netskope

How to Get SASE Right the First Time

7 Keys to Victory— and What to Ask Your Vendor

How to Get SASE Right the First Time

7 Keys to Victory—and What to Ask Your Vendor

In less than two years, the concept of Secure Access Service Edge (SASE) has spawned more vague and dubious marketing than any other recent security or networking trend. “Simplify your architecture,” “Consolidate your approach,” “Get better control of your environment,” “Converge security and networking”...all of these ideas sound good in theory, but what do they really mean? How do you get to the practical level of building a SASE architecture and delivering its promised benefits?

What’s important is context: you need real-time context for users, apps, and data to enable granular policy controls, protect data wherever it is accessed, and deliver threat protection. Here are seven critical considerations for investing in the right technology and building an architecture that helps you get SASE right...the first time.

Caveat emptor: Most purported “SASE” vendors can’t deliver even half of these requirements today.

#1

Achieve Full Visibility of SaaS Apps and Shadow IT

Cloud app adoption is up 20% year-over-year where large enterprises average 2,415 apps and medium enterprises with 500-2,000 users access 690 distinct apps. Given less than 3% of these apps are managed, the blind spot for personal instances and Shadow IT presents risks for data exposure and threats.

What to ask your vendor:

- Can you provide inline SaaS and Shadow IT visibility to profile thousands of apps with rich details on content and context, including user, device, app, instance, app risk rating, category, activity, content, and action? (Note: This requires the ability to decode cloud traffic beyond the URL and header identification you'd find in a legacy web gateway.)
- Can you clearly differentiate app instances such as when a user moves data from a company instance (managed) to a personal instance (unmanaged)?
- Can you profile a wide mix of app risks and attributes, and customize ratings for compliance, security, and other profiles?
- Can you provide data visualizations that profile data risks, threats, and overall cloud risk posture, in ways non-technical executives will easily

#2

Prevent Unintentional or Unapproved Data Movement

Working remotely, 83% of users access personal apps on managed devices and upload an average of 20 company files per month into unmanaged apps. As remote working continues, it's easy for remote users to make desktop screen captures of slides, documents, or even whiteboards, plus share files, copy files, or sync files between the cloud and devices. This is why data context is a core principle of SASE architecture to understand if the right data is going to the right user in a risk-averse context.

What to ask your vendor:

- Can you provide activity policy control of user app activity using context, data, and risk ratings? (Just controlling uploads and downloads is nowhere near sufficient.)
- Can you differentiate activity-level controls in the context of company and personal instances of an app?
- Can you enable conditional and contextual access controls in real-time? (Ask about policy-driven, step-up authentication, for example.)
- Can you profile data sensitivity based on DLP rules and policies, compliance templates, and machine learning classifiers for documents and images—including screenshots, source code, or IDs?

#3

Assess Data Posted or Added to Cloud Apps

One year into the pandemic and more than two-thirds of users are still working remote as companies consider long-term remote work policies. This has driven an 80% surge in collaboration apps in the first six months and a 97% increase for personal use of managed devices. The ability to post, edit, or create content so easily in apps is essential, yet creates risks for data exposure.

What to ask your vendor:

- Can your data protection and cloud DLP capabilities profile app risk, user risk, device posture, and data sensitivity using adaptive policy controls?
- Do you employ machine learning classifiers for documents and images?
- Can you provide templated regulatory compliance reporting?

#4

Deliver Real-time User Coaching

Things were simple in the old world of allow-or-block; however, there are now many gray areas that can potentially put company data and users at risk. The key to real-time coaching of users on specific content and actions is understanding the context and then having a variety of options to respond including risk alerts, proceed or cancel warnings, providing justification, or suggesting safer app alternatives.

What to ask your vendor:

- Can you provide conditional and contextual user alerts based on risk alerts, proceed or cancel warnings, or activity and data access justification? (Including suggesting safer app alternatives.)
- Can you offer app risk ratings to help companies keep data away from high-risk apps, plus apply conditional use for medium-risk apps?
- Can your data protection and cloud DLP profile data inline using patterns, dictionaries, custom regex, fingerprinting, exact data match, machine learning classifiers for documents and images, and regulatory compliance templates?

#5

Manage BYOD and Third-party Access to Apps

Legacy web security solutions live in a world of managed users and web traffic. But today's reality is that users, partners, consultants, and even customers have their own unmanaged devices (BYOD) and often require access to managed apps. Meeting this need requires expanding web gateways for cloud traffic with both forward and reverse proxies where the second supports unmanaged devices using identity services to guide traffic for analysis. The net result is a clientless experience for users and the data and threat protection you require.

What to ask your vendor:

- Do you provide reverse proxy support to enable unmanaged (BYOD) devices and third-party users to access managed apps? (Can that be done with a clientless experience through identity service? How about with granular policy controls?)
- Can you provide control of app activity for given user, data, activity, device, context, and risk ratings?
- Can you enable conditional and contextual access controls in real-time? (Ask about policy-driven, step-up authentication.)

#6

Mitigate Cloud-enabled Threats

The leading targets for phishing attacks over the past two years were SaaS, webmail, and cloud storage. Fake login forms hosted in cloud storage evade legacy web, email, and endpoint defenses to phish users for access credentials. Microsoft is the most impersonated brand in phishing attacks for both web and email today, which is no surprise as Office 365 is the leading app suite.

What to ask your vendor:

- Do your data protection and cloud DLP capabilities profile data inline, including form inputs to detect access credentials (including company domains) to block phishing attacks?
- Do you offer inline SaaS visibility to profile thousands of apps with rich details on content and context, including user, device, app, instance, app risk rating, category, activity, content, and action?
- Can you provide universal and custom app connectors to enable policies to focus on specific areas like Google Forms that are often used to create fake phishing forms hosted in the cloud?
- Do you deliver threat protection to analyze multi-stage attacks for malicious downloads, redirects to malicious URLs, malicious scripts and macros, plus threat intelligence IOC sharing between defenses including endpoints, SIEMs, SOAR, and IR solutions?

#7

Protect Sensitive Data in Documents and Images

Working remotely enables users to freely take screen captures of online documents, images, and even whiteboards. Important documents, source code, resumes, and other sensitive data can flow between company and personal instances of managed apps, or to unmanaged Shadow IT apps freely adopted by users. The problem with legacy DLP is registering data or too many alerts from rules, patterns, or dictionaries. What's required is inline analysis of documents and images out-of-the-box—it's here and machine learning classifiers are a game-changer.

What to ask your vendor:

- Do your data protection and cloud DLP capabilities profile data inline, including new machine learning-based classifiers for images (e.g., IDs, passports, screenshots) and documents (e.g., source code, resumes, tax forms) ready to use? (Ask about Train Your Own Classifier, which is important for any user's desired document or image.)
- Do you provide inline SaaS and Shadow IT visibility to profile thousands of apps with rich details on content and context, including user, device, app, instance, app risk rating, category, activity, content, and action? (This enables data protection, cloud DLP, and ML-based classifiers to profile documents and images.)
- Can you enable conditional and contextual user alerts based on data sensitivity, app risk, app instance, activity, or other attributes?

Bottom Line

Data context is critical to a successful SASE architecture

As cloud and SaaS adoption continues, the choice to block with security controls impedes business processes and productivity. When it comes to data movement, data sensitivity, conditional and contextual access and activity controls, and real-time coaching, data context is required for an adaptive real-time policy to reduce risks.

Get it right the first time and consolidate and reduce complexity by replacing legacy SWG with cloud and web inline analysis with a Next Gen SWG solution providing the data context for your SASE architecture.

Netskope, a global cybersecurity leader, is redefining cloud, data, and network security to help organizations apply Zero Trust principles to protect data. The Netskope Intelligent Security Service Edge (SSE) platform is fast, easy to use, and secures people, devices, and data anywhere they go. Netskope helps customers reduce risk, accelerate performance, and get unrivaled visibility into any cloud, web, and private application activity. Thousands of customers, including more than 25 of the Fortune 100, trust Netskope to address evolving threats, new risks, technology shifts, organizational and network changes, and new regulatory requirements. Learn how Netskope helps customers be ready for anything, visit netskope.com.