

# SASE的发展与未来

演讲嘉宾：金湘宇 NUKE

嘉宾职务：赛博谛听创始人



# 当前网络安全行业发展遇到的瓶颈，软硬件堆砌模式不可维系

- 当前的企业网络安全解决方案以本地化部署产品为主，随新概念、新产品推出，不断在出口进行堆砌
- 伴随企业发展，企业边界出口链路不断进行扩充，带宽不停增加，本地化产品为主的部署方式不能实现弹性部署



出口带宽1G



出口带宽10G



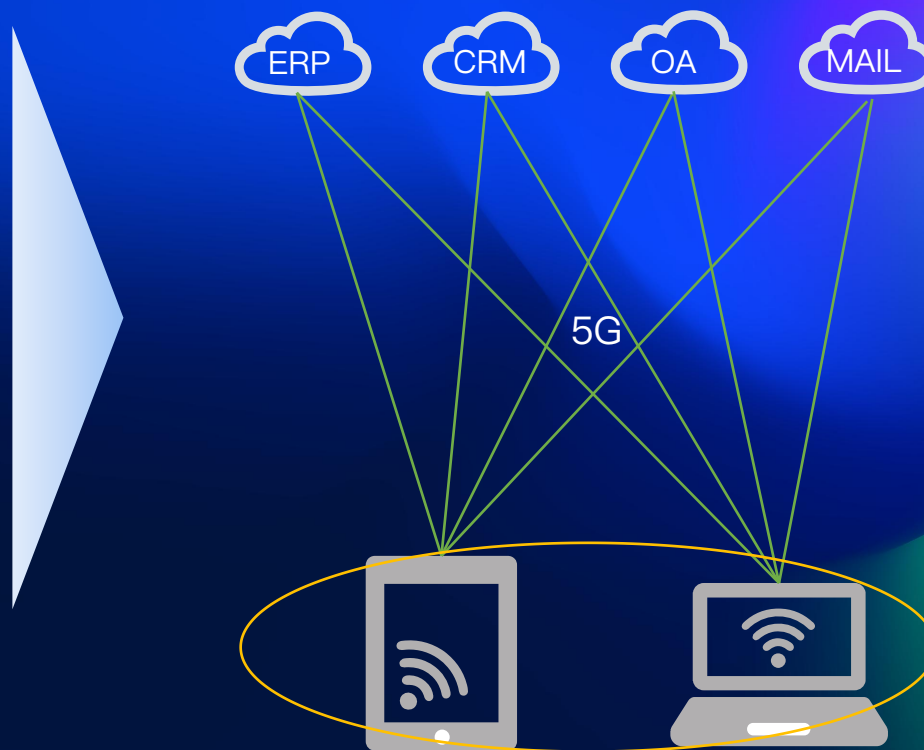
\*投资示意，非真实部署

# 网络基础设施架构也在迅速改变，解决方案继续升级

- 5G、SDWAN、云计算、边缘计算、物联网等新技术正迅速改变网络基础架构，终端设备逐渐取代网络设备成为企业网络的新边界和新中心，网络及网络安全的能力交付逐渐将迁移至云端
- 随企业接入网改变，企业侧的计算和存储架构也将随之改变，包括终端在内的计算和存储将逐渐迁移至云端



网络设备和安全设备是网络的边界，也是网络的中心

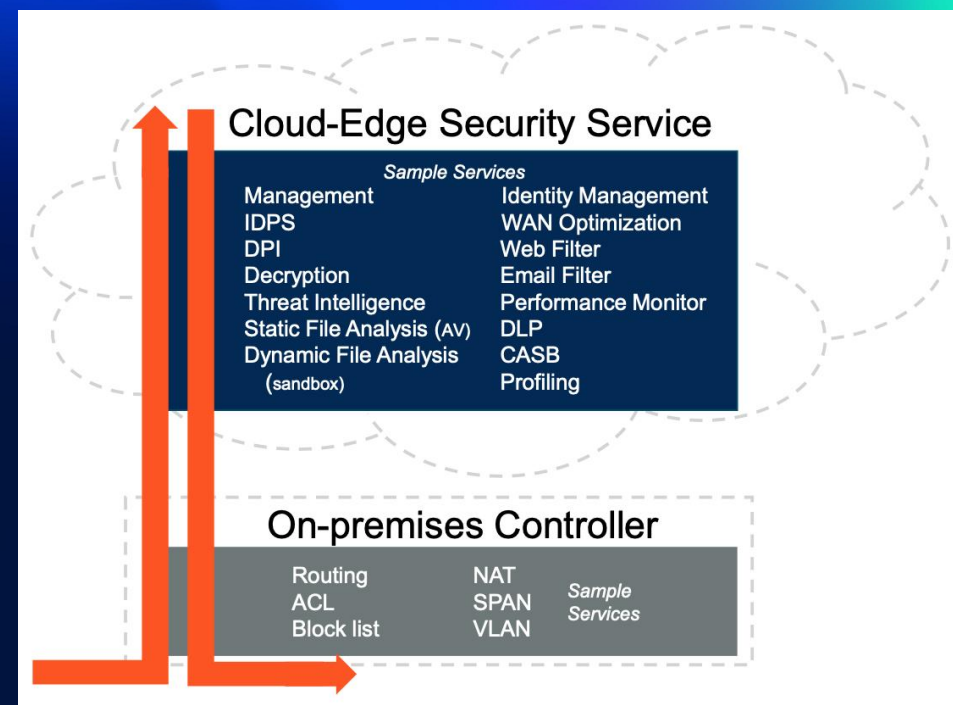
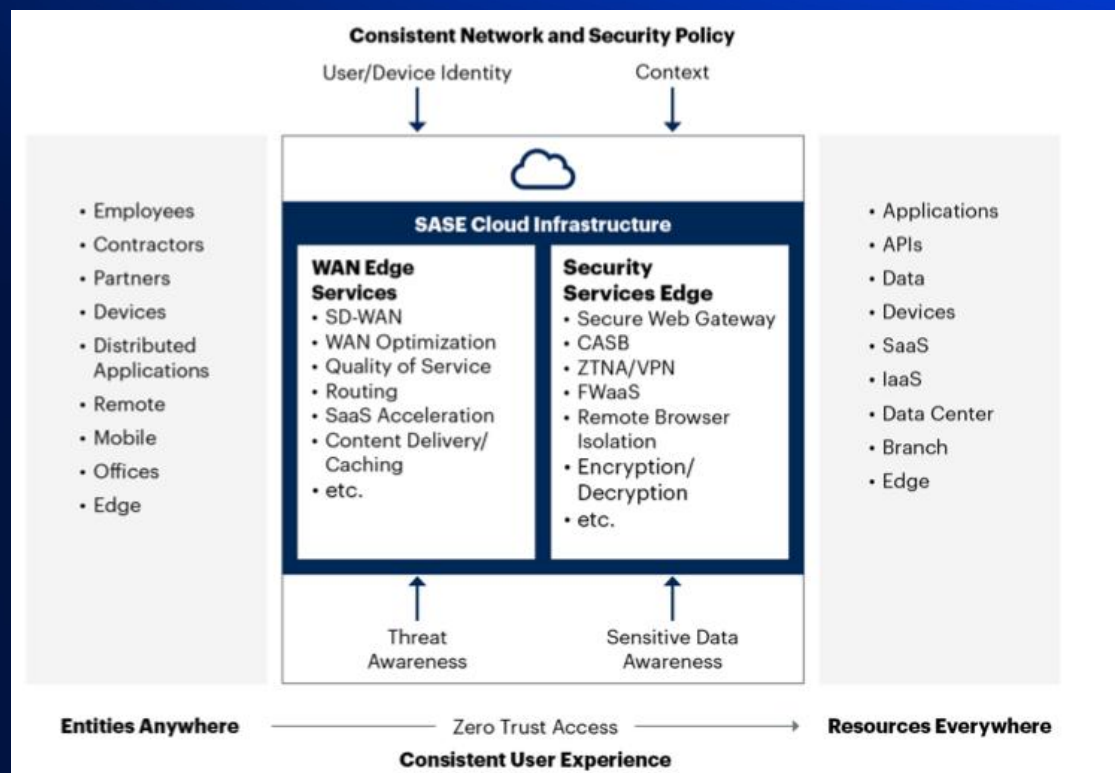


终端设备成为网络的新边界和新中心



# 安全服务访问边缘SASE成为当前企业网络安全最热门概念

- Gartner预测，到2024年，30%的企业将采用同一供应商提供的云交付的SWG、CASB、ZTNA和分支机构防火墙即服务（FWaaS）功能，而2020年这一比例还不到5%。
- 到2025年，至少60%的企业将有明确的战略和时间表来采用SASE，包括用户、分支机构和边缘访问，而2020年只有10%。
- 到2023年，为了提供灵活、经济高效的可扩展带宽，30%的企业地点将只有internet WAN连接，而2020年这一比例约为15%。



# SASE和零信任的差异

## Zero Trust Architecture

- ✓ Does not include Network Functions
- ✓ Requires Identity, Credential and Access Management (ICAM) system and Asset Management systems for continuous monitoring and evaluation
- ✓ Continuous Diagnosis and Mitigation (CDM) of all assets
  - Security Lifecycle Management
  - Manage Assets
  - Manage accounts for people and services
  - Manage Events
- ✓ Logical components: CDM System, Industry Compliance, Threat Intelligence, Activity Logs, Policy Engine, Policy Administrator, Policy Decision Point, Policy Enforcement Point, Data Access Policy, PKI, ID Management System, SIEM System

## Secure Access Service Edge

- ✓ Includes Network Functions
- ✓ Does not mandate Asset Management, however, requires authentication and authorization
- ✓ Does not specify CDM, but does refer to device posture checks and UEBA
- ✓ Logical components: Router, VPN, NGFW, CDN, SDP, DLP, ZTNA, SWG, RBI, SDWAN, Sandbox, CASB, WAN-OP, WAF, DNS

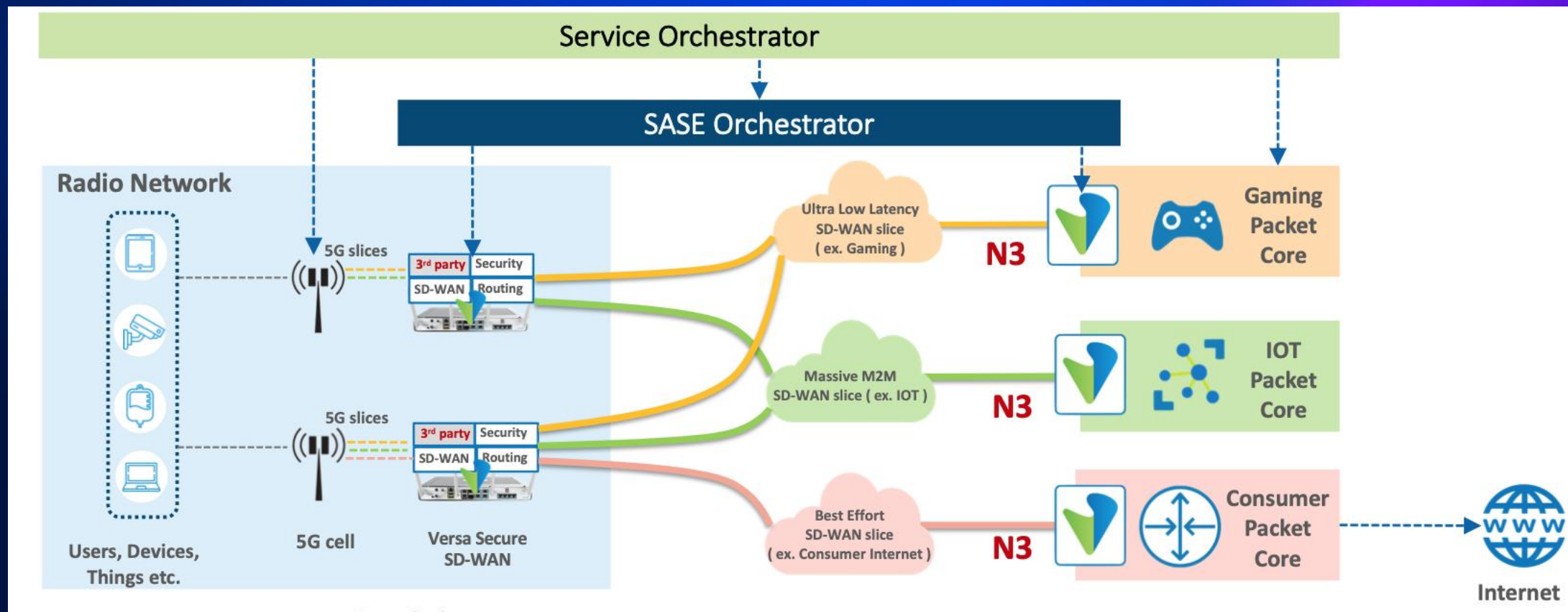
# SASE的典型能力清单

REST API									
Orchestration / Provisioning			Control Plane (BGP RR)			Analytics / Visibility			
Templates	NETCONF	SNMP	SSH	IPFIX	NETFLOW	KAFKA	ZTP	URL-ZTP	Cloud Integration
SSL, TLS Proxy	Anti-Virus	NG-IPS	File Filtering	Anti-Malware	Network DLP	RAC-RAS	Cloud-based Sandboxing	Cloud-based File Filtering	Cloud-based URL Lookups
NGFW	IP Reput. & Filtering	URL Feeds & Filtering	Captive Portal	Single Sign-On	SAML, RADIUS	User, Group Policy/Traffic	DNS Proxy	DNS Reput. & Filtering	Device Type Policy
Cloning & Striping	Voice, Video CODECs	MOS Based TE	DNS Assist Traffic Eng	SaaS DCA & DIA Traffic Opt	URL Based Traffic Mgmt	Forward Proxy	TLB for WAN ADC	TCP Optimization	Reverse Proxy
Y1731 Path Performance	Multiple Active Links	Any / All Topologies	Dynamic IPsec Overlay	App Traffic Engineering	App Policy Forwarding	Application Traffic Ctrl	App QoS, Traffic Shaper	DPI/Application ID	Pair-wise Keys
uCPE	Service Chaining	3rd Party VNFs	IP Geo Location	Flow Mirroring	DOS Protection	CGNAT	Stateful FW / ALG	IKE IPsec Transport	Dev ID & Logging
BGPv4	Route Reflector	MP-BGP MPLS/L3VPN	IGMP v2/3	PIM SM	PIM SSM	Route Policies	MP-BGP EVPN	NG-MVPN	802.1x
Shaping, Marking	QoS, HQoS	IPAM (DHCP)	VRRP	RIPv2 OSPFv2/v3	VRF	IPv6	BFD	IRB	FEC
LAG	VLAN, QinQ	PPPoE	Flow or Packet LB	xSTP	VS, Bridge Domain	VXLAN EVPN	PPP, MLPPP	F. Relay MLFR/HDLC	Fabric Traffic Management
100M/1/2.5/5/10GE	Native LTE, LTE Adv.	WiFi Client, AP	Native 5G	GPON	G.Fast	A/VDSL	T1/E1	100 GE	DOCSIS
Multi-tenant Everything – RBAC per tenant – 5 levels of hierarchy									
Flexible HA Deployments – Private & Public Clouds, Cloud CPE, uCPE, White/Grey Box CPE									

■ Routing
 ■ SD-WAN
 ■ Security



# SASE的未来-与下一代通信结合实现内网全边缘服务化



# THANKS