...making excellence a habit.™

Secure access service edge

The future of network security

The future of network security

With digital transformation and cloud-first strategies becoming the new normal for many organizations the question key executives must ask is what percentage of your workloads are running in a public cloud?

Users are connecting from anywhere and to globally disparate services, many not under the control of the requesting organization. The traditional security infrastructure strategies no longer apply in modern architecture such as Software as a Service (SaaS), which cannot be contained by the cloud client from a traditional legacy network security mindset, based on its nature, and requires a cloud-native approach to security governance.

94%

of Google traffic is encrypted via their transparency report

Secure Access Service Edge

Secure Access Service Edge (SASE), as described by Gartner in "The Future of Network Security Is in the Cloud" report refers to the partial or full centralization and consolidation of cloud-delivered network and network security solutions. Primary examples of network and network security solutions include Cloud Access Security Brokers (CASB), Secure Web Gateways, Firewall as a Service, Software Defined Wide Area Networks, and Zero-Trust Network Access. These services have been developed as a response to the challenges faced by organizations.

These challenges include the need for users, devices, and data to be protected by the security policies irrespective of where they are located, when they connect, or what device they connect with.

Further to this, a very high and growing percentage of internet traffic is encrypted with Google demonstrating that 94% of Google traffic is encrypted via their transparency report [1] (02/02/2020).

In addition to legitimate web and application traffic, bad actors are also using encryption to obfuscate their activities and there are now several free providers of SSL certificates which removes the previous cost boundary. To be able to combat these encrypted threats and to analyze and control legitimate workflows, organizations need to be able to inspect this encrypted traffic.

Traditionally, inspection has been expensive and difficult to implement smoothly on-premises. Legacy boxes needed to be sized, purchased, and repurchased when the traffic requirements increased. There was also an element of wastage as the appliances always had to have processing power in reserve and hence unused capacity. Cloud computing provides a solution via the ease and automaticity of scalability and therefore greatly increased service availability, intelligent resource utilization, performance, centralized administration and reporting combined with positive perception by the users. We now break down the individual cloud delivered components that compose the SASE model and map how SASE can reduce organizational risks.

[1]* https://transparencyreport.google.com/https/overview

A Secure Web Gateway as a Service (SWGaaS) is a proxy solution designed to protect organizations and users against web-based threats. A core feature of this solution is URL filtering, to block and caution websites and applications, based on policy. Advanced features vary and can include SaaS application control (social media only available to non-marketing users outside of working hours), malware protection, anti-virus, SSL inspection, sandboxing, browser control and data loss prevention.

A Cloud Access Security Broker or CASB allows the monitoring, security policy creation, and policy enforcement of and against cloud services in use by the organization. It sits in between the client and the cloud service and enforces policy via direct API connection. It is possible to set the same policy across multiple cloud applications such as data loss prevention and collaboration control. Vendor offerings also include continuous API-based IaaS and PaaS security policy configuration review which may include triggers for alerting and auto-remediation purposes should a misconfiguration be detected that would impact the organizations security posture.

With Zero Trust Network Access (ZTNA), the security industry is moving from network to identity as the perimeter. Applications are dark by default where there are no public IP addresses or VPN gateways exposed for malicious actors to port scan, users are given access to applications on specific ports, and not put on the network and given the opportunity to move laterally. Greatly increased security and granular control and monitoring are the main themes here as is third-party contractor access to specific applications which has proved to be detrimental to organizations security in the past.

Firewall as a Service policy and enforcement are from the client edge to the cloud. Baseline feature-sets here include rulesets and more advanced offerings allow next-generation features such as application definitions and fully qualified domain names-based rules. Software updates are no longer the responsibility of the client, with the cloud provider managing this element via the shared responsibility model. Configuration drift and management is more easily governed by the organization due to the consolidated nature of the service and its management plane via the web-based admin portal and API exposure.

> With Zero Trust Network Access (ZTNA), the security industry is moving from network to identity as the perimeter.

As more applications are migrated from the datacentre to the cloud, the requirement for expensive network circuits reduces and the need for a more modern network solution arises. With software defined wide area networks, branch traffic will egress from a local breakout directly to the internet, via the network and security elements of the SASE platform. The legacy solution of backhauling traffic to a traditional datacentre security stack for inspection and control creates bottlenecks, can be a risk to availability and is expensive.

Historically edge devices were configured manually at each site. Software definition enables the benefits of standardisation and automation. SD-WAN features include Quality of Service (QoS), optimized routing paths, increased redundancy, application awareness, traffic optimisation and reduced latency. Coexistence with existing leased lines for legacy datacentre workload use cases is possible and the WAN control planes for each SD-WAN-enabled location are now centralized in the form of the SASE management plane. Please see below for a typical CISO journey into SASE.

A SASE Journey

A CISO for a large financial organization is looking for a solution to facilitate the modernization of his current network and security stack. They have been tasked with extending the organizations security policies to incorporate cloud workloads and applications and understand that there are differences to be aware of in policy mapping, translation, and the technical solutions themselves.

Some of the current pain points for the CISO and the current portfolio of legacy solutions are:

Insufficient visibility

The organization has issues with blind spots around mobile users and traffic inspection. They will need to address concerns such as shadow IT and visibility and control over sanctioned cloud applications.

A SASE Solution enables easy to implement, scalable SSL inspection and remote user protection regardless of location. This would ensure that the organization have wide-reaching visibility and control over the threats faced by them. The Secure Web Gateway and Cloud Access Security Broker portions of a SASE solution will allow visibility and control over sanctioned and unsanctioned cloud applications.

> A CISO for a large financial organization is looking for a solution to facilitate the modernization of his current network and security stack.

01 Weak integration

Integration is key for security products and platforms and the CISO has never been completely happy with the integration options exposed by the vendors in his organizations' stack.

A SASE Solution should have strong integration between products within the SASE suite. Data sharing between the network and security modules and attribute-based policies that cross and combine modules allow for more integrated, granular, and adaptive policy creation.

02 Unacceptable availability and performance

Non-global coverage, poor service availability, latency issues resulting in an unacceptable performance for the global and mobile teams have been major pain points in the past. The situation has exacerbated since moving core workloads to the cloud.

A SASE solution includes global points of presence and peering with other cloud service providers, increasing availability and reducing latency. From an architecture perspective, having security engines scanning in parallel as opposed to serial chained engines will increase the speed of threat detection and prevention, and increase performance for the end user.

03 Cost

Legacy appliances are expensive to buy, maintain, and upgrade or replace when new versions become necessary.

The above concern is reduced with a cloud native SASE solution. Replacing hardware with a SASE service and the consolidation of products can result in cost savings for the organization. If bandwidth or inspection requirements change, the system will scale accordingly. New features are rolled out globally across the cloud service and remove the requirement for the client to purchase software or hardware upgrades.

There are also potential IT cost reductions due to a unified administrative portal and less of a requirement for operational maintenance based on the shared responsibility model shift. In addition, there are also more automation opportunities available, enabling the organization to develop cost-reducing workflows.

04 Complexity

As the organization has grown through acquisition and there are some isolated network and security product silos remaining, this is an opportunity to rearchitect. The current stack is comprised of multiple administrative interfaces with specialist knowledge requirements and multiple agents. The agents have created various issues over the years including CPU utilization problems, troubleshooting and conflicts between the multiple different agents required for each product.

A single integrated SASE platform, interface, and device agent addresses each of these issues with minimal portals, less interfacing with external suppliers and simplified troubleshooting.

05 Fixed limitations in legacy IT

The CISO has experienced availability issues with the fixed limitations of the legacy network and security appliances. These issues have ranged from general throughput issues to the ability to inspect encrypted traffic, to an incident where a security appliance disabled critical security features when a threshold on a CPU was breached.

The cloud-based SASE model allows for the rapid elasticity of resources, reducing cost and increasing availability. This is not the case with traditional fixed-limit appliances.

> SASE provides a strong and logical approach with the ability to adapt to the new cloud-first world which will be key in an organization's security success going forward.

06 Slow and error-prone manual processes

As the business scales at a rapid pace, the stakeholders are finding that their traditional network and security rollout model is slow and error prone.

A SASE Solution facilitates automation and standardization. Faster site rollouts are possible with SASE based on its software-defined nature and errors are less likely with properly designed and monitored automated processes. Changes made outside of the corporate change management process will be automatically flagged and actioned accordingly. Software definition also results in automatic documentation should the provider expose controls that allow the exporting and backup of configuration. It is possible to copy or clone site configurations and policies to standardize and expedite the rollout process.

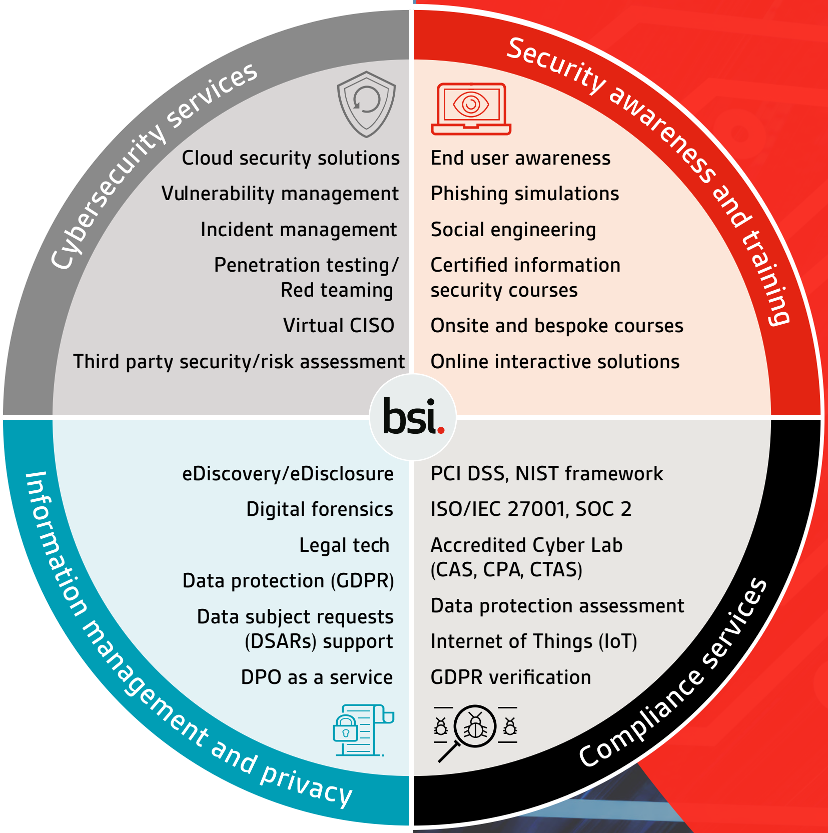
Conclusion

In conclusion, SASE provides a strong and logical approach with the ability to adapt to the new cloud-first world which will be key in an organization's security success going forward. SASE is integrated, cheaper, automated, highly available, simple, fast, and enables the organization to expand visibility into its operations and threats. Organizations should conduct appropriate due diligence as more SASE offerings become available to ensure their supply chain is highly resilient. A well-architected cloud native approach enables enhanced availability, scalability, and lower latency based on the decoupling of functions, parallel scanning, and the use of PaaS services.

Protect your information, people and reputation with BSI

Expertise lies at the heart of what we do. As trusted advisors of best practice, we empower you to keep your business safe through a diverse portfolio of information security solutions. Whether it's certification, product testing, and consultancy services or training and qualifying your people, we'll help you achieve your security goals.

Our Cybersecurity and Information Resilience Consultancy Services include:



Cybersecurity services

- Cloud security solutions
- Vulnerability management
- Incident management
- Penetration testing/ Red teaming
- Virtual CISO
- Third party security/risk assessment

Security awareness and training

- End user awareness
- Phishing simulations
- Social engineering
- Certified information security courses
- Onsite and bespoke courses
- Online interactive solutions

Information management and privacy

- eDiscovery/eDisclosure
- Digital forensics
- Legal tech
- Data protection (GDPR)
- Data subject requests (DSARs) support
- DPO as a service

Compliance services

- PCI DSS, NIST framework
- ISO/IEC 27001, SOC 2
- Accredited Cyber Lab (CAS, CPA, CTAS)
- Data protection assessment
- Internet of Things (IoT)
- GDPR verification

Our expertise is accredited by:

CREST | PCI Security Standards Council QUALIFIED SECURITY ASSESSOR | CYBER ESSENTIALS | CREST STAR | CHECK IT Health Check Service

Find out more

IE/International	UK	US
Call: +353 1 210 1711	+44 345 222 1711	+1 800 862 4977
Email: cyber.ie@bsigroup.com	cyber@bsigroup.com	cyber.us@bsigroup.com
Visit: bsigroup.com/cyber-ie	bsigroup.com/cyber-uk	bsigroup.com/cyber-us

bsi.