netskope

5 Critical SASE Use Cases for Hybrid Work Environments

5 Critical SASE Use Cases for Hybrid Work Environments

The pandemic has accelerated the adoption of hybrid working models centered on cloud-based networks, data centers, and applications. And while 63% of high-growth enterprises have deployed hybrid working[1], the approach can challenge underprepared networking and security teams. Unreliable, high-latency home networks can affect user productivity, and security gaps can emerge from a lack of cloud awareness. Meanwhile, expensive and complex legacy network and security systems provide a further barrier to uptake. For these and other reasons, leveraging security service edge (SSE) capabilities, as part of a secure access service edge (SASE) architecture, is now critical to successful hybrid deployments.

netskope

[1] Source: Accenture https://www.accenture.com/us-en/blogs/business-functions-blog/hybrid-workforce

5 Critical SASE Use Cases for Hybrid Work Environments

Use Case #1 | Ensuring Robust Network Performance, User Experience, and Security

Use Case #2 | Maintaining Visibility and Control in the Cloud

Use Case #3 | Protect Against Cloud-Enabled SaaS and Web Threats

Use Case #4 | Prevent Data Exposure, Theft, and Insider Risk

Use Case #5 | Achieving Cost Savings and Operational Efficiencies

netskope

Ensuring Robust Network Performance, User Experience, and Security

With hybrid working, security teams must find a balance between security on the one hand, and network performance/user experience on the other. This is because any impact on users creates a risk that they will look for ways to circumvent security controls. Legacy security solutions negatively impact user experience either because they are siloed, which adds latency to the network, or they are centralized, which means traffic must be routed through the perimeter security stack and rely on slow, outdated technologies like MPLS and VPN.

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

Ubiquitous cloud-native architecture with global data centers eliminates the need for remote traffic to be routed through the central network for security inspection. Rather, a cloud-native architecture enables security inspection to be embedded in streamlined, direct-to-internet traffic patterns that reduce latency. Additionally, a converged SSE platform, which makes up the security stack needed for SASE, enables a "single-pass" approach that performs all security inspection in one place, making security transparent to the user experience as an efficient, low-latency "bump in the wire."

Zero-trust network access (ZTNA) provides another means of ensuring that traffic does not need to be routed back to the corporate network. By utilizing ZTNA, security and network teams can enable efficient, secure access to private applications, whether they reside on the corporate network or in the cloud.

Edge security capabilities also help to reduce network latency while increasing the overall reliability of the network. Look for cloud-native platforms that enable full compute at every service point for real-time, inline processing at scale, and which have direct peering partnerships with cloud, content delivery networks, and SaaS providers for additional performance gains.

Tight integration with software-defined wide-area network (SD-WAN) solutions means that you can eliminate slow and costly MPLS connections that force all branch office traffic back through the corporate network. Instead, your users can benefit from fast, affordable "direct-to-internet" broadband connectivity to web and cloud applications, boosting their productivity.

Digital experience management (DEM) tools provide organizations with granular end-to-end visibility of user activity, with actionable insights into network and application performance, making it easier to troubleshoot and optimize the user experience. With DEM capabilities, you can be sure that your cloud security delivers the protection you need without performance trade-offs.

02

Maintaining Visibility and Control in the Cloud

Legacy security architectures struggle to maintain security visibility and control as applications and data move into the cloud. With hybrid working, organizations must mitigate the additional security risk of allowing unmanaged devices and home/public networks to access corporate resources. Networking teams cannot allow security controls to impact network performance and, as a result, some are choosing to bypass security controls, opening the business to risk.

Look for the following SSE capabilities to manage this use case in a SASE architecture:

Embedded data protection technologies that extend to wherever data resides, and monitors and prevents sensitive data from being accessed and uploaded by remote workers to unmanaged cloud applications or websites.

Threat protection technologies, including sandboxing and remote browser isolation, which detect and prevent even the most advanced attacks. Look for tools that are capable of detecting and stopping malware from cloud-enabled threats across the hybrid working environment and in real time. The right approach will help address data exfiltration and insider threats, alert on account compromise, and highlight anomalous user behavior.

Risk management technologies that automatically assess and improve organizations' cloud security postures. These tools should be able to scan across the full range of the enterprise cloud apps and services to understand content and context, such as corporate versus personal instances, app risk, and data sensitivity, thereby enabling adaptive controls that meet the precise needs of the organization.

Advanced behavioral analytics with AI/ML models has the potential to detect unknown threats and anomalous behavioral patterns hidden in network data, which makes them an indispensable part of any comprehensive cybersecurity solution for hybrid working. The key to success is to find a solution capable of capturing the full spectrum of user activities across SaaS applications, cloud infrastructure, and the websites that users visit.

Reverse proxy capabilities that enable unmanaged devices to access corporate resources without compromising corporate security. This capability provides a buffer zone between external devices and internal systems, so remote workers are unable to directly access the network without first being checked by the reverse proxy.

Zero-trust network access (ZTNA) provides highly granular access to applications and resources, reducing the lateral movement risk entailed by granting network-wide access to VPN users. Unlike with VPNs, ZTNA provides contextual, risk-optimized application access, rather than unfettered network access. With an "inside-out" connectivity architecture, ZTNA minimizes the overall attack surface area by eliminating the exposure of protocols and services to the public internet.

Protect Against Cloud-Enabled SaaS and Web Threats

As hybrid working embeds applications, data, and users outside the network perimeter, the cloud becomes the new attack surface for enterprises. Cybercriminals have adopted the cloud themselves and are using it to successfully deliver threats. Leveraging trusted domains, valid certificates, and instances of the same managed apps enterprises themselves use, these threats can easily pass unnoticed. All stages of the cyber kill chain are now cloud-enabled from reconnaissance to data exfiltration and persistence.

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

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.

Access credentials in forms—given identity, app, and data are the new security control planes, it's no surprise that cyberattacks 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 is another benefit of technology convergence in the cloud (see above) where the various elements of an SSE solution can share intelligence, making it more likely that cloud-based threats will be discovered. Also, investments in threat intelligence feeds can be automated for sharing with tools like Cloud Threat Exchange (CTE) and enterprises can avoid overwhelming their 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.

Prevent Data Exposure, Theft, and Insider Risk

Given that hybrid working environments require the migration of data into the cloud, data context is a core principle of SSE, within a SASE architecture. Legacy defenses are unable to see data flows across either managed or unmanaged apps, and cloud services fall short for this use case. Additionally, without understanding the risk associated with cloud applications, it's impossible to limit the access, or user activities, for those cloud apps where data may be at risk of compromise.

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

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

Data protection controls reduce the surface area before invoking 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. Look for a DLP tool that provides a rich understanding of content, context, instance, category, and the risk level of cloud applications being used. These variables, not found in legacy web defenses, can be used to build effective data protection policies directly in the cloud.

Achieving Cost Savings and Operational Efficiencies

As hybrid working becomes the norm, the cost and complexity of security threatens to spin out of control. The average organization manages 76[2] different security tools, and every time a new threat or IT change emerges, they need to consider adding a new one. In addition to the incremental solution cost is the need for more people and time to manage security across separate tools, policies, and reports. Meanwhile, enterprises are looking to move away from costly MPLS and VPN technologies to SD-WAN, but struggle to do so due to the lack of in-built security.

[2] Source: https://www.infosecurity-magazine.com/news/organizations-76-security-tools/

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

Security technology convergence—particularly the convergence of secure web gateway (SWG), cloud access security broker (CASB), data loss prevention (DLP), ZTNA, and Firewall-as-a-Service (FWaaS) systems—in a single cloud delivered solution—dramatically simplifies the purchasing and installation process for enterprises. At the same time, it also optimizes ongoing solution management through a common agent and management console. Meanwhile, the unified policy management enabled by this convergence greatly simplifies the administrative process.

SD-WAN integration enables organizations to achieve huge cost savings by removing the need for slow, inefficient, and costly MPLS branch office connections in favor of fast, affordable broadband, while also reducing the cost of extensive HQ WAN connectivity. Integrating SWG technologies with the SD-WAN ensures you can secure and protect your web, cloud, and SaaS traffic as you migrate to the more cost-effective networking model.

Zero-trust network access (ZTNA) eliminates the need for heavy VPN clients for hybrid workers, and further reduces costs at the HQ network in the form of bandwidth and VPN infrastructure. Additionally, with application discovery and API for automation, ZTNA further simplifies the operations around private application management, user access provisioning, and ongoing maintenance.

Summary

Applying SASE capabilities means that security in cloud-first, hybrid working enterprises doesn't need to come at the cost of performance or productivity.

From here on in, a significant proportion of the workforce will operate outside of a corporate office location, with the expectation of being able to work and access information from any device and location. In fact, it's estimated that 50%[3] of the U.S. workforce will work from home in the long term, as employers embrace the flexibility and convenience of hybrid working. As this shift unfolds, enterprises will need to lay the right technology foundation. Here, by leveraging SSE capabilities as part of a SASE strategy, businesses can transform their branch offices with a cloud architecture that seamlessly integrates security with an efficient and cost-effective SD-WAN to align perfectly with the cloud-first architectures of the modern enterprise.

Beyond the branch, SASE capabilities can also help secure and empower workers in remote and home locations by establishing a ubiquitous cloud fabric that enables fast, easy, and secure access to web, cloud, and private apps from any device or location. As a result, enterprises will be able to make their businesses more agile, better mitigate security risks, and simplify operations to realize a better total cost of ownership.

[3] Source: https://www.inc.com/bill-murphy-jr/a-stanford-economist-who-studiesremote-work-says-half-of-allworkers-will-make-thisbig-change-in2022.html

For More Information

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.

Learn how Netskope helps customers be ready for anything on their SASE journey, visit netskope.com.