SCTE® CABLE-TEC EXPO®
FAST FORWARD 2021

ATLANTA, GA
OCTOBER 11-14

SCTE
a subsidiary of CableLabs®

UNLEASH THE POWER OF LIMITLESS CONNECTIVITY

2021 Fall
Technical Forum
SCTE® • NCTA • CABLELABS®

SCTE
a subsidiary of CableLabs®

Security & Privacy

SD-WAN Security and SASE

Charuhas Ghatge

Product and Solutions Marketing
Nuage Networks by Nokia

Agenda

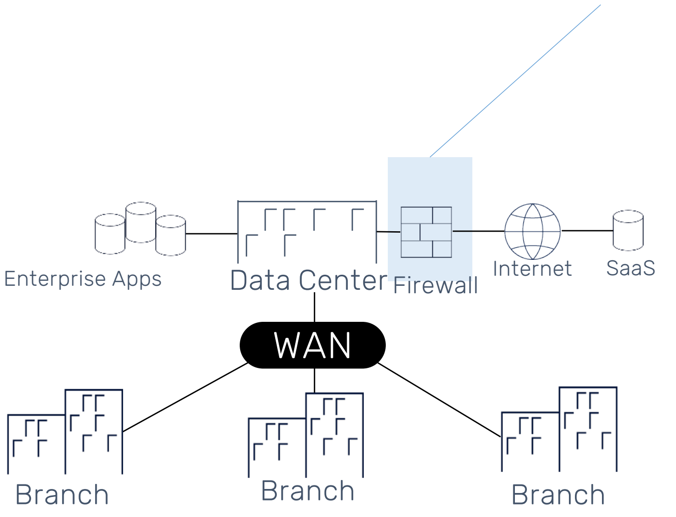
SCTE. CABLE-TEC EXPO. ATLANTA, GA > OCTOBER 11-14

- Security for SD-WANs
  - ❑ Branch Security Requirements
  - ❑ SD-WAN Security Paradigm – Prevent-Detect-Respond
  - ❑ Security Functions – IPS/IDS/Web Filtering, Security Monitoring and automated Response to threats
  - ❑ SD-WAN Security – Customer Verticals and Use Cases

- Secured Access Service Edge (SASE)
  - ❑ What is SASE? Why is it needed?
  - ❑ Components of SASE
  - ❑ Deployment Considerations
  - ❑ A SASE Implementation

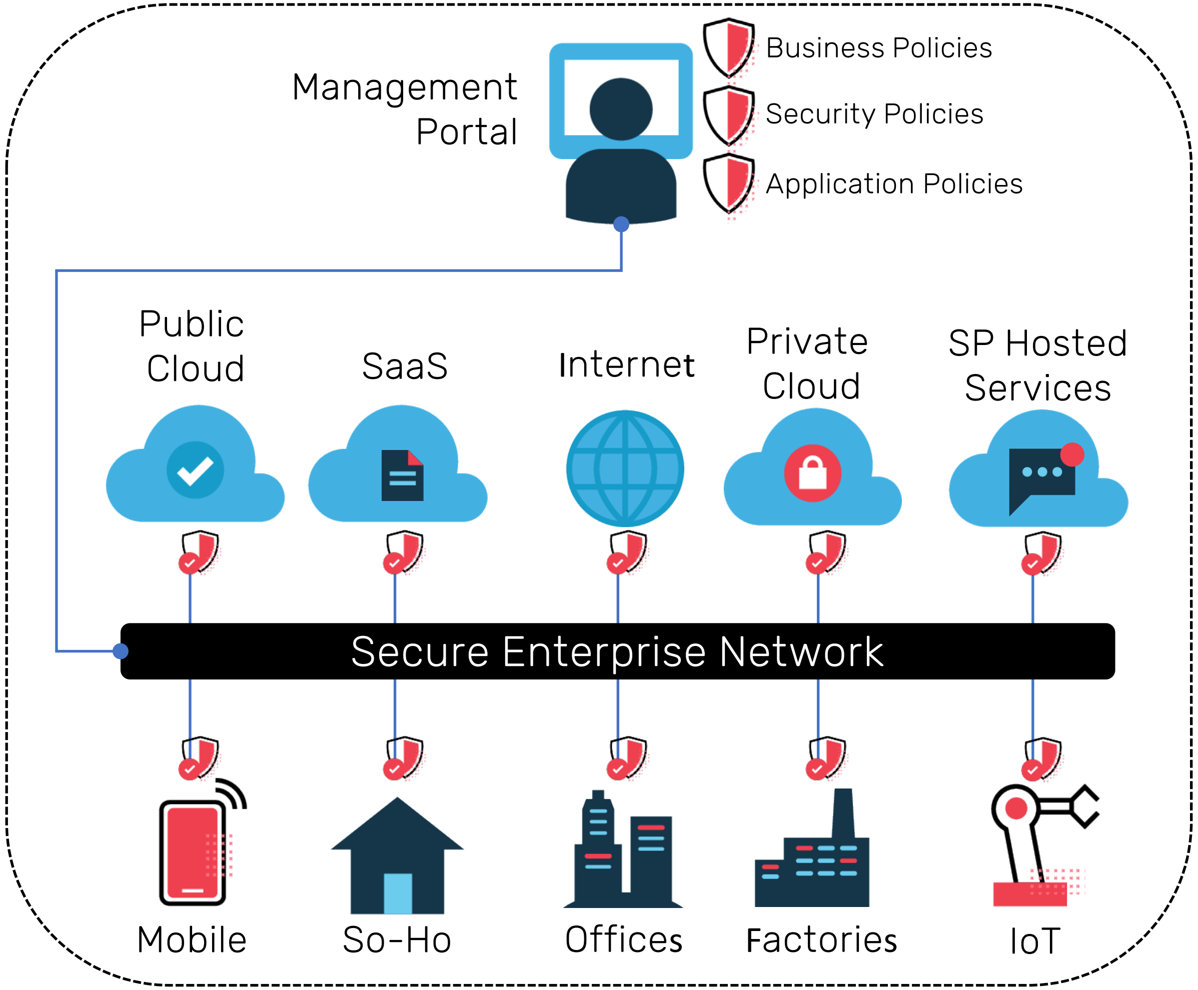
Enterprise Network Evolution

Perimeter Security



- Hub-spoke
- Branch-DC
- Centralized Security

Universal Security Framework



Branch Security Needs to Evolve with Threat Landscape

Requires automated, end-to-end approach based on Analytics

Prevent

Need to secure local internet breakout access from branch (e.g., L3-7 Firewall, URL Filtering, IDS/IPS)

Prevent lateral malware spread from branch to DC

Detect

Need real-time visibility and monitoring for all traffic entering or leaving branch to detect emerging threats

Respond

Need to automate response to mitigate security threats in near real-time

Branch Edge Security Requirements

Advanced Security Features

Stateful Firewall

- Protect branch network access from outside
- Restrict branch user access to corporate network and internet using protocol/ports

L7 Application Control

- Restrict branch user access to select applications (e.g., allow Skype for Business, block Facebook)

URL/Web Filtering

- Limit branch user access to internet content, block malware
- White-list access to cloud services
- Regulatory Compliance

Threat Prevention (IDP, Anti-Virus)

- Detect/block known threats from outside to branch as well as from branch to DC/internet
- Protect branch users from network-based virus/malware (e.g.. via Web, Email, File downloads)

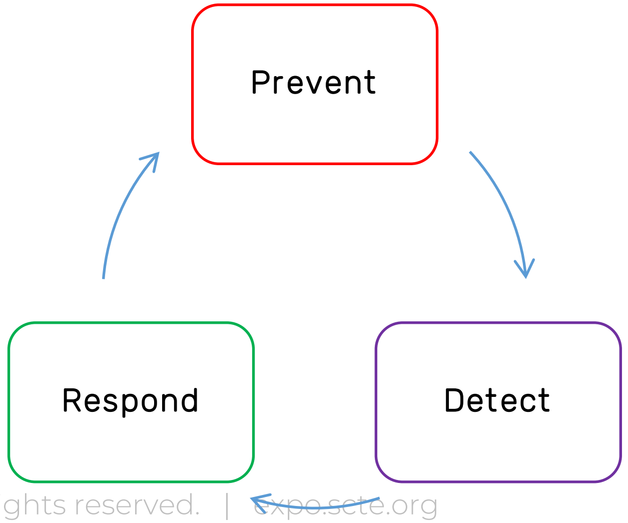
Real-Time Security Analytics and Automation

- Visibility into all traffic from branch to internet and DC/cloud
- Detect new zero day threats
- Automate response based on analytics to limit malware spread

SD-WAN Security

Key Features

- End to End Security Policy
- L3-L7 Application Firewall
- SaaS Application Control
- Web/URL Filtering
- Threat Prevention (IDP)
- Hosted Third-Party VNFs/Cloud Security



- Visibility and Security Monitoring
- Contextual Flow Visualization
- Near Real-time Alerts Based on Network Analytics

- Dynamic Security Automation
- Automated Policies Based on Network Security Analytics
- Dynamic Service Insertion for Threat Mitigation

Key Benefits

- ✓ Secure branch user to local internet breakout access
- ✓ Prevent unauthorized access to malicious web content
- ✓ End-to-End Segmentation and Security Policy for Threat Prevention and to prevent lateral spread of malware
- ✓ Fast Detection and Rapid Response based on Security Analytics

SD-WAN Security – Customer Use cases

Healthcare

Identification of malware activity at branch site (doctor’s office) based on Nuage embedded network traffic analytics

Financial/Banking

Securing guest user access to internet from a bank branch office using L3-7 firewall and embedded URL filtering

Managed Service Provider

Value added security services for SD-WAN using embedded security capabilities or using partner security VNF

Secured Access Service Edge (SASE)

- Why SASE - What Problem is being solved
- Evolution of Enterprise Networking & Security Needs

Why

- SASE Description, Status and Key Requirements
- What is SASE, Where is it on Hype Cycle, No Standards, 5-10 year Journey vs. a defined destination, major requirements (Gartner)

What

- Vendor SASE implantation
  - How they can meet key requirements
  - Incremental Options and Benefits

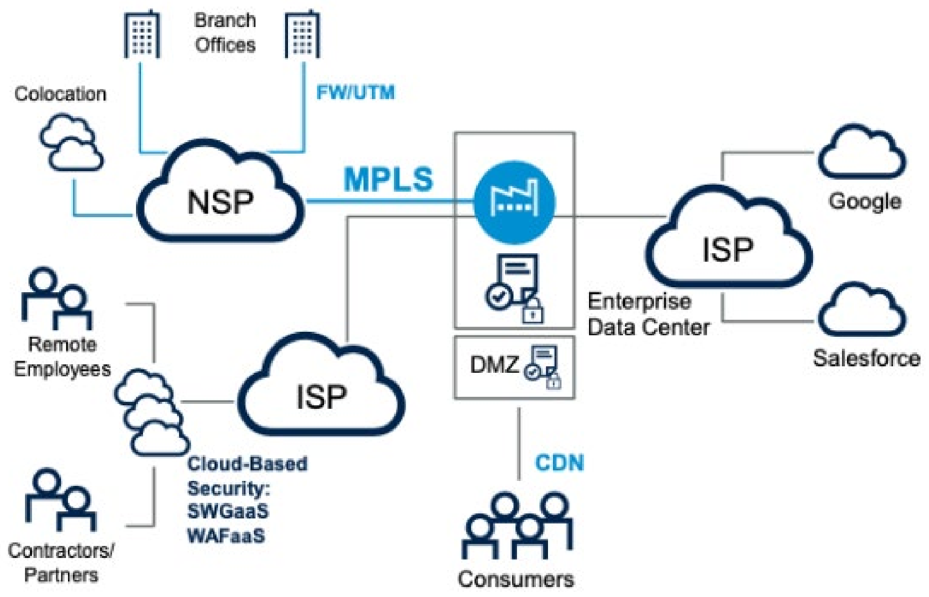
How

- Deployment Considerations
- Consider the state of Industry, SD-WAN technology, Security technology, Enterprise.
- Need for flexibility: Rip and replace vs. evolution – undefined standards, dynamic and evolving threats, vendor lock-in, dynamic needs, flexibility.

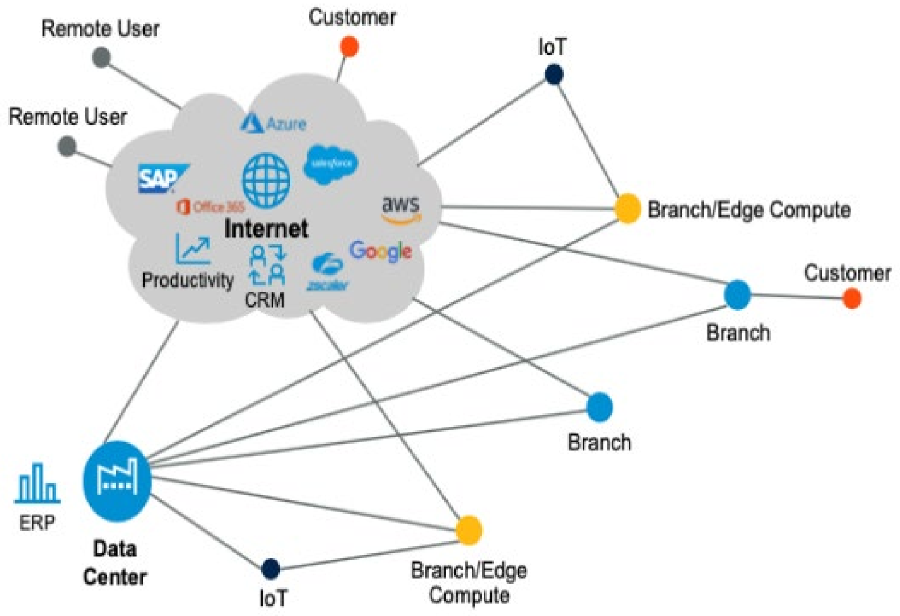
When

New architecture needed for eecurity and connectivity

Connect to Datacenter/HQ



Connect to Clouds (Private, SaaS, Public)



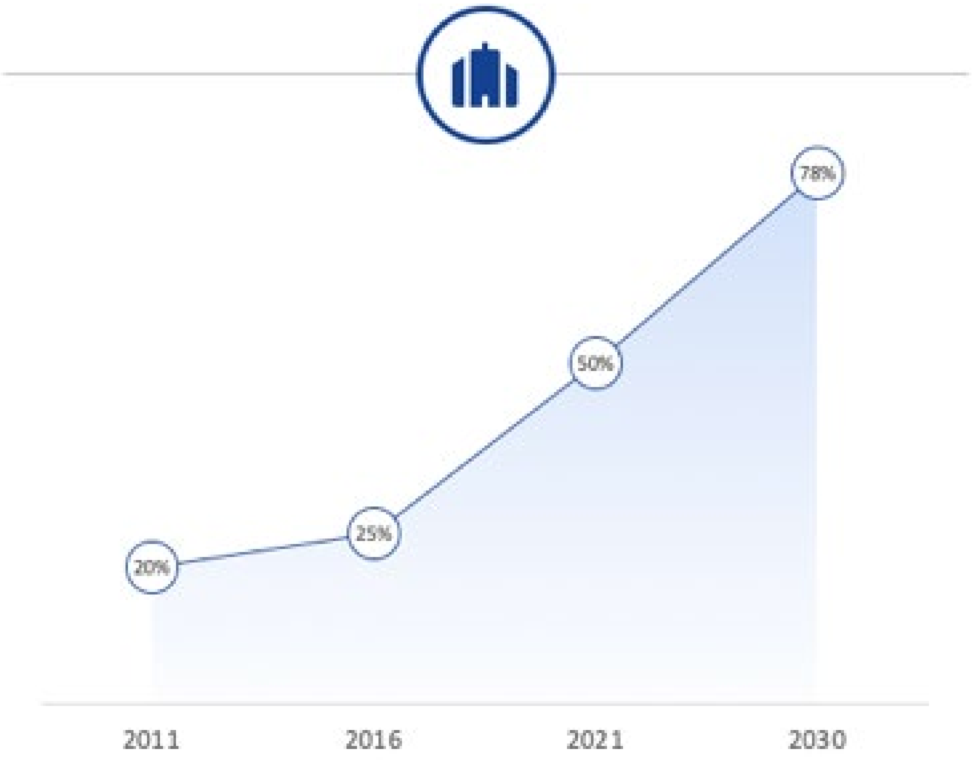
Connectivity from Anywhere

- Traditional Security (VPN) is overwhelmed
- IT Operations are stretched
- Growing Network performance and costs

Source: Gartner

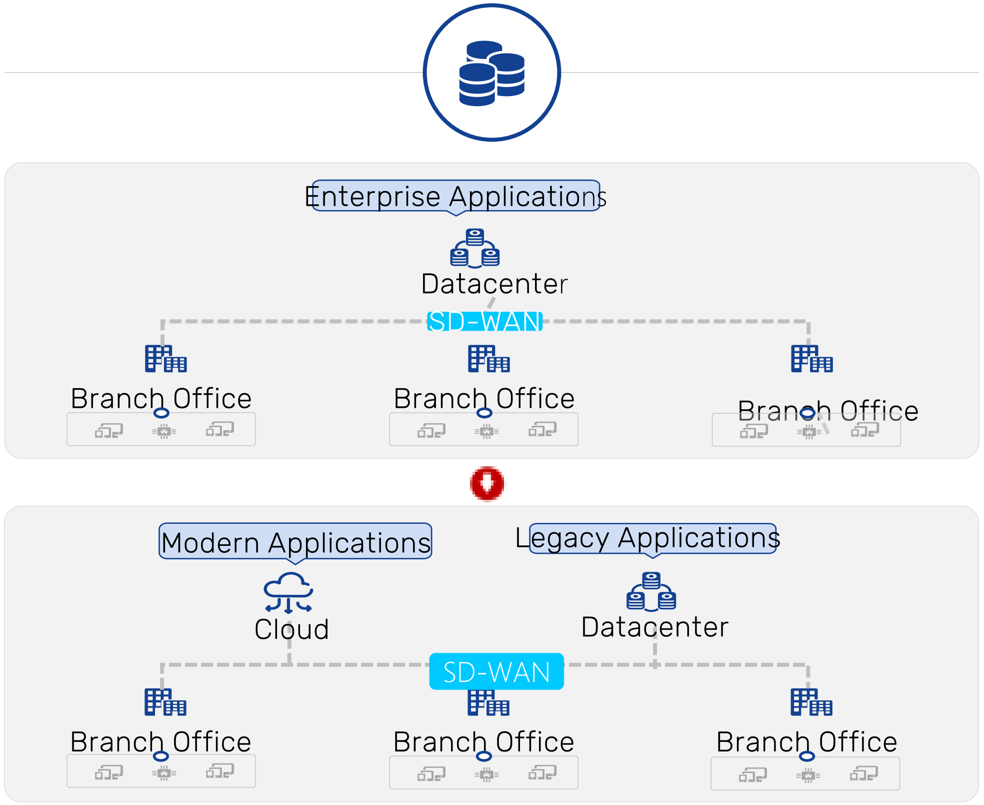
Migration of Enterprise to Cloud requires Cloud-Centric Connectivity & Security

Enterprise Applications Migrate to Cloud

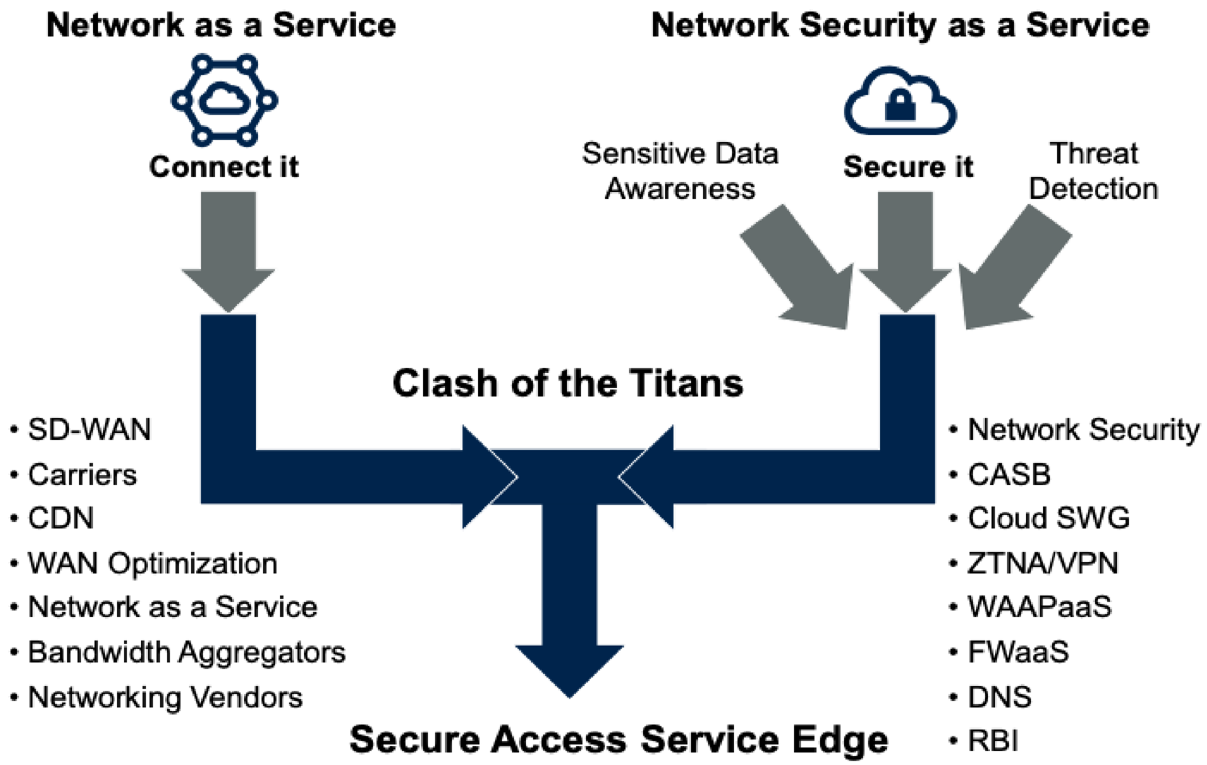


*Source: Gartner

SD-WAN architecture is evolving



SASE Framework and its Use Cases



Network as a Service

Connect it

- SD-WAN
- Carriers
- CDN
- WAN Optimization
- Network as a Service
- Bandwidth Aggregators
- Networking Vendors

Network Security as a Service

Sensitive Data Awareness

Secure it

Threat Detection

- Network Security
- CASB
- Cloud SWG
- ZTNA/VPN
- WAAPaaS
- FWaaS
- DNS
- RBI

Clash of the Titans

Secure Access Service Edge

SASE Use Cases

- Connect user from anywhere
- POP-centric Cloud access with assured SLA
- Secure WAN access with end to end security protection
- Enhanced Application experience
- Enterprise Digital Transformation
- Simplification of Security & Network Operations
- Migration and adoption of Cloud
- Networking for IoT and Industry 4.0

SASE Networking Requirements & vendor Implementation

Networking Requirements	Description	Vendor
Comprehensive Routing capabilities	Full stack of routing protocols to support switching and routing personalities	✓
Access and Connectivity to and from Anywhere	Seamless connectivity and policy management across fixed (internet, L2 and L3) and mobile WANs	✓
Performance based POP selection	Support for multiple paths and PoPs and performance-based selection ability	✓
Application aware routing and traffic steering	Providing optimal application experience based on application types	✓
Hybrid WAN support (e.g. Full MPLS/Ethernet) for legacy Datacenter access	Seamless integration of existing networking to access data center and apps	✓
Multi-Cloud & Hybrid Cloud connectivity	Policy based access to and across applications in private cloud and multiple public clouds	✓
Connectivity Security – VPN, IPSec	Embedded encryption and end point security	✓
WAN Optimization & Bandwidth Aggregation	Optimizing the use of available network for availability and performance	✓
SD-WAN Service Portal	Multi-tenant SD-WAN portal hosted by CSP for the visibility and control. Enabling co-management with enterprise	✓

SASE Security Requirements and vendor Implementation

SASE Requirements	Description	Vendor Implementation guidelines
IPS	Intrusion Prevention system	Preferably Native
IDS	Intrusion Detection System	Preferably Native
Firewall	Stateful Firewall	Preferably Native
Realtime Security Analytics & Automation	With end to end visibility and control for each application, the operator can detect, protect resources at a very granular level, and use automation to respond in real-time to threats.	Native, multi-tenant platform and should be cloud delivered (analytics and management can be hosted by SP)
SWG and DNS Filtering	Secure Web Gateway is used to protect users and devices from online security threats by enforcing internet security and compliance policies and filtering out malicious internet traffic.	Preferably Native
ZTNA	Zero trust network access is a set of technologies that operates on an adaptive trust model, where trust is never implicit, and access is granted on a “need-to-know,” least-privileged basis defined by granular policies. A seamless and secure connectivity to private applications without exposing apps to the internet.	Provided via integration with specialized cloud security vendor
CASB	Cloud Access Security Broker - According to Gartner, a cloud access security broker (CASB) is an on-premises or cloud-based security policy enforcement point that is placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as cloud-based resources are accessed.	Provided via integration with specialized cloud security vendor
DLP	Data Loss Prevention - DLP provides visibility across all sensitive information, everywhere and always, enabling strong protective actions to safeguard data from threats and violations of corporate policies.	Provided via integration with specialized cloud security vendor
FWaaS	Firewall as a Service	Policy Management layer for FWaaS should be multi-tenant and hosted in SP cloud.

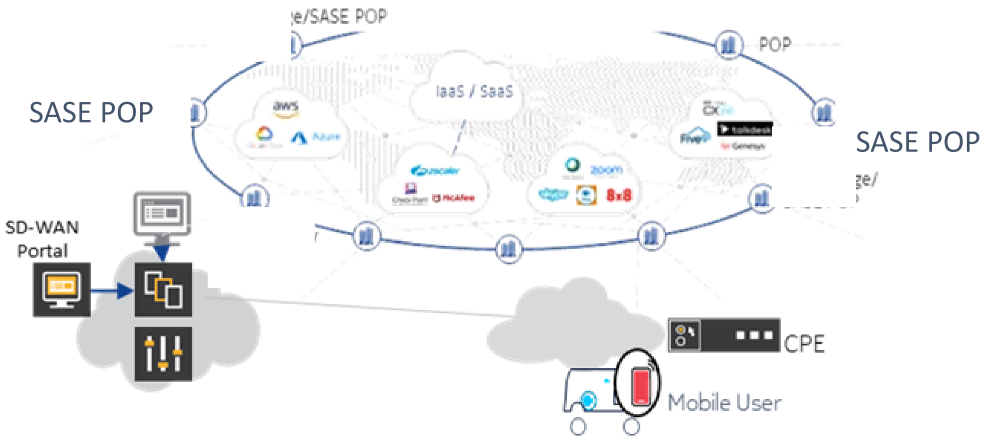
SASE Solution: Options to incrementally evolve towards SASE

1 SD-WAN embedded Security

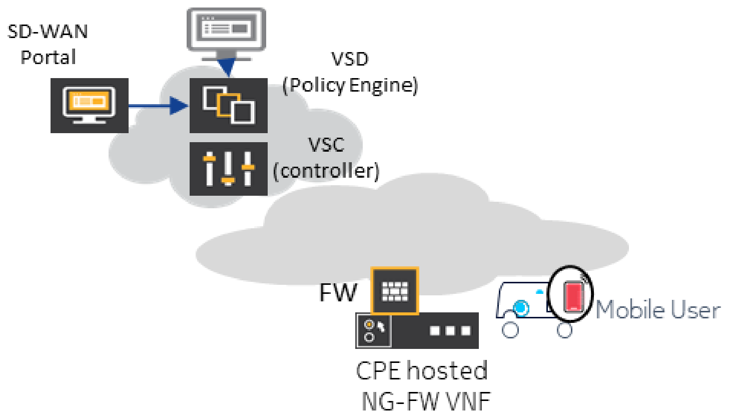
E2E L3-4 stateful micro segmentation	URL / Web filtering	IDS/IPS	Contextual visibility and security monitoring	Automate security policy based on alerts
L7 and SaaS application control	Host or Service chain to third party security functions	Anti-Virus DDOS protect user identity		
Prevent			Detect	Respond

Enabled by VSS Analytics

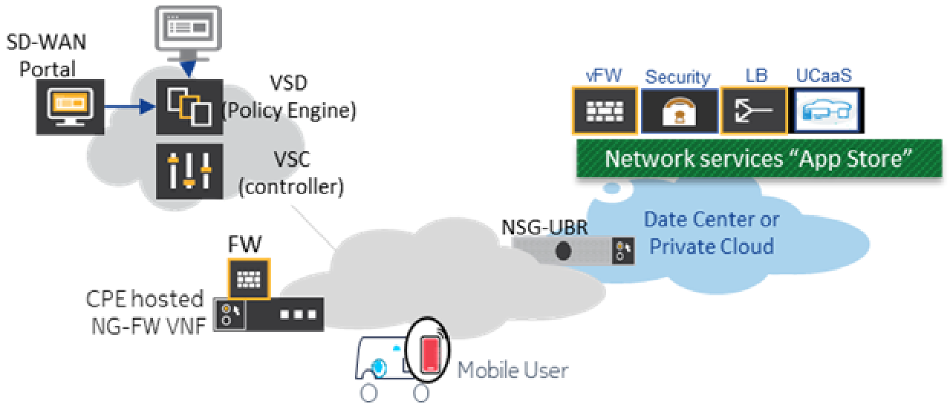
4 SASE Platform



2 Augment with hosted 3rd party Firewall VNF on CPE



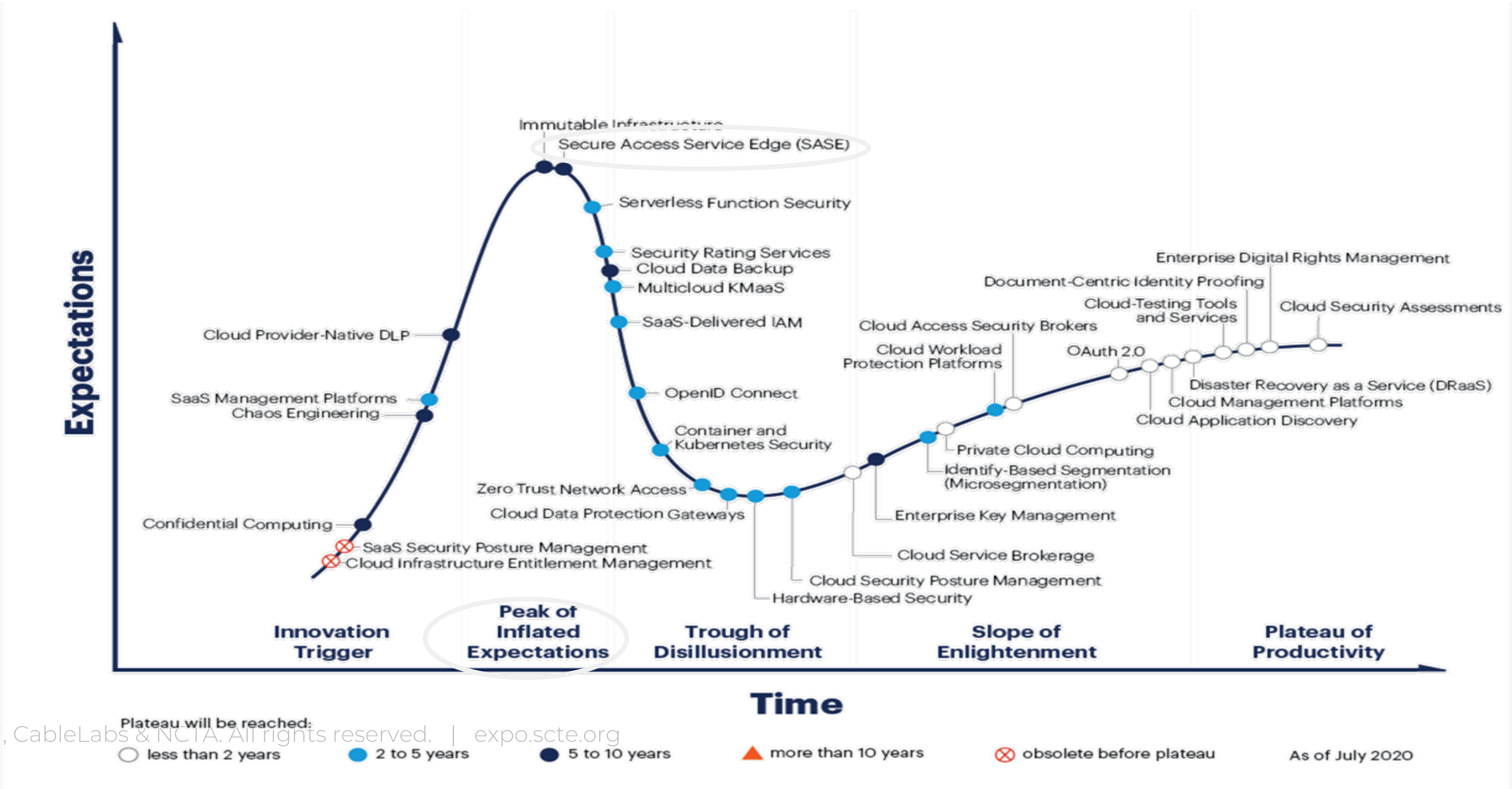
3 MSP's Cloud Security (SASE) through Service-Chain



Considerations and Conclusions

Caveats on SASE @Peak of Inflated Expectation on Hype Cycle

SASE is at the Peak of Inflated Expectation on Gartner’s hype cycle



SASE Deployment Considerations

Flexibility becomes critical in an evolving and dynamic space

- SD-WAN and Cloud Security solutions are widely deployed
- A rip-n-replace SASE deployment is not practical. Pragmatic solution requires utilizing investments
- A complete SASE solution from a single vendor would:
  - compromise completeness
  - reduce flexibility in a very dynamic space of enterprise security
  - risk the vendor lock-in
  - SD-WAN enjoys MEF standard, cloud security is evolving

- A good SASE solution should provide flexibility:
  - A highly scalable and feature-rich SD-WAN supporting connectivity from anywhere - SD-WAN is the foundation of SASE
  - Exhaustive native security functions within SD-WAN
  - Integration with cloud security platforms for advanced and evolving security functions
- This flexibility enables MSP to:
  - Create best-fit SASE solution for enterprise clients
  - Differentiate against single vendor cookie cutter solution

SCTE® CABLE-TEC EXPO® FAST FORWARD 2021

ATLANTA, GA
OCTOBER 11-14

SCTE®
a subsidiary of CableLabs®

Thank You!

Charuhas Ghatge

Product and Solutions Marketing
Nuage Networks by Nokia
Charuhas.Ghatge@nokia.com