

云网安融合 新趋势

01081

王安宇

云安全联盟大中华区 首席技术官 (CTO)



目 录 CONTENTS

- 01 办公安全进化论
- 02 SASE的核心价值
- 03 SASE在全球的落地实践
- 04 未来展望



科技的进步重塑人们的工作与生活

践AI·重构数智生产力
2025 数字 创新 大会

农业革命 Agriculture Revolution



工业革命 Industrial Revolution



信息革命 Information Revolution



智能革命 Intelligent Revolution

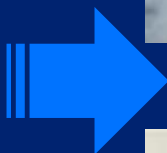


工作模式不断变化

践AI·重构数智生产力
2025 数字创新大会



大型办公室、集中办公



远程会议



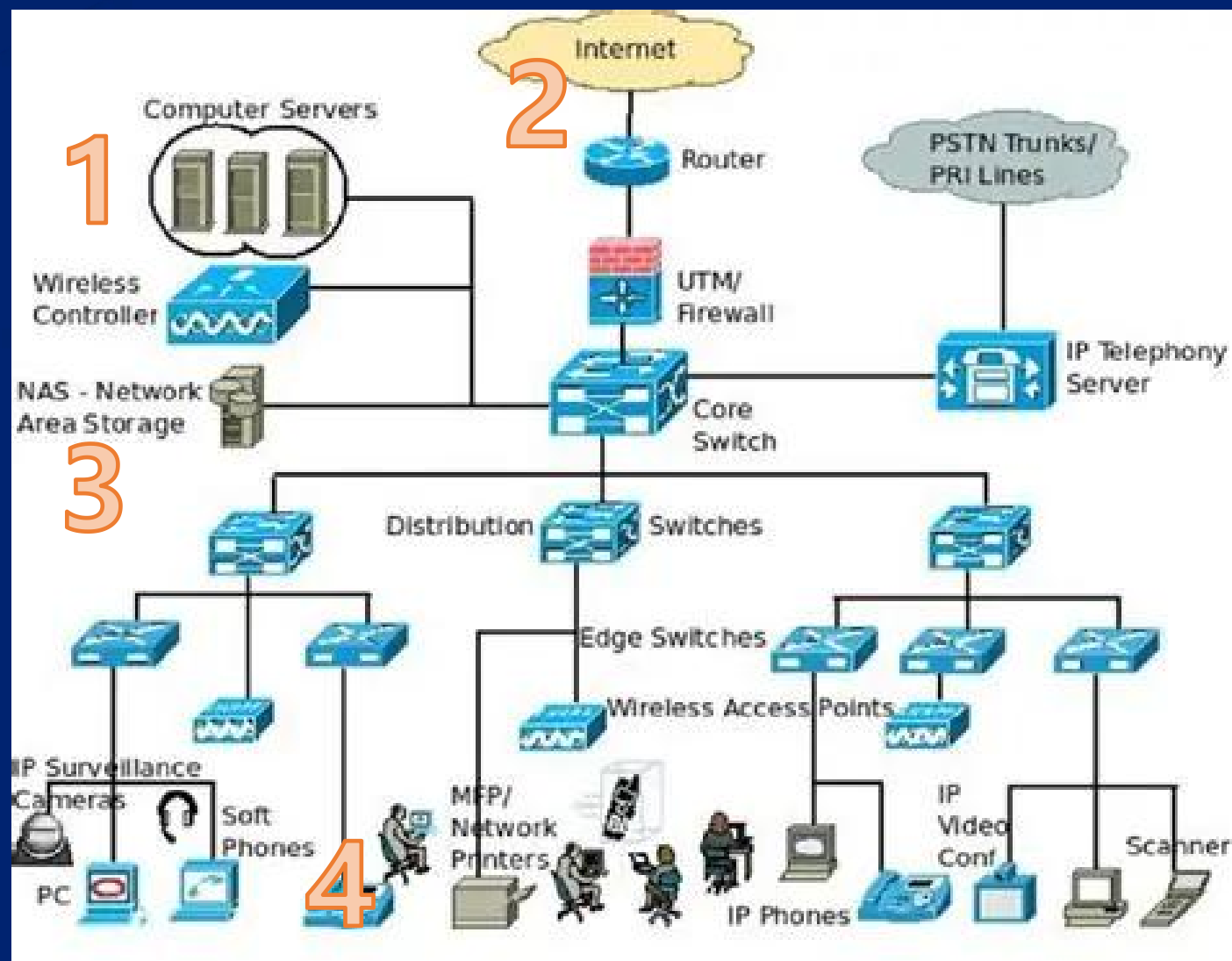
移动办公



居家办公



小型办公室



云化趋势

组织不再需要构建或管理本地的IT资源。

网络趋势

网络类型复杂，边界逐渐模糊。

数化趋势

数据不再仅保存在数据库，其形态和外延发生变化。

用户趋势

远程办公、移动办公、合作伙伴访问越来越多。

传统的城堡与护城河安全模型逐渐失效

践AI·重构数智生产力
2025 数字创新大会

“城堡与护城河”是一种网络安全模型，其中**网络外**的任何人都无法访问内部数据，但网络内的每个人都可以。

将组织的网络想象成城堡，将网络边界想象成护城河。一旦吊桥降下，且有人穿过，他们就可以在城堡场地内自由活动。同样，一旦用户连接到此模型中的网络，他们就能够访问该网络中的所有应用程序和数据。

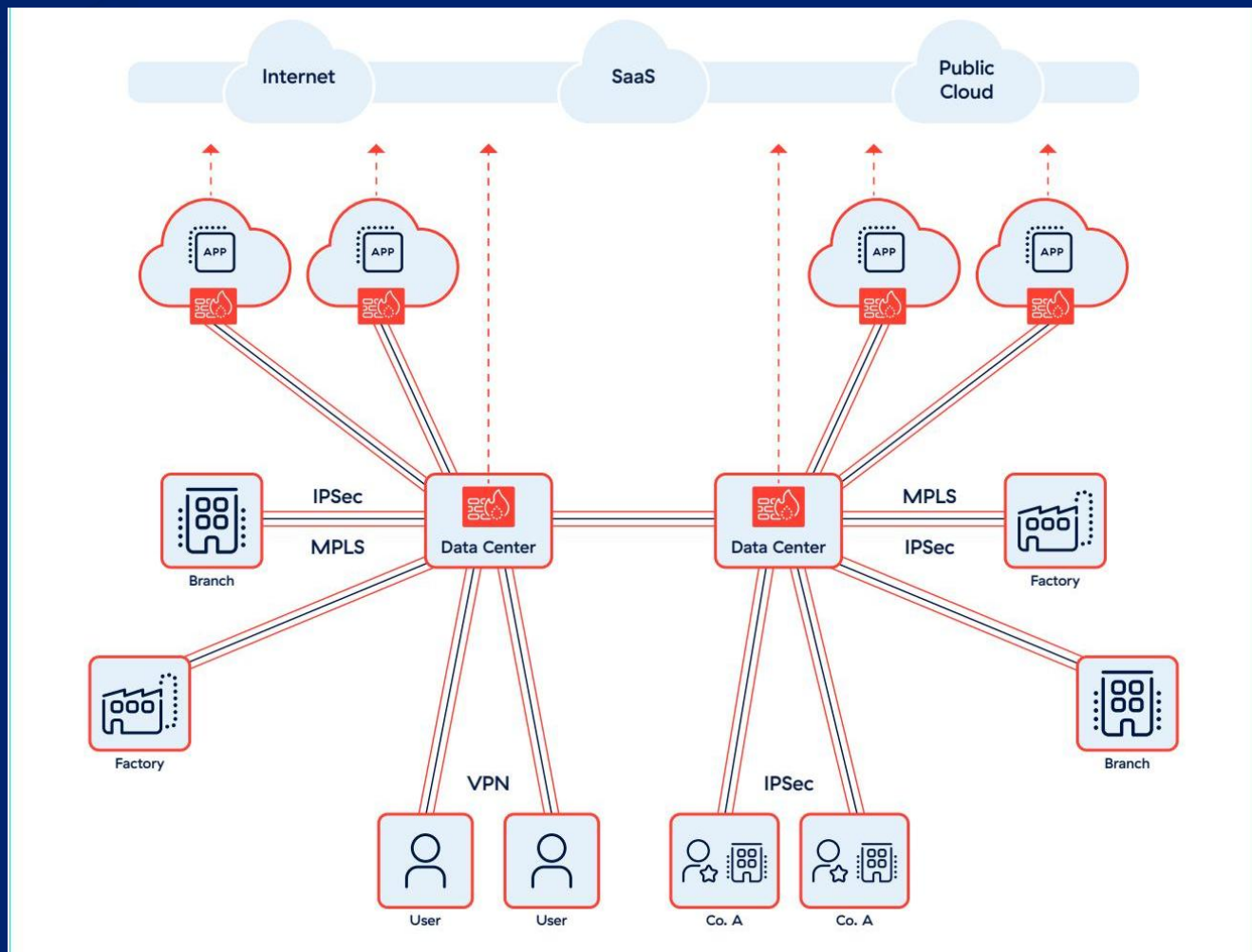
使用这种模式的组织会投入大量资源来保卫他们的**网络边界**，就像一座城堡可能会在吊桥附近放置最多的警卫一样。

组织会部署防火墙、入侵检测系统 (IDS)、入侵防御系统 (IPS) 和其他可阻止大多数外部攻击的安全产品——但在阻止**内部攻击**、**内部威胁**和**数据泄露**方面并不那么有效。



基于防火墙和VPN的网络架构存在局限

践AI·重构数智生产力
2025 数字创新大会



攻击面扩大

网络扩展到更多地点、用户、设备、云端。VPN、防火墙具备公网地址。

安全风险高

底层设备（硬件和虚拟化）缺乏大规模检查加密流量的扩展性，而86%的威胁来自于加密流量。

横向移动

接入网络即可访问相关资源。存在数据丢失和泄露的风险。

成本和复杂性高

网络复杂，安全产品多，昂贵且难以采购、配置和维护。

影响用户生产力

需要将大量数据传输到中心数据中心，这会导致延迟，从而影响数字体验。

防火墙漏洞频出，影响网络安全性

践AI·重构数智生产力
2025 数字创新大会



CVE-2024-3400:

在 Palo Alto Networks 的 PAN-OS 中发现了一个零日命令注入漏洞。它被评为最高严重性分数 10.0，未认证用户可利用该漏洞在目标系统上以 root 权限执行任意命令。



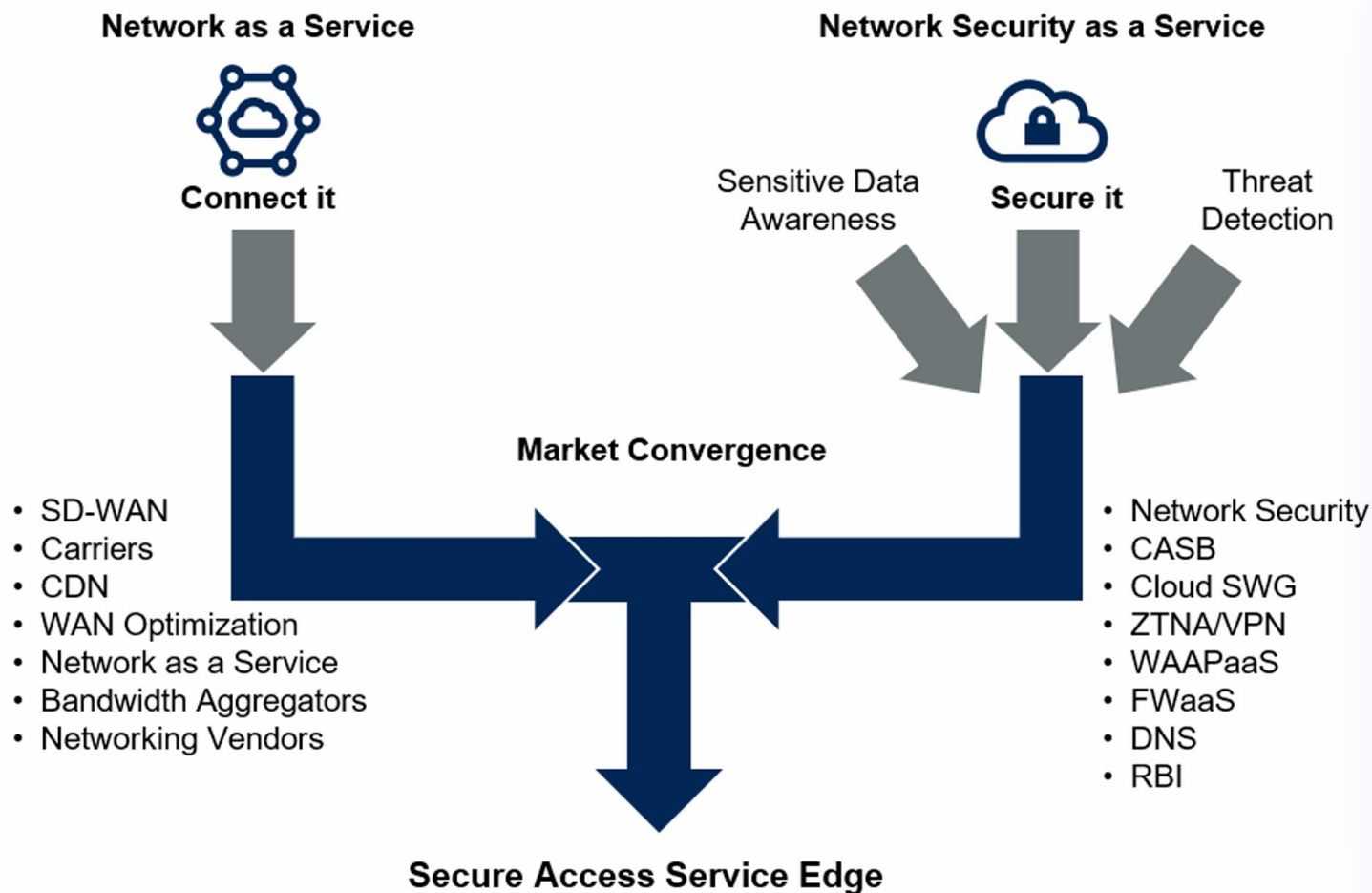
CVE-2025-20333、CVE-2025-20362和 CVE-2025-20363 :

2025年9月25日，思科修复影响思科安全防火墙自适应安全设备（ASA）和思科安全防火墙威胁防御（FTD）软件的VPN Web服务器的三处安全漏洞，这些漏洞已在实际环境中被利用。

SASE: Network (Security) as a Service

践AI·重构数智生产力
2025 数字创新大会

SASE Convergence



CDN: content delivery network; RBI: remote browser isolation; WAAPaaS: web application and API protection as a service.

演进趋势

- 企业**数据中心**不再是网络安全架构的中心。
- 数字化业务和边缘计算已颠覆了传统访问需求，越来越多的用户、设备、应用、服务和数据都位于**企业外部**而非内部。
- 复杂性、延迟以及对解密和检查加密流量的需求，将推动网络和安全即服务能力整合到云交付的**安全访问服务边缘**（SASE）的需求增加。
- 应用SASE策略需要检查和理解**数据上下文**。
- 为了让用户能够随时随地获得**低延迟**的访问，企业需要具备全球广泛的接入点（POP）和互连的SASE解决方案。

Gartner: SASE度过炒作，稳步攀升，将产生实在的商业价值

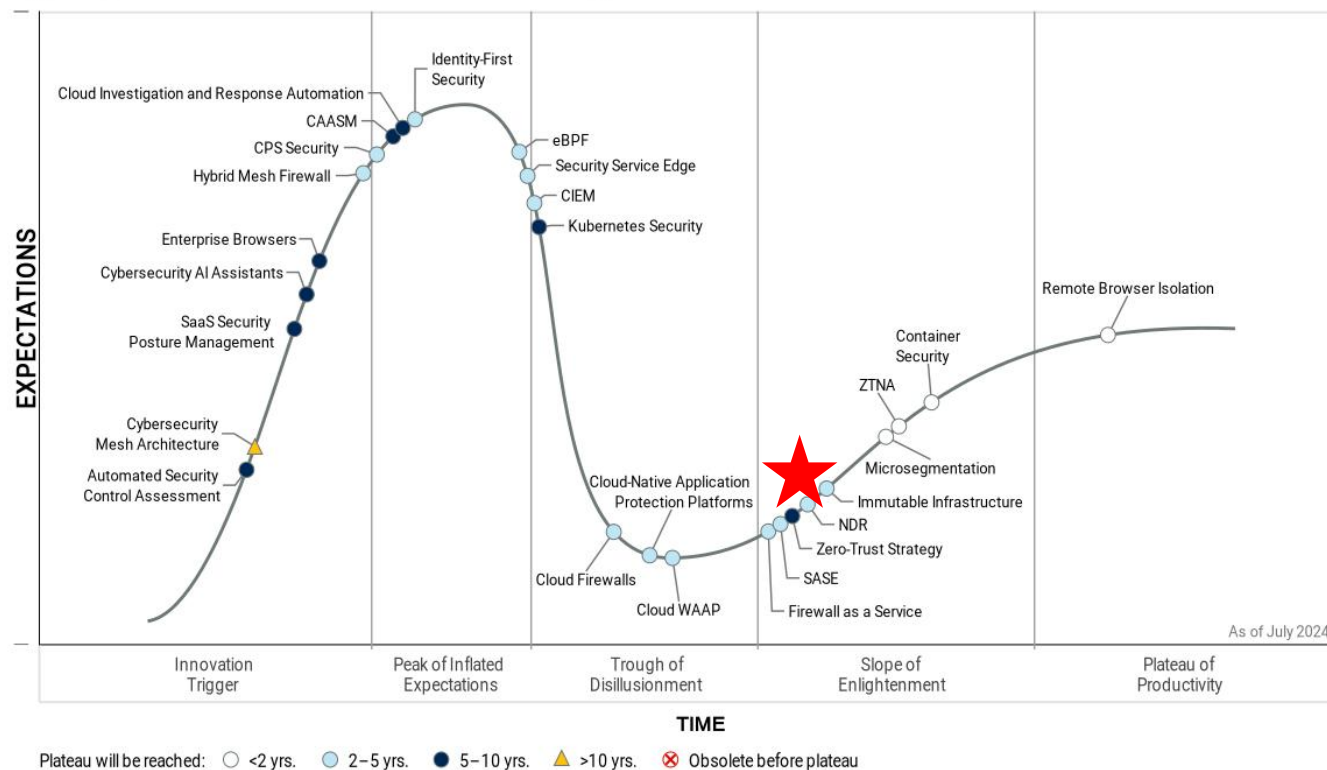
践行AI·重构数智生产力
2025 数字创新大会

2020

2024



Hype Cycle for Workload and Network Security, 2024

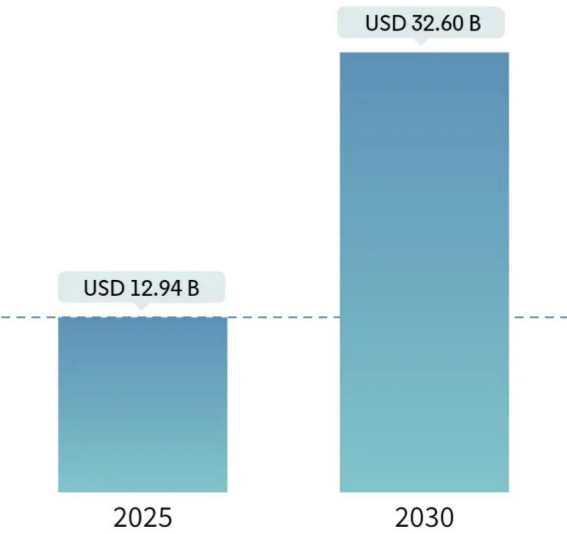


SASE获得市场认可。全球 SASE 市场蓬勃发展。

Mordor Intelligence 研报

Secure Access Service Edge (SASE) Market

Market Size in USD Billion
CAGR 20.29%



Source : Mordor Intelligence

Market Overview

Study Period	2019 - 2030
Market Size (2025)	USD 12.94 Billion
Market Size (2030)	USD 32.60 Billion
Growth Rate (2025 - 2030)	20.29% CAGR
Fastest Growing Market	Asia Pacific
Largest Market	North America
Market Concentration	Medium

Major Players



*Disclaimer: Major Players sorted in no particular order

概述

- 全球安全访问服务边缘 (SASE)市场预计将从 2024 年的34 亿美元增长到 2034 年的303 亿美元。
- 预计 2025 年至 2034 年预测期内复合年增长率将达到 24.3% 。
- 根据产品供应情况，安全即服务 (SECaaS)在 2024 年占据市场主导地位，占有57% 的份额。
- 从组织规模来看，大型企业占据明显领先地位，占据62%的市场份额。
- 在垂直领域方面，IT 和电信行业占比最高，为25%，凸显了其对安全、可扩展的访问解决方案的迫切需求。

目 录 CONTENTS

- 01 办公安全进化论
- 02 **SASE的核心价值**
- 03 SASE在全球的落地实践
- 04 未来展望



云网安融合：优势和价值

践AI·重构数智生产力
2025 数字创新大会

雇员 & 合作伙伴



3A 体验

Anywhere, Anytime, Any Device

安全团队



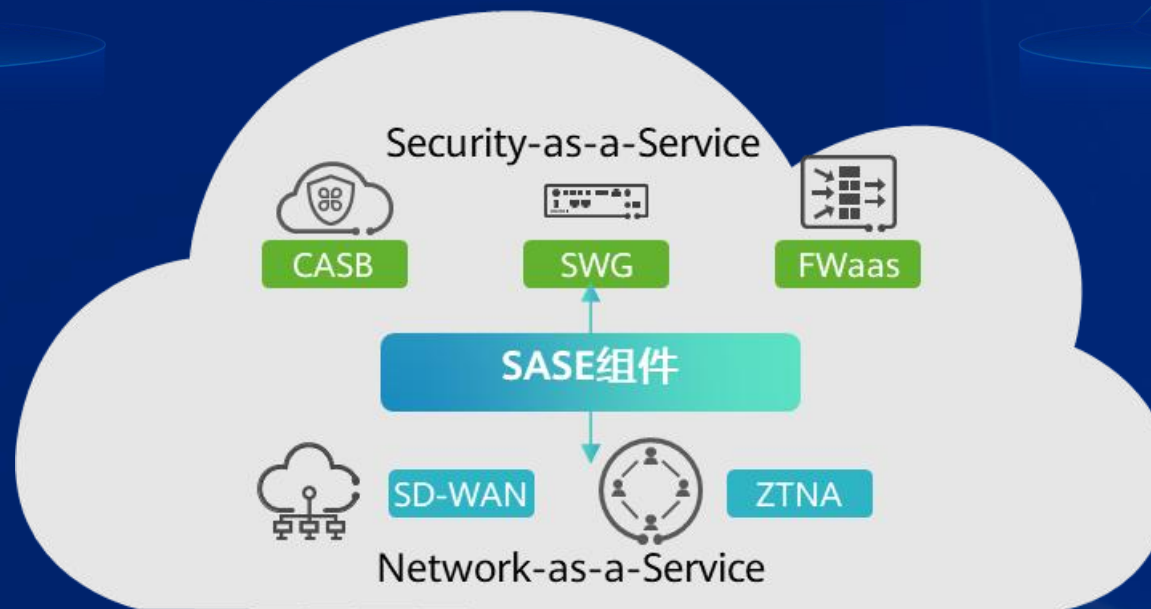
效率 & 质量

统一策略、简化运维、全局可见、快速响应

企业



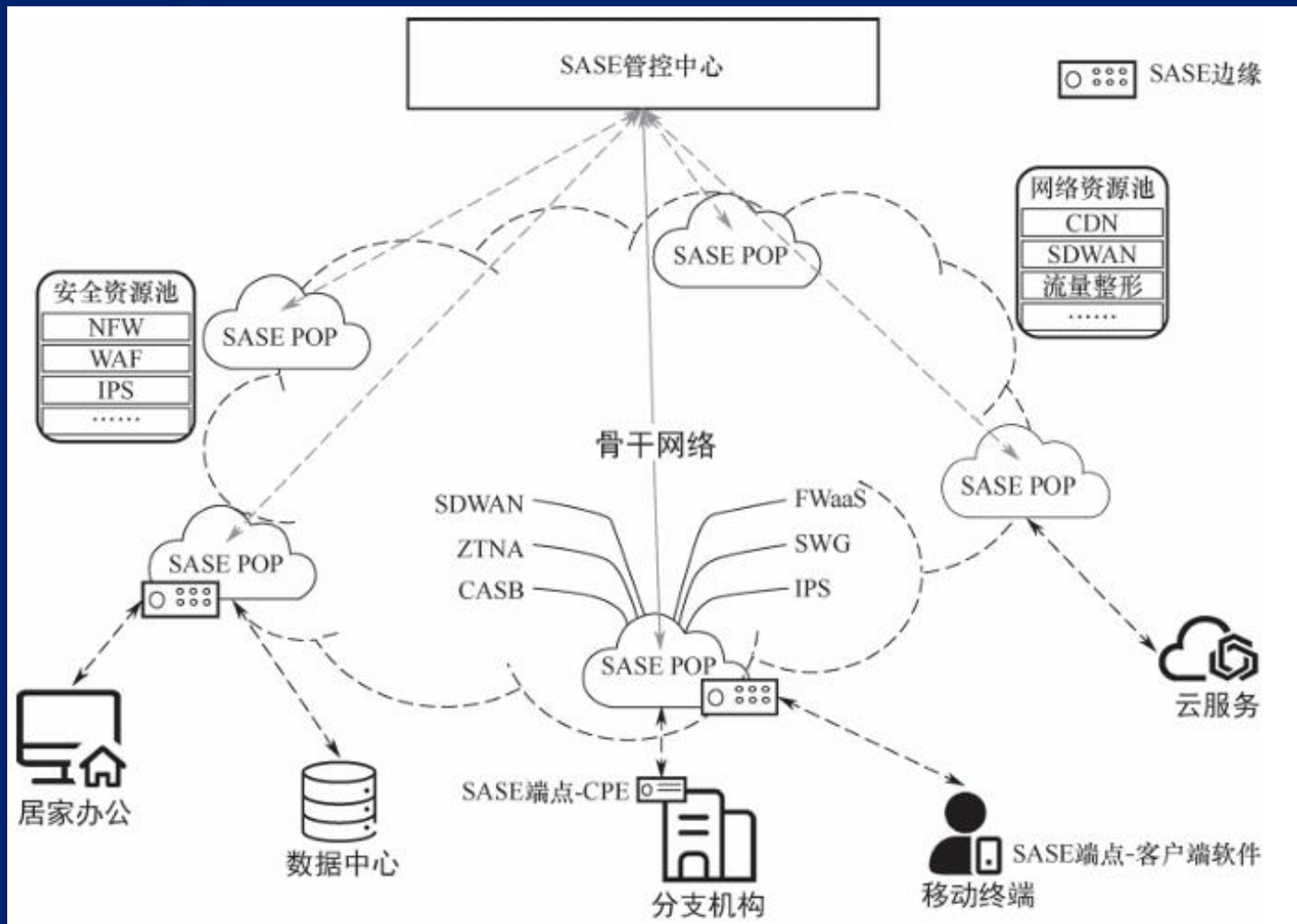
降低总体拥有成本。
提升业务敏捷性和韧性。



SASE关键组件

践AI·重构数智生产力

2025 数字创新大会



管控中心

提供网络和安全的管理服务。集中管理策略、用户和设备。负责功能编排。

PoP

提供用户可以订阅的网络和安全功能。负责网络优化、安全检查。

边缘网关

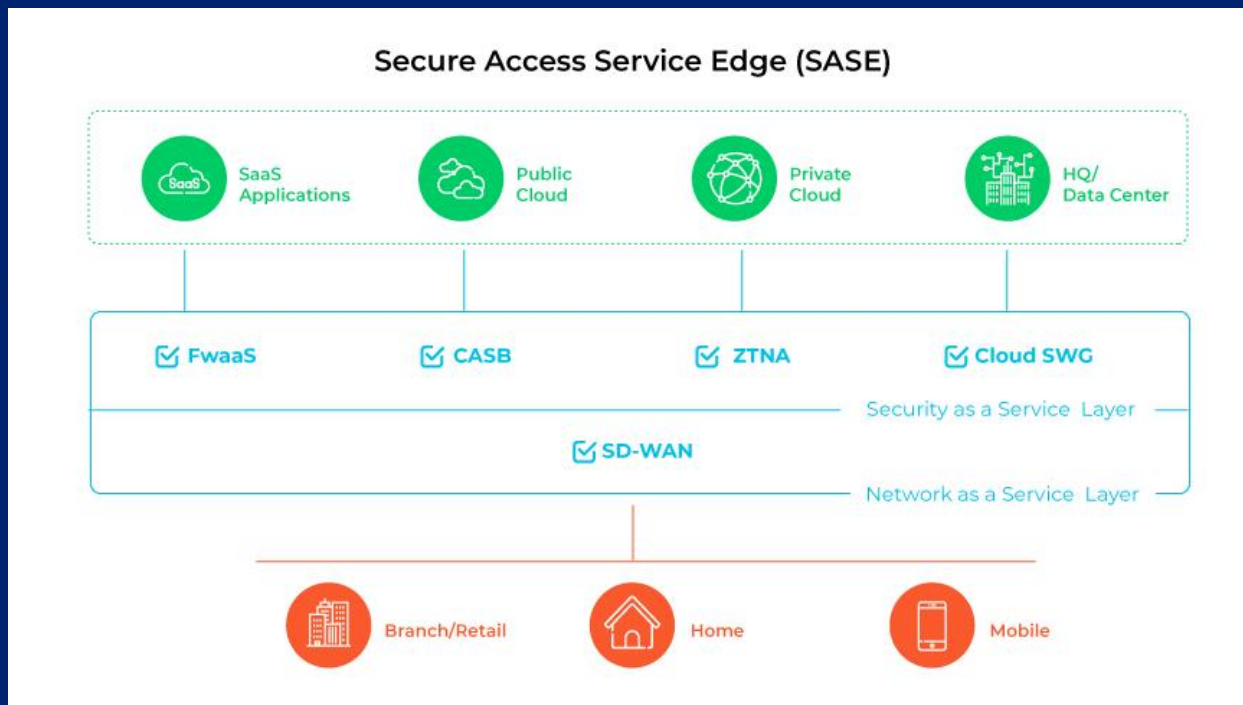
靠近用户，提供网络接入。根据用户订阅，加载相应的网络和安全的功能。

端点

软件客户端或用户侧网关。负责到边缘网关的网络接入。

SSE：安全能力核心

践AI·重构数智生产力
2025 数字创新大会



防火墙即服务 (FWaaS) & 数据防泄露 (DLP): 提供新一代的防火墙能力以及在数据流转的全链路中防止敏感信息外泄。

云访问安全代理 (CASB): 为企业使用的云服务和SaaS应用提供可视性与数据安全控制。

零信任网络访问 (ZTNA): 取代传统VPN, 实现按需、最小权限的应用程序访问, 收缩业务暴露面。

安全Web网关 (SWG): 保护员工上网安全, 过滤恶意内容, 防止网络威胁。

安全存取服务边缘 框架将进阶网络和安全性功能整合到统一的云端解决方案中。这种融合为分布式企业带来实质效益。

增强安全性

- 安全存取服务边缘 提供强大的网络威胁防护。透过整合安全功能，可消除与不同点解决方案相关的漏洞和漏洞。零信任网络存取是 安全存取服务边缘 的基础，可确保只有经过验证的用户和装置才能存取资源，进而降低未经授权入侵的风险。



降低复杂度

- 管理多个安全和网络工具非常麻烦。安全存取服务边缘 透过将这些功能整合到单一平台，简化营运。这简化了管理、降低了开销，并让 IT 团队能够专注于策略计划。



节省成本

- 传统安全模式需要大量硬设备和软件授权的资本支出。安全存取服务边缘 云端的云端原生方法可消除这些前期成本，转换为更可预测的订阅模式。这为组织节省了大量成本。



改善性能

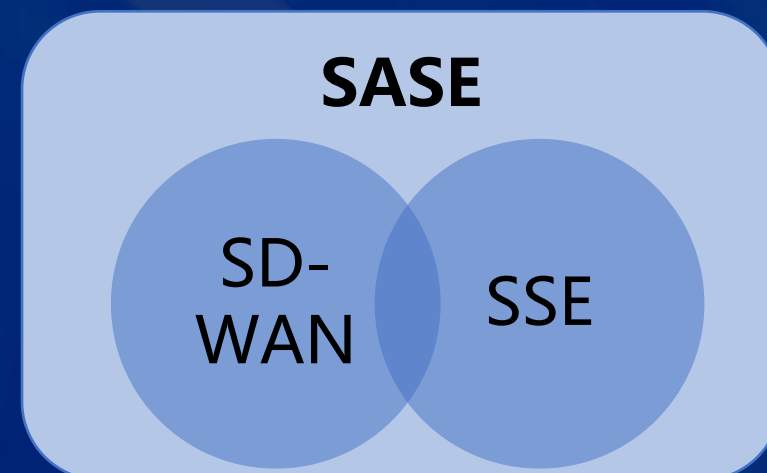
- 安全存取服务边缘 利用 SD-WAN 技术优化网络流量，并排定关键应用程序的优先级。这可确保提供更好的使用者体验，即使是远程访问云端资源的远程工作人员也一样。增强的效能可提升生产力并改善业务成果。



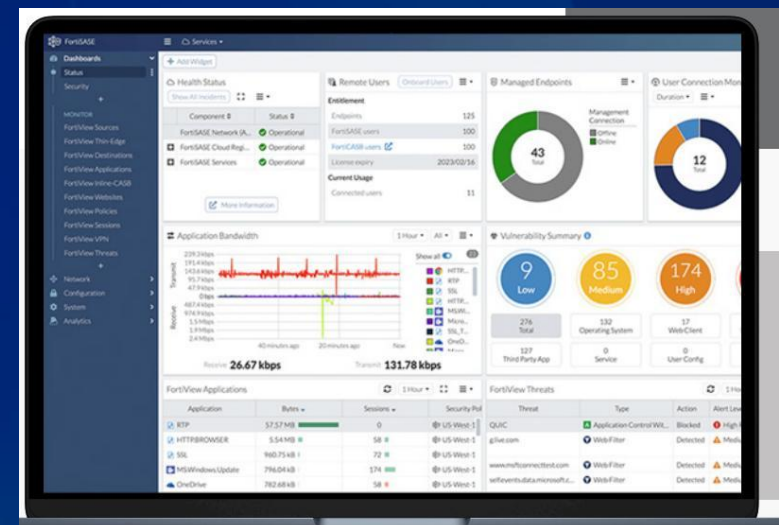
简化管理与降低成本

践AI·重构数智生产力
2025 数字 创新 大会

通过单一平台取代过去多厂商、多产品的碎片化方案，极大简化技术堆栈和运维工作。



云服务模式有助于降低硬件成本和IT资源投入。



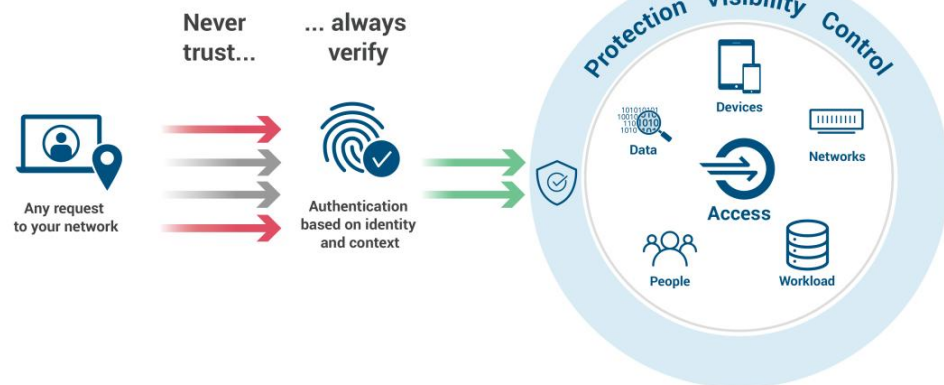
无处不在的安全防护

践行AI·重构数智生产力
2025 数字创新大会

将安全功能推至云边缘，靠近用户，实现零信任原则，即“从不信任，始终验证”。

确保员工无论在家中、分支机构还是在途中，都能获得一致的安全策略和访问体验。

Zero Trust Security

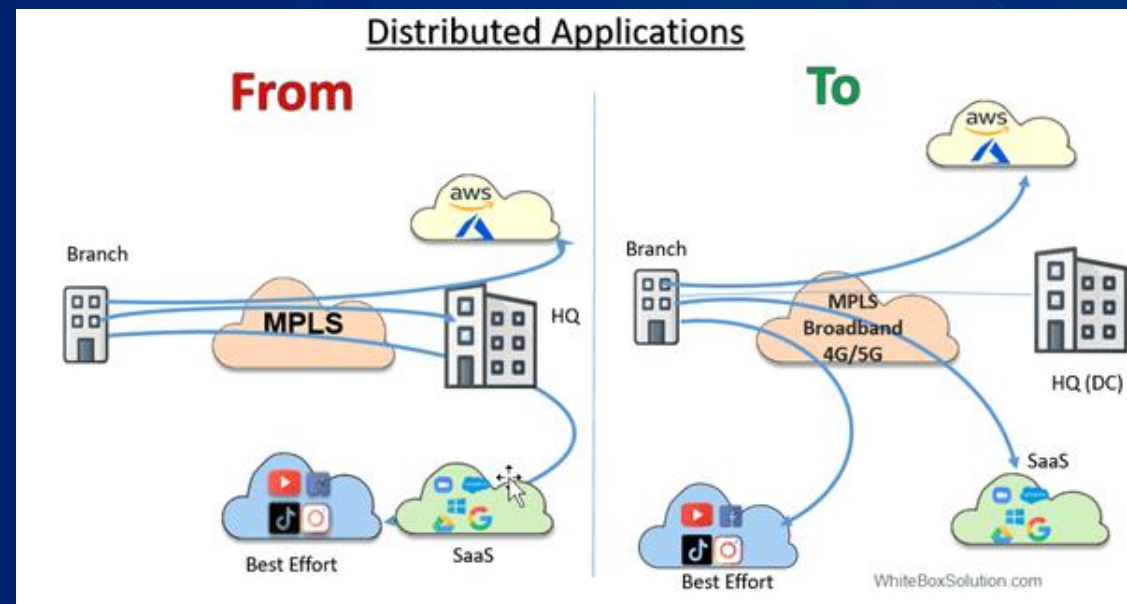
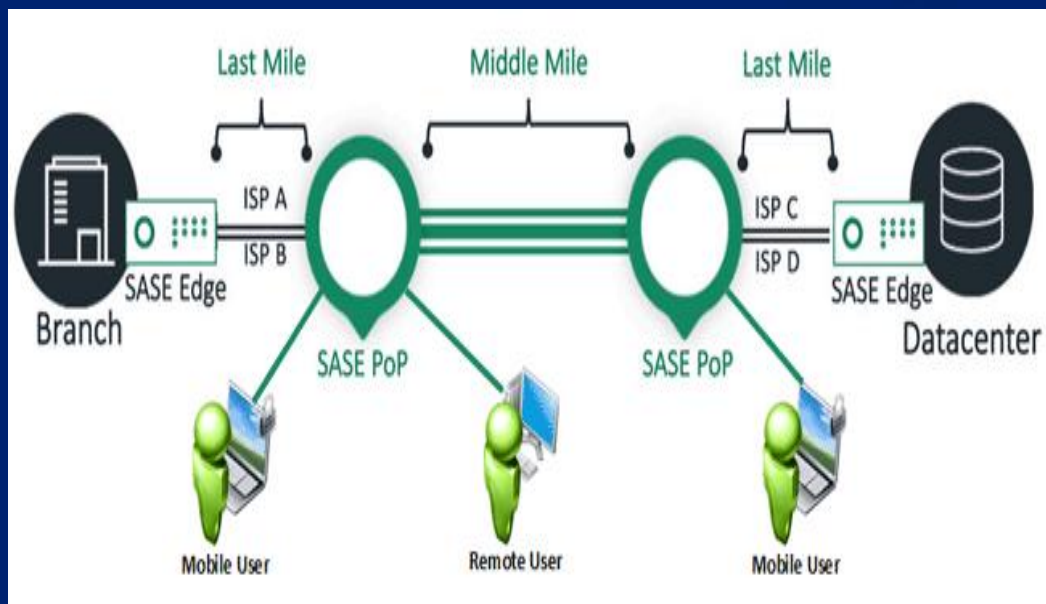


优化用户体验与性能

践行AI·重构数智生产力
2025 数字创新大会

通过全球分布的接入点（PoP），让用户就近接入，减少延迟和性能损耗。

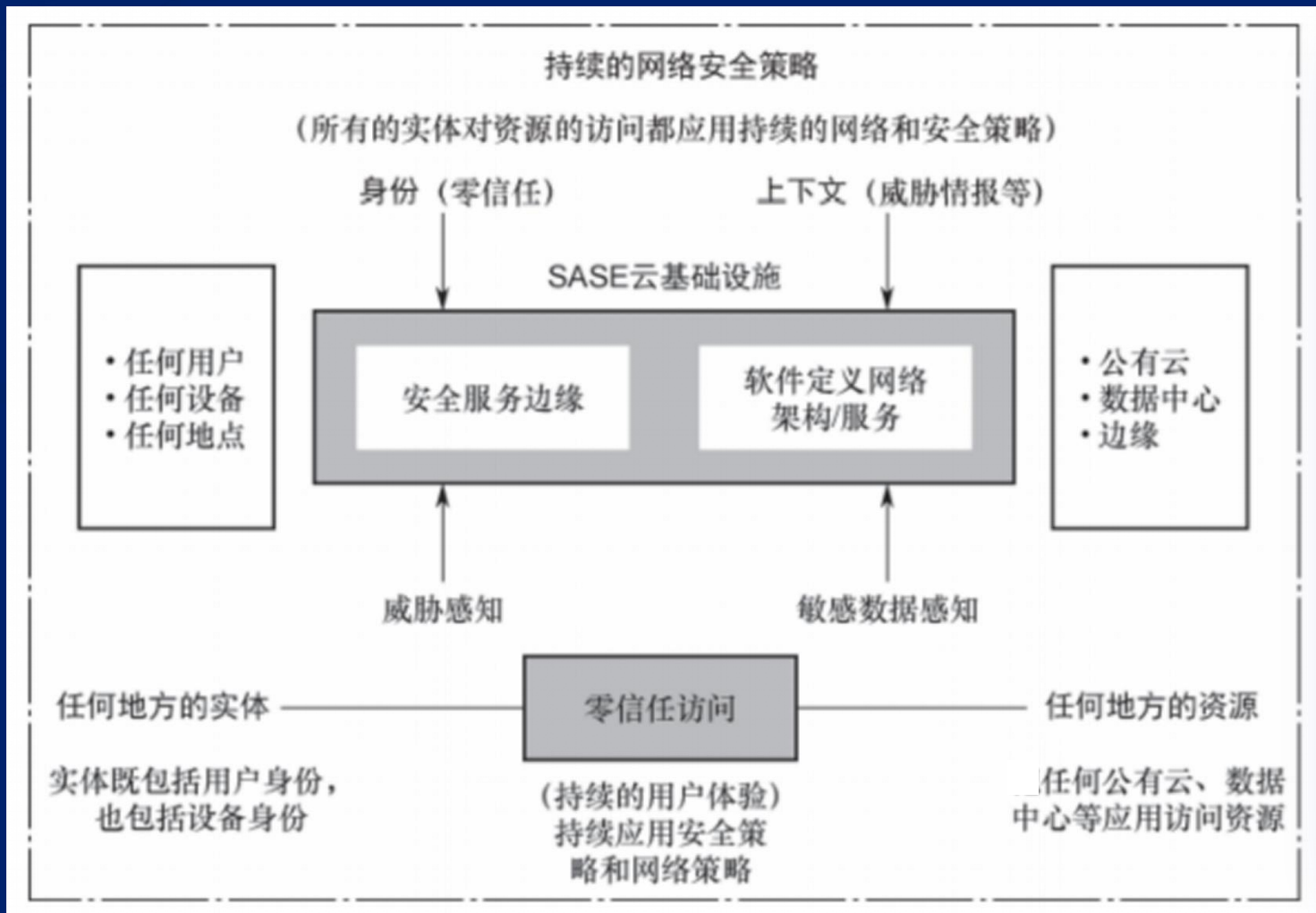
告别传统架构中所有流量都必须回传至数据中心导致的性能瓶颈。



目 录 CONTENTS

- 01 办公安全进化论
- 02 SASE的核心价值
- 03 **SASE在全球的落地实践**
- 04 未来展望

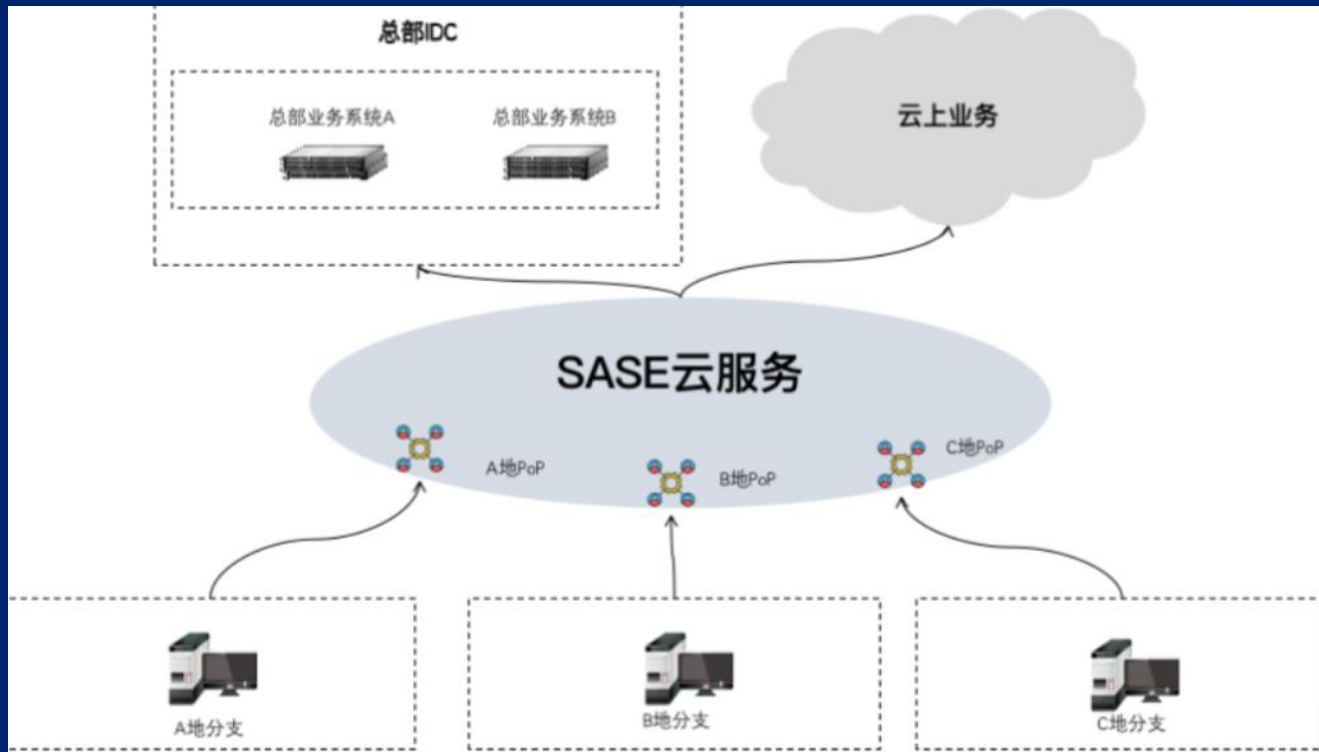




逻辑框架

- 将网络功能云化，安全功能云化，并基于架构层面的统一编排，以云服务的方式提供给最终用户。
- 对所有的实体和访问资源应用持续的、统一的网络策略和安全策略。
- 策略为基于身份的访问权限判断，基于威胁的感知和决策。威胁来自于：网络威胁、敏感数据的访问或者传输。

SASE适合场景1：跨地域分支机构



业务痛点

- 网络设计、部署，初始化成本高。
- 为保障总部数据安全和网络安全，投入成本高。
- 一线IT或安全驻场，人力成本高。

部署价值

- 多地域、靠近分支机构所在地的PoP节点接入，优化访问链路信息传输效率。
- 基于零信任的安全终端管理、通信加密、多因素身份认证、最小权限、动态访问控制等安全能力，保障访问过程的安全。
- 基于互联网的接入，比专线等形式降低成本。
- SaaS云服务的交付模式，比VPN等传统设备+私有化部署的形式支持更好的可扩展性。

SASE适合场景2：远程和移动办公

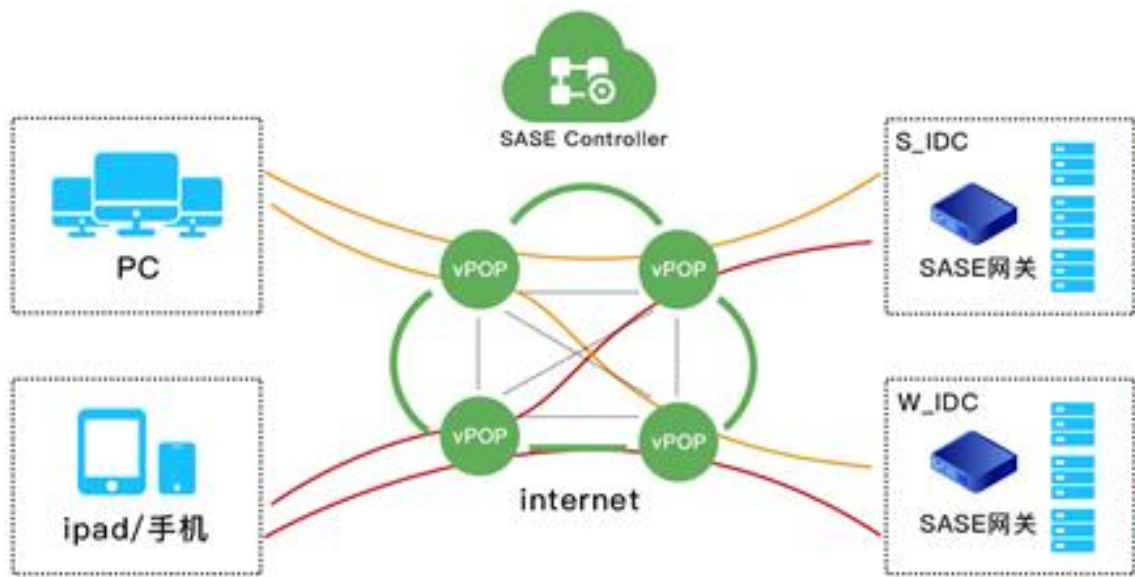
践AI·重构数智生产力
2025 数字创新大会

业务痛点

- VPN接入不同系统方式复杂，效率低。
- 远程访问质量不稳定。
- IT运维+安全团队频繁处理各类工单。

部署价值

- 用户实现就近的PoP节点接入，优化访问链路信息传输效率，保障客户体验。
- 基于零信任的安全终端管理、通信加密、多因素身份认证、最小权限、动态访问控制等安全能力，保障访问过程的安全。
- PoP节点的网络安全服务，保障移动办公电脑的上网安全。
- 对所有用户提供一致的安全管理，减少网管维护成本。
- SaaS云服务的交付模式，比VPN等传统设备+私有化部署的形式支持更好的可扩展性。



SASE适合场景3：连锁及加盟企业

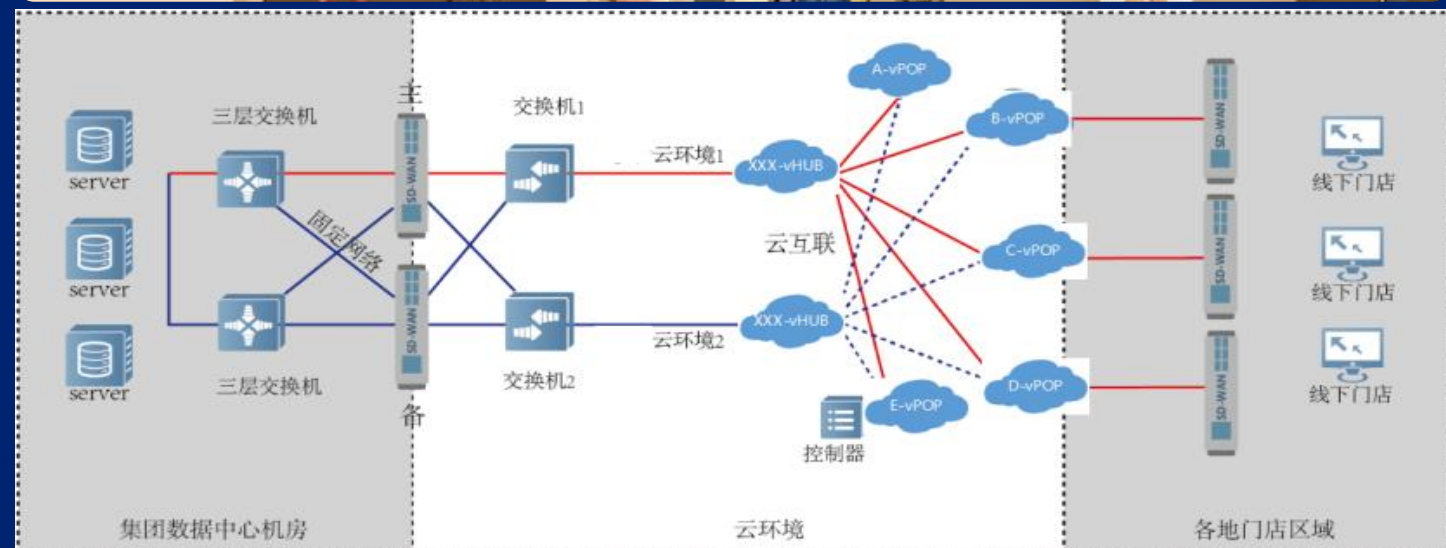
践AI·重构数智生产力
2025 数字创新大会

业务特点

- 分布范围广
- 员工数量众多
- 网络和安全需求多元化

部署价值

- 全网冗余、确保业务连续性，避免单点故障。
- 集中控制，简化运维，SD-WAN技术实现“零配置”下发。
- 增强安全，满足合规，安全管理员可以在云端统一对所有连锁或加盟网点的业务访问进行审计管控、信息文件防泄漏和终端威胁检测等安全防护。
- 降低成本、提升效率：通过互联网实现连锁或加盟网点到骨干网PoP的SD-WAN接入，免去了铺设“最后一公里”的线路。



部署模式



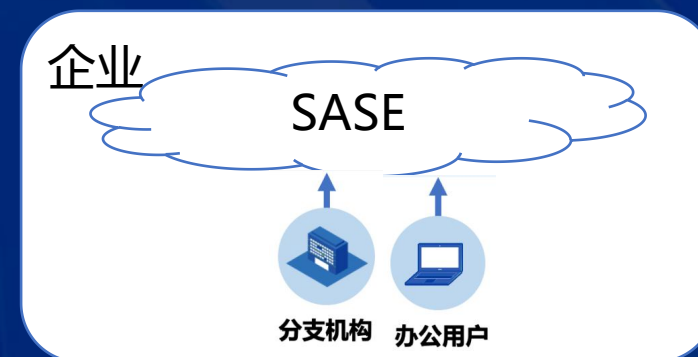
云服务模式

适合追求敏捷和轻量化部署的中小企业。
无需大量的硬件资源投入。成本相对较低。



一体化模式

线上线下结合。
适合中国IT环境的特色方案。例如，将零信任设备（如aTrust）部署在本地以满足数据驻留要求，同时结合云端的SWG和DLP服务，实现灵活性与合规性的统一。



本地化模式

满足金融、政府等对数据和控制面有严格要求的行业。
成本相对最高。

成功部署的五步法

践AI·重构数智生产力
2025 数字创新大会

明确业务驱动

厘清SASE要解决的核心问题，是保障混合办公体验，还是满足合规要求。

整合网络与安全

致力于原生融合，而非多产品的简单捆绑，以实现真正的策略一致。

零信任访问控制

将用户、设备和上下文的动态评估作为访问决策的新锚点。

选择合适的部署模式

根据企业现状和发展战略，选择最适合的落地路径。

统一管理 与可视化

通过统一控制台实现策略下发、威胁分析和运维管理，这是降低复杂性的关键。

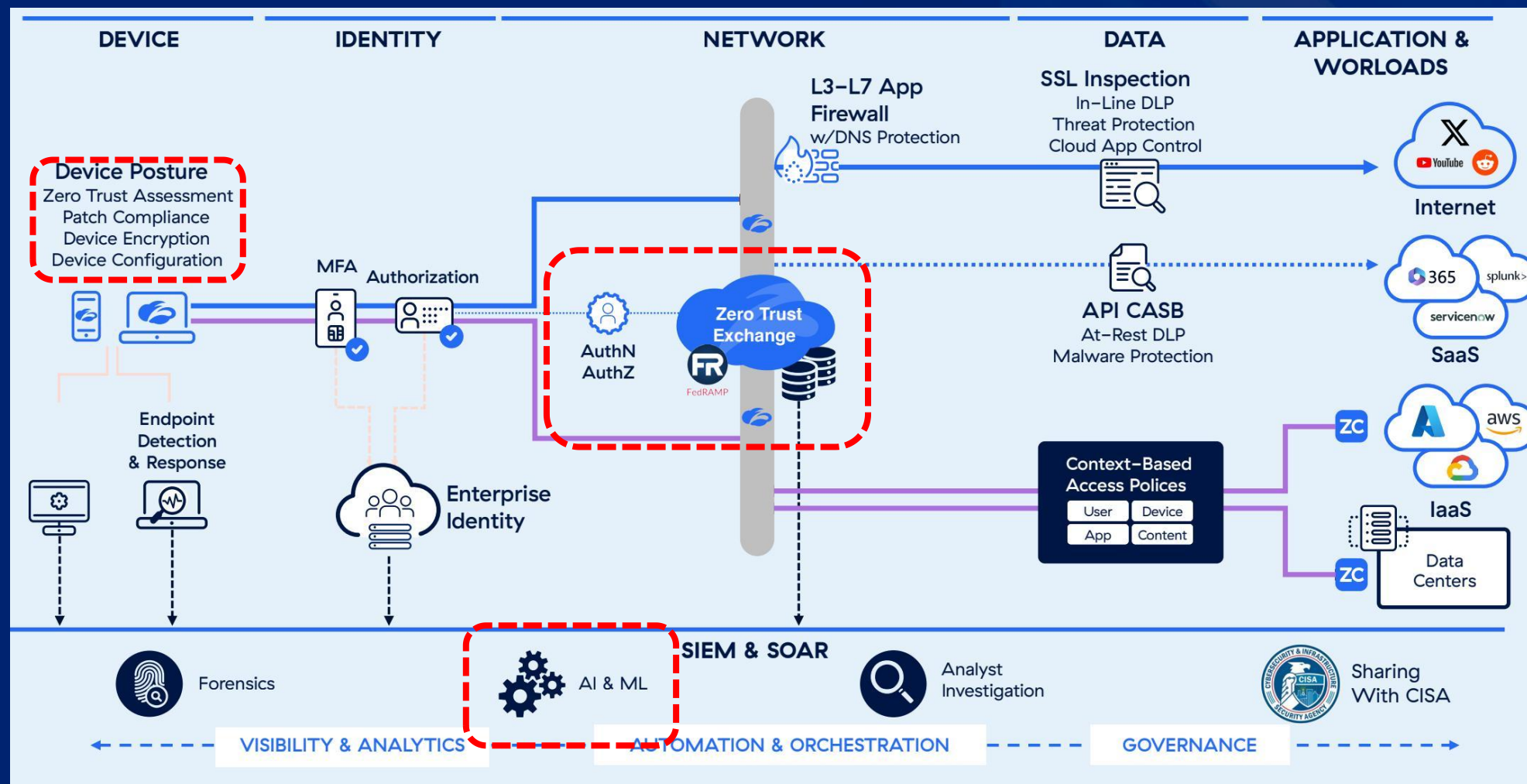
目 录 CONTENTS

- 01 办公安全进化论
- 02 SASE的核心价值
- 03 SASE在全球的落地实践
- 04 **未来展望**



人工智能与零信任的融合，实现更智能、自适应的安全

践AI·重构数智生产力
2025 数字 创新 大会



SASE的演进方向

践AI·重构数智生产力

2025 数字创新大会



AI的深度融合：AI引擎将更广泛地应用于用户行为分析、异常流量检测和未知威胁识别，提升安全自动化和智能化水平。



越来越多的企业会选择将SASE的监控、响应和运维交由专业服务团队托管



持续演进的一体化平台：市场将更倾向于由单一供应商提供的、高度集成的平台方案，以持续降低复杂性和运维成本。

演进方向

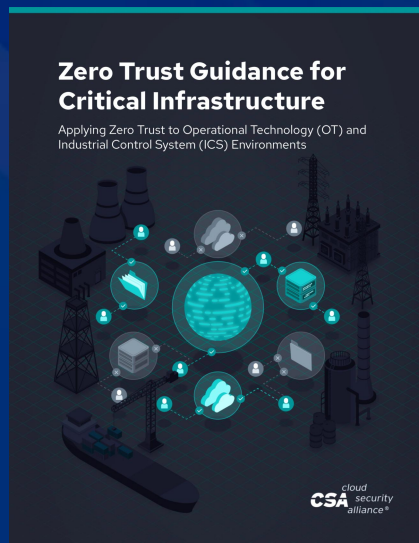
SASE

CSA GCR: 致力于零信任和SASE的研究和推广

践行AI·重构数智生产力
2025 数字创新大会

CSA

- CSA自2019年以来，发布了接近100份零信任的研究报告。
- “零信任”术语的提出者在CSA总部工作。
- CSA GCR 发布《SASE安全访问服务边缘白皮书》。



CSA

- CCZT（零信任能力认证）是行业第一个零信任专家认证。
- CSA GCR 推出了行业首个 AI for Cybersecurity的专家认证 (CAIDCP)。
- 一系列课程，赋能云数智安的行业转型。



THANK YOU

