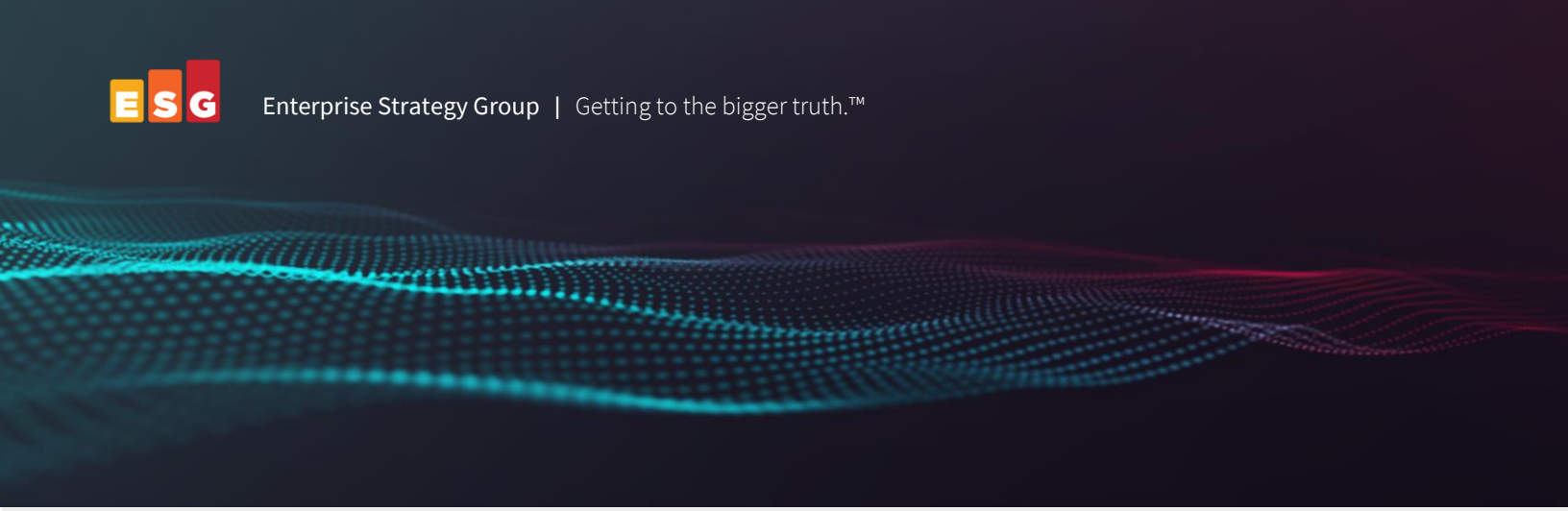


ESG WHITE PAPER

Top Ten Considerations for Your Next-generation SD-WAN

By Bob Laliberte, ESG Senior Analyst; and Leah Matuson, Research Analyst

March 2021

This ESG White Paper was commissioned by Palo Alto Networks and is distributed under license from ESG.

Contents

Networking in a Modern, Distributed Cloud Environment

The need for organizations to change to meet evolving business environments is not a new concept. However, what is new in our current moment is the pace of change. Organizations across all industries now have to adapt to a rapidly evolving IT and application environment. These changes have been accelerated by a global pandemic that is forcing employees to work remotely and by the adoption of modern applications that are distributed across corporate data centers, multiple public clouds, and increasingly, edge locations. Unfortunately, both of these efforts create more IT complexity.

Given these drivers, it should come as no surprise that organizations have accelerated their digital transformation efforts. In fact, according to ESG research, 22% of organizations report that their digital transformation initiatives are mature (having implemented and optimized several initiatives), while another 50% report that their initiatives are in process (currently implementing and executing initiatives),[1] as compared to just 12 months ago where 19% of organizations were digitally mature and only 39% were in process.

It is also important to note why these organizations are embarking on these digital transformation journeys. ESG research found that organizations' top goals for these digital transformation efforts include the ability to drive greater operational efficiencies (56%), the adoption of tools and processes to allow users to interact and collaborate in new ways (49%), and the ability to provide better and differentiated customer experiences (40%). Clearly, all these goals (see Figure 1) are meant to enable organizations to embrace those changes and ensure continued business resilience.

Figure 1. Digital Transformation

Source: Enterprise Strategy Group

Highly Distributed Environments Need to be Connected

The pandemic, in addition to shifting employees to work remotely, has also been a driving force to accelerate the shift of applications to the cloud. In fact, ESG research shows that one of the most significant lasting impacts of the pandemic will be the increased adoption of cloud applications (24%). Additionally, nearly half (45%) of respondents report that their organizations now have a cloud-first strategy for deploying new applications, up from 38% last year.

[1] Source: ESG Research Report, *2021 Technology Spending Intentions Survey*, January 2021. All ESG research references and charts in this eBook have been taken from this research report, unless otherwise noted.

For these highly distributed environments, organizations not only need to ensure connectivity, but also security. Business-critical data and applications are no longer confined to on-premises data centers. Employees can work from anywhere on almost any device. As a result, both applications and users must be protected, regardless of location. With a fluid perimeter and growing attack surface, ESG research reveals that strengthening cybersecurity is the most commonly cited business initiative (47%) driving technology spending this year (see Figure 2).

Figure 2. Focus on Cloud and Security

Source: Enterprise Strategy Group

To connect and protect a highly distributed environment, organizations must implement network solutions that have tightly integrated security, while still ensuring the requisite level of performance and positive customer experiences. According to ESG research, organizations will be spending more now to implement long-term technology strategies to provide more flexible and resilient IT infrastructure in the event of future major business disruptions (53%). Furthermore, those organizations with more mature digital transformation initiatives will spend more on IT solutions as well (4.33% increase in organizations with mature initiatives versus just a .15% increase in organizations with no initiatives on their roadmap). Consequently, organizations must be able to implement innovative, next-generation technologies and solutions that ensure seamless and secure application delivery across a highly distributed environment.

Legacy Network and Security Architectures Limit Progress

Unfortunately, most legacy solutions are just not capable of supporting the massive digital transformation taking place across the board. Architectural limitations hinder innovation, impact performance, and often cost more to maintain and operate. These legacy solutions include both hub-and-spoke network architectures and castle and moat security architectures and may also include some first-generation (defined as network-only packet-based) SD-WAN solutions.

Legacy Network Architecture Doesn't Work in Highly Distributed Environments

Hub and Spoke Network Design

Originally designed for consolidated data centers that contained all relevant applications, hub and spoke networks were designed for private data centers that housed most corporate applications not intended for complex and highly distributed modern application environments. In this model, network traffic from a remote site will traverse the data center and then access a cloud-based application or even another remote site. Initially, many remote work solutions mimicked this model,

using VPNs with data center concentrators and firewalls to route traffic to cloud applications. While this approach served as a temporary solution, it is not an appropriate long-term solution. Challenges with a legacy network architecture include:

- Cost of solution. Typically, legacy network solutions leverage expensive and inflexible fixed lines from telecommunications providers. Not only are MPLS links costly, especially in high availability configurations, they may also require a last mile build-out, which can add further expense.
- Lack of agility. Fixed line MPLS networks often require time-consuming build-outs that can delay connections. Plus, with these connections, it may also be time consuming to add or move links. With the increased demand to place applications in edge locations, many organizations struggle to find fixed line connections to these locations.
- Impact to performance. Organizations still using a legacy network architecture are hairpinning network traffic through the data center, which generates unnecessary latency and can impact application performance. These legacy network environments democratize the application traffic, as all the applications (Guest WiFi and SAP) have the same priority and in the event of failure, all of this application traffic will fail over to the backup link. In many cases, this will involve a time-consuming manual process. Also, security is enforced in the data center and can impact network performance.

Legacy SD-WAN also Creates Significant Hurdles

Legacy SD-WAN

While an improvement over the legacy network architecture, many first-generation SD-WAN solutions can also create hurdles when building out a highly distributed modern application environment. These early solutions are heavily focused on the network traffic only and can create the following challenges:

Network layer visibility only: These early solutions are focused on packet-based Layer 3 traffic information and, as such, have limited visibility into the application layer. As a result, these solutions can deliver on network quality-of-service levels, but network teams may struggle to guarantee application service level agreements (SLA). For applications in the cloud and edge, organizations may need to implement additional solutions to provide visibility.

Inconsistent security posture: Most early solutions partnered with security vendors to bolt on security solutions at the branch, which require additional time and effort to install and manage. Additionally, this could also lead to an inconsistent security posture based on an organization's existing edge security solution. This problem is further exacerbated by a highly distributed remote worker environment. In fact, a top challenge related to supporting an increased number of remote workers reported by ESG research respondents was the increased volume of cybersecurity vulnerabilities resulting from remote workers.[2]

Manual processes and procedures: Given the increasing pressure on organizations to deliver positive experiences in an increasingly distributed and complex environment, operations teams cannot be effective using manual processes and procedures. While great strides have been made in day one provisioning activities, in many cases day two operational and lifecycle management tasks are performed manually.

Regardless of the network solution currently used, virtually all organizations struggle to overcome the complexity inherent in highly distributed application and worker environments. In fact, ESG research indicates that three quarters (75%) of respondents believe their IT environment is more complex than it was two years ago, but what is fueling this complexity? The top five drivers reported by respondents highlight the challenges with securely connecting a distributed environment. The drivers include the increase in remote workers due to COVID-19 work-from-home mandates (49%), new data security

[2] Source: ESG Research Report, *The Impact of the COVID-19 Pandemic on Remote Work, 2020 IT Spending, and Future Tech Strategies*, June 2020.

and privacy regulations (38%), higher volumes of data (38%), the changing cybersecurity landscape (35%), and an increase in number and types of endpoints (32%).

RFP Checklist: 10 Things Organizations Need to Move Forward with Long-Term Planning

As organizations move forward, deploying long-term solutions to ensure application-focused, secure connectivity for a highly distributed cloud environment and remote workforce, operations teams should add the following items to their RFP checklist.

Next-generation SD-WAN solutions should:

1. Focus on applications: Digital transformation initiatives and modern application environments result in a highly distributed application environment, and, as such, require solutions that enable users to have a positive experience regardless of application location. Therefore, next-gen SD-WAN solutions need to include Layer 7 application visibility and control. Armed with this higher-level information, organizations can accelerate the migration of applications to the public cloud or multiple public clouds (this should include both IaaS and SaaS) with the assurance that any policy and path decisions are predicated on ensuring application SLAs and not just the network.

2. Be easy to use: Given the already complex environments, organizations need solutions that don't require a PhD to deploy and operate. This includes the ability to rapidly deploy and provision a solution in remote locations without requiring technicians to visit each remote site. Essentially, next-generation SD-WAN solutions need to be plug and play, allowing users to simply connect the power and network to make them operational. Also, given the convergence of networking and security, any solution should include role-based access to ensure both network and security teams can access and create policies.

3. Provide higher levels of automation: The highly distributed environments are becoming so complex that they are exceeding the ability for operations teams to effectively manage them using time-consuming manual tasks. As a result, organizations need to leverage solutions that leverage intelligent automation for tasks that not only include day one provisioning (zero-touch provisioning) but also the ability to automate day two tasks like the ability to self-optimize and self-heal the SD-WAN environment. This includes the ability to rapidly identify the correct domain level at which the issue is located, either the network or application, which in turn can drive faster problem resolution. Technologies such as artificial intelligence and machine learning will be key to underpinning intelligent automation.

4. Leverage cloud management/delivery: Given that most organizations have a distributed workforce due to the pandemic and need to ensure that in the future workers can be productive from any location, it will be imperative that next-generation solutions leverage cloud management. Operations teams need to easily access the management console to create application, security, and compliance policies. The cloud-based management will ensure centralized policies with distributed enforcement at all locations. This is key for day two lifecycle management, as it will ensure that any security patches are automatically delivered, ensuring a consistent security posture. Furthermore, if these cloud-based management solutions leverage modern application architectures, it ensures that new product functionality or security upgrades can be added to the environment seamlessly and in a timely fashion, as opposed to as biannual or annual releases.

5. Facilitate the convergence of network and security: The emergence of the secure access service edge (SASE) framework emphasizes the need for tight integration between network and security functions (and teams). Next-generation SD-WAN with secure access is a great way to get started. However, organizations looking to follow the entire framework need to ensure that additional security capabilities are or will be fully integrated into the solution.

This includes the ability to provision next-generation firewalls (NGFW), zero-trust network access (ZTNA), secure web gateways (SWG), cloud access security brokers (CASB), and remote browser isolation (RBI) services, etc., from the centrally managed cloud console. As previously mentioned, role-based access is important to help with this convergence. Organizations need to decide if they are going to leverage a single vendor for convergence or pursue a best-of-breed approach and understand the pros and cons of each.

6. Ensure high levels of performance: Regardless of the network being used, next-generation SD-WAN solutions need to be able to utilize and optimize traffic over virtually any one or multiple network connections, including MPLS links, internet broadband connections, and cellular networks (including 4G and soon 5G), as well as to use cellular connectivity for a tertiary failover connection. The ability to leverage multiple network links is key to ensuring high availability, including the ability to use fixed lines for primary and failover noted. However, with the rollout of 5G, organizations should also consider this a viable primary link in the near future. Any SD-WAN solution should be able to take full advantage of all available bandwidth to optimize traffic and automatically select the optimal path based on the priority of the application. To do that effectively, solutions should have both Layer 3 (network) and Layer 7 (application) level visibility.

7. Deliver end-to-end visibility: To better understand and optimize the experience, solutions need to have complete end-to-end visibility, from an endpoint device to the application, regardless of where either is located. This could include IoT sensors at edge locations and employees' homes to applications housed in corporate data centers, edge locations, or public clouds. The ability to deliver granular Layer 3 and 7 visibility will accelerate troubleshooting by rapidly isolating network and application issues. Plus, insights gleaned from both environments will also enable organizations to develop policies that are optimized for their specific environments.

8. Reduce costs: Despite growing complexity, IT budgets are still constrained. However, next-generation SD-WAN solutions can dramatically reduce network costs by replacing expensive MPLS links with cost-effective broadband connections. These cost reductions can really add up if an organization was previously using multiple MPLS links for high availability. This is especially true in legacy network architectures (hub and spoke) since the second link is only used for failover. SD-WAN solutions can leverage both in an active-active mode. In addition to the network costs, next-generation solutions that integrate security can reduce the amount of on-premises hardware and software needed at each location, along with any associated maintenance costs.

9. Enable higher levels of agility: The ability to rapidly connect to new locations has proven to be a very important capability during a global pandemic. Next-generation SD-WAN solutions must be able to support employees at both work and home locations. The ability to leverage both fixed line broadband or MPLS and cellular connectivity will provide greater levels of flexibility and agility related to where the technology can be deployed. Another key attribute for next-generation SD-WAN will be the ability to leverage asymmetrical deployments—that is, the ability to connect to the cloud and optimize traffic with just one appliance at the corporate location (as opposed to symmetrical deployments that require an appliance at each end of the connection or very close to the end for SaaS environments).

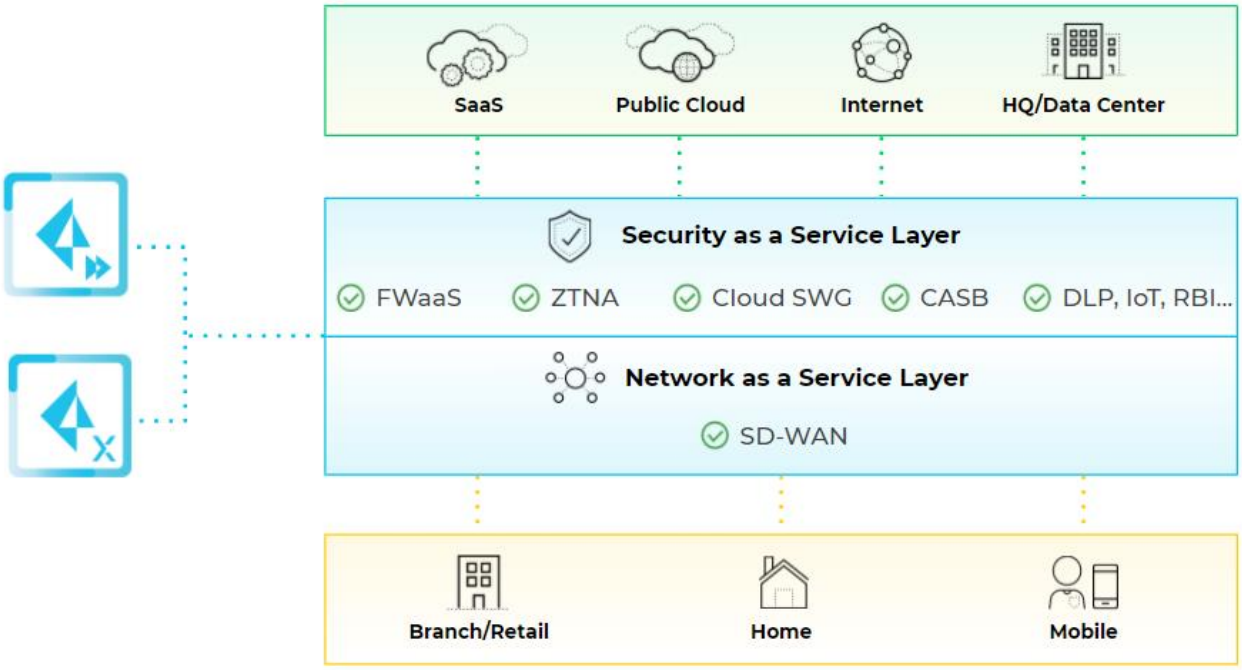
10. Accelerate innovation: This is a very important criterion. The fact that next-generation SD-WAN solutions can help to save on network costs and deliver additional bandwidth is good, but the real value attained from what organizations can do with the additional bandwidth is even more important. Organizations should be thinking about how they can deliver better experiences and innovative new services (such as bandwidth-intensive video or voice apps) to their customers. Next-gen SD-WAN solutions can also be the foundation to consolidate additional services at the edge. Organizations should think beyond SASE and contemplate what other services could be integrated into this solution to extend its value.

Palo Alto Networks Accelerates Next-generation SD-WAN

Solutions Designed to Accelerate the Adoption of Secure Distributed Application Environments

No stranger to creating next-generation technology, Palo Alto Networks has added SD-WAN to the Prisma family when they acquired CloudGenix back in April 2020. The aptly named Prisma SD-WAN (formerly CloudGenix SD-WAN) will enable organizations to take advantage of the next-generation SD-WAN technology to securely connect applications that are distributed across data centers, multiple public clouds, and edge locations to users located in the campus, branch, or home. When combined with Prisma Access, organizations can accelerate the implementation of a comprehensive SASE framework (see Figure 3).

Figure 3. Palo Alto Networks Comprehensive SASE Solution



Source: Palo Alto Networks

Palo Alto Networks Prisma SD-WAN

Palo Alto Networks' Prisma SD-WAN is a next-generation, application-defined solution capable of leveraging cost-effective broadband connections and the ability to take advantage of 4G and 5G networks for backup or even potentially primary connectivity. Prisma SD-WAN will work hand in hand with Prisma Access to deliver a robust SASE solution. The Prisma SD-WAN solution is:

Application-defined

To ensure a positive experience for organizations, despite having both their applications and workers distributed, the Prisma SD-WAN takes advantage of visibility into both Layer 3 network information and Layer 7 application information. Armed with information like CODEC and MOS (mean opinion score) for voice and video, organizations can create better informed policy decisions that will optimize traffic based on application SLAs and not just network SLAs. This level of visibility will ensure a positive experience for workers accessing collaboration tools like Zoom or Teams from branch and

home offices. Plus, the ability to isolate network and application traffic can dramatically reduce troubleshooting times since it enables operations teams to focus their efforts and work more efficiently.

Because Prisma SD-WAN has application visibility, it can provide value to organizations with just one appliance at edge locations (asymmetric deployment). This will increase agility and accelerate the time to benefit from an SD-WAN solution.

Highly automated

Recognizing the need to drive higher levels of operational efficiency, Prisma SD-WAN delivers not only day one automation, but also significant day two automation. To enable organizations to maximize agility and rapidly deploy SD-WAN solutions at remote sites quickly, Prisma SD-WAN leverages zero-touch deployment (ZTD). This allows non-technical staff to connect power and network to devices at remote locations (branch and home with the ION 1000) and allow the centralized cloud-based management solution to provision each device based on preset policies.

Day two automation capabilities include both self-healing and self-optimizing. The self-healing capabilities include the ability to correlate events across to determine the root cause of any problem and rectify it without human intervention. For problems that require additional attention, Palo Alto Networks has streamlined the workflow by integrating with ServiceNow and delivering detailed information regarding any problem from both network and application domains. The ability to leverage dual fixed line and cellular back ensure Prisma SD-WAN can ensure high availability and business resiliency. The other day two automation capability is self-optimization. This automated process ensures that applications traversing the WAN links get and maintain the appropriate levels of service based on the policies established for them. More importantly, Prisma SD-WAN will automatically adjust traffic over the best possible path. This includes the ability to leverage the Palo Alto Networks' cloud native backbone instead of traversing the internet to ensure the best possible performance.

Cloud-delivered

Prisma SD-WAN leverages an easy-to-use cloud-based management console that enables operations teams (NOC, SOC) to leverage role-based access to access information and create policies from corporate locations or home offices. Utilizing the cloud benefits organizations by reducing the amount of hardware that needs to be deployed, while enabling accelerated lifecycle management. Prisma SD-WAN can deploy security patches and new functionality seamlessly, eliminating the need for maintenance windows and downtime.

Another key benefit of utilizing a centralized, cloud-based management console is that the operations team can easily create policies that are instantly distributed to all edge locations. With tight integration with Prisma Access, organizations can ensure a consistent security posture.

Prisma SD-WAN also employs a key technology it refers to as CloudBlades, which is a platform to enable innovation at edge locations. CloudBlades use APIs to tightly integrate third-party services that can be deployed at the edge. In addition to security services, this will provide the opportunity for voice services or other operational services without the need for additional hardware or software. Currently, CloudBlades provides support for Prisma Access, ServiceNow, Microsoft, Slack, Equinix, Amazon, RingCentral, PagerDuty, and more. More importantly, organizations can build their own applications to connect with CloudBlades via a developer program.

Prisma Access, Palo Alto Networks' Comprehensive Cloud-based Security Solution

A proven leader in developing innovative security solutions, Palo Alto Networks developed Prisma Access to enable organizations to extend their security functions to remote corporate locations and remote workers. It provides a comprehensive portfolio of security functionality to accelerate an organization's SASE journey, with cloud-based

management, next-generation networking, and network security services. It also provides end-to-end visibility from the endpoint (including IoT sensors) to the applications located in the cloud.

Prisma Access offers multiple cloud-based security functions, including ZTNA for application access control and threat protection. Firewall-as-a-service (FWaaS) leverages NGFW security to protect remote locations with threat detection. Secure web gateway (SWG) blocks malicious sites and prevents data loss using machine learning (ML). Cloud access security broker (CASB) ensures that network traffic between on-premises devices and cloud providers (Iaas and SaaS) is in compliance with an organization's security policies. Data loss prevention (DLP) acts to prevent breaches and improves compliance and data privacy. Browser isolation/remote browser isolation (BI/RBI) separates browsing activity from endpoint devices, shrinking the attack surface of devices. Internet of things (IoT) security helps protect organizations against potential cyberattacks from network-connected IoT devices, mitigating downtime, lost productivity, and revenue.

The Bigger Truth

In today's always-on business environment, organizations need to invest in long-term business resilience solutions that enable performance and security across a highly distributed environment (both application and users). ESG research validates the accelerated adoption of cloud-based applications. As such, highly available, secure, and performant connectivity is essential to ensure productivity and positive user experiences—without trading off performance for security or vice versa.

To be successful, organizations must focus on the applications. With this mantra in mind, it follows that any technology solutions deployed must employ next-generation technologies that have visibility into the application environment. Innovative solutions that effectively converge network, security, and other capabilities can overcome a variety of limitations created by legacy environments. Only then will companies be able to accelerate the journey to create a robust SASE framework. Taking a single vendor approach to SASE like Palo Alto Networks has done will simplify the integration of network and security technologies, streamline the support, and ensure efficient problem resolution.

Palo Alto Networks' Prisma SD-WAN and Prisma Access checks all the boxes for organizations to deliver application- and network-optimized performance with tightly integrated security to drive innovation across highly distributed cloud and user environments and jumpstart the journey to SASE.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188