ESG WHITE PAPER

Embracing the Hybrid Workforce

How A Unified Network, Security, and Digital Workspace Solution Supports the Modern Enterprise

By John Grady, Senior Analyst; Bob Laliberte, Senior Analyst; and Leah Matuson, Research Analyst

March 2021

This ESG White Paper was commissioned by Citrix and is distributed under license from ESG.

Contents

Executive Summary

In many ways, the pandemic has only served to accelerate significant changes to enterprise IT architectures that were already starting to take hold. Many organizations were struggling to support more distributed environments due to the increasing use of public cloud services and a more mobile workforce well before March 2020. However, the pandemic certainly forced organizations to prioritize these issues and begin to consider more modern network and security solutions to better address the new normal.

The proliferation of applications in the cloud and dispersion of users from corporate locations has significantly complicated user security, access, and application performance. The emergence of secure access service edge (SASE) represents a modernization of security approaches to better address modern distributed environments through convergence with network services in a cloud-centric architecture. Through a unified approach to application delivery, secure access, and digital workspace, organizations can ensure quality of service and consistent security, and maintain efficient management for access across all types of applications for users regardless of location or device.

Through a unified approach to application delivery, secure access, and digital workspace, organizations can ensure quality of service and consistent security, and maintain efficient management for access across all types of applications for users regardless of location or device.

Fundamental Changes to Where and How We Work Have Complicated Securely Connecting Users to Applications

Organizations across the board continue to prioritize digital transformation strategies. Specifically, ESG research has found that nearly three-quarters (72%) of organizations report being in the process of implementing and/or optimizing multiple digital transformation initiatives.[1] The wide umbrella under which digital transformation falls means any number of objectives can drive these projects. However, the most reported objectives of digital transformation include becoming more operationally efficient (56%) and adopting tools and process to allow users to interact and collaborate in new ways (49%). The cloud is clearly a key enabler of digital transformation and can help address both of these objectives. Therefore, it should be no surprise that the traditional castle and moat security model of protecting applications—and hub and spoke architectures to provide access to them—have been rendered ineffective. These models simply cannot support new, highly distributed cloud environments.

Applications Proliferate and Shift to the Cloud

In today's IT landscape, cloud has become nearly ubiquitous. ESG research indicates that 94% of organizations are using public cloud services to one extent or another (e.g., IaaS or SaaS). But more notably, the transition to the cloud will continue to accelerate, with organizations citing that more than three-quarters (79%) of their current on-premises applications and workloads are strong or potential candidates to move to public cloud services over the next five years (see Figure 1).

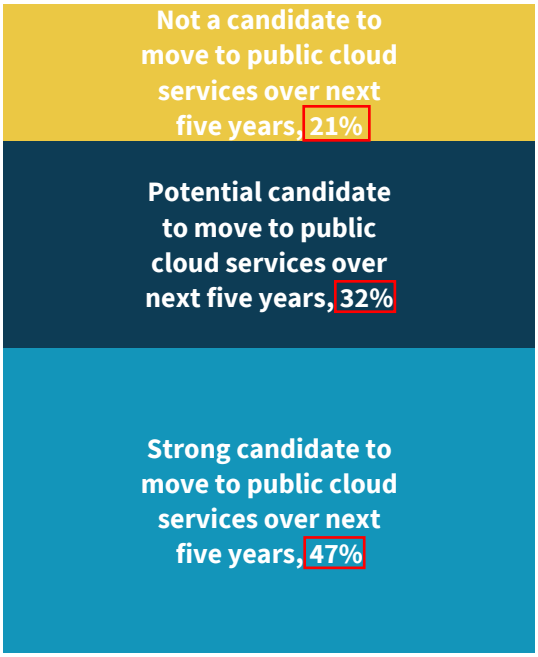
The pandemic has certainly hastened this shift to the cloud, with many organizations anticipating that the most significant and lasting impact of COVID-19 will be the increased adoption of cloud services. Yet, while the term "cloud" is often used whether referring to SaaS, IaaS, or PaaS, the different management responsibilities, security requirements, and access

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

models of each significantly increase the complexity many organizations face when shifting applications to the cloud. As a result, providing consistent and secure connectivity and access to these resources continues to be a challenge for many organizations.

Figure 1. Nearly 8 in 10 Remaining On-premises Workloads Will Be Cloud Candidates over the Next Five Years and COVID Has Caused an Even More Aggressive Cloud Push

Think about all of the applications and workloads that your organization currently runs in your on-premises data centers. What percentage of these workloads are/aren't candidates to move to public cloud services over the next five years? (Percent of respondents, N=664)



Source: Enterprise Strategy Group

The Pandemic Accelerates the Shift to Remote Work

In addition to greater numbers of corporate resources residing in public clouds, the users accessing them are increasingly located outside of the corporate network and corporate-controlled locations. While a growing number of organizations had enabled workers to be mobile to some extent prior to the pandemic, the sudden shift to having a majority of employees work remotely caught many organizations unprepared.

A number of organizations have already asked employees to return to the office and others are looking to return to a more normal state of operations at some point in 2021. Still, a lasting impact of the pandemic for many companies will be a recognition that work is what you do—not where you do it—meaning that location flexibility will be a mandate to ensure business resiliency moving forward.

User Experience, Policy Management, and Security Are Challenged

As a result of these and other changes, the enterprise perimeter has become amorphous. Users who may be anywhere in the world must access corporate applications that may reside in corporate data centers (though these applications are increasingly located in the public cloud) from any number of devices (either corporate or personal) and expect to do so

seamlessly. However, traditional network and security solutions were not designed with these dynamics in mind. As a result, it should come as no surprise that organizations experience significant challenges when attempting to support a distributed environment with on-premises, siloed tools.

Ensuring Quality of Service (Experience)

Maintaining a consistent user experience with regards to corporate applications is no easy feat. Traffic from remote users must traverse not only the public internet where significant bottlenecks can occur, but first battle for often sparse bandwidth on the home network. Think of it as a tug-of-war, with various family members competing for adequate fuel to support their own bandwidth-intensive applications, such as online classes, gaming, or streaming videos. Service chaining separate security tools further stresses performance, adding a layer of inefficiency as to how traffic is processed. For instance, encrypted traffic may need to be decrypted multiple times depending on the number of tools that have been service chained. This process adds latency, impairing performance, and ultimately degrading the user experience.

Consistently Enforcing Security

In addition to performance impact, security efficacy can suffer. With employees working from a variety of locations and accessing resources from assorted devices, it has become difficult for organizations to consistently enforce security. Enforcing security across separate tools depending on what application is being accessed, from which device, and whether the user is on-premises or working remotely is a recipe for complexity at best and security incidents at worst.

Efficiently Managing Policy

Managing policies for disparate sets of tools across various locations and threat vectors remains a significant obstacle for security teams struggling with a shortage of personnel and skills. In fact, ESG research shows that 38% of respondents cite operational inefficiency due to inconsistent policy management across different tools as one of the top issues resulting from the use of disparate tools that have the most negative impact on their business.[2]

Managing policies for disparate sets of tools across various locations and threat vectors remains a significant obstacle for security teams struggling with a shortage of personnel and skills.

Further, managing siloed network and security policies across disparate toolsets slows provisioning, limits network visibility, and ultimately increases operational costs. This means when issues arise, such as slowing application performance, or even experiencing downtime, staff must work across multiple consoles to uncover and address the problems. The process is labor-intensive and time-consuming. The result—rising costs and a negative impact to employee productivity and satisfaction.

Prioritizing Use Cases is A Good Starting Point, But Often Only the Beginning

To address the challenges of ensuring quality of service posed by the amorphous enterprise perimeter, effectively managing policy, and consistently enforcing security, it often makes sense to prioritize organizational needs by starting with solving for a specific use case. While there are many such examples, a handful stand out as critical when considering both the current nature of remote work and the likely evolution to a hybrid workplace environment in the coming months.

[2] Source: ESG Master Survey Results, *Transitioning Network Security Controls to the Cloud*, July 2020.

Applying Consistent Threat Prevention Across Remote and Office Locations

In the past, when most users worked in corporate offices and remote work was the exception rather than the rule, maintaining threat prevention was relatively straightforward. Branch office and remote user traffic was backhauled through the corporate data center for inspection through costly VPN and MPLS solutions. In today's world, with traffic originating from, and destined for, a multitude of locations, achieving that level of consistency through a traditional hairpinned model is much more complicated.

According to ESG research, respondents cited cybersecurity as one of their organization's biggest challenges with regards to the shift to work from home, with 42% reporting that supporting larger numbers of remote workers has increased the volume of cybersecurity vulnerabilities. Thus, shifting security enforcement to the cloud is one viable approach to maintaining consistent threat protection across all locations.

Protecting Users Accessing the Internet and Unmanaged Web Applications

The lines between web usage and cloud application usage have blurred. Whereas five to 10 years ago the secure web gateway was the core control for users accessing the internet, the composition of internet traffic has changed and become more application-centric, shifting the focus to the cloud access security broker (CASB). Not surprisingly, ESG research indicates that nearly one-third (30%) of organizations say that their existing secure web gateway (SWG) solutions are good for URL filtering and threat protection for web usage but do not help secure cloud usage.[3]

The convergence of secure web gateways and cloud access security brokers is critical to providing consistent, centralized policy across all traditional internet and unmanaged web application traffic via a single-pass, proxy-based architecture.

Secure web gateways cannot provide the granular visibility or control to effectively manage the use of personal and unsanctioned cloud applications, creating potentially exploitable blind spots and challenging security teams. Yet, they remain an effective tool for protecting users accessing websites and browsing the internet. CASBs provide more granular application visibility, control, and data governance than secure web gateways are capable of. As a result, the convergence of secure web gateways and cloud access security brokers is critical to providing consistent, centralized policy across all traditional internet and unmanaged web application traffic via a single-pass, proxy-based architecture.

Delivering the Same Experience and Digital Workspace to Users, Regardless of Device or Location

As organizations have expanded their use of SaaS- and IaaS-based applications, users are calling up those applications from different devices, creating inconsistencies as to how they are accessed. A user may need to connect to a VPN to access an internal, on-premises application, while going through a single sign-on portal for web applications. Access to applications from personal devices may need to be blocked in this model due to security concerns. To ensure productivity and user satisfaction, employees must be able to access all corporate applications and services necessary to perform their jobs, ideally from a consistent digital workspace experience, regardless of the ownership of the device used.

Employing Granular, Data-centric Control of Managed SaaS Applications

While employees must have access to those applications necessary to perform their jobs, organizations must be diligent in properly governing their sanctioned SaaS applications. While massive amounts of sensitive corporate data are shifting to the cloud, the critical data protection control point for many organizations has shifted from on-premises data loss

[3] Source: ESG Master Survey Results: *Transitioning Network Security Controls to the Cloud*, July 2020.

prevention solutions to CASBs. CASB support for a broad set of API integrations to business-critical applications is essential to monitor usage and properly enforce data security policy.

Streamlining Provisioning and Ensuring Application Optimization

Prior to the pandemic, organizations needed the ability to connect to a new edge location, either as the result of a merger and acquisition or business growth. At the onset of the pandemic, organizations needed to ensure connectivity to hundreds, or thousands, of home offices to provide optimized experiences for contact center agents or other customer-facing employees. Fortunately, SD-WAN technologies with zero-touch provisioning from centralized policies enabled organizations to roll out this technology in days, not months. Furthermore, the ability to segment and optimize application traffic ensured that mission- or customer-critical applications always took priority and delivered positive experiences. The SD-WAN technology also provides optional cellular backup to ensure high availability in both remote office and home environments.

Supporting Zero-trust Strategies

Interest in zero-trust security approaches has significantly increased over the past few years, with the pandemic further highlighting the need to move beyond a location-based trust model. In fact, ESG research shows that 63% of organizations report incorporating zero-trust tenets into their security program to one extent or another.[4]

While there are many tools that support zero-trust strategies, a few stand out with regards to securing employee access to applications. A growing number of organizations are exploring zero-trust network access (ZTNA) as a replacement for broadly permissive VPN approaches. Additionally, remote browser isolation capabilities that support zero trust by assuming traffic is untrustworthy and isolating it from corporate resources to prevent being compromised are gaining interest. Finally, critical to any zero-trust strategy is the ability to implement a least-privilege approach. This ensures that users only have access to the resources they need and are properly authenticated prior to accessing those resources and that validation continually occurs to ensure any changes in a user's security posture are identified and addressed.

Cloud-delivered Security and SD-WAN Help But Do Not Go Far Enough

To better address these issues, many organizations have begun to move from centralized, appliance-based network security controls towards multi-function, distributed, cloud-delivered solutions for better scalability, flexibility, and performance. Similarly, SD-WAN adoption has accelerated to help streamline provisioning, improve quality of service, and optimize cost.

Yet, while separate cloud security and SD-WAN approaches may solve one or two of the identified use cases, over time, many organizations will need to address most, or even all. Layering on additional tools to solve for each incremental use case becomes costly, inefficient and, ultimately, ineffective. Rather, a platform-based approach that can extend to address additional use cases provides extensibility and investment protection over the long term. However, to effectively provide this broad coverage, a wide-ranging set of capabilities is required.

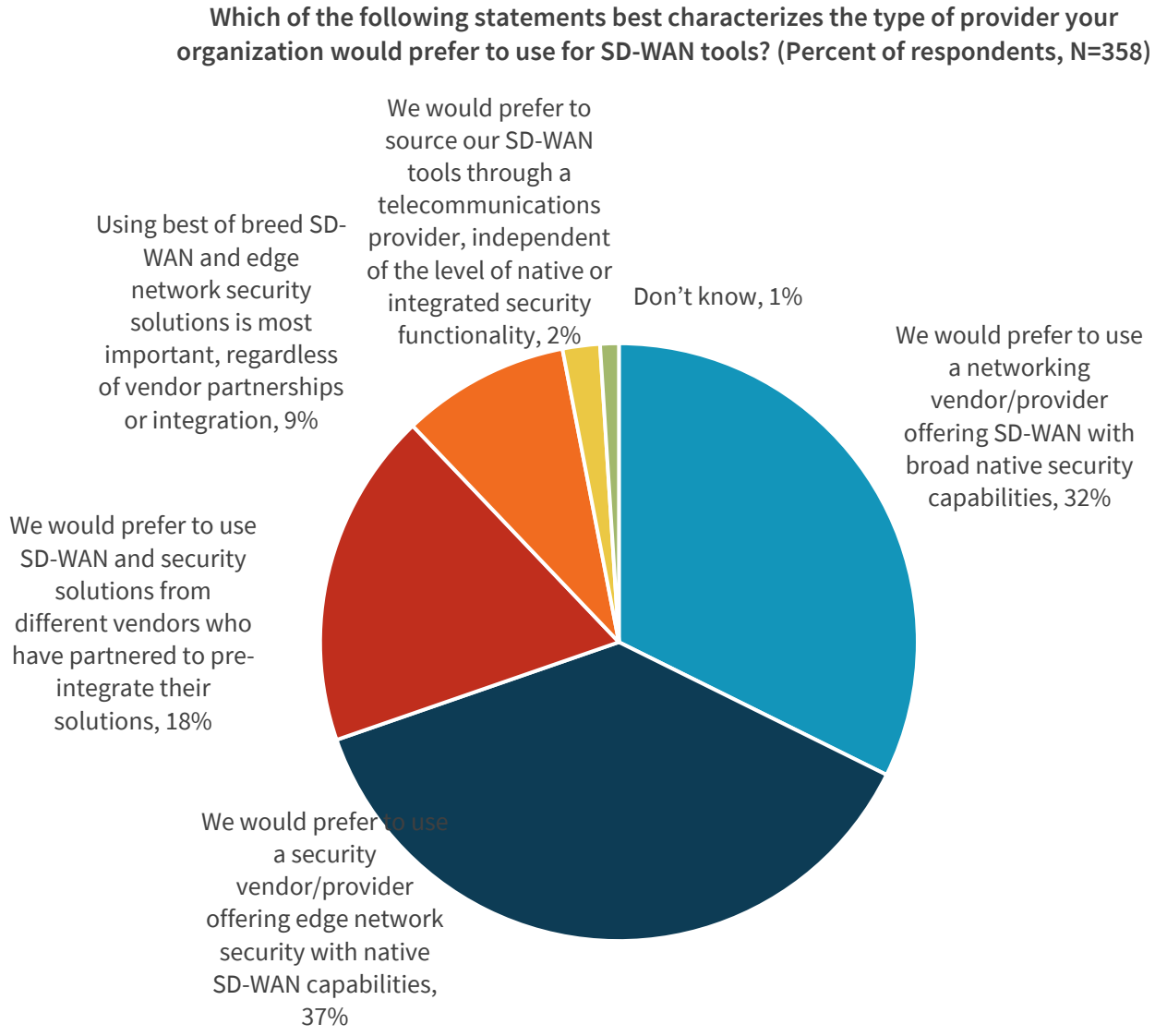
A platform-based approach that can extend to address additional use cases provides extensibility and investment protection over the long-term.

[4] Source: ESG Master Survey Results, *Network Security Trends*, March 2020.

Exploring the Requirements of a Unified Approach to Enable the Modern Workforce

The concept of a converged, cloud-native security and networking architecture has gained significant traction over the last year. Often referred to as secure access services edge (SASE), this approach has seen a significant increase in awareness, interest, and adoption over the last 12 months. Specifically, according to ESG research, 68% of organizations report that they currently use or would be very likely to consider a SASE architecture. Furthermore, 69% of respondents indicate that their preference for SD-WAN tool provider is a single vendor delivering both network and security functionality (see Figure 2).[5]

Figure 2. Strong Interest in Converged Security and Networking



Source: Enterprise Strategy Group

Organizations interested in working with a single vendor cited the following key drivers for adoption of this approach: operational efficiencies attained by security and networking teams, improved threat prevention and detection efficacy, and deeper vendor partnerships.[6]

[5] Source: ESG Master Survey Results: *Transitioning Network Security Controls to the Cloud*, July 2020.
[6] Ibid.

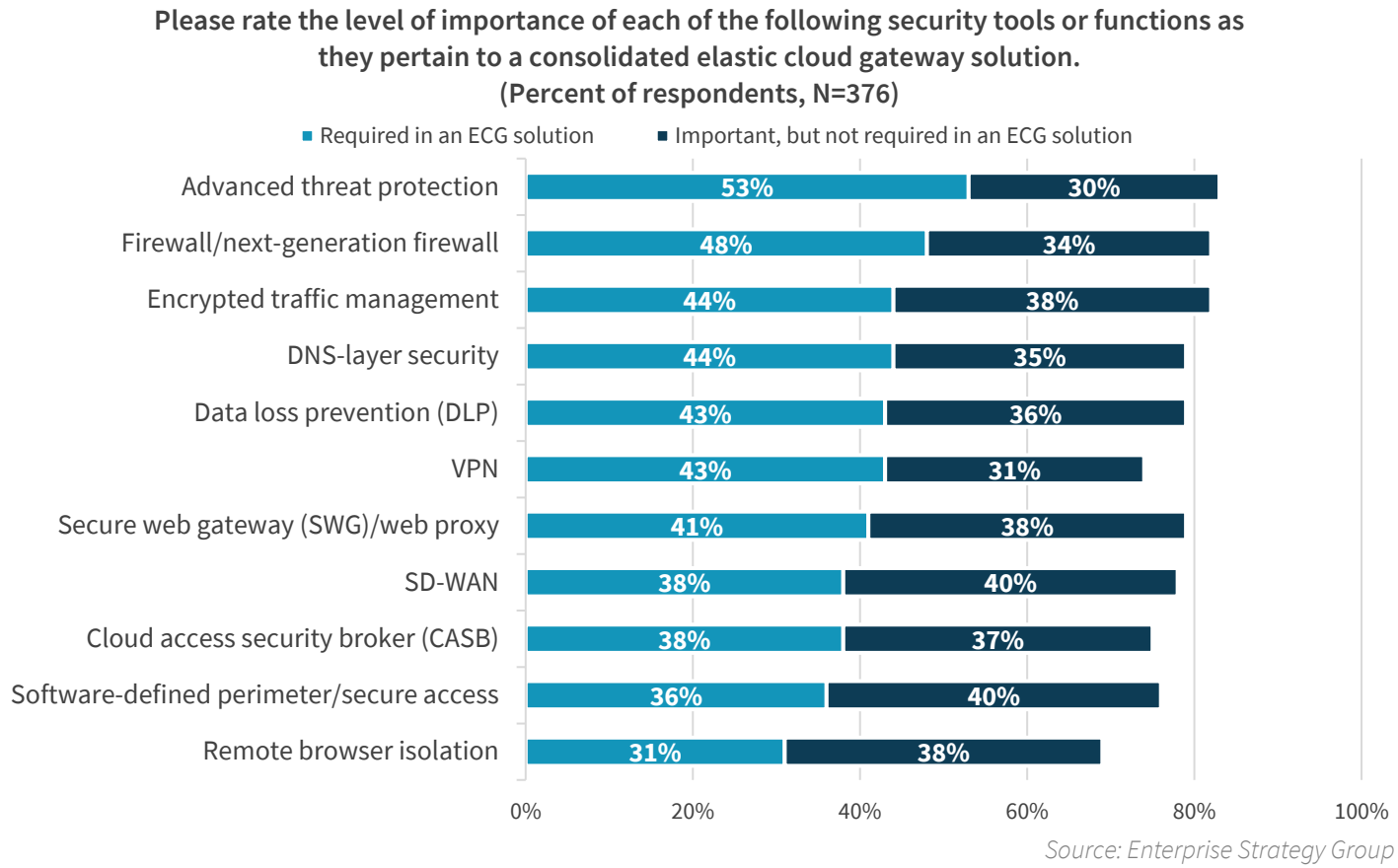
Furthermore, consistent training, procurement, and technical support efficiencies also go hand in hand when working with a single vendor. Finally, there can be some risk involved with a multi-vendor approach, such as changes in partnership arrangements or unplanned mergers and acquisitions. When considering a single-vendor SASE approach, organizations should prioritize effective security, a consistent user experience, and truly unified management.

Organizations interested in working with a single vendor cited the following key drivers for adoption of this approach: operational efficiencies attained by security and networking teams, improved threat prevention and detection efficacy, and deeper vendor partnerships.

Effective, Cloud-based Security

In the scramble to meet the increasing need for converged network and security solutions, many vendors have had to prioritize one area over the other. Some networking providers have added security capabilities such as stateful firewalling, URL filtering, and signature-based anti-malware, but remain somewhat basic in their functionality. However, effective solutions must include a variety of strong, if not best-in-class, security capabilities and not functionality added as an afterthought (see Figure 3).[7]

Figure 3. Strong Security Capabilities Are Essential To SASE[8]



Source: Enterprise Strategy Group

Subsequently, it is vital for organizations to be diligent in determining if a solution specifically provides the following requisite features:

[7] Ibid.

[8] At the time of this research, the term elastic cloud gateway (ECG) was used rather than SASE, though it was defined in the same way SASE would be.

- Multi-mode CASB to address both unsanctioned and sanctioned SaaS application usage through both proxy-based and API implementations.
- Next-generation firewall-as-a-service for ingress/egress traffic inspection.
- Advanced malware prevention capabilities to detect sophisticated threats.
- Remote browser isolation capabilities to ensure that unknown threats are partitioned from, and cannot compromise, user devices or corporate resources.
- Zero-trust network access to facilitate one-to-one connections between users and applications and support broader enterprise zero-trust initiatives.

Consistent Experience and Performance

With an increasingly distributed application and new worker environment, organizations need solutions that consistently deliver good performance and positive experiences. While network connections will play a significant role in enabling this, organizations also need to ensure they are secure. Solutions can no longer afford to trade network performance for security. Therefore, the solutions should employ the following:

- Direct Internet Access, which offers the ability to directly connect to cloud-based applications (IaaS or SaaS) and other branch locations without backhauling through the data center.
- Increased bandwidth to accommodate data growth and innovative new services.
- Policies that ensure that mission-critical applications are segmented and are given priority over other applications.
- High availability. In addition to leveraging multiple active broadband or MPLS links, solutions should also include the ability to provide cellular backup (4G, and in the future, 5G).
- Broad set of global points of presence (local access points for ISPs) to provide resiliency and seamless failover.
- Single pass inspection to improve performance over service-chained architectures.
- Consistent and secure application access via single sign-on and digital workspace capabilities.

Unified Management

With many organizations having patched together solutions to accommodate their rapid shifts towards the cloud and remote work, it may seem as if any SASE solution would be an improvement over the status quo. Yet, while many solutions are being positioned as SASE, the level of integration across tools and capabilities can significantly vary. To fully deliver the benefits of SASE, organizations need a unified management portal that ensures that network provisioning, security policy, and reporting are integrated to provide consistency and improve operational efficiencies.

For SD-WAN, this requires automating the provisioning process to automatically configure the connection from branch offices to cloud applications, users to cloud security tools, and users to corporate applications. Security policies are applied as offices are brought online.

The Citrix Approach for Secure Access Service Edge (SASE)

Citrix is well known for its digital workspace and networking technologies but has been steadily adding security capabilities over the last few years. The Citrix portfolio encompasses a wide range of solutions that assist organizations to enable a burgeoning hybrid workforce, specifically offering secure access to applications with a modern, reliable, and unified approach to SASE.

Citrix Secure Internet Access

Citrix Secure Internet Access is a cloud-delivered, unified security solution offering protection for all users accessing the internet and SaaS applications regardless of location. The solution's instance-based architecture provides data segregation between different enterprises and regions to ensure privacy and verify compliance is met.

The platform boasts more than 100 globally distributed points of presence (PoPs), supplying the scalability needed to meet modern enterprise requirements for compute-intensive capabilities at scale (such as SSL/TLS decryption). IP address persistence enables easier integration with upstream SaaS vendors.

The security functionality of Citrix Secure Internet Access includes secure web gateway; firewall; CASB; data loss prevention; and advanced malware protection, with capability parity across all PoPs. The solution also uses a single-pass architecture to allow these inspection capabilities to maintain a strong user experience and reduce latency. Additionally, more than 10 threat intelligence engines provide IT with real-time analysis and updates across the platform.

Citrix SD-WAN

Citrix SD-WAN combined with SASE technology enables a secure, consistent, and enhanced user experience. The Citrix SD-WAN architecture provides a reliable means for direct access to the internet and data center, as well as to branch and edge locations, quickly connecting to any location, including home offices. Centralized control ensure policies are enforced at the edge and application traffic is automatically prioritized based on enterprise policy to ensure optimal user experiences.

Tightly integrating with Citrix Workspace delivers the best user experience with Citrix claiming an up to five times performance improvement using visibility into the Citrix HDX technology for site, session, and user reporting, while also ensuring faster troubleshooting. Application optimization and reliability is accomplished leveraging sub-second failover, packet-level prioritization, and dual-side QoS.

The Citrix dedicated private network overlay service offers redundant and resilient high-performance connectivity to thousands of SaaS, UCaaS, and cloud exchanges. Flexible deployment options are provided through direct onramps to Azure, AWS, and GCP clouds, as well as the ability to utilize zero-touch provisioning (ZTP) for edge appliances with support for LTE and WiFi connectivity.

Citrix Workspace

The Citrix Workspace platform is used by 100 million users across 400,000 organizations in 100 countries (including 98% of the Fortune 500), for centralized application access. The vendor's introduction of Citrix Secure Workspace Access builds on that extensive experience and dramatically strengthens the security component of its approach.

Utilizing zero-touch network access allows organizations to move beyond legacy VPN-centric approaches, and implement identity-centric, least-privilege models to support zero-trust strategies. Remote browser isolation ensures that potentially malicious traffic is prevented from exploiting corporate resources by partitioning content from the user's device. With Citrix Secure Workspace Access, users benefit from a secure, consistent experience, regardless of where they are located.

Citrix Differentiation Through a Unified Approach

Citrix's unified management and orchestration provides a fully integrated approach that can help mitigate risk, increase agility, amplify performance, boost productivity, and enhance the user experience. The platform delivers:

Comprehensive Security for the Hybrid Workforce

Citrix provides comprehensive enterprise protection through a tightly knit set of globally distributed security services. This ensures consistent protection for all users, regardless of location, endpoint operating system, or the applications they are accessing (e.g., internal or SaaS, encrypted or conventional, on-premises or cloud-delivered). By minimizing the potential for threats to gain a foothold in the enterprise environment, risks to corporate revenue and customer trust are mitigated. Further, this location agnostic approach enables enterprises to continue to adopt global hiring practices, increase work-from-home initiatives, expand their salesforces, and generally focus on supporting the right employees regardless of from where they might work.

Operational Agility Through a Unified Single-vendor SASE Approach

The modern enterprise must be ready for anything—mergers and acquisitions, rapid organic growth, cloud expansion, even the next societal or macroeconomic disruption to name a few. Enterprises require operational agility across networks, endpoints, and security infrastructure—everything that enables them to securely and efficiently conduct business. Citrix enables improved operational agility by helping organizations reduce their vendor footprint while adopting a fully integrated, cloud-enabled solution.

Consistent Employee Experience Across All Devices and Locations

To enhance user satisfaction and boost productivity, employees must enjoy a consistent, transparent experience across all locations and devices. Although point solutions may help solve part of the problem (for example, replacing VPN with ZTNA to modernize secure access), the addition of siloed point tools can adversely impact users. Through its comprehensive solution employing a unified networking and security architecture, Citrix can help achieve higher efficiency, hence, greater performance, for all users.

The Bigger Truth

Traditional security and network solutions are unable to provide the necessary protection and performance highly distributed modern networks require. SASE approaches have emerged specifically to address these shortcomings through a converged, cloud-centric architecture. But make no mistake—this is a transformational shift. As a result, many organizations are likely to begin their SASE journey with a particular aspect of SASE and expand in the future. Given that, it is beneficial to prioritize vendors that offer the requisite scalability, flexibility, and overall capabilities to support a single vendor approach, especially as organizations look to expand their SASE focus over time.

The Citrix approach to SASE provides defined solutions for the critical use cases that organizations struggle to address today: effective protection for users across all devices and locations, secure access to corporate applications, and a consistent application experience for users across devices and locations. Most importantly though, is the tight integration of these capabilities and centralized management experience that Citrix has delivered to provide a truly unified approach 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