germany. **Hong Kong:** J.P. Morgan Securities (Asia Pacific) Limited (CE number AAJ321) is regulated by the Hong Kong Monetary Authority and the Securities and Futures Commission in Hong Kong, and J.P. Morgan Broking (Hong Kong) Limited (CE number AAB027) is regulated by the Securities and Futures Commission in Hong Kong. JP Morgan Chase Bank, N.A., Hong Kong is organized under the laws of the United States with limited liability. **India:** J.P. Morgan India Private Limited (Corporate Identity Number - U67120MH1992FTC068724), having its registered office at J.P. Morgan Tower, Off. C.S.T. Road, Kalina, Santacruz - East, Mumbai - 400098, is registered with the Securities and Exchange Board of India (SEBI) as a 'Research Analyst' having registration number INH000001873. J.P. Morgan India Private Limited is also registered with SEBI as a member of the National Stock Exchange of India Limited and the Bombay Stock Exchange Limited (SEBI Registration Number - INZ000239730) and as a Merchant Banker (SEBI Registration Number - MB/INM000002970). Telephone: 91-22-6157 3000, Facsimile: 91-22-6157 3990 and Website: [www.jpmpi.com](http://www.jpmpi.com). For non-local research material, this material is not distributed in India by J.P. Morgan India Private Limited. **Indonesia:** PT J.P. Morgan Sekuritas Indonesia is a member of the Indonesia Stock Exchange and is regulated by the OJK a.k.a. BAPEPAM LK. **Korea:** This material is issued and distributed in Korea by or through J.P. Morgan Securities (Far East) Limited, Seoul Branch, which is a member of the Korea Exchange (KRX) and is regulated by the Financial Services Commission (FSC) and the Financial Supervisory Service (FSS). **Japan:** JPMorgan Securities Japan Co., Ltd. and JPMorgan Chase Bank, N.A., Tokyo Branch are regulated by the Financial Services Agency in Japan. **Malaysia:** This material is issued and distributed in Malaysia by JPMorgan Securities (Malaysia) Sdn Bhd (18146-X), which is a Participating Organization of Bursa Malaysia Berhad and holds a Capital Markets Services License issued by the Securities Commission in Malaysia. **Mexico:** J.P. Morgan Casa de Bolsa, S.A. de C.V. and J.P. Morgan Grupo Financiero are members of the Mexican Stock Exchange and are authorized to act as a broker dealer by the National Banking and Securities Exchange Commission. **New Zealand:** This material is issued and distributed by JPMSAL in New Zealand only to "wholesale clients" (as defined in the Financial Advisers Act 2008). JPMSAL is registered as a Financial Service Provider under the Financial Service providers (Registration and Dispute Resolution) Act of 2008. **Pakistan:** J. P. Morgan Pakistan Broking (Pvt.) Ltd is a member of the Karachi Stock Exchange and regulated by the Securities and Exchange Commission of Pakistan. **Philippines:** J.P. Morgan Securities Philippines Inc. is a Trading Participant of the Philippine Stock Exchange and a member of the Securities Clearing Corporation of the Philippines and the Securities Investor Protection Fund. It is regulated by the Securities and Exchange Commission. **Russia:** CB J.P. Morgan Bank International LLC is regulated by the Central Bank of Russia. **Singapore:** This material is issued and distributed in Singapore by or through J.P. Morgan Securities Singapore Private Limited (JPMSS) [MCI (P) 018/04/2020 and Co. Reg. No.: 199405335R], which is a member of the Singapore Exchange Securities Trading Limited, and/or JPMorgan Chase Bank, N.A., Singapore branch (JPMCB Singapore) [MCI (P) 052/09/2020], both of which are regulated by the Monetary Authority of Singapore. This material is issued and distributed in Singapore only to accredited investors, expert investors and institutional investors, as defined in Section 4A of the Securities and Futures Act, Cap. 289 (SFA). This material is not intended to be issued or distributed to any retail investors or any other investors that do not fall into the classes of "accredited investors," "expert investors" or "institutional investors," as defined under Section 4A of the SFA. Recipients of this material in Singapore are to contact JPMSS or JPMCB Singapore in respect of any matters arising from, or in connection with, the material. As at the date of this material, JPMSS is a designated market maker for certain structured warrants listed on the Singapore Exchange where the underlying securities may be the securities discussed in this material. Arising from its role as a designated market maker for such structured warrants, JPMSS may conduct hedging activities in respect of such underlying securities and hold or have an interest in such underlying securities as a result. The updated list of structured warrants for which JPMSS acts as designated market maker may be found on the website of the Singapore Exchange Limited: <http://www.sgx.com>. **South Africa:** J.P. Morgan Equities South Africa Proprietary Limited is a member of the Johannesburg Securities Exchange and is regulated by the Financial Services Board. **Taiwan:** J.P. Morgan Securities (Taiwan) Limited is a participant of the Taiwan Stock Exchange (company-type) and regulated by the Taiwan Securities and Futures Bureau. Material relating to equity securities is issued and distributed in Taiwan by J.P. Morgan Securities (Taiwan) Limited, subject to the license scope and the applicable laws and the regulations in Taiwan. According to Paragraph 2, Article 7-1 of Operational Regulations Governing Securities Firms Recommending Trades in Securities to Customers (as amended or supplemented) and/or other applicable laws or regulations, please note that the recipient of this material is not permitted to engage in any activities in connection with the material that may give rise to conflicts of interests, unless otherwise disclosed in the "Important Disclosures" in this material. **Thailand:** This material is issued and distributed in Thailand by JPMorgan Securities (Thailand) Ltd., which is a member of the Stock Exchange of Thailand and is regulated by the Ministry of Finance and the Securities and Exchange Commission, and its registered address is 3rd Floor, 20 North Sathorn Road, Silom, Bangrak, Bangkok 10500. **UK and European Economic Area (EEA):** J.P. Morgan Securities plc ("JPMS plc") is a member of the London Stock Exchange and is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Registered in England & Wales No. 2711006. Registered Office 25 Bank Street, London, E14 5JP. Unless specified to the contrary, material is distributed in the UK and the EEA by JPMS plc. This material is directed in the UK only to: (a) persons having professional experience in matters relating

to investments falling within article 19(5) of the Financial Services and Markets Act 2000 (Financial Promotion) (Order) 2005 ("the FPO"); (b) persons outlined in article 49 of the FPO (high net worth companies, unincorporated associations or partnerships, the trustees of high value trusts, etc.); or (c) any persons to whom this communication may otherwise lawfully be made; all such persons being referred to as "relevant persons". This material must not be acted on or relied on by persons who are not relevant persons. Any investment or investment activity to which this material relates is only available to relevant persons and will be engaged in only with relevant persons. Research issued by JPMS plc has been prepared in accordance with JPMS plc's policy for prevention and avoidance of conflicts of interest related to the production of Research which can be found at the following link: [J.P. Morgan EMEA - Research Independence Policy](#). U.S.: J.P. Morgan Securities LLC ("JPMS") is a member of the NYSE, FINRA, SIPC, and the NFA. JPMorgan Chase Bank, N.A. is a member of the FDIC. Material published by non-U.S. affiliates is distributed in the U.S. by JPMS who accepts responsibility for its content.

**General:** Additional information is available upon request. The information in this material has been obtained from sources believed to be reliable. While all reasonable care has been taken to ensure that the facts stated in this material are accurate and that the forecasts, opinions and expectations contained herein are fair and reasonable, JPMorgan Chase & Co. or its affiliates and/or subsidiaries (collectively J.P. Morgan) make no representations or warranties whatsoever to the completeness or accuracy of the material provided, except with respect to any disclosures relative to J.P. Morgan and the Research Analyst's involvement with the issuer that is the subject of the material. Accordingly, no reliance should be placed on the accuracy, fairness or completeness of the information contained in this material. Any data discrepancies in this material could be the result of different calculations and/or adjustments. J.P. Morgan accepts no liability whatsoever for any loss arising from any use of this material or its contents, and neither J.P. Morgan nor any of its respective directors, officers or employees, shall be in any way responsible for the contents hereof, apart from the liabilities and responsibilities that may be imposed on them by the relevant regulatory authority in the jurisdiction in question, or the regulatory regime thereunder. Opinions, forecasts or projections contained in this material represent J.P. Morgan's current opinions or judgment as of the date of the material only and are therefore subject to change without notice. Periodic updates may be provided on companies/industries based on company-specific developments or announcements, market conditions or any other publicly available information. There can be no assurance that future results or events will be consistent with any such opinions, forecasts or projections, which represent only one possible outcome. Furthermore, such opinions, forecasts or projections are subject to certain risks, uncertainties and assumptions that have not been verified, and future actual results or events could differ materially. The value of, or income from, any investments referred to in this material may fluctuate and/or be affected by changes in exchange rates. All pricing is indicative as of the close of market for the securities discussed, unless otherwise stated. Past performance is not indicative of future results. Accordingly, investors may receive back less than originally invested. This material is not intended as an offer or solicitation for the purchase or sale of any financial instrument. The opinions and recommendations herein do not take into account individual client circumstances, objectives, or needs and are not intended as recommendations of particular securities, financial instruments or strategies to particular clients. The recipients of this material must make their own independent decisions regarding any securities or financial instruments mentioned herein and should seek advice from such independent financial, legal, tax or other adviser as they deem necessary. J.P. Morgan may trade as a principal on the basis of the Research Analysts' views and research, and it may also engage in transactions for its own account or for its clients' accounts in a manner inconsistent with the views taken in this material, and J.P. Morgan is under no obligation to ensure that such other communication is brought to the attention of any recipient of this material. Others within J.P. Morgan, including Strategists, Sales staff and other Research Analysts, may take views that are inconsistent with those taken in this material. Employees of J.P. Morgan not involved in the preparation of this material may have investments in the securities (or derivatives of such securities) mentioned in this material and may trade them in ways different from those discussed in this material.

"Other Disclosures" last revised October 10, 2020.

---

**Copyright 2020 JPMorgan Chase & Co. All rights reserved. This material or any portion hereof may not be reprinted, sold or redistributed without the written consent of J.P. Morgan.**