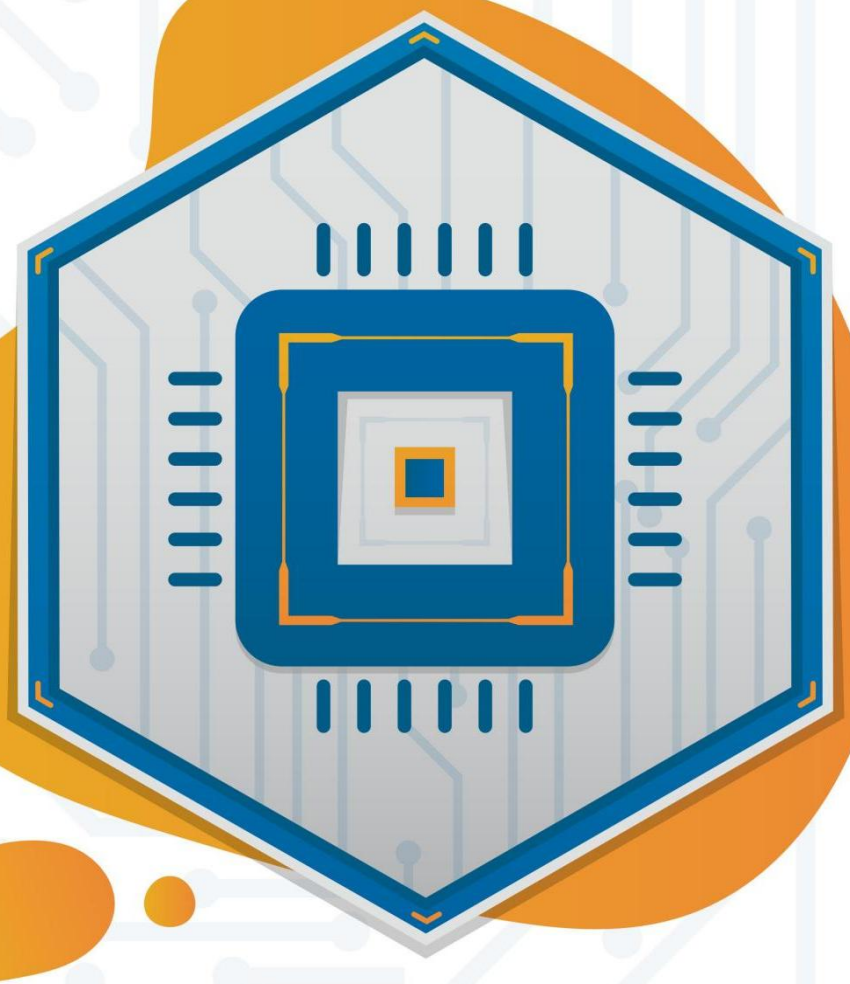
解读SSE



CSA GCR cloud security GREATER CHINA REGION alliance ®

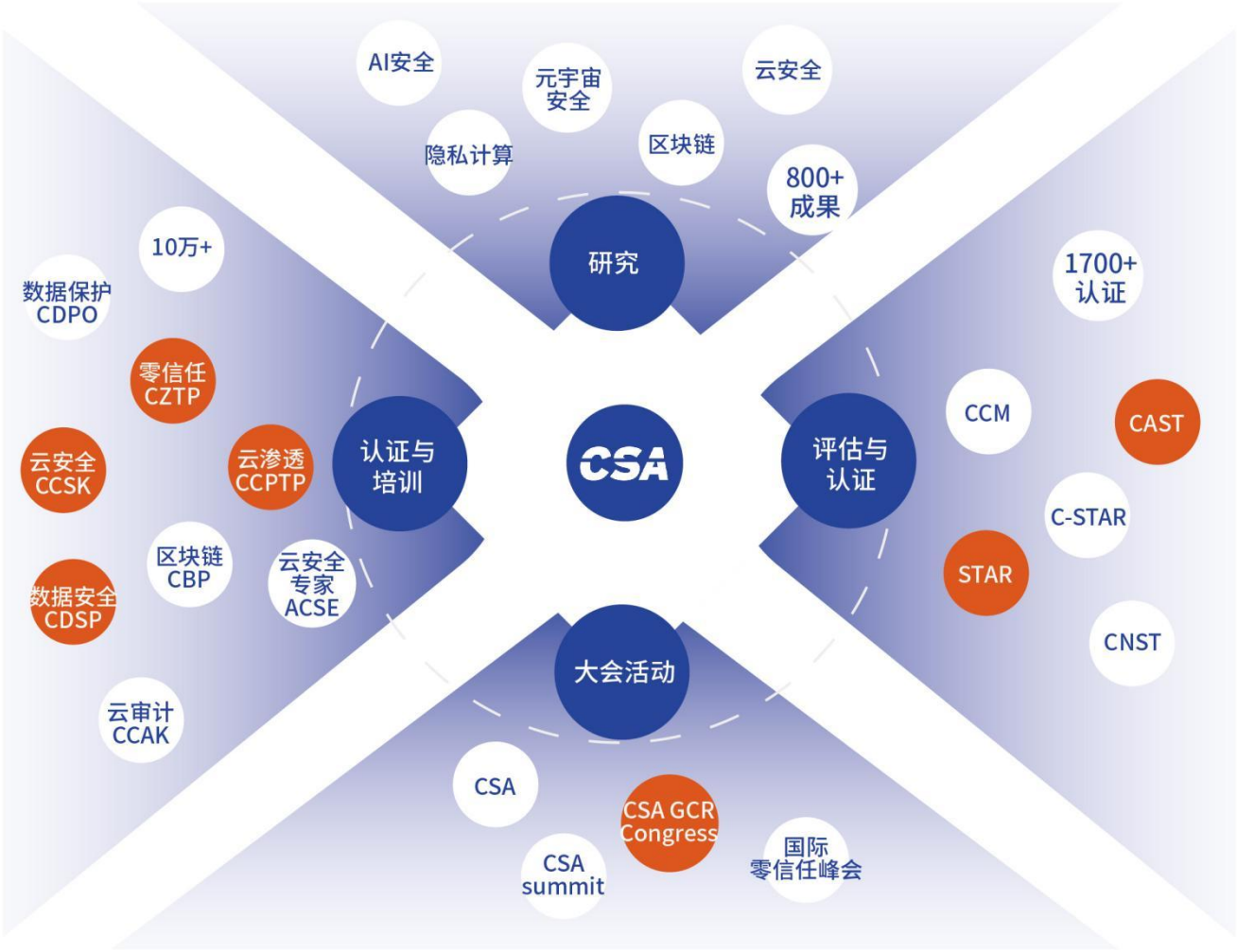
联盟简介

云安全联盟(Cloud Security Alliance,CSA)是中立、权威的全球性非营利产业组织,于2009年正式成立,致力于定义和提高业界对云计算和下一代数字技术安全最佳实践的认识,推动数字安全产业全面发展。

云安全联盟大中华区(Cloud Security Alliance Greater China Region, CSA GCR)作为CSA全球四大区之一,2016年在香港独立注册,于2021年在中国登记注册,是网络安全领域首家在中国境内注册备案的国际NGO,旨在立足中国,连接全球,推动大中华区数字安全技术标准与产业的发展及国际合作。

我们的工作

联盟会刊下载地址
了解联盟更多信息



加入我们

CSA大中华区官网
(https://c-csa.cn)

点击会员

加入联盟

填写相关申请信息

成为CSA会员

JOIN US

致谢

《解读 SSE》由 CSA 大中华区 SASE 工作组内专家撰写，感谢以下专家的贡献：

工作组联席组长：

何国锋　　林冠烨

贡献者名单

原创作者：

岑义涛　　常向青　　崔灏　　王茜　　张超　　钟施仪

审核专家：

毕亲波　　常向青　　黄超　　吕士表　　袁淑美　　姚凯

研究协调员：

崔灏　　司玄

贡献单位：

防特网信息科技(北京)有限公司（Fortinet）　　新华三技术有限公司

绿盟科技集团股份有限公司　　奇安信科技集团股份有限公司

深信服科技股份有限公司　　天融信科技集团股份有限公司

网宿科技股份有限公司　　中国电信股份有限公司研究院

北京启明星辰信息安全技术有限公司　　腾讯云计算（北京）有限责任公司

（以上排名不分先后）

关于研究工作组的更多介绍，请在 CSA 大中华区官网（https://c- csa.cn/research/） 上查看。

在此感谢以上专家。如译文有不妥当之处，敬请读者联系 CSA GCR 秘书处给予雅正! 联系邮箱 research@c-csa.cn； 国际云安全联盟 CSA 公众号。

序言

随着混合办公时代的到来，云服务的高速增长和用户办公场景移动性的增加导致以边界防护为主的网络安全防御体系不再适用于当今企业网络架构，用户在企业网络之外访问云服务成为普遍现象。为保护远程用户和云资源，Gartner 在 2019 年提出安全访问服务边缘（Secure Access Service Edge，SASE）概念，2021 年又提出安全服务边缘（Secure Service Edge，SSE），以云原生的技术通过边缘交付安全能力，允许企业通过云服务实施安全策略以促进对 Web、云服务和私有应用程序的安全访问。作为网络安全解决方案的当下热点，SSE 目前仍缺乏直观深度的解析以便进行深入研究和推广，尤其需要将其与 SASE 区别开。

SASE 工作组邀请业内专家，从技术视角客观解读 SSE，明确 SSE 与其他理念的异同，并分析 SSE 的缘起、主要应用场景、关键技术与核心能力，最后展示 SSE 厂商图谱和市场格局。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

目录

致谢 **3**

序言 **5**

1 SSE 是什么 **7**

2 为什么 SASE 之后又提出 SSE **8**

3 SSE 主要应用场景 **11**

3.1 互联网应用安全访问的服务场景 11

3.2 公有云私有应用安全访问的服务场景 12

3.3 企业数据中心应用安全访问的服务场景 13

3.4 物联网远程接入安全访问的服务场景 13

4 SSE 关键技术与核心能力 **14**

5 SSE 厂商图谱和市场格局 **15**

5.1 全球市场概况 15

5.2 海外厂商概述 16

5.3 国内厂商概况 19

6 结语 **20**

1 SSE 是什么

安全服务边缘 (Security Service Edge，SSE) 是以云原生的技术通过边缘交付安全能力，有助于安全访问网站、软件即服务 (SaaS) 应用程序和私有应用程序。功能包括访问控制、威胁保护、数据安全、安全监视，以及通过基于网络流量检测或应用 API 集成的方式实现对应用的使用控制。SSE 作为云化服务，可通过本地网关类设备或软件客户端接入。

2019 年，Gartner 将安全访问服务边缘（Secure Access Service Edge，SASE）定义为一种新兴的方案，网络服务（最显著的是 SD-WAN）功能与网络安全功能（如 SWG、CASB、FWaaS 和 ZTNA）结合，支持数字化企业的动态安全访问业务和互联网的需求。

2021 年，Gartner 在《2021 年 SASE 融合战略路线图》中提出了 SSE，如果说 SASE 描述了一个架构框架，将网络和安全整合为从云提供的统一服务，那么 SSE 则分离了 SASE 框架的网络即服务部分，描述了该框架的安全即服务部分。与 SASE 相比较，SSE 专注于统一所有安全服务，包含但不限于：安全 Web 网关 (Secure Web Gateway，SWG)、云访问安全代理 (Cloud Access Security Broker，CASB) 、零信任网络访问 (Zero Trust Network Access，ZTNA)和防火墙即服务 (FireWall as a Service，FWaaS)等安全能力。与之对比，SASE 同时还专注于网络服务的简化和统一，包括软件定义广域网 (Software Defined Wide Area Network，SD-WAN)、广域网优化、服务质量 (QoS) 以及其他通过改进路由到云应用程序的技术。

有必要说明，零信任是由 Forrester 提出的遵循“永不信任、持续验证”原则的安全理念。ZTNA 是零信任在访问接入控制方面的实现。SSE 中包含 ZTNA、SWG、CASB 等能力，因此 ZTNA 是 SSE 中的一个核心能力。

Gartner 预测，到 2025 年，实施基于代理的 ZTNA 的组织中 70%将选择 SSE 提供商而不是独立产品，该比例远高于 2021 年的 20%。到 2025 年，购买 SSE 相关安全服务的组织中有 80%将购买整合的 SSE 解决方案而不是独立的云访问安全代理、安全 Web 网关和 ZTNA 产品，该比例远高于 2021 年的 15%。

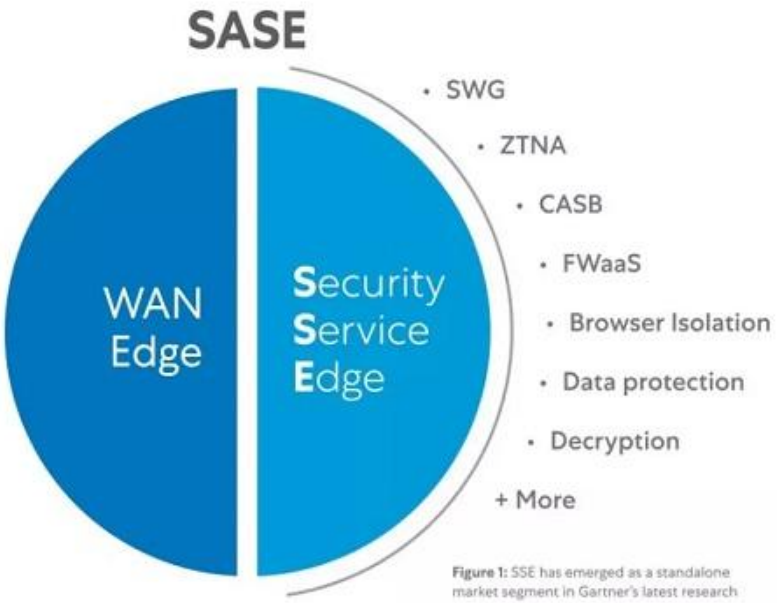


图 1 SSE 与 SASE 的关系

2 为什么 SASE 之后又提出 SSE

纵然 SASE 作为在混合办公时代下解决分支办公和远程访问的网络及安全融合型解决方案备受 Gartner 和业界厂商推崇，并获得了客户的高度关注，但是在落地层面仍然面临了诸多问题，比如：

- 具备完整 SASE（包含 SD-WAN 和 SSE）能力的供应商仍然屈指可数
- 客户已经建设了 SD-WAN，需要避免重复投入
- 客户内部组织结构不同，如果是网络/基础设施和安全为独立团队，则会单独决策，高度融合的 SASE 不会成为该类企业的选择
- 由于安全事件导致客户临时发起纯安全的项目需求，比如传统 VPN 向 ZTNA 的改造项目，这类项目不涉及网络部分的新增建设需求
- 客户自身没有诸多分支办公室，只是租用了零散的办公场所或区域中心，核心需要解决应用安全访问及互联网安全访问等问题，没有组网需求

因此不难发现，SASE 这种将网络和安全能力高度融合的“大一统”解决方案固然尤其吸引人的地方，但是不同的客户实际情况阻碍了“标准完整”的 SASE 项目落地。SASE 能够为客户提供更简便的交付与使用，不论是从技术、财务、流程等诸多方面均无需考虑多种硬件，多种服务和多供应商的结合问题。

SASE 比较适合中型规模且具有较为分散的分支型企业，因为他们负责 IT 和基础设

施的人员通常较少，且技术栈的广度和深度都有所欠缺。

一旦客户是大型企业，有独立的网络和安全团队，就要在预算、策略管理、事故责任认定等方面需要“分清”，则势必会出现网络和安全能力分开建设的情况。尤其是当网络在早几年已经完成了 SD-WAN 改造，此类客户就更无必要选择融合型的 SASE 方案，这时纯粹的云安全服务 SSE 则是客户的最佳选择。

另一方面，随着企业混合办公趋势的常态化，企业 IT 和安全合规团队需要更多考虑如何能够让随时随地办公的员工始终符合企业安全管理要求以及所在国家的安全法规要求。在这种情况下，只有终端安全显然是不够的，需要为员工提供一个永远在线、按需扩展、不影响应用访问体验的“上网安全云”，让员工能够随时随地，安全、合规的“上网”访问互联网、部署在公有云或私有云基础设施的企业业务系统，及在 SaaS 服务运行的业务系统。在这样的情况下，无节点间组网需求，SSE 无疑是“上网安全云”的最佳实践，选择供应商提供的 SSE 安全服务边缘实现弹性可扩展，多点接入的完善互联网访问安全栈。

在供应商和产品技术层面，虽然在 SD-WAN 和 SSE 魔力象限中列席的厂商都很多，但是能够同时满足 SD-WAN，ZTNA，SWG，CASB 等关键能力且都具备业界领先水平的厂商少之又少。擅长网络产品的厂商在安全能力方面较弱，且无法提供云原生安全服务交付；而安全能力擅长的厂商又始终难以提供完善的高级路由、应用感知的路由，进而无法支持业务驱动的动态组网场景。与此同时，当下混合办公、应用访问的关键技术——ZTNA 更是横跨 SASE 中网络和安全两大组件的重要技术能力，想实现较好的产品化、工程化支持多环境，多终端类型，多应用类型，不论对上述那种厂商都是不小的挑战。随着云化普及，客户应用从数据中心转移到云上，从自建系统到逐步采用第三方 SaaS。这种场景下企业无点对点的组网需求，需要的是通过部署在边缘 POP 的 ZTNA，SWG，CASB 等 SSE 能力。

综合客户需求和方案能力成熟度两方面看，完整 SASE 方案的落地都具有明显挑战，在这样的情况下，Gartner 将用户互联网访问的两大关键安全产品魔力象限（SWG 和 CASB）合并为 SSE 魔力象限，并在此之后发布的 Single-Vendor SASE（单供应商 SASE）市场指南中明确指出了交付 SASE 的三种方式：完全由一家供应商提供的单供应商 SASE、由显而易见的多供应商提供的 SASE、由服务商打包提供的 Managed（托管型）SASE，其中 Managed SASE 某种意义上也认为是单供应商 SASE。此上均表明了 SASE 的落地任重而道远，且需要充分考虑不同客户的实际情况。SSE 应运而生，以云服务的形式仅交付关键安全能力，将 SASE 能力解耦，更灵活的实现落地，为用户提供简单易用、灵活付费、弹性扩容的安全云服务，当客户产生了 SD-WAN 需求时，则可以与之结合，实现完整 SASE

能力。

虽然 Gartner 视 SASE 为网络安全的未来，也必须要面对客户需求多样化以及供应商产品与技术成熟度的事实。Gartner 对 SASE 是未来这一判断有一些值得大家注意的基本假设，即：遍及全球或大洲的分布式企业、业务高度上云、员工无处不在办公、企业追求效率而不是成本等等。因此不难发现，如果客户不符合上述的全部条件，或者在当期及未来项目中不涉及更多需求，那么确实是不需要 SASE 这一融合了网络和安全全部能力的架构。安全厂商也不需要在自己不熟悉的网络能力方面增加投入，只需要专注自身最擅长的安全能力，并以云原生的方式实现能力融合与交付即可。

因此，作为 SASE 在安全能力“化身”的 SSE，必将在实际项目中扮演更重要的角色，毕竟技术成熟度高且落地快、客户需求明确且内部权责划分清晰。在 SSE 落地之后，结合客户已有的 SD-WAN，SASE 就是一件水到渠成的事情了。

3 SSE 主要应用场景

基于 SSE 的架构和基础安全能力，SSE 的典型应用场景主要包括四个方面：互联网应用安全访问的服务场景、公有云私有应用安全访问的服务场景、企业数据中心应用安全访问的服务场景、物联网远程接入安全访问的服务场景。

3.1 互联网应用安全访问的服务场景

企业分支通过互联网以网络设备接入到边缘安全防护 POP 点，通过 CASB、SWG 等安全功能，对访问互联网的各类应用（互联网应用或是企业 SaaS 应用）进行安全防护，包括根据 URL 分类库和流量内容识别对互联网应用网站的允许或拒绝访问，采用白名单或黑名单策略对发现与识别的应用程序进行访问管理，扫描 Web 内容中的垃圾邮件、恶意软件和病毒并进行相应的过滤，并能够有效应对勒索软件、凭证盗窃、网络钓鱼等基于 Web 的网络攻击威胁。在私有化场景可通过组网方式（如专网或者 SD-WAN）接入到私有化 SSE 的边缘安全防护 POP 点。

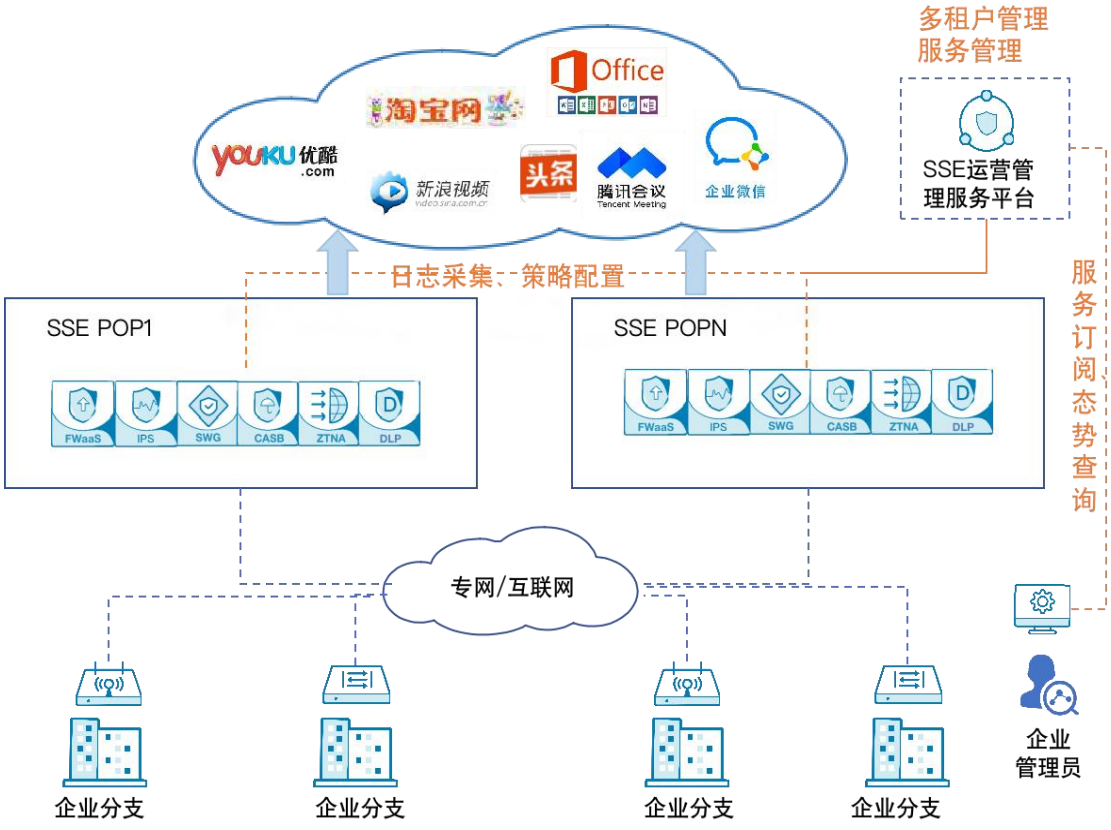


图 2 互联网应用安全访问场景

3.2 公有云私有应用安全访问的服务场景

企业分支通过互联网接入到 SSE 的边缘安全防护 POP 点，或者 SOHO 办公的终端通过零信任方式接入 SSE 的边缘安全防护 POP 点，通过 FWaaS、CASB、ZTNA 等安全功能，针对访问多种公有云（如运营商公有云、阿里腾讯公有云、华为云）的私有应用进行安全防护，包括针对应用数据加密、威胁检测、数据管理、风险评估等功能，防止或减轻网络钓鱼、帐户接管和恶意软件等安全威胁，并帮助企业识别影子 IT，保护连接的设备和数据免受未授权终端或者恶意软件的威胁，监控用户行为，将其与基准模式进行比较以及标记异常活动，最终保护用户和云服务商之间的安全访问连接。采用零信任接入方式，针对用户账号、密码、口令、终端环境基线属性等信息对用户身份进行实时认证，结合数据上下文制定应用的访问策略、识别风险并根据风险优先级动态调整应用访问策略。

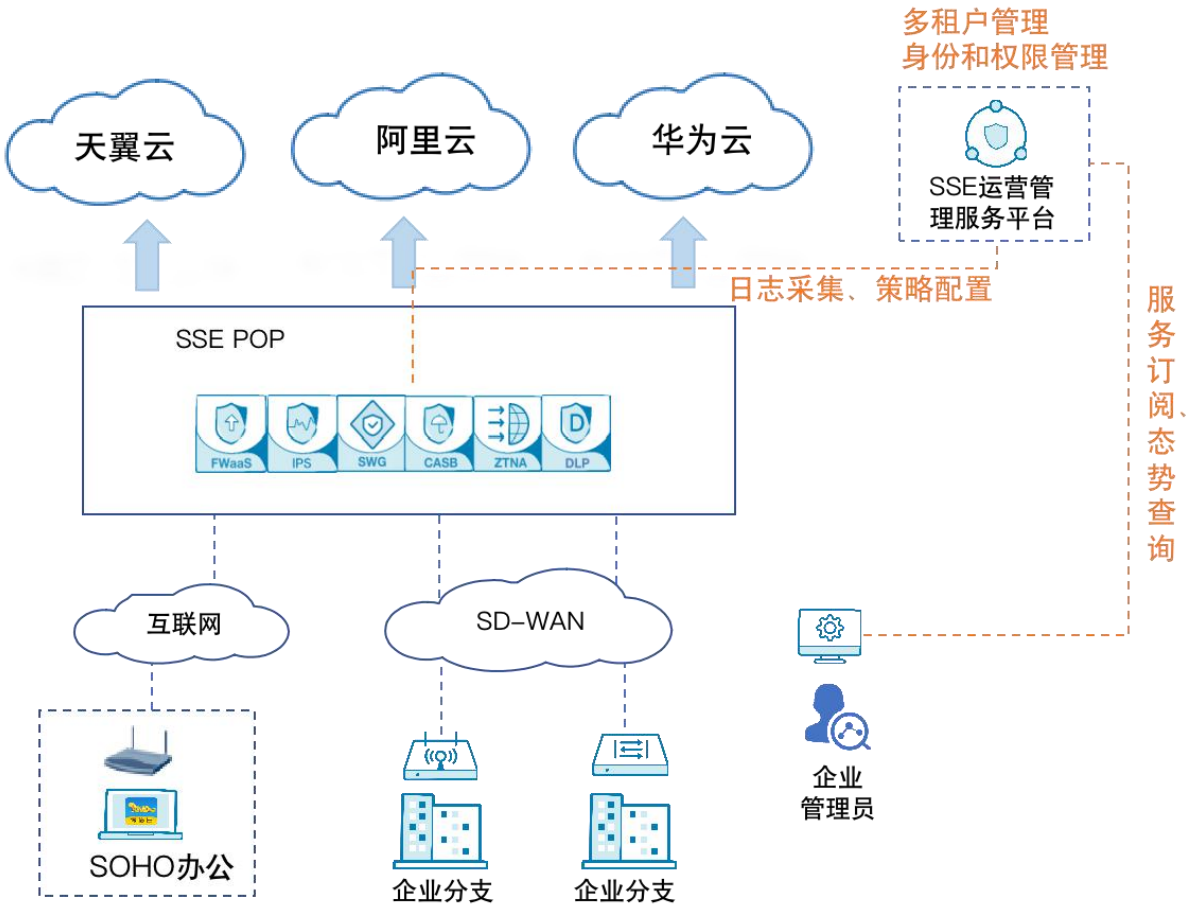


图 3 云应用安全访问场景

3.3 企业数据中心应用安全访问的服务场景

企业分支通过互联网接入到 SSE 的边缘安全防护 POP 点，或者 SOHO 办公的终端通过零信任方式接入 SSE 的边缘安全防护 POP 点，通过 FWaaS、CASB、ZTNA 等安全功能，针对访问企业数据中心的私有企业应用程序进行安全防护，针对用户账号、密码、口令、终端环境基线属性等信息对用户身份进行实时的认证，结合数据上下文制定应用的访问策略、识别风险并根据风险优先级动态调整应用访问策略。

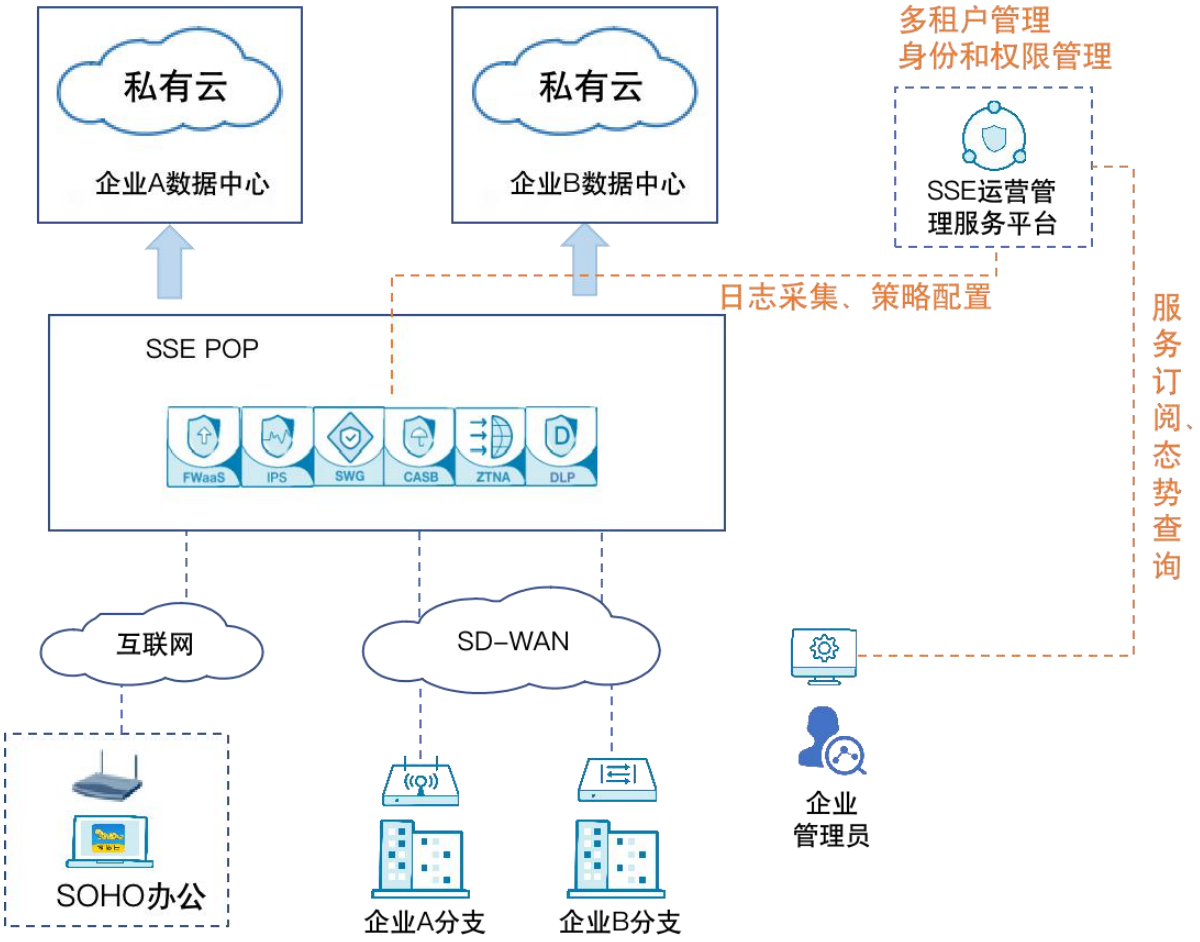


图 4 企业数据中心安全访问场景

3.4 物联网远程接入安全访问的服务场景

物联网智能终端远程接入场景，使用固定边缘接入设备或直接通过运营商物联网卡/SIM 卡/eSIM 卡接入互联网，并通过物联网终端安全套件或代理边缘接入设备登录 POP 点的零信任访问网关，进行数据安全采集回传。SSE 的边缘安全防护 POP 点，通过 FWaaS、ZTNA 等安全功能对不同接入的物联网终端进行在网状态检测及非法接入进行检测，对恶意终端发起的 DDOS 攻击及非法访问进行及时拦截并告警。

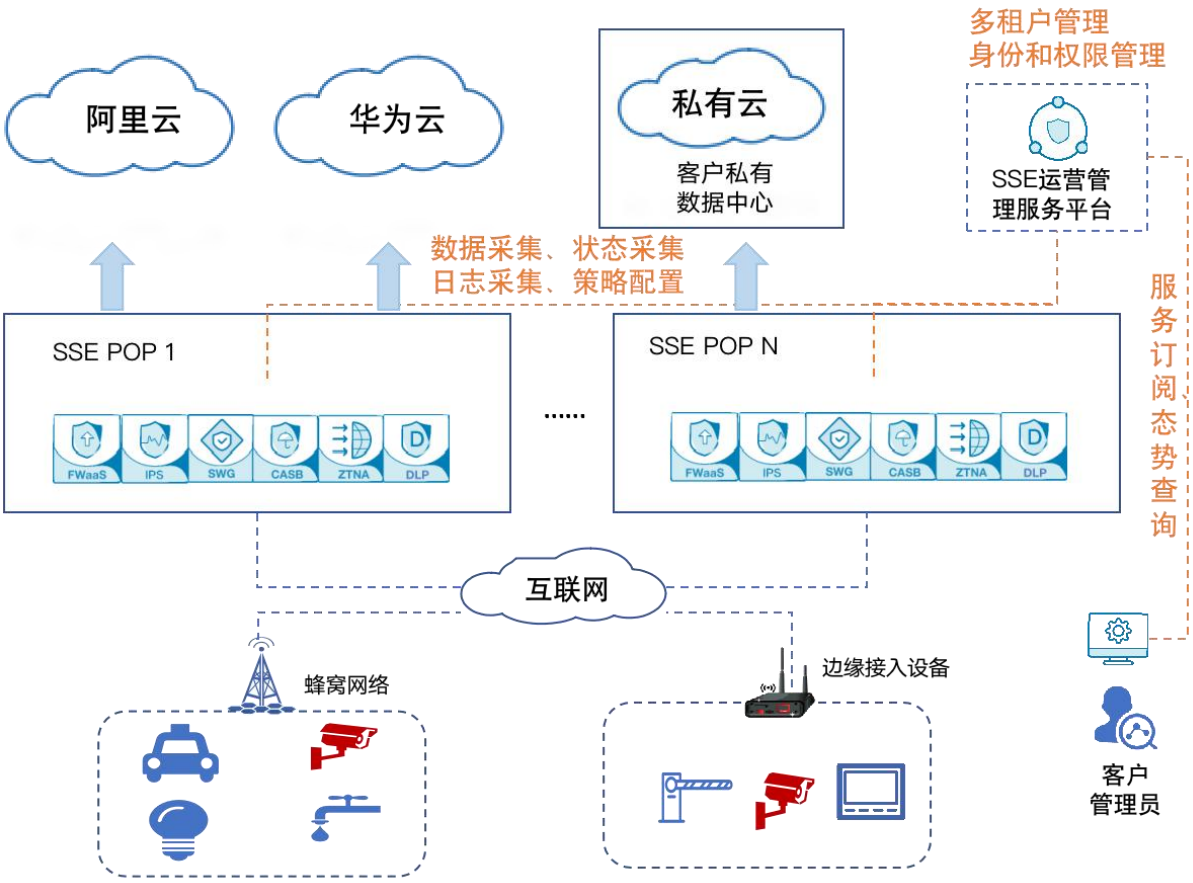


图 5 物联网远程接入安全访问场景

基于 SSE 架构还可扩展到其它应用场景，例如企业的多云访问的安全防护场景，企业的应用等保安全服务场景等。

4 SSE 关键技术与核心能力

SSE 支持多种安全访问场景，不同的安全场景所需的核心能力不同，上网安全场景所需的核心能力包括 SWG、FWaaS；访问 SaaS 应用场景需要加载 ZTNA、CASB 等能力；物联网 IoT 场景需要 ZTNA、FWaaS 等能力。

SSE 核心能力主要包括：

1）ZTNA

ZTNA（Zero Trust Network Access，零信任网络访问）默认假定任何用户都是不可信任的，不可访问任意内容，仅当用户身份、终端设备环境、上下文行为均被判定为可信的情况下，该用户才能访问授权可访问应用和数据。与 VPN 不同，VPN 允许用户基于 IP 授权访问内网，ZTNA 相较于 VPN 可以做到更精细化的访问控制。

2）SWG

SWG（Secure Web Gateway，安全 Web 网关）可使用多种防御技术保护企业组织免受来自 Web 网站的威胁，它位于用户和 Web 网站之间，一般采用代理模式代理用户访问 Web 的流量，并在流经 SWG 服务节点时执行多项安全检查，包括 URL 过滤、恶意代码检测、Web 访问控制等等，检查完毕后再将流量发往对应要访问的网站或将网站流量返还给用户。好的 SWG 服务可以对加密流量做到同样的安全检测。

3）FWaaS

FWaaS（Firewall as Service，防火墙即服务）是一种基于云的防火墙，它可以整合来自企业组织总部、移动用户等各个位置的流量，可以对多来源的流量进行分析。FWaaS 通常支持 IDS/IPS、高级威胁防御、DNS 安全等功能。

4）CASB

CASB（Cloud Access Security Broker，云访问安全代理）可以识别和检测云应用程序中的敏感数据，还可以下发安全策略，例如身份验证和单点登录（SSO）。它可以防止用户注册和使用未经企业 IT 组织授权的云应用，同时帮助企业减少影子 IT，避免安全合规事件的发生。

除上述核心能力以外，还可以提供其他安全服务，例如数据防泄漏（DLP）、远程浏览器隔离（RBI）、云沙箱等等。

SSE 的关键技术和 SASE 是一致的。[1]

5 SSE 厂商图谱和市场格局

5.1 全球市场概况

参考 Gartner 2022 年 2 月 15 日发布的《Magic Quadrant for Security Service Edge》，SSE 市场现状如下：

2020 财年 SSE 市场的收入在 2.4 至 26 亿美元之间，同比增长 19% 至 21%。这个市场的供应商改进了 SWG、CASB 产品，更直接地与 SWG 和 CASB 领域的厂商竞争，一些新晋厂家也补全这两种功能，来争夺 SSE 机会。

各供应商主要方案差异：

[1] 参见 SASE 的白皮书:https://www.c-csa.cn/research/results-detail/i-1753/

1）架构差异：一些厂商提供统一的 SSE 平台，一些厂商则是将多个组件进行松散打包。部分方案必须安装客户端，而另一些同时也可以提供无客户端（依赖网络）的方案。

2）安全组件成熟度差异大：各厂家在云安全组件、数据安全功能、云基础设施等方面能力成熟度差距比较大。同时各厂家普遍尝试加入数字体验监控（Digital Experience Monitoring）能力，以应对用户的业务访问体验问题。

5.2 海外厂商概述

收录到 2022 年 Gartner SSE 魔力象限的厂家如下[2]：

图 6 Gartner 2022 年 SSE 魔力象限

[2] 参考 Gartner 2022 年 2 月 15 日发布的《Magic Quadrant for Security Service Edge》

厂家概述、优劣势如表 1 所示。

象限	厂商	概述	优势	劣势
领导者	Zscaler	其主要的 SSE 产品包括 Zscaler Internet Access (ZIA)、Zscaler Private Access (ZPA) 和 Zscaler Digital Experience (ZDX) 服务。它还提供 CSPM 和 Zscaler 云保护。 客户为各行业的中大型组织。	1、第一个引入 DEM 的公司，能够收集和分析最终用户体验。 2、市场投入大，收入和新客户数量迅速增长。 3、提供强大的 SWG 功能和易于使用的 ZTNA 产品。 4、有更强大的 SD-WAN 合作伙伴生态。	1、价格高，续费价格会上涨。 2、数据安全等能力落后于其他厂商。 3、报表功能性能差，需要购买额外的 SIEM 模块处理。
	Netsope	SSE 产品作为 Netskope 安全云平台的一部分提供，包括下一代 SWG、CASB 和 Netskope 私有应用访问 (NPA)。 客户为众多行业的中型到超大型组织。	1、模块化部署在 Newedge 云，受到客户欢迎。 2、提供高级数据安全功能。支持 OCR，支持通过机器学习识别图像类型和文本。 3、提供强大的 SLA。SLA 提供标准的 5 个 9 可用性，并保证未加密 Web 流量的延迟小于 10 毫秒，加密流量的延迟小于 50 毫秒。	1、云防火墙 7 层协议只支持 HTTP 和 HTTPS。 2、基本的 VPN 隧道配置依赖 SD-WAN 合作厂商。 3、2020 年发布 ZTNA 服务 NPA、2021 年支持无客户端访问，发布时间晚。 4、价格竞争力弱。
	McAfee Enterprise	SSE 产品是 MVISION 统一云边缘 (UCE) 服务。还提供例如 XDR 和端点安全等产品。 它的客户规模从小到大，来自各个行业。	1、SSE 方案完整且紧密集成，包括 SWG、CASB、ZTNA、RBI、数据安全等。 2、提供 CSPM 和 SaaS 安全状态管理 (SSPM) 功能、数字体验监控 (DEM)、DLP 。 3、定价模式简单、具竞争力。	1、开发和发布 ZTNA 和 FWaaS 功能的时间比较晚。 2、缺乏与其经过认证的 SD-WAN 提供商的紧密集成。
远见者	Forcepoint（Bitglass）	SSE 产品包含 SWG、CASB 和 ZTNA。 它的客户往往是来自多个行业的大型企业。	1、数据安全功能强大，可使用专有的 FPSL（可编程 SASE）功能进行定制，并集成在 SWG、CASB 和 ZTNA 功能中； 2、AJAX-VM 技术可以实现无客户端访问。 3、提供超过 300 个基于 AWS 的云 POP 点。 4、使用其 SmartEdge 代理来实现内容解密和检查，改善整体延迟。	1、SmartEdge 依赖客户端，ZTNA 不支持 UDP 2、Forcepoint (Bitglass) 对市场的反应在过去一年有所放缓。例如，它专注于扩展其云 POP 并将其 FPSL 功能扩展到其现有平台内的其他模块，而不是添加 FWaaS 等新功能。
	Lookout	Lookout 的 SSE 产品包括 CASB、SWG 和 ZTNA。还提供移动端点安全产品。 它主要服务于许多行业的大中型企业。	1、拥有强大的数据安全能力，包括水印、加密、标记化等高级功能等。 2、在 Web、SaaS 和私有应用程序中深入集成了数据安全。	1、几乎没有与 SD-WAN 合作，专注于移动操作系统而非非移动设备的威胁防御。 2、缺乏 FWaaS 产品，直到 2021 年 8 月才通过 OEM 引入 RBI。

挑战者	Palo Alto Networks	SSE 产品主要由 Prisma Access 和 SaaS 安全服务组成。提供云管理、DEM 等，支持 API 与 RBI 等第三方技术的集成。 服务于各个行业的各种规模的客户。	1、财力雄厚，客户基础庞大，持续投入让客户迁移安全能力到 SSE。 2、保持 ZTNA 端点和应用程序之间的流量内联，可以为在网和离网用户提供一致的 ZTNA 规则。	1、功能模块没有很好整合，如 RBI 依赖于合作伙伴。 2、设置和管理相对复杂。 3、部分功能需要基于 PA 的防火墙，导致对非 PA 防火墙用户竞争力弱。 4、功能模块多且复杂、价格高。
	Cisco	思科 SSE 包括：Cisco Umbrella 、 Cloudlock 和 Duo Beyond。2021 年推出 DLP、身份验证、RBI	1、客户接受度高，期望 SSE 和思科 SD-WAN 结合。 2、入门级产品简单易用，如 XDR 产品 SecureX 集成的 Umbrella DNS Security Essentials 和 Umbrella DNS Security Advantage 。并且 AnyConnect VPN 可以满足许多远程访问要求。 3、支持情报集成。	1、数据安全功能比较基础，缺乏自动化的高级分析。 2、组件集成差，基础组件价格低，但整套方案昂贵。 3、功能推出较慢，没有基于客户端代理的 ZTNA 方案，最近才发布 RBI。
利基者	Broadcom	SSE 产品包括： Symantec Web security service Cloud SOC（CASB） Symantec secure Access cloud （ZTNA） 客户类型： 大企业，行业客户	1、SWG 具有优势地位 2、有广泛客户群体，了解最终用户的风险评分。 2、DLP 先进，如 OCR、指纹识别和矢量机器学习。 3、Broadcom 通过仅销售基于云的 SSE 许可证简化了定价。如果客户需要本地设备，则硬件成本会额外增加。 4、是市场上率先推出 SWG、CASB 和 ZTNA 组件的公司之一。	1、销售战略侧重于全球最大的公司，其他潜在客户很难获得技术支持。 2、没有很好地集成。需要部署多个客户端，使用多个控制台，缺乏集成导致功能混乱。
	iboss	提供 SASE 产品，包含 RBI、CASB 等 客户集中在北美和欧洲，它在亚太地区的影响力较小，它的客户来自许多行业。	1、ZTNA 功能默认提供，定价具有竞争力 2、技术支持能力强、响应时间快、SLA 达到 7 个 9，承诺延迟不超过 100ms 3、RBI 口碑好 4、核心能力采用容器化架构，也可以私有化部署。	1、缺少 API，没有基于 API 的 CASB、DLP 方案 2、ZTNA 评分是不透明的 3、销售合作伙伴和 MSSP 合作伙伴缺乏
	Versa	SSE 产品是 Versa SASE，还提供广域网边缘基础设施产品。 客户范围包含从许多行业的中型到超大型组织。	1、数据安全方案能力强，包括对指纹识别、加密、水印、编辑和其他高级操作的支持。 2、网络技术能力强，在现有广域网边缘基础设施上叠加 SSE，安全能力领先于专注于 SD-WAN 的厂商。	1、UI 复杂。 2、主要面向现有的 SD-WAN 客户。 3、技术文档质量差，学习难度高。

	Forcepoint	SSE 产品包括： 云安全网关、CASB、私有应用访问产品 客户范围从许多行业的小型组织到大型组织	1、提供了风险用户的仪表板视图，支持自定义策略来评估用户风险和采取策略。 2、集成 DLP 和 RBI 功能，不单独收费。	1、组件集成度差，需要多个控制台。 2、缺少 iOS 和 Android 的代理客户端。 3、客户端 F1E 的故障排除有问题，厂家支持质量和响应能力下降。 4、ZTNA 只支持 web 应用访问，导致使用率低。

表 1 Gartner 2022 年 SSE 魔力象限厂家概述

5.3 国内厂商概况

随着 SSE 概念的兴起，国内有不少安全企业也积极探索 SSE 产品和服务。

国内 SSE 厂商概况如表 2 所示。

厂商	提供能力	技术特点	主打场景、主打行业
绿盟	FWaaS 高级威胁防御 安全 Web 网关 Web 应用防火墙 ZTNA 上网行为管理 入侵防护	多种代理转发模式 安全防护+安全运营	主打场景： 远程办公、对外业务防护、多分支办公 主打行业： 政府、企业、教育、能源、医疗、金融
奇安信	FWaaS 高级威胁防御 安全 Web 网关 Web 应用防火墙 数据防泄露 ZTNA	安全防护+安全运营 （攻防实战）	大型央国企 政府行业 教育行业 金融行业 远程办公
深信服	SWG ZTNA CASB 高级威胁防御 数据防泄漏	基于云原生技术的 POP 点 集成防火墙和 SDWAN	主打场景：多分支上网安全、组网安全、混合办公安全、业务安全访问 主打行业场景：企业多分支、教育城域网、政务服务（税务分支、公积金营业厅等）、金融营业厅等
天融信	ZTNA SWG CASB 高级威胁防御 数据安全控制 数据防泄漏	综合安全能力	各类云化场景 远程办公场景 政府行业 卫生行业

新华三	FWaaS Web 应用防火墙 IPS/IDS DDoS ZTNA 防病毒	安全防护+安全运维+安全运营服务	主打场景： 远程办公、分支访问 主打行业： 运营商、政府、医疗、教育、金融、能源、企业
网宿安全	DDoS Web 应用防火墙 BOT 和 API 安全 ZTNA FWaaS SWG	基于全球边缘计算 POP 的企业基础设施和应用安全防护、集成 SD-WAN 和零信任的企业办公安全	主打场景：远程办公、多分支办公、对外业务防护 主打行业：金融、政府、企业、教育、能源、互联网

表 2 国内厂商概述[3]

6 结语

企业数字化转型和业务上云是 SASE 的重要驱动力。由 Gartner 在 2019 年提出的 SASE 架构预计会成为网络安全架构的一种最佳实践。而落地的过程中，我们可以看到，因为用户网络基础设施的建设进程和厂商自身的技术优势和选型，SASE 发展出一可独立交付的产品形态 SSE。

作为 SASE 的一个分支，独立的安全服务交付能够更好的融入用户当前的网络建设当中，提供上网安全、SaaS 应用防护和移动办公安全等服务。因无需改造网络基础设施，因此 SSE 提供用户一个过渡到 SASE 更优雅的选择。在中国落地发展的过程中，因为行业属性和数据合规的要求，出现了不少私有化的需求，企业通过本地化的部署实现专有的 SSE 服务。我们相信，如同公有云和专有云的发展，公有和专有 SSE 也会在中国均衡的发展，满足不同行业用户的需要。除了专有 SSE 的发展，我们很兴奋的看到有厂商对 IoT 场景的探索，进一步的扩大了 SASE 的应用场景。因为 SASE 能非常好的适应与解决广泛接入终端的安全架构，拥有更多离散接入的 IoT 场景无疑也是 SASE 未来一个非常大的发展方向，期待明年能看到有更多的厂商参与带来更多的最佳实践。

最终，希望通过这份解读能够帮助用户和行业参与者，对 SSE 和其在全球的发展能够有更多理解。让 SASE 这类的技术可以在中国加速的应用和发展，以领先全球的形态和技术出现，守护各行各业的网络安全。

[3] 注：厂商信息主要来源于 CSAGCR 联盟成员单位，若有缺失，欢迎联系 CSAGCR SASE 工作组补充。

CSA GCR cloud security alliance GREATER CHINA REGION ®

Cloud Security Alliance Greater China Region

扫码获取更多报告

云安全联盟大中华区
官网：https://c-csa.cn 电话：0755-86548359
地址：上海市浦东新区东育路255弄5号3FB30（前滩国际经济组织集聚区）/
广东省深圳市南山区粤海街道北京航空航天大厦1号楼905