Top 5 SASE Use Cases for Remote Workers

netskope

Top Five SASE Use Cases for Remote Workers

Strategically planning and deploying a secure access service edge (SASE) architecture is now center stage after the global pandemic forced organizations to try and manage two to three times the number of remote workers. Given two-thirds or more of your workforce is now remote, understanding the top security use cases for SASE provides an important perspective on relevant capabilities often not delivered by existing legacy security solutions. The new normal is here and is likely going to stay awhile, so thinking strategically about your security is paramount.

Top Five SASE Use Cases for Remote Workers

Use Case #1 | Preventing Unintentional Data Movement

Use Case #2 | Getting the Right Data to the Right People

Use Case #3 | Coaching Users and Identifying High-Risk Users and Apps

Use Case #4 | Safely Enable Direct-to-internet with Conditional and Contextual Access

Use Case #5 | Protection from Cloud-enabled SaaS and Web Threats

Preventing Unintentional Data Movement

For CISOs and security leaders in 2020, this is the leading use case as they migrate to SaaS and cloud services and desire to control data movement for their increasing base of remote workers. Simply put, blanket allow and deny controls no longer work for cloud apps as most must be allowed. Instead, cloud apps require granular policy controls for data movement. Remote working is also increasing the use of collaboration tools, such as Microsoft Teams and Slack, making it even easier to share and move data inside and outside organizations.

01

Preventing Unintentional Data Movement +

Look for the following SASE capabilities to manage this use case:

Instance-awareness provides the ability to differentiate between, and set policy for, different instances of the same cloud app. Users may have their own personal instance of your business' app making it very easy to move data from a company instance to a personal instance (e.g. OneDrive/Company to OneDrive/Personal), or between apps (e.g. OneDrive/Company to G-drive/Personal).

To/From User Control provides the ability to control data movement to and from particular users or email domains for managed and unmanaged apps. This control picks up where instance awareness is not always possible. It keeps unintentional or unapproved data movement under control by limiting who data can be shared with, and which credentials can be used to sign into apps.

Activity Control provides the ability to control app activities involved in data movement for both managed and unmanaged apps, such as download, upload, post, browse, delete, view, and share.

App Risk and App Categories provide the ability to control data movement by a specific app and its risk rating profile, or by a category of apps. The leading cloud data movement flows for app categories are between Cloud Storage apps, then to Collaboration, Webmail, and CRM solutions from Cloud Storage.

Behavior Anomaly Detection provides the ability to use machine learning (ML) models and sequential anomaly rules to detect outliers from normal baseline behaviors. Detections include bulk uploads, downloads, deletes, rare events, failed logins, proximity, risky countries, and data exfiltration, to name a few. The key element for this capability is the rich contextual metadata collected and stored for baselines and ML analysis.

02

Getting the Right Data to the Right People

Cloud adoption also migrates data and this makes data context a core principle of a SASE architecture. A heavy cloud edge close to users providing security and network services is built around data context for data and threat protection. Legacy defenses unable to see data flows in managed and unmanaged apps and cloud services fall short for this use case. With increased remote working, business process workflows for loans, job applications, human resources, real estate, and other scenarios have now moved online and increasingly involve the transfer of personal identity information (PII) in forms and images.

02

Getting the right data to the right people

Look for the following SASE capabilities to solve this use case:

Data Protection Controls reduce the surface area before invoking data loss prevention (DLP) by blocking malicious and risky websites, blocking high-risk apps, blocking uploads to unmanaged apps and instances, and restricting sharing activities to approved domains.

Advanced Cloud DLP provides the ability to apply cloud DLP to data in motion for managed devices via forward proxy, data in motion for unmanaged devices via reverse proxy, and via API for data at rest in managed apps. New advances, including AI/ML classifiers for documents and images, accurately detect IDs, passports, tax forms, resumes, desktop screenshots, and many other items without data registration.

Single Pass provides the ability to apply data protection to web, managed apps, unmanaged apps, IaaS public cloud user traffic, and custom apps in one solution with one pass, including contextual policies, compliance templates, exact data match, fingerprinting with a degree of similarity, and more than 3,000 data identifies for more than 1,400 file types.

Coaching Users and Identifying High-Risk Users and Apps

Coaching users in real-time is preferred by CISOs over one-time education events to drive behavior and reduce risks. Cloud adoption changes the control planes to identity, apps, and data, and the first two can have risk profiles while data can be classified. Given how “allow” is the new normal, understanding data context enables coaching within granular policy controls impossible with only simple allow or deny controls. In the past security defenses managed a red zone to block and a green zone to allow, but now with cloud adoption and remote working we have an increasing gray zone in the middle to manage.

03

Coaching users and identifying high-risk users and apps

Look for the following SASE capabilities to solve this use case:

Coaching Users provides the ability to coach users in real-time to use safer alternative apps, request a justification for their activity, or provide a warning before they can proceed with a data movement activity. Many customers note ~90% of the time, when users are educated and warned, they do not proceed with data movement and cancel the action.

App Risk Ratings provide a risk profile for tens of thousands of apps across seven or more characteristics using 50 or more attributes defined by the Cloud Security Alliance (CSA). Often these risk profiles can be customized, such as increasing the weighting for GDPR compliance as an example. Policy controls should use app risk levels to determine policy actions, invoke coaching, or block and recommend safer app alternatives.

User Confidence Ratings provide a time period running risk profile for behavior including web, apps, activities, and alerts for a user confidence index rating with an understanding for the maximum point spread between rating events. The user index rating should be able to invoke policy actions such as step-up authentication or blocking an activity.

Safely Enable Direct-to-internet with Conditional and Contextual Access

Safely enabling web, app, and cloud service use is what defines the gray area between what we block and allow. Rich granular policy controls using conditional and contextual attributes make safely enabling access possible for remote workers. Conditions for the current risk profile of the user and app alongside data and threat protection analysis pair with the context of the app, instance, category, user, device, location, data, and activity to enable SASE policy controls, plus retrospective analysis, investigations, and threat hunting.

04

Safely enable direct-to-internet

Look for the following SASE capabilities to solve this use case:

User/Device/Location provides the context of who the user is, whether they are using a managed or unmanaged device, and their current location for policy controls to help determine when data can be viewed only or downloaded. For example, company devices may download certain types of data while personal devices can only view that data.

App/Instance/App & URL Category/Data/Action provides context of the app, category, instance, data, and action for granular policy controls. Uploading company sensitive data to a personal instance for a known managed app or to personal webmail would be questionable.

User Index and App Risk Ratings provide a conditional state of both the user (based on recent behavior analysis) and the app to determine the confidence level for policy actions. A low confidence rating for a user may trigger a step-up authentication or blocking activity based on data classification and action. For apps with low confidence ratings, safer alternatives can be recommended, or users can be alerted and only proceed by providing a justification for using the app.

Data and Threat Protection while you may have the right user, app, data, and action for context with clear conditional access, you still need inline real-time data and threat protection, and this should apply across user traffic to web, apps, and cloud services - something not every solution can provide.

Protection from Cloud-enabled SaaS and Web Threats

Cybercrime has adopted cloud apps faster than many organizations to successfully deliver threats. Cybercriminals are using trusted domains, valid certificates, and instances of the same managed apps you use and allowed unchecked to bypass through your inline defenses (as is often recommended by cloud providers but is poor security practice). Phishing users' credentials for SaaS apps now ranks top of the list in APWG Phishing Trends reports, and file-based malware continues to decline as an initial attack vector. All stages of the cyber kill chain are now cloud-enabled from reconnaissance to data exfiltration and persistence.

05

Protection from cloud-enabled SaaS and Web threats +

Look for the following SASE capabilities to solve this use case:

Access Credentials in Forms given identity, app, and data are the new security control planes, it is no surprise that cyber-attacks focus on stealing credentials plus using brute force attacks for access. Use Cloud DLP to determine if login credentials are posted in undesired web forms created by cybercriminals and posing as trusted managed apps and instances. This type of cloud phishing easily evades legacy endpoint, email, and web defenses.

Threat Intelligence Sharing provides bi-directional threat intelligence sharing between defenses in your SASE consolidated security stack including Netskope, endpoints, SIEMs, SOARs, and IR solutions. Also, investments in threat intelligence feeds can be automated for sharing with tools like the Cloud Threat Exchange (CTE) and you can avoid overwhelming your web filtering configuration.

Cloud Threat Research provides focus on cloud-enabled threats and requires visibility of data and context within apps and cloud services for user traffic. If your legacy security solution cannot see the data in the cloud app, then exposing the threat is unlikely. Using a back-up defense with an endpoint has its limitations as many cloud-enabled threats do not impact endpoints.

Advanced Threat Protection provides multiple defenses for detection after all possible prevention checks are complete, including de-obfuscation and recursive file unpacking, pre-execution analysis and heuristics, bare-metal sandboxing, machine learning analysis, plus behavior analysis to detect insider threats, account compromise, and data exfiltration.

Summary

The value of data context within a SASE architecture to protect remote users is vital.

Consider an employee that accesses a document within your organization's collaboration app, a document in which a third-party collaborator has put a link to another document hosted in a different cloud app. But that link is malicious, and it takes our original user to a phishing page - which looks exactly like the cloud app login page they expect to see and is hosted within a well known and "trusted" cloud service. Our employee unwittingly enters their credentials and they are stolen.

This entire scenario executes in the cloud with no files or file segments written to endpoints to analyze. The legacy mindset of file downloads with malware has to shift to include cloud-enabled threats, plus unintentional or unapproved data movement between cloud apps. Users and data are in the cloud freely adopting apps to enable their business processes. Our job is to safely enable cloud access understanding the new gray area between allow and deny to protect our data.

For More Information

Netskope can help you secure your remote workers no matter where they are. For more details, please contact your local Netskope sales representative or channel partner or refer to the following web pages:

Securing Remote Workers:
https://www.netskope.com/solutions/securing-remote-workers

Move Beyond VPNs:
https://www.netskope.com/solutions/virtual-private-networks

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.**