Secure Access Service Edge
SASE

@BCS, The Chartered Institute for IT

Michael Attenberger
December 12th 2023
Today’s Speaker

Michael Attenberger
Head of Sales Engineering
Open Systems
Agenda

- SASE Overview
- Why SASE
- SASE Components
- Benefits
- Future of SD-WAN
- Open Systems Managed SASE
- Q&A
Overview
SASE
The Evolution towards SASE
SD-WAN Defined

Traditional WAN

- Network centric
- Hub-and-spoke topologies with central Internet exit point
- Each WAN hardware configured individually
- Slow deployment and activation time
- Expensive network infrastructure with MPLS
- SLA but no failover nor redundancy

SD-WAN

- Application centric and better performance
- Local Internet breakout
- Central orchestration
- Automated site deployments, configurations, and operations
- Cheaper network infrastructure costs and even more bandwidth
- Automatic failover and redundancy with multiple connections

### Diagram

- **Connection**
  - (MPLS, Ethernet, etc.)

- **WAN Hardware**
  - Configuration Provisioning

- **VPN Connection**
  - (MPLS, 5G, Ethernet, etc.)
  - Multiple Links actively used

- **Local Internet Breakout**
SD-WAN Challenges

**Global Performance**
The global Internet is not predictable. Complex underlay strategy with multiple providers and technologies is required to achieve best performance.

**Remote Users**
SD-WAN itself has no support for remote users. An additional solution (e.g. ZTNA) is required.

**Integrated Security**
Local Internet breakout requires local security (e.g. FW, SWG, NDR). SD-WAN does not bring those security capabilities out-of-the-box.

**Cloud Readiness**
Physical data centers disappear and integration with public clouds is limited. Corporate applications move to SaaS.
SASE
Secure Access Service Edge

SSE
CASB
SD-WAN
FW
IDS/IPS
Access

ATP
ZTNA
SWG
AV
Security
Edge
SASE

What?

SSE  ATP  AV  SWG
CASB  SD-WAN  ZTNA
FW  Security  SASE
Access  IDS/IPS  Edge
SASE

Secure Access Service Edge

SD-WAN + SSE → SASE
SASE
Secure Access Service Edge

WAN Service Edge + Security Service Edge

Supplier
Remote Users
On-Site User
IoT/OT

SaaS
Data Center
Cloud/ IaaS
Internet

SD-WAN
Connectivity
ZTNA
SWG
CASB
Firewall
SASE

Secure Access Service Edge

Globally enforced SD-WAN and security policies
Why SASE?
Current Trends

Macro Trends Driving Networking and Security

Apps, Workloads, and Sensitive Data Anywhere

Managed and Unmanaged Endpoints Anywhere

B2B Customers

Factories

Partners/Contractors

Data Centers
Security: The move to the cloud

"by 2025 80% of organizations will have adopted a strategy to unify web, cloud services, and private application access using a SASE/SSE architecture, up from 20% in 2021."

The primary benefits of selecting a consolidated SSE product over stand-alone products are single-agent deployment, consistent policy enforcement, single-pass decryption and content inspection, unified policy management and simplified vendor management.
Business Problems

The Challenges We Hear about:
• Data is Everywhere: in the cloud and in the data center
• Users are Anywhere: office, home, travel
• Legacy Networking is perimeter based using MPLS to central datacenter
• Legacy Security is perimeter appliance based: SWG, FW, IPS/IDS, SEG, etc.
• IT is faced with a global shortage of cyber security talent

IT needs cloud-based Networking and Security in a single service that supports hybrid data security and network requirements.

What challenges are you facing? Do these resonate?
SASE

Connect

WAN Service Edge
- Application Visibility
- Bandwidth Control
- Path Selection
- Application Optimization
- Encryption & Routing
- Network Function
- Line Operations Service
- Multi-Cloud Connect

Secure

Security Service Edge
- ZTNA
- CASB
- Cloud Sandbox
- Anti-Malware
- Secure Web Gateway
- Firewall
- DNS Filter
- Threat Protection

SASE
SASE Components

Firewall

- Local Deployment
  - Mantained by Local IT

- Local
  - Managed by Global IT

- Local

- Global Policy
SASE Components

ZTNA

Zero Trust

Context-based Access Control
Continuous Validation

User
Any User
Any Device
Any Location

Apps
Any Corporate Application
Anywhere

Any Corp

Applications

Cloud

Data Centers

SaaS

ZTNA

Identity

Device

Endpoint Verification
Risk
Location
Time
Other Context

Users, Devices

Any User
Any Device
Any Location

Any User
Any Device
Any Location
SASE Components

Secure Web Gateway

- Authentication
- URL Filter
- SSL Scanning
- Cert Validation
- Malware Protection
- Threat Protection
- Cloud Sandbox
**SASE Components**

**CASB**

1. **Secure Web Gateway**
   - Protect users from incoming threats
   - Block malicious sites

2. **Cloud application discovery and risk assessment**
   - Discover apps and identify most risky services
   - Risk
   - Usage

3. **Block risky applications**
   - Don’t allow-access to risky or non-compliant apps
   - Enforce CASB policy on the Secure Web Gateway

© 2023 Open Systems. All rights reserved. Proprietary & Confidential
Managed SASE

Managed Secure Access Service Edge
SASE Benefits
SASE Options

- Separate Vendors for SSE and SD-WAN
- Single Vendor for SSE and SD-WAN
- Purchase as a Product or Managed Service
Key Use Cases to Start with for move to SASE

- Network and Security Simplification
- Eliminate VPN
- Consolidate security services into a unified SASE platform
- Secure Work from Anywhere Employees
- MPLS Replacement
SASE Advantages

- Reduced Complexity
- Single Solution
- Reduced Costs
- Increased Employee Productivity
- Better User experience
- Increased control
- Better data protection
- Key part of implementing a Zero Trust strategy
Deciding what approach is right for you

Where are you on your connectivity and cloud journey?

NOC staffing

How many SASE Vendors do you want?

Do you want it managed by a third party?
## Single vendor SASE benefits

<table>
<thead>
<tr>
<th>Improved Security Posture</th>
<th>Improved Staff Efficiency</th>
<th>No integration between SSE and SDWAN to break</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Reduced attack surface</td>
<td>• Reduced IT headcount needs</td>
<td>• Single data lake, data model</td>
</tr>
<tr>
<td>• Reduced complexity:</td>
<td>• Faster deployment</td>
<td>• Single POP so latency reduction eliminating</td>
</tr>
<tr>
<td>consolidated vendor</td>
<td>• Eliminates feature</td>
<td>multiple hops (SDWAN to SSE, etc.)</td>
</tr>
<tr>
<td>and interfaces</td>
<td>redundancy</td>
<td></td>
</tr>
<tr>
<td>• Consistent policy:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cloud and on prem</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Managed SASE

Security built in
Drive digital transformation without compromising on security

Access everywhere
Ensure global access and high performance for everyone

Service redefined
Get direct access to experts who support you 24x7 in all situations

Edge to scale
Scale up and out with unified functionality on an agile platform

No longer decide between

Usability
Accessibility
Availability
Functionality

Security
Performance
Quality
Compatibility
SASE
Future of SD-WAN
SASE
SD-WAN Backbone
SASE

SD-WAN Backbone

First Mile

SD-WAN Backbone

Last Mile

= Cloud PoP
WAN Backbone

RTT = 20ms

Internet

RTT = 20ms

MPLS

= Cloud PoP
Question
What is needed to turn off SD-WAN?
Question
What stops you from going that path?
Open Systems
Managed SASE
What you get with Managed SASE from Open Systems

The Difference

Onboarding

Operational Excellence

Strategic Excellence
The Open Systems Difference: Comprehensive, Unified, Easy to Use

**SASE:** Comprehensive SASE solution delivered as a Managed Service

**Unified:** A single vendor, single platform solution for SD-WAN and SSE that supports your cloud journey with full hybrid support

**Easy to Use:** Managed Service with single portal for customer interaction
Open Systems Managed SASE

WAN Service Edge
- SD-WAN
- WAN Encryption and Routing
- Application Visibility
- Bandwidth Control
- Path Selection
- Application Optimization
- Mobile Entry Point
- Partner Connect
- Multi-Cloud Connect
- Connectivity Service
- ISP Line Operations Service

Security Service Edge
- ZTNA
- SWG
- CASB
- Firewall
- Threat Protection
- Network Detection And Response
- Cloud Sandbox
- Secure Email Gateway

Platform
- Notifications, alerting and ticketing
- DevSecOps
- Policy Management
- Network Analytics
- Security Reporting

© 2023 Open Systems. All rights reserved. Proprietary & Confidential
How is Open Systems Different?

Table Stake Capabilities

- SD-WAN
- Firewall
- MEP
- CaaS
- ZTNA
- SWG
- CASB
- SEG

Tight integration & Seamless System

- Single pane of glass
- Observability
- Policy Management
- Single Unified Platform
- Cloud
- Appliance
- Hybrid & Multi Cloud

Renowned & Unmatched Service

- 3rd Level Engineers 24/7
- DevSecOps
- Dedicated TAMs
- Local Empowered Engineers

Peace of Mind Beyond Partnership

- Flat Fee
- Onboarding Roll Out incl.
- HW & SW Upgrades incl.
- Lifecycle Management incl.
- Unlimited Tickets
- Unlimited Calls
- Management Options

SASE Service Value

Comprehensive

Unified

Easy to Use
## Open Systems by the numbers

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Years of innovating for customers</td>
<td>30</td>
</tr>
<tr>
<td>Net promoter score</td>
<td>66</td>
</tr>
<tr>
<td>Enterprise retention rate</td>
<td>97%</td>
</tr>
<tr>
<td>Installations</td>
<td>10k+</td>
</tr>
<tr>
<td>Users</td>
<td>1.5M+</td>
</tr>
<tr>
<td>Delivering services in 180+ countries</td>
<td>180+</td>
</tr>
<tr>
<td>Follow-the-sun operations</td>
<td>24x7</td>
</tr>
</tbody>
</table>

Open Systems helped GEA transition from MPLS to SASE, and they've been a valuable collaborative Partner during our move to the cloud.

Gert-Jan Terpstra, Director Service Owner IT – Network Services
Thank You