netskope

Securely Work From Anywhere:

A Playbook for Success

Optimize Your Workforce, and Move Toward SASE, with Considerations for Cloud, Networking, and Security

There's Never Been a Better Time to Optimize

When the COVID-19 pandemic descended on us, enterprises took a make-it-happen approach to maintaining their operations. Employees up and down organizational structures were told to work from home, and IT teams were tasked with making that happen. The timeline was short, and approval processes moved quickly, which meant changes to network access and security were made more quickly, and in some cases more haphazardly, than in a "normal" situation.

We did what we needed to do in that moment, each of us scrambling to support our company's work-from-home needs. But now we're out of crisis mode. CIOs, CISOs, Networking leads, and other decision makers need to take a deep breath, look around, and evaluate whether their networking and security infrastructures are optimized to support the business in the long run, and if they can adequately support a "work from anywhere" environment where flexibility and various hybrid work modes are favored over large-scale returns to corporate office environments.

It's been a very challenging 18 months, but there's also never been a better time to optimize.

Using This Playbook

Each section of this playbook is intended to address a different aspect of how you can optimize for a Work from Anywhere scenario.

We've included a list of questions by section that should help guide your thinking—and set you up to move forward with the right decisions, not "more initiatives."

Assess Your Team Strengths and Gaps

Not all moves are specific to technology and infrastructure, and in fact, the dawn of Work from Anywhere represents a key moment in time to look at whether you have the right people in the right roles, doing the right things.

According to IDC, about $6.8 trillion will be spent by enterprises on digital transformation (Dx) projects through 2023. The benefits of digital transformation ensure that businesses will stay agile, competitive, and cloud-first, turning functional IT and security cost centers into true business enablers. Nearly 90% of IT decision maker-level respondents to a recent survey by Censuswide and Netskope, for example, are either actively working on a Dx project or have just completed one.

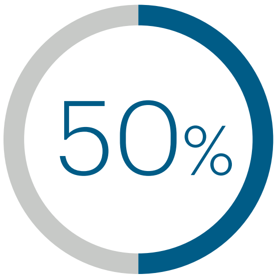
Major considerations for assessing the strength of your current team and how to bridge gaps include:

Networking and Security Team Collaboration. The abovementioned Censuswide research points to an ongoing schism between network and security professionals that inhibits the timely success of Dx projects. Networking and Security team friction is an old story, but there are several ways to reduce this friction and achieve better outcomes.

Hiring from Unexpected Sources. You've heard about the shortage of cybersecurity talent, but an overemphasis on technical skills often creates that shortage artificially. Even the most basic security technologies are hugely dynamic. In most companies, the IT infrastructure is currently in the midst of a massive transition from on-premises to cloud-based systems. Security teams are having to learn new technologies. More than that, they are having to adopt an entirely new mindset, shifting from a focus on protecting specific pieces of hardware to a focus on protecting individuals and applications as their workloads increasingly move outside the corporate network. Rather than feed into the notion of a cybersecurity skills shortage, look to backgrounds such as financial analysis or marketing or executive communications that lend themselves well to security team functions. It's not only OK, but encouraged, to think outside the box when building the security team of the future!

Ask the Right Questions:

- Are our networking and security teams collaborative, functional, or at odds?
- Are we creating opportunities for better collaboration using techniques such as DevOps-style agile teaming, shared OKRs, or operational shifts such as SNOCs?
- Have we examined our entire team and identified our biggest talent gaps in both networking and security?
- Have we considered alternative hiring pools where certain skill sets would adapt well to filling those talent gaps?



of CIOs believe that a lack of collaboration between specialist teams stops their organization from realizing the benefits of digital transformation.

Invest in Next-Gen SWG

The concept of Work from Anywhere confirms we operate in a cloud-first world now, and that applies to everything from mitigating threats to investing in the right infrastructure.

Consider:

- The majority of malware is now delivered via cloud apps
- Nearly half of all cloud apps in use in the enterprise have a poor CCI rating
- 83% of users upload data to personal apps on managed devices
- Cloud phishing continues to increase, using cloud-hosted baits and targeting cloud credentials
- Legacy web security is blind to more than 50% of traffic. Why build your secure access security edge (SASE) architecture around a web-only proxy for one lane of traffic?

You need a Next-Gen SWG that can analyze five lanes of user traffic including web, SaaS, Shadow IT, public cloud services, and custom apps in the public cloud. Rich details for content and context about users, apps, and data enable granular policy controls plus data and threat protection as the core of your SASE architecture (more on that later).

50%+ → 62%

JAN 2020 → **JUNE 2021**

At the beginning of 2020, the majority of malware downloads still came from the web. But starting about Q2 2020, the majority of malware downloads began to come from cloud apps, increasing every quarter. As of now, over 62% of all malware downloads come from cloud apps.

Ask the Right Questions:

- Can I have consistent inspection and policy enforcement among users anywhere and data anywhere?
- Do I have visibility of all SaaS and SaaS, including shadow IT, in use by all users, anywhere in my environment?
- Can I determine how my users are using the data and via which apps or services?
- Can I determine the data's sensitivity both at rest and in transit?
- Do I understand the security posture of SaaS and Shadow IT?
- Do I understand and can I qualify the risk of SaaS and web-based applications being used in my environment?
- Can I control how data is transferred, manipulated, or accessed via cloud and web-based services and applications?
- How confident am I in the authenticity of the user? Am I sure there hasn't been any credential compromise?
- Can I easily integrate incident response and forensics capabilities for SaaS- and web-based activity?
- Is my user experience performance-driven, frictionless, and transparent?
- Can I apply risk-based conditional access based on user behavior, data sensitivity, and application characteristics?
- Can I inspect and apply policy without hairpinning to the data center, thus preserving my cloud service user experience?

Evolve Your Network Architecture and Say Goodbye to Your VPN

Many VPNs exist as appliances within an enterprise's on-prem security stack, backhauling traffic to allow secure access to the network whether employees are on-prem or not. As the traditional perimeter disappears, and the security stack follows suit into cloud services, there's no sense in paying for the upkeep of a costly VPN appliance, especially when Zero Trust Network Access (ZTNA) approaches are much more aligned to cloud-first environments and significantly reduce your capital expenses over several years.

Quite a few companies still require users to be on VPN and backhaul all traffic through the data center, even if they are using cloud-destined applications. The problem is that they are relying on equipment they deployed pre-pandemic when only a very small proportion of the workforce was offsite. Their systems are not sized appropriately for this volume of remote work. They might manage this discrepancy by kicking anyone who's idle off the VPN, but then an employee who steps away to refill a cup of coffee might have to launch a new VPN session. Once again, security is undermining staff productivity, and employees may be tempted to find workarounds. And we have to ask, has this made our security posture better? We may have inadvertently given more access than required to the assets we are trying to protect.

Beyond VPN technology is the fact that most enterprises today use an architecture that relies heavily on "hairpinning" or what's also commonly referred to as traffic backhauling. The preferred approach has been to have all client requests to the internet sent (or hairpinned) from the branch back to a central location, like the data center, where security enforcement happens, and only then—after being scanned—the traffic goes onward to the internet. The same applies whether it's making a request for web content or interacting with a business-critical SaaS app. On the server response, the traffic then needs to follow the same circuitous path back through the data center, to the branch, and ultimately to the user's desktop.

One doesn't need to be a network engineer to realize this approach is going to impact user experience, adding latency and slowing things down significantly. With the unarguable shift of applications and data to the cloud, and the growing volume and criticality of this traffic, one of the great attractions of the cloud security model is to eliminate hairpinning and dramatically simplify network design. The future will increasingly be about sending traffic direct-to-net with a cloud-first approach to security.

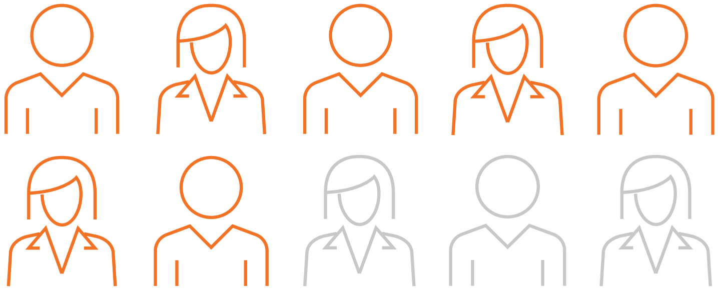
Ask the Right Questions:

- Do we have a plan to phase out our costly VPNs and transition to Zero Trust Network Access (ZTNA)?
- Are we evolving our network design or merely relying on common, but misleading design choices such as virtual points of presence (vPOP)?
- Does our network architecture depend on public cloud infrastructure—and therefore the public cloud provider's edge data centers—to provide regional exit points for network traffic?
- Are we able to go direct-to-net with our traffic? How do we know? How would we explain how and why to a non-technical leadership team?

Consolidate Your Tools and Eliminate Waste

If you're coming out of the pandemic with more security tools and networking and security services than before, it's time to consider a more streamlined approach.

As public health teams bring the pandemic to a resolute end, security functions are experiencing the re-emergence of budget pressures. Leaders, especially CISOs, need to evaluate how they are using the tools they currently have in place. Ruthlessly weed out solutions that are no longer effective in the post-pandemic reality and optimize those that will continue to be useful in a Work from Anywhere setup.
Note: This assessment isn't the kind of task that ends with marks on a compliance checklist. Instead, the CISO should come out of this process with a deep knowledge of the ways in which each solution is valuable to the organization. Those that no longer provide adequate value should be removed.



More than 70% of security executives believe their budgets will shrink this year

Ask the Right Questions:

- Can we effectively audit all of our networking and security products or services today?
- Are the tools that worked well two years ago adequate to protect the company's greatly expanded attack surface, with employees spread all over the place? How do we know?
- How is each product or service in the company's technology supply chain moving the organization forward?

Apply Zero Trust Principles All the Way to Data Protection

Today there are many isolated Zero Trust projects focused on networks, users, devices or isolating servers. The main miss on most of these projects and technologies is that they are not focused on the data. We must go beyond access control and isolation and provides continuous, real-time access and policy control based on users, devices, apps, threats, and data context. This approach is the only effective way to dynamically manage risk across a mix of third-party applications and a Work from Anywhere workforce that needs always-on access to cloud apps and data to stay productive.

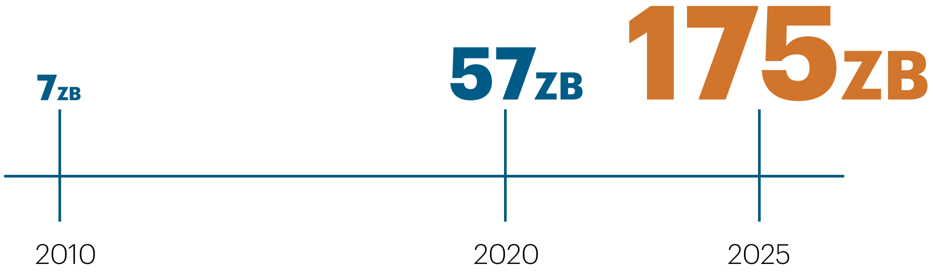
If this sounds like it's time to update how we think about data loss prevention (DLP), that's correct. DLP is founded on the pre-cloud idea that everything is inside a data center and essentially protected by a perimeter. The job of data protection in that setting is to prevent data from leaking out in unauthorized ways and to stop bad things from getting in.

But in the cloud era, the traditional premise of DLP no longer applies. Yes, there is still crucial data housed in the data center inside the perimeter. But in most organizations, there is now as much or more data in SaaS applications and in private applications hosted in the public cloud. To protect this data, while also doing a better job of protecting data in the data center, we must rethink data protection in a way that is fully cognizant of the way users really work these days. We have to protect a much wider, much more dynamic attack surface.

Data protection is ultimately about context. Knowledge of the interplay between user, device, app, and data enables security teams to define and enforce conditional access controls based on data sensitivity, app risk, user behavior risk, and other factors. Choose security and networking solutions that focus on data protection—everywhere data is used and accessed—above all.

Ask the Right Questions:

- Can we apply Zero Trust principles all the way to data access, or are we still stuck at access control and isolation only?
- What is our overall DLP and data protection strategy?
- What solutions are available to us today that focus on cloud data protection?



By 2025 it's anticipated there will be 175 zettabyes (ZB) of data (up from 57 ZB in 2020 and 7 ZB in 2010)

Re-Evaluate CAPEX and OPEX Spending

Hand-in-hand with tool consolidation (see p. 6) is the opportunity to realistically evaluate your capital and operational expenses in network and security and make strategic moves toward the savings a properly implemented cloud-centric architecture can provide.

At their most basic level, security budgets are often linked to employee numbers and securing an employee is an expense typically assessed for each budgetary year. Accuracy in predicting employee growth, organically and/or via M&A, is difficult and causes overprovisioning or tactical add on expenses.

The shift to consolidated security cloud services offers the immediate benefit of replacing complex appliances that require operational and engineering resources to maintain. For example, shifting from legacy SWG appliances to a consolidated approach (NG-SWG, see p. 4) inclusive of SWG, CASB, and DLP functionality can yield many enterprises more than $10M in savings over a three-year period.

It will be challenging to identify all of the areas to consolidate or reduce capex or opex expenses all at once, but taking advantage of the current moment to optimize for Work from Anywhere can turn up savings opportunities everywhere.

Ask the Right Questions:

- In what tangible ways should our capex and opex forecasting change with a Work from Anywhere scenario?
- How quickly can we make those changes?
- What are our top 3-5 areas to reduce capex spend in the next 12-36 months?
- What are our top 3-5 areas to reduce opex spend in the 12-36 months?
- What specific security or networking technology investments catalyze the most long-term savings?

$150.4 billion

Cloud security is the fastest-growing market segment in a forecast of $150.4 billion to be spent worldwide on security and risk management solutions in 2021.

Assess Your Overall SASE Readiness

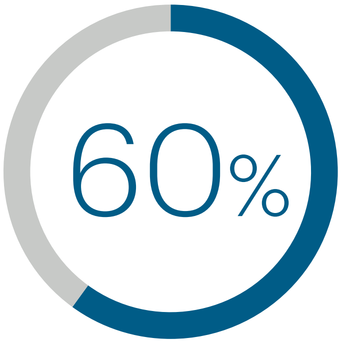
Much like the term "cloud" 10 years ago or "Zero Trust" five years ago, SASE is often over-marketed and under-explained. But as you enable Work from Anywhere and move toward SASE inclusive of the other needs addressed in this playbook, it's important to assess your readiness not in terms of individual technologies such as CASB and SWG, but in how your teams and tools are set to address four fundamental transformations.

- **Networking transformation** reduces backhauling, hairpinning, and latency to provide direct to cloud access between users and apps. Remote working is at an all-time high and staying that way. Users are embracing direct-to-cloud access as opposed to using VPNs and MPLS networking to backhaul to central office egress points for web and cloud services.
- **Security transformation** reduces data center, office, and branch office security appliances, moving to a cloud secure access edge with a single pass inspection of user traffic for web, managed SaaS, unmanaged SaaS (Shadow IT), public cloud services, and custom apps in these cloud services. These five types of user traffic all require data and threat protection with granular policy controls by user, group, or OU, and by app, instance, activity, data, and other contextual variables.
- **Application transformation** migrates apps from the data center to new SaaS replacement choices.SaaS app adoption has nearly doubled year over year from an average of 1,295 apps per organization in 2019 to 2,415 in 2020. The key point for app transformation is less than 2% of these apps are managed by IT with administration rights. The rest are freely adopted by users and business units making Shadow IT a growing security risk.
- **Data transformation** migrates data out of the data center into apps and cloud services where most of the data resides, however, data exposure happens via boundary crossings into personal instances of managed apps, unmanaged apps (Shadow IT), or data shared via collaboration, social, and web activity. All teams must evaluate how they control unintentional or unapproved data movement, protect data and IP from cloud and web-enabled threats, and provide granular policy controls based on data context to apps and cloud services with data protection and advanced DLP.

None of these four transformations favors a singular focus on CASB, SWG or any other specific technology.

Ask the Right Questions:

- What is our approach to network transformation and what are our top 3 priorities in the next 12 months?
- What is our approach to security transformation and what are our top 3 priorities in the next 12 months?
- How are we addressing Shadow IT today, and what are the next moves we need to make to address the growing problem of unmanaged application use in our teams?
- Are we able to ensure security everywhere data is used and accessed?
- How ready are we for SASE today? What is missing?



of enterprises will have a SASE strategy by 2025

Netskope, the SASE leader, safely and quickly connects users directly to the internet, any application, and their infrastructure from any device, on or off the network. With CASB, SWG, and ZTNA built natively in a single platform, the Netskope Security Cloud provides the most granular context, via patented technology, to enable conditional access and user awareness while enforcing zero trust principles across data protection and threat prevention everywhere. Unlike others who force tradeoffs between security and networking, Netskope's global security private cloud provides full compute capabilities at the edge.

Netskope is fast everywhere, data centric, and cloud smart, all while enabling good digital citizenship and providing a lower total-cost-of-ownership.

To learn more visit, https://www.netskope.com.

netskope

The Netskope security cloud provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, and private apps from anywhere, on any device. Only Netskope understands the cloud and takes a data-centric approach that empowers security teams with the right balance of protection and speed they need to secure their digital transformation journey.

To learn more visit, https://www.netskope.com.