RESEARCH
Influence and insight
through social media

October 2020

SASE

A Changing World Calls for a Different Kind of Network

WHITE PAPER

Prepared by
Zeus Kerravala

ZK Research
A Division of
Kerravala Consulting

INTRODUCTION: NETWORKS ARE STRETCHED TO THEIR LIMITS

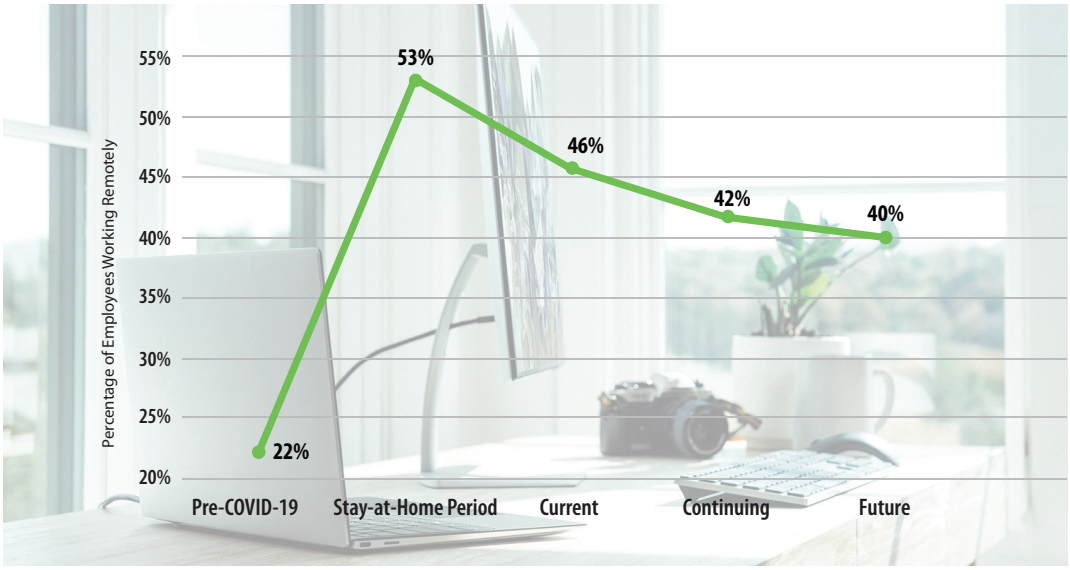
The past 12 months have seen change accelerate at a historically fast pace. What would usually take many years happened almost overnight. The global COVID-19 pandemic hit businesses hard, with workers chased out of their offices and into their homes. The ZK Research Work-from-Anywhere Study documented the drastic change in where people work. Before the outbreak, about 22% of employees worked remotely (Exhibit 1). That figure jumped to 53% immediately after the pandemic started and dipped to 46% as restrictions eased. The study showed that about 42% of office workers will continue to work remotely even after their companies clear them to return to the workplace. In addition, 40% of office workers—nearly double the pre-pandemic levels—will maintain their working-from-home capabilities into the future.

Networks that were accustomed to the predictable needs of offices and branches were stretched to their limits by COVID-19—and it doesn't appear that we'll ever see those pre-COVID work-from-home levels again. To adapt, companies have had to accelerate their transition to digital technologies such as cloud, mobility and video in an effort to keep workers productive and ensure customer service levels remain high.

Before the pandemic, many businesses explored their options for digital transformation, but most were moving relatively slowly. They were carefully assessing their next steps and planning a rollout that would stretch over several years. The pandemic turned those plans on their heads, and businesses suddenly had to accelerate their digital transformations.

The challenge for companies playing catch-up is that all the enabling digital technologies they need in order to ensure they can compete in the future are network centric. Consequently, the

Exhibit 1: Many Workers Won't Go Back to the Office



ZK Research Work-from-Anywhere Study, 2020

ABOUT THE AUTHOR

Zeus Kerravala is the founder and principal analyst with ZK Research. Kerravala provides tactical advice and strategic guidance to help his clients in both the current business climate and the long term. He delivers research and insight to the following constituents: end-user IT and network managers; vendors of IT hardware, software and services; and members of the financial community looking to invest in the companies that he covers.

Legacy networks were not designed to handle the long list of challenges that digital organizations face.

network is more important than ever. However, legacy networks were not designed to handle the long list of challenges that digital organizations face.

It's time for the network to evolve to provide precisely what businesses need in this changing world—it's time for networks to transform into a secure access service edge (SASE). SASE enables companies to support future needs without worrying if the network can handle the demands. It can provide connectivity, security and optimized app access for all employees, no matter where they work, enabling access to the apps they need on the devices they use.

In this report, ZK Research examines the challenges legacy networks face; details how SASE will be the next phase of the network evolution; and looks closely at the SASE service offered by VMware.

SECTION II: THE CHALLENGES WITH LEGACY NETWORKS

Think for a moment about the origins of legacy networks. They were designed in the hub-and-spoke era to support branch offices and corporate locations. In the digital era, networks have a much broader and highly complex remit. While they still must support those branches and corporate locations, they also have to accommodate people working from home, mobile workers in remote areas and critical corporate assets both in the cloud and on the edge.

Traditional networks employ that hub-and-spoke model, which is kind of like building a highway from one city to another with no off-ramps. Once you're on the road, your destination is predetermined. You don't have the option of going anywhere else. There's no turning back. The same is true of the hub-and-spoke legacy network. The connections are fixed, and the transit of data is limited because there is no flexibility to move beyond the ways that were envisioned.

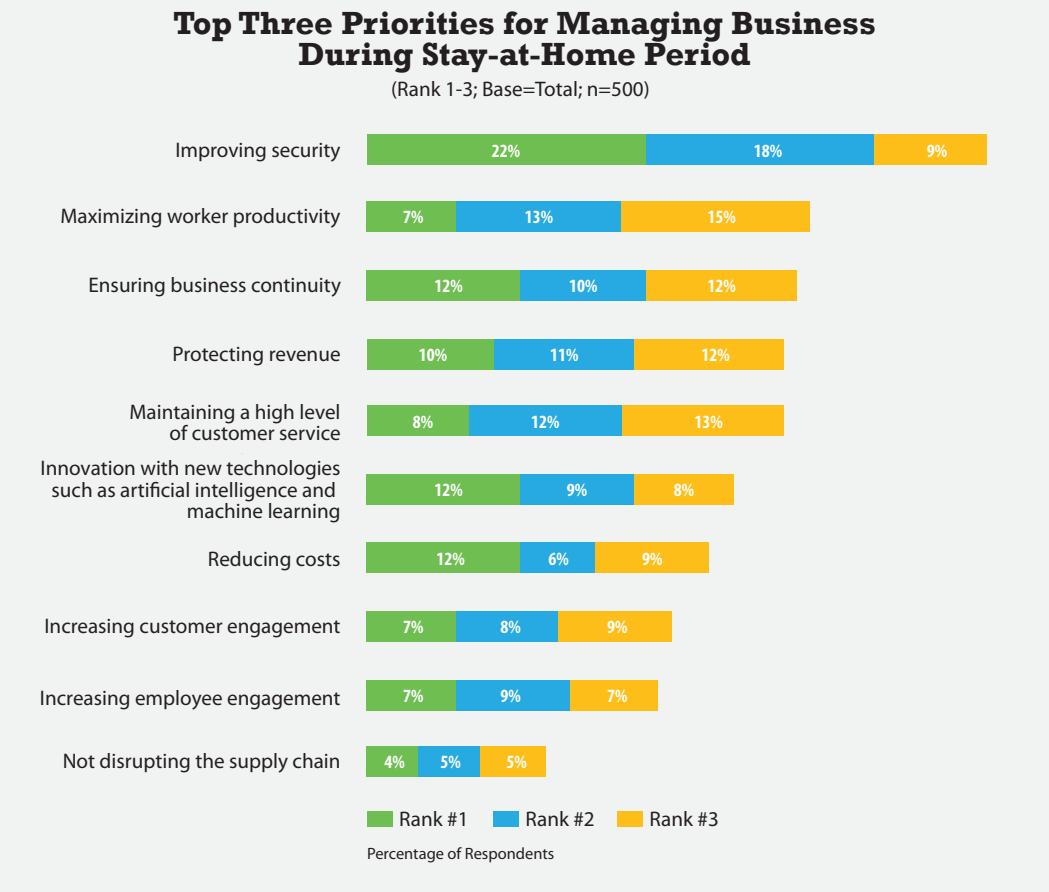
In the cloud era, which demands access from just about anywhere, hub-and-spoke is a highly inefficient operating model. In addition, the visibility and control of legacy networks don't extend to off-net activities (i.e., accessing cloud-hosted applications in software-as-a-service [SaaS] or infrastructure-as-a-service [IaaS] environments), so application performance is inconsistent.

In the ZK Research Work-from-Anywhere Study, 49% of respondents said improving security was one of their top three concerns (Exhibit 2). Maximizing worker productivity came in second, with 35% ranking it in their top three.

Even though security is a top priority, a legacy network can't deliver the kind of security digital businesses need because it was designed for branches and corporate offices. As a result, companies have found it hard to extend the same safeguards to workers at home and on the go. When legacy networks do employ security, it's not really meant for protecting remote workers. Instead, it's an overlay that uses on-premises hardware. If employees are scattered and they're using diverse apps and countless devices, the last thing companies need is a rigid, brittle, tough-to-maintain piece of gear humming away on premises.

In addition to the concerns outlined above, traditional networks are a chore to manage and lack scalability. Manual intervention is the order of the day. With significant human capital devoted to just keeping them running, legacy networks are intensive to operate. If a problem crops up, a person

Exhibit 2: Security and Productivity Are Top of Mind



ZK Research Work-from-Anywhere Study, 2020

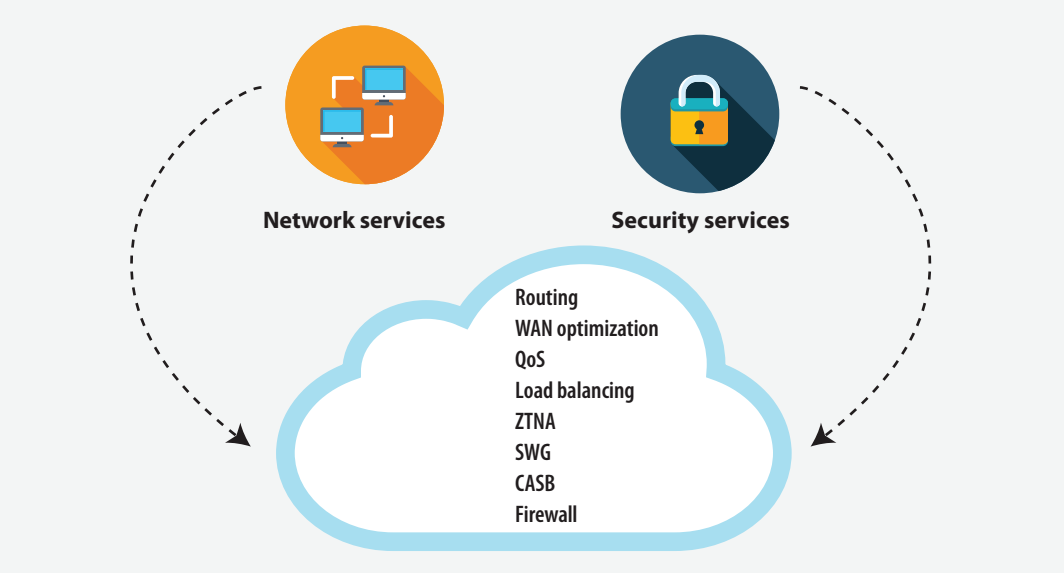
needs to track it down, diagnose it and apply a fix. This leads to problem resolution that moves like molasses as well as significant unplanned downtime that directly impacts the bottom line. In addition, troubling intermittent issues that aren't present when IT arrives can really sap resources. Because SASE was built for the needs of the modern digital business, it can address all of these challenges, including the ability to rewind to see the state of the network when an issue occurred.

SECTION III: INTRODUCING SASE

SASE is the next phase of network evolution. It builds on the software-defined wide-area network (SD-WAN) concept and integrates network services and security services by delivering them from the cloud. SASE includes all critical network functions, such as routing, load balancing and quality of service (QoS). Also, SASE covers the security functions necessary to run a network in the digital era (Exhibit 3) delivered from the cloud for multitenant services including the following:

Zero-trust network access (ZTNA), which only allows traffic from authenticated users, devices and applications

Exhibit 3: SASE Converges Network and Security Functions



ZK Research, 2020

Secure web gateway (SWG), which protects companies from threats that come via the web vector

Cloud access security broker (CASB), which monitors activity on the network and enforces policies

A next-generation firewall, which mitigates unauthorized access to the network

These are some of the key benefits of SASE:

Application quality assurance: Ensures a good application experience whether working from the office or remotely

Operational simplicity and ROI: Simplifies operations and reduces support complexities by unifying networking and security

Intrinsic security: Provides intrinsic security by unifying network, endpoint, identity and cloud security control points

Cloud first: Designed with a cloud-first approach for operational efficiency and future readiness

SASE handles the needs of branches as well as people working from anywhere in the world.

In addition to those benefits, SASE handles the needs of branches as well as people working from anywhere in the world—whether it's the office, home or somewhere on the road. Plus, it provides the orchestration and edge network intelligence a company needs, along with secure access, cloud web security, an SD-WAN gateway and a cloud firewall. And for employees who need access to apps, it provides seamless access to the applications we all use every day.

SASE provides reliable Voice over Internet Protocol (VoIP), unified communications (UC), collaboration and SaaS access, delivering a quality user experience that legacy networks all too often fail to provide. The improved user experience, combined with an optimized last mile, means companies can provision sites in minutes and gain visibility across any link, all while reducing the Multiprotocol Label Switching (MPLS) burden.

For employees, ease of connection is essential. Therefore, SASE should make life simpler for them, with minimal equipment to set up and simple links to click to complete the process. Once completed, an employee at home, in a branch or at a mobile site is assured high-quality, reliable access with iron-clad security. The access should work seamlessly with home networks while separating home apps and activities from business apps and preventing unauthorized access to corporate resources.

SECTION IV: VMWARE OFFERS A ROBUST SASE SOLUTION

VMware built a robust suite of SASE services on its heritage as a leading SD-WAN provider that was recognized as a Leader in the Gartner WAN Edge Infrastructure Magic Quadrant for three years in a row.

VMware approached the challenge of delivering cloud-based network and security services like the SD-WAN veteran it is, building its own SASE points of presence (PoPs) that enable all users—no matter where they are—to connect securely to the services and apps they need (Exhibit 4).

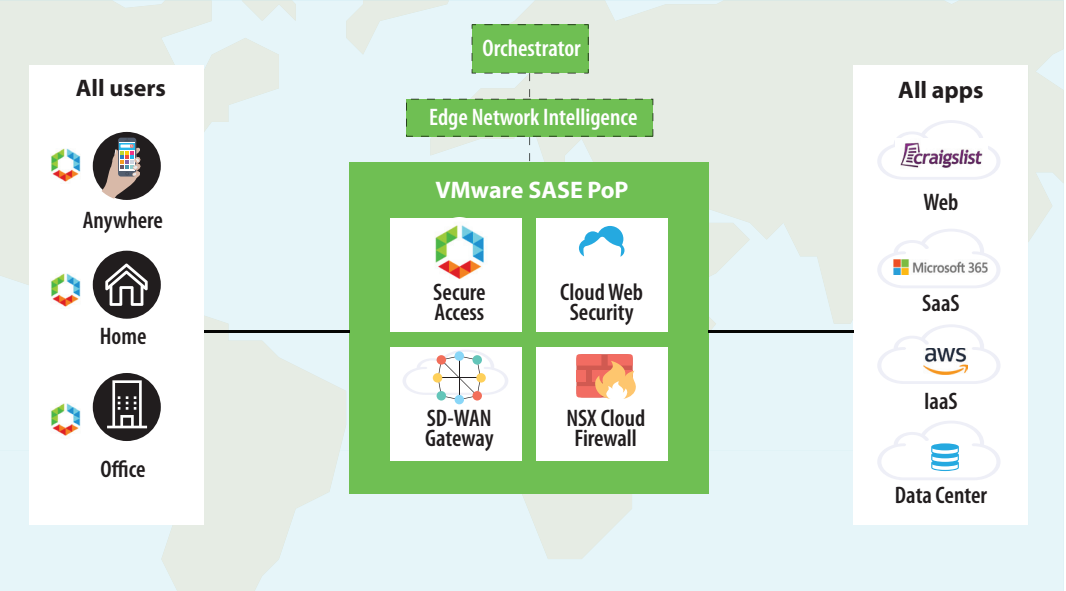
The VMware SASE Platform™ brings together cloud networking and cloud security in a single solution that's flexible, agile, secure and scalable. As a result of the company's global reach, VMware has distributed its PoPs around the world so that companies and employees have a range of on-ramps to SaaS and other cloud services. The cloud-based networking and security services included in the VMware SASE Platform can easily scale to customers' needs.

These are the components of the VMware SASE Platform:

VMware SD-WAN Gateway: This multitenant gateway service and policy control point has more than 2,000 gateways around the globe supported by VMware and its partners to deliver superior application access performance and scale.

VMware Secure Access: VMware SASE Platform provides an onsite-like experience to remote mobile users built on the principle of ZTNA, with the combination of VMware SD-WAN™ and VMware Workspace ONE.

Exhibit 4: VMware SASE Platform Brings Together Cloud Networking and Cloud Security



VMware and ZK Research, 2020

VMware Cloud Web Security: VMware SASE Platform bakes in SWG, CASB, data loss prevention (DLP), URL filtering and remote browser isolation (RBI) so customers get secure, direct and optimal access to SaaS and web resources.

VMware NSX Cloud Firewall: VMware SASE Platform takes an identity-based approach to protecting on-premises applications regardless of where the user is located by leveraging VMware NSX next-generation firewall and advanced security features such as deep packet inspection (DPI) and intrusion prevention system/intrusion detection system (IPS/IDS).

SECTION V: CONCLUSION AND RECOMMENDATIONS

The legacy approach to networks has reached the end of its useful life. The world is different now, and the demands on companies and employees have transformed in a short time. ZK Research offers the following recommendations for companies evaluating SASE options:

Find an SASE solution that can support your future needs. Look into the future without worrying if your network can handle the company's demands. The right SASE solution should provide security, configuration and app distribution for all employees, regardless of where they work, the apps they need or the devices they use.

Consider ZTNA, SWG, CASB and a firewall to be table stakes. SASE should cover all the security functions you need to run a network in the digital era.

Look for a global PoP footprint. SASE PoPs should be distributed around the world so that companies and employees have a range of on-ramps to SaaS and other cloud services.

ZK Research has reviewed the VMware SASE Platform offering and believes it will be a key enabler for organizations looking to deliver secure cloud application access in a multi-cloud world. The company has integrated sophisticated security capabilities (i.e., ZTNA, SWG, CASB, RBI, URL filtering, IPS/IDS and DLP) into its SASE platform, which means the security boundary now extends beyond the data center—reaching the cloud, applications and users. Consequently, VMware has dramatically reduced the attack surface while offering the flexibility and access that today's digital companies need.

CONTACT

zeus@zkresearch.com

Cell: 301-775-7447

Office: 978-252-5314