netskope

ADOPTION GUIDE:
Secure Access Service Edge (SASE)

Is Your Security Architecture SASE-ready?

Is Your Security Architecture SASE-ready?

Market Challenge

Enterprise IT infrastructures are in the midst of dramatic change, restructuring how employees, IT applications and data are deployed and consumed. Digital transformation initiatives have accelerated the move of corporate data to the cloud, complicated by a disbursement of employees who have become increasingly mobile yet, still require secure access with a consistent user experience. In the process, enterprises have realized that their physical network and security infrastructure must evolve to protect an increasingly perimeter-less environment. Cloud services, security and networking are rapidly converging together, creating a new model where security and networking are no longer comprised of discrete appliances and devices but, delivered as software services alongside cloud-based applications. As a result, organizations can expect a simplified cloud-based environment based on the consolidation of multiple security technologies, as well as a much more improved user-experience with a reduction in cost.

Gartner has recently coined the term, 'SASE' (Secure Access Service Edge) to describe this emerging security and network framework. The Gartner SASE model addresses the changing security landscape due to digital transformation, whereby users, data and applications are increasingly outside of the traditional data center and in the cloud and must be managed and secured accordingly. Necessary security services like Secure Web Gateways (SWG), Cloud Access Security Brokers (CASB), Data Loss Prevention (DLP), Advanced Threat Protection (ATP) are converged in this cloud-native model and utilize a global, high-capacity, low-latency edge network for an optimized user experience.

Netskope has been singled out as a leader in this Gartner Report, "The Future of Network Security is in the Cloud" which describes their research, analysis and recommendations. Netskope has built a SASE-ready, cloud-native security platform to dynamically scale and deliver security services to enterprises and their users across the globe.

NETSKOPE'S VISION CLEARLY DEMONSTRATES A RECOGNITION OF THE IMPORTANCE OF THE EMERGING SASE MARKET, AND IT IS FURTHER ALONG IN THAT DIRECTION THAN ANY OTHER CASB VENDOR.

Gartner Magic Quadrant for Cloud Access Security Brokers, October 2019, by analysts Steve Riley and Craig Lawson

SASE Value Pillars

Per Gartner, IT Security leaders should consider the following when pursuing a SASE-ready architecture:

- **Utilize a cloud-native architecture:** Recognize that SASE is an enabler of digital transformation offering better speed, agility and availability. Shift operations from managing security boxes to delivering policy-based security services via a cloud-native, microservices-based environment.

- **Consolidate security defenses:** Consider converging cloud and web security technologies to simplify configuration and operations and reduce cost (i.e. SWG, CASB, ZTNA, DLP).

- **Follow a data-centric model:** implement context-aware controls to readily detect and prevent sensitive data movement to/from the web and the cloud, as well as between corporate and personal instances of cloud apps

- **Protect against cloud-enabled threats:** The threat landscape is far different today vs. several years ago as cloud-born threats like phishing are dominant. Get cloud-threat savvy and combine inspection capabilities for threat and data to make an efficient, single-pass inspection solution.

- **Evolve your remote access strategy:** Legacy VPNs requiring hairpinning back to a main office are ineffective, costly and cumbersome to maintain. Consider adopting a zero-trust approach in which you safely connect users and applications together no matter where they are vs merely providing less secure network access.

- **Use a robust, global edge network:** As cloud and internet service providers offer networks based on cost efficiencies, it's best to consider a SASE-ready architecture that provides a high-performance and high-capacity network across the globe without compromising security. Check out the network infrastructure offered by your security vendor to verify if it truly is SASE-ready and capable of supporting "cloud heavy" communications. If using Software-defined Wide Area Network (SD-WAN) solutions, connect with this edge network for extended efficiency and performance.

- **Integrate cloud controls:** As stated previously, while consolidation of security technologies like CASB, |SWG, CSPM and more are essential for being SASE-ready, it's also just as important to converge and integrate your management and administration tools to reduce complexity and increase efficiencies. Solutions with truly integrated consoles and user interfaces, as well as integrated endpoint clients (agents) offer simplicity vs. chaos.

This Adoption Guide elaborates on the above points to help you better understand how to assess and implement a SASE-ready security architecture.

Cloud-Native Architecture

Market Challenge

SASE operates in the cloud to protect an organization's data, users and applications in the cloud and requires a new framework in which advanced network and security functions are provided natively in the cloud. This requires a microservices approach to the architecture in order to rapidly build and deliver new features, elastically scale to match demand, and must be architected for high-resilience as well as low latency. An architecture that relies on traditional network and security appliances that are merely ported to the cloud as software, is not SASE-ready. This common, yet hodgepodge, approach simply does not scale, suffers from interoperability issues, is unable to deliver new features quickly and, finally, delivers security services with much higher latency.

SASE Benefit

A cloud-native architecture, built from the ground-up, ensures that your SASE vendor understands how and why utilizing a microservices software architecture can deliver seamless security services that best match your risk reduction requirements. It also future-proofs your investment in an architecture that rapidly adapts to the changing enterprise network and security market, building new products natively and delivering security services without hindering business productivity or impacting the end-user experience.

Top Questions to Ask

- Ask your SASE provider how they built their cloud platform. Is their architecture future-proof in the cloud?
- Did they simply port security appliances or software to the cloud?
- Or did they build their platform natively from the ground up on a microservices software architecture?
- How is it optimized to rapidly deliver new features?
- Can their underlying network infrastructure provide low-latency and high-capacity worldwide?

TRADITIONAL ENTERPRISE NETWORK AND NETWORK SECURITY ARCHITECTURES THAT PLACE THE ENTERPRISE DATA CENTER AS THE FOCAL POINT FOR ACCESS ARE INCREASINGLY INEFFECTIVE AND CUMBERSOME IN A WORLD OF CLOUD AND MOBILE.

Gartner, The Future of Network Security Is in the Cloud, August 2019, by analysts Neil MacDonald, Lawrence Orans and Joe Skorupa

Next Generation Secure Web Gateway (NG SWG)

Market Challenge

Secure Web Gateways (SWG) have been used to protect enterprise users from accessing malicious websites that diminish the overall security of an organization. Through a SWG, security teams can identify, categorize and block malicious content or malware from entering a corporate network via web traffic. The SWG market is moving from physical appliances to delivering SWG capabilities from the cloud. Going forward, a SWG should be built natively in the cloud, to identify, manage and secure web traffic and more at scale.

SASE Benefit

SASE enables delivery of SWG capabilities along-side other cloud-delivered network and security services such as CASB, DLP and ATP. These consolidated security services are what Netskope refers to as a Next Generation Security Web Gateway (NG SWG). This solution identifies and decodes web traffic and cloud-based applications, deriving detailed context such as personal and corporate instances of the same cloud app (e.g. Office 365, Gmail, Slack). Enterprises benefit by obtaining a big-picture view of the cyber-threat landscape that targets their organizations by incorporating context obtained from the integrated security and network services within this SASE-ready platform. The NG SWG extends protection by identifying, managing and securing web traffic and cloud-based applications, detecting and mitigating cloud-based threats, and lastly, enforcing data loss protection capabilities—all with a unified policy enforcement engine.

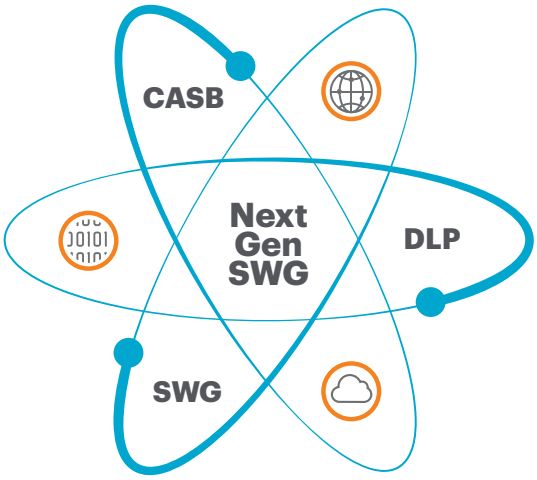
Top Questions to Ask

- Does your vendor support all of the capabilities of a Next Generation Secure Web Gateway as part of their SASE architecture?
- Does your SASE vendor understand granular context of application instances such as distinguishing between personal instances and corporate instances of cloud applications (e.g. Office365, G Suite, Slack)?
- If not, how does your SASE vendor protect against exfiltration of sensitive data within approved cloud applications?
- If not, how do they protect against data exfiltration outside of the corporate perimeter by a malicious insider or cybercriminal?

EVALUATE THE SHORT-TERM OPPORTUNITIES FOR SASE SERVICE CONSOLIDATION AND COMPLEXITY NOW; FOR EXAMPLE, PARTIAL OR FULL CONSOLIDATION ACROSS CASB, SWG, ZTNA, VPN AND REMOTE BROWSER ISOLATION CAPABILITIES...

Gartner, The Future of Network Security Is in the Cloud, August 2019, by analysts Neil MacDonald, Lawrence Orans and Joe Skorupa

Netskope Next Generation Secure Web Gateway



Cloud-native, unified CASB + SWG + DLP

Cloud Access Security Broker (CASB)

Market Challenge

As enterprises move their applications to the cloud, they can no longer rely on on-premises firewalls to protect their data since these appliances are blind to modern cloud traffic like API calls and JSON. Furthermore, corporate data has moved primarily from a centralized data center within the enterprise perimeter to an increasing number of SaaS apps and public cloud/IaaS services outside the perimeter, compounding the ability of security operations (SecOps) teams to manage security policies in a consistent and coherent manner. Cybercriminals have moved their attack vectors to target corporate data located across SaaS and IaaS apps that often have limited native security controls. Customers require a deeper set of security controls to enable more granular visibility into activities performed across SaaS, Web and IaaS services, regardless if they are performed from managed or unmanaged devices.

SASE Benefit

CASBs based on SASE can help organizations deliver consistent security controls across SaaS, Web and IaaS services, minimizing their attack surface and protecting their most sensitive data. CASBs can help customers enable both data-in-motion and data-at-rest security controls through a combination of deployment modes. Using a combination of API-enabled and inline defenses, modern CASBs discover cloud apps in use and assess their risk, while also protecting against sensitive data loss and threat propagation using DLP and ATP capabilities. Protecting the most sensitive corporate data across managed and unmanaged cloud apps, a modern CASB is the foundation for a SASE-ready architecture and complements other necessary security technologies.

FOR THE THIRD CONSECUTIVE YEAR, GARTNER RECOGNIZES NETSKOPE AS A LEADER IN THE MAGIC QUADRANT FOR CLOUD ACCESS SECURITY BROKERS BASED UPON COMPLETENESS OF VISION AND ABILITY TO EXECUTE.

Gartner Magic Quadrant for Cloud Access Security Brokers, October 2019, by analysts Steve Riley and Craig Lawson

Top Questions to Ask

- Does your SASE vendor offer both API-enabled (data-at-rest) and Inline (data-in-motion) controls over corporate data stored in cloud applications?
- Can they apply the same data loss prevention (DLP) polices across cloud apps and websites, under a single policy framework and management console?
- Can they decode user, location, activity, application, instance information and more in support of context-aware, granular policy controls?
- Can they distinguish between instances of the same cloud apps, such as recognizing personal and corporate instances of Gmail or Office365?

Data Loss Prevention (DLP)

Market Challenge

Organizations have always struggled with the growth and control of sensitive data and this has only exacerbated with the rapid growth of cloud applications and services, as well as increasing mobile users working remotely. The primary issue for enterprises has been scaling data classification, ensuring that sensitive data is properly labeled so that a DLP policy can accurately detect and prevent sensitive data from leaving the enterprise. In a cloud-first world, legacy DLP solutions fail at tracking sensitive data loss and exfiltration to personal cloud services and devices and continue to suffer from excessive false positives. Further compounding the burden for organizations are the regulatory requirements (e.g. PCI, PHI, HIPAA, GDPR) that mandate protections for customer data that mean hefty fines for non-compliance, as well as a tarnished corporate brand. Organizations have realized that traditional on-premises DLP solutions are simply not architected for how data is rapidly growing and where data is moving–towards the cloud.

SASE Benefit

SASE enables data protection as an integrated part of the cloud security framework. Modern cloud DLP solutions provide full visibility and, in the best cases, context awareness of data movement across clouds as well as mitigation of loss and exfiltration. In order to scale and optimize DLP, policies must be data-centric, emphasizing the actual data regardless of the application. DLP policy management becomes more simplified as the same policies can be applied across all cloud applications and websites, ensuring the same set of DLP policies are applied to data-at-rest and data-in-motion, resulting in always-on protections wherever sensitive data travels. A SASE-ready framework should effectively identify, classify and understand data, to provide a granular understanding in support of policies based on context, such as user, device-type, file type, data identifiers and more. Lastly, in support of compliance, intuitive and customizable monitoring and reporting are essential to ensure organizations meet the regulatory demands placed on them.

THE BIGGEST CLOUD SECURITY CHALLENGES FACED BY CYBERSECURITY PROFESSIONALS ARE DATA PRIVACY (52%) AND DATA LOSS LEAKAGE (51%).

2019 Cloud Security Report, Cybersecurity Insiders, March 2019

Top Questions to Ask

- Does your SASE vendor have a limited number of supported apps or services for their DLP?
- Can the DLP engine identify and process the data patterns that are relevant to your business?
- Can the same DLP policy be applied to data-at-rest and data-in-motion use-cases?
- Are they using Artificial Intelligence or Machine Learning (AI/ML) to enhance their DLP? How?
- Does your SASE vendor's DLP solution support protect any user, device, or location including using browsers, sync clients or mobile apps?
- How long do they maintain rich metadata for web traffic and cloud services in support of enhanced analysis? *(Hint: 90 days should be a minimum.)*

Advanced Threat Prevention (ATP)

Market Challenge

SecOps teams are tasked with building layered security protections, delivering a defense-in-depth security model that requires multiple threat intelligence feeds, endpoint protection, cloud threat protections and traditional network defenses. This common strategy is challenging as SecOps teams typically follow a best-in-class security approach that is complex, costly and difficult to maintain–especially with disparate products, limited staff and expertise; or they pursue a single vendor solution that may provide less complexity and cost, but lacks required security capabilities (e.g. granular controls or SSL/TLS decryption). With the rapid rise in cloud-enabled threats such as phishing, legacy solutions are increasingly blind to threats and pose significant risk. What's needed is a cloud-native solution that scales to support real time (fast scanning) and deep scanning (sandboxing) threat protection across the cloud to effectively expose and mitigate any malware and threats.

SASE Benefit

An ATP solution based on a SASE model can significantly help reduce complexity and cost for SecOps and Incident Response (IR) teams, while enhancing threat efficacy and scale. A SASE-based ATP solution can help centralize all security events collected across managed and unmanaged clouds, providing a single, consolidated view into all activities using a multi-layered approach (e.g. recursive unpacking, pre-execution heuristics, sandboxing, ML). This solution must collect rich metadata from web and cloud traffic for further analysis and investigation–supporting inhouse IR teams or Managed Detection and Response (MDR) services. Lastly, a SASE-ready ATP solution must prevent and detect threats using modern cloud service 'kill chains'–something that legacy defenses, even modern endpoint defenses, miss.

PHISHING ATTACKS ON SAAS/WEBMAIL AT 36% NOW LEAD OVER PAYMENTS AND FINANCIAL INDUSTRY THREATS AND REQUIRE INSTANCE-AWARENESS FOR 1000s OF CLOUD SERVICES TO BLOCK THEM.

Anti-Phishing Working Group, Phishing Activity Trends Report, May 2019

Top Questions to Ask

- Does your SASE vendor have a limit for the number of TLS encrypted un/managed cloud services they can inspect?
- Can they describe how they would prevent a rogue or personal instance of a cloud service delivering a cloud phishing attack?
- How do they provide the same threat protection defenses for remote offices and users–whether they're using browsers, sync clients or apps?
- Do they have ATP capabilities that are powered by AI/ML?
- Do they have third-party integrations with EDR, RBI, SIEM, and SOAR solutions, plus threat intel sharing?

Zero Trust Network Access (ZTNA)

Market Challenge

Organizations have become more global and dispersed and that requires stretching the enterprise perimeters to remote office workers. Remote users require secure access to corporate resources that ensures organizational security without impacting the user-experience. Security teams have traditionally relied on complex and expensive VPN appliance implementations (IPSec & SSL/TLS) that do not scale and incur growing maintenance costs while being cumbersome to manage. Furthermore, with the traditional "open" network access of VPNs, sensitive data can easily be exfiltrated to cloud applications while compromised accounts or insiders can move laterally within the network, performing nefarious activities. With applications and data rapidly moving to the cloud, SecOps teams require a modern secure access solution that easily scales while allowing remote users secure access to select private applications in public clouds and data centers regardless of location.

SASE Benefit

A SASE provider can deliver a cloud security solution that enables application-level access to private applications based on Zero Trust principles. This includes the authentication of users, and device posture checking and classification, *before* connecting users to select private apps. Furthermore, published private applications should not be visible or accessible by unauthorized users, reducing the attack surface and helping to prevent cyberattacks and intrusions. This approach mitigates the need to deploy costly WAFs and DDoS protection services to prevent cyber-attack campaigns from impacting the operation and accessibility of corporate applications. A SASE-ready access solution should simplify and enhance the overall remote access experience while utilizing the same high-performance infrastructure available to other cloud-native security technologies and controls.

OVER 75% OF RESPONDENTS SEE VALUE IN CONSOLIDATING ZTNA SECURITY SERVICES WITH OTHER CLOUD-BASED SECURITY SERVICES SUCH AS CASB AND SWG.

Cybersecurity Insiders 2020 Zero Trust Report, February 2020

Top Questions to Ask

- Does your SASE vendor provide a Zero Trust strategy?
- If so, how have they implemented their ZTNA solution? Did they port a third-party vendor's product into their platform?
- Are published corporate applications accessible from anywhere on the internet?
- Are inbound connections required or utilized in their remote access solution?
- Do they still require a WAF or DDoS protection services to complement the protection of published applications?

Software-Defined WAN (SD-WAN)

Market Challenge

The SD-WAN market emerged as an alternative way for enterprises to address the costly implementation of MPLS circuits to securely connect remote offices to their corporate networks. Adding to the burden, remote offices are required to deploy multiple physical network and security appliances at each location that could include: SWGs, SSL/TLS inspection, anti-malware, Next-Gen Firewalls, IPS, VPNs, etc. For the average organization, these costs can quickly escalate, increasing pressure on budgetary limits for CapEx and OpEx to run the corporate network. SD-WAN products complement and work well with security solutions to provide secure access, if integrated properly.

SASE Benefit

SASE allows for a seamless integration of SD-WAN functionality in a cloud-based architecture where SD-WAN functionality is built natively alongside security services, which helps to scale performance and delivery for remote office users. Organizations can reduce the cost and complexity of deploying multiple network and security appliances across the entire enterprise network. SASE-ready architectures enable SD-WAN edge solutions to be directly connected to the edge cloud network, avoiding the complexity of deploying physical SD-WAN hubs. This access model can also help simplify multiple overlays that drive up complexity for enterprise network management.

Top Questions to Ask

- How does your SASE provider implement their branch-to-branch connectivity solution via SD-WAN?
- How many physical appliances must your SASE provider deploy in order to deliver SD-WAN functionality? If this number will increase as your business grows, are you prepared to pay for and maintain it?
- Is their solution integrated with a cloud-native platform or is it at physically separate co-locations with disparate network and security functions that can impact your user performance?

Global Edge Network

Market Challenge

As organizations have become more global and dispersed, they have realized that deploying applications from a centralized location doesn't scale. Users requiring access from remote or less populated locations often suffer from a poor user experience. Productivity diminishes as end users wait or are required to unnecessarily repeat application tasks. Overcoming the performance limitations of the public internet and first mile only services is essential as more data, apps and users move to the cloud. This places tremendous pressure on IT teams that are responsible for delivering the proper secure infrastructure for applications and data worldwide. A vendor's global network architecture determines how long customer data travels to and from the closest Points of Presence (POPs) before it is processed, potentially increasing end-to-end latency. In the end, the underlying network infrastructure affects the scale and efficacy of security controls and traditional, spotty networks are inadequate for cloud-first organizations.

ENTERPRISE TRAFFIC SHOULD RARELY TRAVERSE THE PUBLIC INTERNET. INSTEAD, THE INTERNET IS USED FOR A SHORT HOP TO THE SASE FABRIC, WHERE IT IS THEN INSPECTED BASED ON POLICY AND OPTIMIZED FOR BEST PERFORMANCE USING FAST-PATH ROUTING AND PEERING ARRANGEMENTS.

Gartner, The Future of Network Security Is in the Cloud, August 2019, by analysts Neil MacDonald, Lawrence Orans and Joe Skorupa

SASE Benefit

A SASE-ready provider will deploy their services through a global cloud edge network, delivering security services closest to the end-user, optimizing routing and availability, while enabling, if not accelerating, inline security functions like DLP and ATP. This allows processing to be done quickly with minimal latency and interruption to the end-user. Vendors that backhaul customer traffic to centralized data centers simply break the SASE model and are unable to deliver all the required network and security services demanded by enterprises, creating bottle-necks that introduce latency that weakens protections and frustrates users. In order to be able to scale on demand, anywhere, anytime, SASE architectures require an intelligent global distribution of POPs and data centers with auto-failover functions in order to deliver the best possible experience to users worldwide. Key peering relationships with Tier-1 ISPs and CSPs help optimize routes between end-users and managed application providers, resulting in a satisfactory overall user experience.

Top Questions to Ask

- How reliant is your SASE vendor on the public internet for their cloud security service?
- What amount of excess capacity do they manage for their cloud security service?
- How do they define a POP? Are their POPs all consistent with similar capacity and latency thresholds?
- Are these POPs available to all customers worldwide–or are there limitations?
- Who are the Tier-1 ISP providers they peer with?
- Do they manage and optimize the entire cloud infrastructure, including the first, middle and last mile?

Single Console, Single Agent, One Cloud

Market Challenge

SecOps teams have long suffered from managing and maintaining multiple disparate products and consoles, sourced from a variety of security vendors. This means the increasingly complex design, configuration and management of their security infrastructure. Furthermore, SecOps teams struggle with a hodgepodge of product-centric security consoles that amplify the complexity, wasted time and effort in working in this "console chaos". The same challenge exists for agents on endpoints. Many diverse agents combat endpoint resources and slow down security functions like DLP, Endpoint Protection (EPP) and private app access. Unfortunately, most large security companies provide a portfolio of hardware- and software-based security products that have been assembled together through acquisitions. While some integration may exist, the results are the same: a dissimilar set of security products that doesn't improve the security posture and only complicates and weakens it.

SASE Benefit

A SASE-ready solution should be truly unified vs. loosely integrated. Beware of products that require separate configurations and dashboards as a way to connect multiple products into common workflows. A SASE architecture that was architected from the beginning with one console, one policy engine, and one agent for SWG, CASB, and more ZTNA ensures simplified management, consistent policy deployment, and a streamlined approach to providing fast and secure access to the cloud and web. This way, IT security teams must only learn one console/GUI with an intuitive workflow to configure, operate and monitor their security posture, Lastly, integration with third-party security tools is essential and a SASE-ready solution should offer REST APIs, plus threat intelligence sharing, based on standards, to extend its capabilities.

Top Questions to Ask

- Ask your SASE vendor, how many consoles they require to configure their security portfolio of web, public cloud, private cloud, and data center apps? Are these consoles merely dashboards connecting to multiple systems without any workflow or policy enforcement integration?
- How many of their security defenses are made for the cloud (vs hosted in the cloud) and integrated?
- Do they have a single, extensive policy engine?
- How do they handle integrations with third-party tools and is it cumbersome?

How Netskope Can Help

Netskope is a market-leading cloud security vendor. Its Security Cloud platform delivers cloud-native, cloud-smart security services to customers worldwide without compromising performance. Netskope helps customers solve their most critical security requirements, protecting their applications and data from elusive threats. Data-centric in design, the Netskope cloud security platform is architected to understand and protect SaaS, web and IaaS environments while accessed from any device. Powered by Cloud XD™, Netskope enables contextual control of your security policies based on user-type, device-type, application, instance, activity, data category and more. This lays the foundation for applying granular security controls across SaaS, Web and IaaS environments, all managed from a single console with unified policy enforcement.

The following are benefits that your organization will realize from the SASE-ready Netskope platform:

Data-Centric

- Offers context-aware, data-centric protection, following data everywhere it goes.
- Provides visibility where traditional security technology is blind
- Protects sensitive data regardless of where it travels: Cloud, Web and IaaS.

Cloud-Smart

- Understands the language of the cloud such as API calls and JSON.
- Cloud XD™ enables powerful context that enable granular security controls
- Applies universal security controls across both Cloud, Web and IaaS.

Fast

- Offers NewEdge™: a global high-capacity, high-preforming network infrastructure optimized for user experience
- Enables real-time security functions (e.g. SSL/TLS inspection, DLP) at scale, without compromising performance
- Provides an undisrupted, higher-performance and secure experience when accessing the internet.

For more information on how Netskope can help you become SASE-ready, please check out these web pages, or contact your local Netskope sales representative.

SASE: https://www.netskope.com/about-SASE

Netskope Security Cloud Platform: https://www.netskope.com/platform

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.