SASE, what is it?

BCS ISSG Early Careers Webinar

Luke Hebditch
- Technical Solutions Specialist, Cloud Security EMEAR, Cisco
- BCS ISSG Committee Member

Thursday 1st April 2021
Agenda

- Who am I? My journey to today
- SASE, another buzzword?
- Q&A
Luke Hebditch

- Technical Solutions Specialist, Cloud Security
- Cisco CCNP Certified in both Security and Enterprise
- Joined Cisco in 2016 via Degree Apprenticeship programme
- Graduated with a 1st – BSc Digital and Technology Solutions: December 2019
SASE, another buzzword?
Historic traffic flows led to the age of the single, on-premise security stack
Changes in the types of traffic, origins, and destinations have inverted the traffic model.

Problems:
- Costs
- Performance
- # Tools/vendors
- Integrations
- Maintenance
A more modern “direct internet access” approach

**Network:**
Decentralized

**Security:**
Protect traffic from multiple locations at the cloud edge
The nature of the network has changed

- **Firewall**: Keep data within the firewall
- **Net**: Manage data inside and outside the firewall
- **Extranet**: Manage data through the firewall
- **Access**: Manage data through IDM and access control
- **Intelligence**: Dynamic content data-centric & person-centric
The Journey to Integrated Business-Security

Visibility & the basics
- Patching
- MFA/IAM
- DNS
- EDR
- Monitoring

Fortify Perimeter
- NGFW/IPS
- WAF/DDoS
- VPN
- Email

Control Zones & Segmentation
- NAC
- Workloads

Expand Control
- Guest
- BYOD

Automated Threat Containment (XDR) / Zero Trust

Unify Visibility
- Centralised Logging
- UEBA/SIEM

Automate workflows with Integration / SOAR

Incident Response

Compliance & Posture

System/network-centric security

Process-centric security

Improving security culture
Process/data-centric security: secure the workflow

Secure communications for email: CEO sending email to shareholder

Secure applications for employees: Employee working remotely

Secure web access for employees: Employee researching product information

Secure communications for collaboration: Subject matter expert consultation
The typical first step to address these issues is to combine cloud-delivered security services.

93% of orgs agree that moving security to the cloud has increased efficiency.

76% of orgs are looking for multi-function cloud security services.
Cloud and Network Evolution

- Networks continue to decentralize
- Applications and data are going to the cloud
- Security and networking functions are converging

- 80% of orgs are shifting to direct internet access (DIA)
- 76% of orgs use SD-WAN extensively or selectively
- 42% of branch office security deployments take over a month
- 68% of branch offices and roaming users were the source of compromise in recent attacks
Next, reduce complexity and improve performance by unifying networking, security and identity

There are many names for this multi-function approach...

Secure Access Service Edge (SASE)

Convergence of networking & security services including SWG, CASB, DNS protection, firewall-as-a-service, SD-WAN, and zero trust network access

...but full agreement on the move to cloud-native aggregation
SASE Architecture Model Fundamentals (Gartner)
Realizing SASE Architecture is a Journey

Consolidation through a single vendor

Effective security and threat protection

Global presence and peering relationships

Support for all devices and agents

Microservices based architecture

Flexible deployment and management
SASE includes more than security

- Networking: SD-WAN, VPN, Remote Access
- Security: SWG, Firewall, CASB
- Identity: Zero Trust for the workforce

Visibility, policy and integration
Thank you