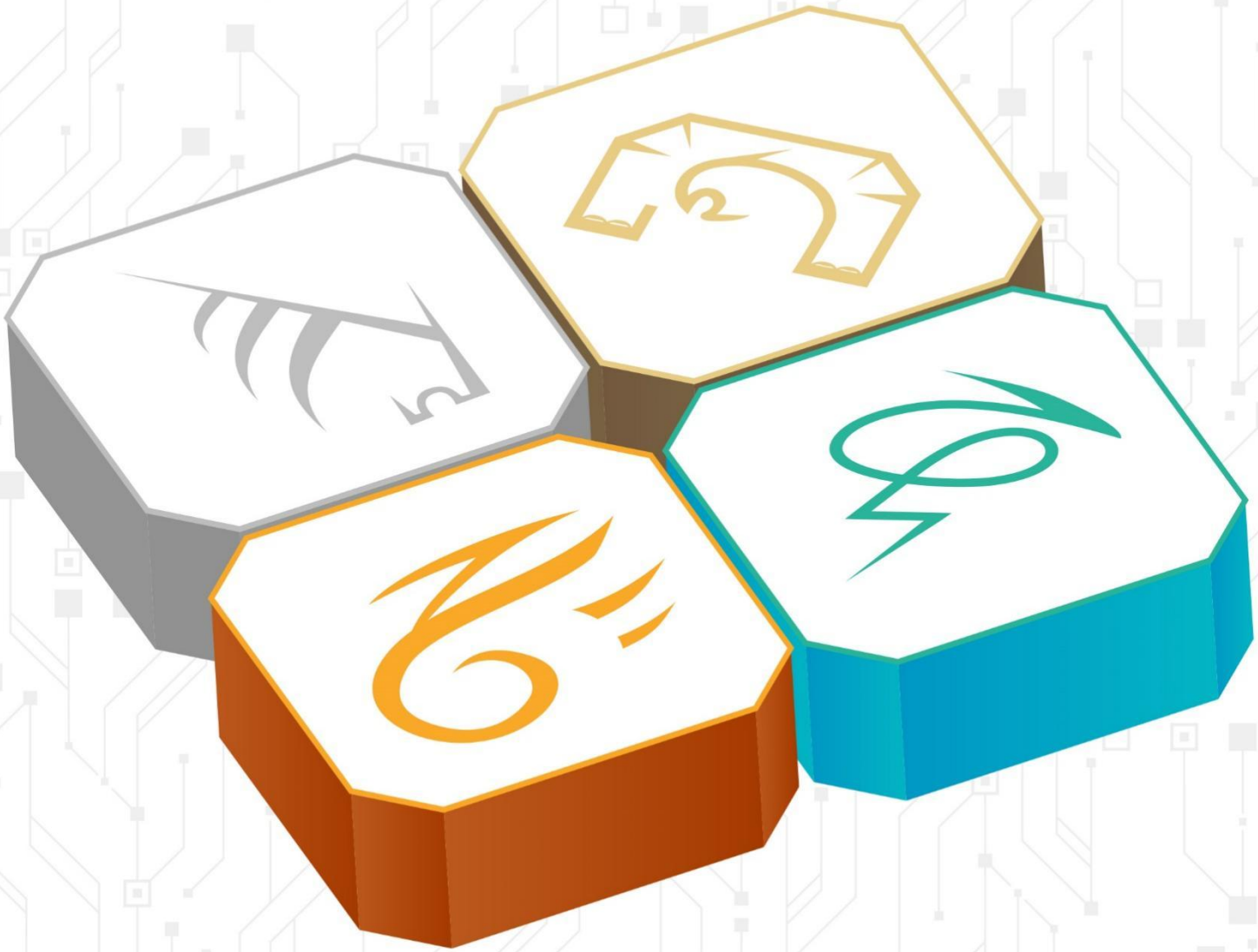
CSA GCR cloud security alliance
GREATER CHINA REGION ®

SASE 神兽方阵报告 (2024)



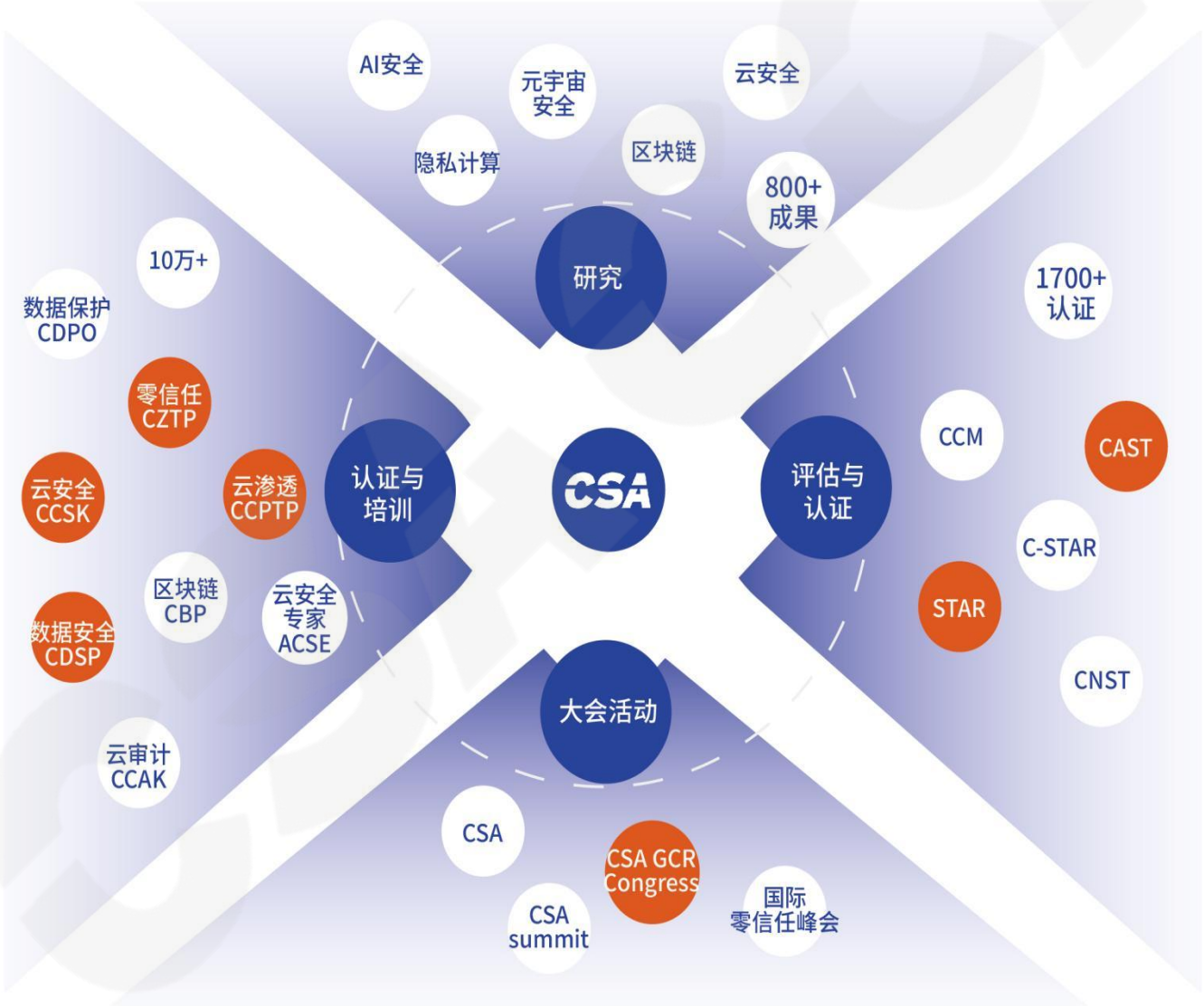
联盟简介

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

《SASE 神兽方阵报告（2024）》由云安全联盟大中华区组织专家撰写，感谢以下专家的贡献：

主要贡献者

何国锋	穆域博	司玄	赵福辰
余思阳	郭鹏程	姚凯	苏泰泉
钟施仪	丁安安	李乐天	唐双林
潘万鹏	欧建军	罗智杰	卜宋博
闭俊林			

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。

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

目录

1 摘要

随着企业办公移动化、应用分布式部署以及业务流量多向流动，传统网络边界逐渐模糊甚至瓦解。网络、安全与云服务割裂运作的模式难以应对复杂需求，急需一种融合一体化的解决方案来整合网络、安全与云，重塑企业网络架构。

安全访问服务边缘（SASE，Secure Access Service Edge）作为一种结合了广域网接入和云端安全的框架理念，通过集成 SD-WAN、零信任等多种网络与安全功能，在云平台上实现统一管理和交付。SASE 通过将安全执行点部署至靠近用户的边缘节点，有效整合云、网络与安全体系，简化架构、提升威胁响应速度、减少安全漏洞，并为企业提供灵活、高效的安全网络环境。

云安全联盟大中华区综合考量技术领先性和市场影响力，对参与调研的 SASE 厂商中评选出 16 家标杆企业，涵盖头部厂商、技术实力突出的厂商以及快速成长的新兴企业。

报告显示，SASE 市场具有以下特点：在安全能力方面，零信任已成为标配，部分厂商深入支持防火墙即服务、安全网关即服务和数据安全等核心能力；在网络能力方面，SD-WAN 作为 SASE 技术核心，支持网络接入、流量分析和灵活组网，但高级功能如网络加速和编排的应用仍需加强。用户需求集中在网络攻击防护、资源弹性伸缩和合规性保障三大方面，覆盖制造业、政府、通信和金融等多个行业。

未来，SASE 将通过统一安全管理和运营平台，构建“云网安”一体化防护体系。随着市场对智能化、一体化解决方案需求的增加，SASE 在全球范围内的应用将持续快速增长，为企业数字化转型提供更加全面的技术支撑。

2 SASE 简介

2.1 SASE 诞生的原因

随着云计算、物联网、5G 等关键技术的不断突破发展，企业数字化转型节奏越来越快。企业为提高核心竞争力，其业务部署环境越来越多样，包括传统的 IDC 机房、私有云、多云、混合云等，同时业务访问端也由单一的内部用户扩展到企业分支用户、企业合作伙伴、远程移动办公终端等。

在这个过程中，安全紧随企业的网络和业务架构演进而发展。数字化转型兴起之前，企业业务流量总量不大、流量以内部流转为主、移动办公需求少且默认企业内流量安全，这种情况下集中式安全栈方案得到大规模应用，这种以企业自建数据中心为核心的中心辐射型网络拓扑备受企业青睐。

近几年，随着云端 SaaS 应用普及和企业员工分散导致企业互联网流量增多，中心辐射型网络架构面对高成本的 MPLS 链路、总部集中上网应用访问体验差、安全边界绕行及总部 VPN 容量挑战等问题，不得不顺势改变网络及安全建设思路。在此阶段 SDN 及 NFV 技术的发展促使企业在云端部署统一网络指挥中心成为可能，分支和总部互联可通过更便宜和更大的互联网宽带进行以分散专线压力。同时，对于远程用户来说，云端部署的安全接入网关类服务能够有效解决集中接入的体验和安全问题，此时云端或者总部集中提供网络调度和近源安全监测防护理念越来越深入人心。

随着数字化转型和上云趋势的演进，越来越多的公有云厂商，甚至有全球业务的 ICT 厂商、互联网厂商都在建设自己的数据中心，这些数据中心随着企业业务的不断扩张，业务范围越来越广，服务数量越来越多，连通性越来越好。也许，是受“云”资源共享商业模式的启发，有声音提出此类拥有全球互联数据中心的企业是否可以将这种互联骨干网作为资源共享出去，企业想要访问的多云、公共 SaaS、互联网等连通问题由此骨干网解决，有互联需求的其他中小型企业均可以把流量引入这张网络中进行流转，同时为了降低时延提供统一的网络就近接入点，在此类接入点上同时部署身份校验、威胁发现、行为监控等按需增值安全服务，这实际上就是当前比较火热未来会成为趋势的安全访问服务边缘 SASE

模型。

Gartner 在 2019 年正式提出了安全访问服务边缘（SASE，Secure Access Service Edge）的概念，通过对 SASE 的定义理解，我们可以认为 SASE 是企业网络和业务架构演进至“云化”“服务化”后的自然而然的安全理念。

2.2SASE 的定义

SASE（Security Access Sevices Edge），即安全访问服务边缘，是 Gartner 于 2019 年在《网络安全的未来在云端》提出的一种网络架构，其定义是 “一种结合了广域网功能和全面的网络安全功能（例如 SWG、CASB、FWaaS 和 ZTNA）的新兴产品，能满足数字化企业的动态安全访问需求。”，SASE 并不是单独的独立系统，而是包含一套技术，从 SD-WAN 和云访问安全代理（CASB）到安全的 web 网关、零信任网络访问（ZTNA）、防火墙即服务（FWaaS）和微分段。除了这些核心功能外，一些 SASE 供应商还会提供其他相关技术，包括 Web 应用程序、API 保护、远程浏览器隔离，以及网络沙箱等。

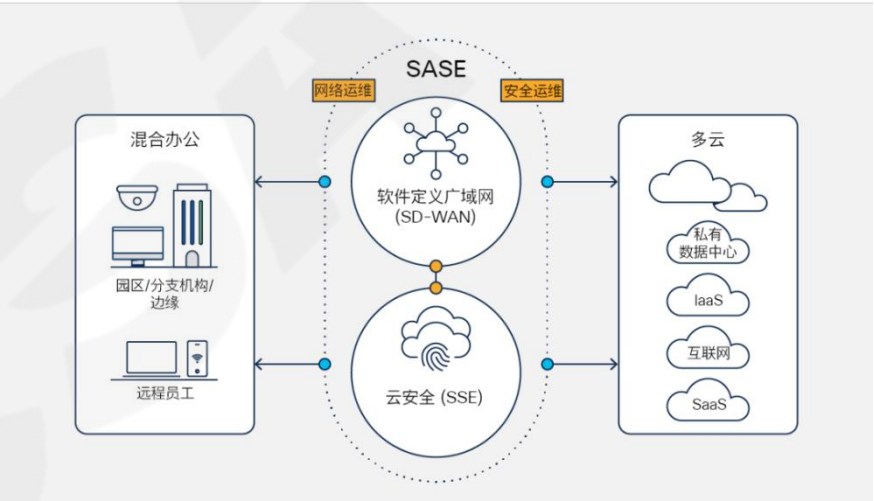


图 1 SASE 帮助实现网络和安全运维的融合

将网络和安全领域相融合可提供对每个连接的端到端可视性，让这两个领域的管理员齐心协力地优化应用体验。集成的工具和集中的控制面板能够提高效率并增进协作。SASE 能够提供这样的融合环境以及集中的统一管理，是一种从根本上简化安全和网络运维的方式（图 1）。

与此同时，SASE 可以为企业提供全网流量的可见性，包括本地、云和移动

端访问应用和互联网的流量，甚至也包括分支之间的流量。此外，SASE 可提供一系列丰富的网络和安全功能，对流量进行安全检测与路由转发，实现企业全流量的威胁检测与控制，并根据应用优先级进行路由，以确保用户访问应用的体验与安全合规均可得到保障。

根据以上定义，SASE 有四个主要特征：

1) 身份驱动

不仅仅是 IP 地址，用户和资源身份决定网络互连体验和访问权限级别。服务质量、路由选择、应用的风险安全控制——所有这些都由与每个网络连接相关联的身份所驱动。采用该方法，公司企业为用户开发一套网络和安全策略，无需考虑设备或地理位置，从而降低运营开销。

2) 云原生架构

SASE 架构利用云的几个主要功能，包括弹性、自适应性、自恢复能力和自维护功能，提供一个可以分摊客户开销以提供最大效率的平台，可很方便地适应新兴业务需求，而且随处可用。

3) 统一边缘访问

SASE 为所有公司资源创建了一个网络，覆盖数据中心、分公司、云资源和移动用户，并积极建设“最后一公里”访问方案，确保不同边缘的流量以最佳方式流向 SASE 网络，然后从那里流向互联网、数据中心和应用程序等。举个例子，软件定义广域网 (SD-WAN) 设备支持物理边缘，而移动客户端和无客户端浏览器访问连接四处游走的用户。

4) 全球分布

为确保所有网络和安全功能随处可用，并向全部边缘交付尽可能好的体验，SASE 云必须全球分布。因此，Gartner 指出，必须扩展自身覆盖面，向企业边缘交付低延迟服务。

从能力层面来看，SASE 需要包含主要的网络和安全能力：

1) 网络即服务（Network as a Service）

- SD-WAN
- 服务质量保障 QoS

- 高级路由
- SaaS 加速
- 内容交付或缓存
- 广域网优化
- 分布式连接

2) 安全即服务（Security as a Service）

- FWaaS
- ZTNA/VPN
- 安全 Web 网关
- SSL 深度检测
- 云沙箱
- IPS 入侵防御系统
- CASB 云访问安全代理
- RBI 远程浏览器隔离

2.3 SASE 的核心优势

SASE 架构的目标是更容易地实现安全的云环境，它在集成管理、安全保障、性能提升、良好体验、资源优化访问方面具有核心优势：

1) 网络和安全集成简化管理和运营

传统的网络安全模型依赖于多个独立的解决方案来保护网络边界，SASE 通过集成网络和安全功能到一个云交付平台，简化了管理和运营，减少了资本支出和运营成本，并且 SASE 允许企业从单一控制点管理所有安全策略，简化了安全政策的制定和执行，减少了配置错误和安全漏洞的风险。

2) 基于零信任模型的安全性

SASE 支持基于身份的零信任安全模型，确保只有经过验证和授权的用户和设备才能访问特定的应用程序和服务，此外，SASE 提供了对网络请求的全面可见性，企业能够基于此实施细粒度的安全策略，确保数据隐私法规的合规性，并保护敏感数据。

3) 分布式访问带来的性能提升和良好体验

SASE 的访问机制可以在用户和云资源之间建立直接、安全的连接，而无需依赖数据中心进行连接。同时，通过 SD-WAN 技术，对网络流量进行优化，提高网络性能，其分布式架构为任何时间、任何地点的用户提供一致的优化体验。

4) 云服务交付优化 IT 资源

SASE 通过云服务的交付模式，减轻了企业在物理网络硬件、安全设备和数据中心上的投资和维护压力。

2.4SASE 的主要应用场景

SASE 通过整合 SD-WAN、防火墙即服务（FWaaS）、安全 Web 网关（SWG）等关键技术，形成了一个统一的服务平台，为企业的数字化转型提供了一种灵活、可扩展的安全架构，以支持企业的快速发展和变化，具有广泛的应用场景，包括并不限于：

- 混合办公

随着混合办公的日益兴起，传统 VPN 无法应对当前网络安全需求，SASE 能够提供就近接入的网络服务同时进行严格的身份验证和策略控制，能够确保办公人员访问企业资源时的安全性和稳定性。使得远程员工无论处于何地都可以安全地访问企业应用程序和数据。

- 多云环境

多云环境为企业带来了灵活性和可扩展性的同时，也带来了一系列挑战，如管理的复杂性、安全控制不一致，以及网络效率问题等，SASE 因其云原生特性和集成化的安全功能，可以帮助企业统一管理和保护跨多个云平台的资源，适应不断变化的云环境。

- 多分支场景

对于拥有多个分支机构的企业，SASE 可以通过简化广域网部署和强化连接实体的安全合规来提升网络的敏捷性和安全性。SASE 的分布式架构允许企业在各个分支地点轻松部署服务，同时确保一致的安全策略。

- 企业防护

依靠 SASE 对边缘的安全强化，企业可以按需部署 SASE 边缘的安全能力服务，包括物联网的连接和安全访问，弹性扩容。同时，能够实现企业内部应用暴露面收敛，员工只有通过 SASE 的 POP 点才能访问到自身权限允许的应用，实现更安全、更隐私、更稳定的访问体验。SASE 统一管控安全能力和企业访问行为，在管控平台统一实现配置、管理、维护等。

3 神兽方阵报告简介

3.1 报告介绍

云安全联盟大中华区在 2022 年《SASE 安全访问服务边缘白皮书》的基础上，对当前市场进行了全面调研与分析，形成了《SASE 神兽方阵报告（2024）》。该报告是一份专注于 SASE 领域、面向中国企业发展的专业分析报告，从技术领先性和市场影响力等多个维度，对 SASE 及其相关安全解决方案进行了全面的评估。

调研发现，在安全能力方面，大多数 SASE 产品已具备零信任基础能力、防火墙即服务（FWaaS）、安全网关即服务（SWG）和数据安全支持，成为解决方案的核心组成。然而，仅有少数厂商支持身份大数据分析，这反映出 SASE 在身份认证与安全分析领域仍存在较大的提升空间。

在网络能力建设方面，大多数厂商具备 SD-WAN 的基础功能，包括网络接入、流量分析、灵活组网以及网络冗余等关键能力。同时，SASE 厂商分布较为均衡，网络/云服务厂商和安全厂商各占半壁江山，少数新创企业也在快速崛起。其中，网络服务商更注重通过 SD-WAN 构建一体化的网络架构，而安全服务商则专注于整合多样化的安全能力。

调研发现，SASE 的用户群体覆盖广泛，涵盖制造业、政府与事业单位、通信、金融等多个行业，主要需求集中在网络攻击防护、资源弹性伸缩和合规性保障三大方面。随着数字化转型的深入，企业对网络和安全的需求逐渐融合，SASE 作为一种全新的解决方案，正逐步走向成熟和普及。

3.2神兽方阵模型

神兽方阵（Mythical Creatures Matrix）模型是云安全联盟大中华区基于中国传统文化“神兽”形象创立的分析数字科技企业的数学工具，适用于对数字科技企业在技术、产品成熟度、市场营销及服务等方面的能力与先进性的分析。神兽方阵模型从技术领先性、市场影响力、专家评审、公开路演四个维度评估，在基于企业数据定量分析的基础上，结合各重点行业业务专家和安全专家组成的评审团的谨慎评估，确保评估结果的专业性与公平性。

神兽方阵以“四象”即青龙、朱雀、白虎、玄武为基础。“四象”又称“天之四灵”，分别是中国古典神话中镇守东南西北四方的神兽，其中青龙为东方之神，是四灵之首；朱雀为南方之神，有浴火重生的能力；白虎为西方之神，也是战斗之神；玄武为北方之神，以防守见长。模型的创立旨在为网络安全领域树立具有中国特色科技标杆企业的行业分析。神兽方阵示意图及该模型中各神兽定位与描述如下。

图 2 神兽方阵模型图

- **青龙神兽企业 - 综合领先型企业**：在 SASE 领域投入高，且研发能力、产品成熟度、市场营收及知名度等方面整体实力强的头部企业。
- **朱雀神兽企业 - 技术深耕型企业**：SASE 产品具备核心竞争力或者技术

壁垒，技术研发实力强，产品成熟度高，并且有良好的市场占有率的企业。

- **白虎神兽企业 - 快速进击型企业：**对市场需求能迅速作出反应，SASE 产品的实现与迭代速度快、产品创新能力强，并且市场占有率高的企业。
- **玄武神兽企业 - 新兴探索型企业：**在 SASE 领域具备成长潜力和市场探索力的企业，在技术研发和市场等方面成长迅速，具备强劲的潜力。

继 2022 年发布《中国零信任神兽方阵分析报告》和 2023 年发布《数据安全平台神兽方阵报告》之后，本报告专注于 SASE 领域。未来，云安全联盟大中华区还将持续推出覆盖云安全、AI 安全、移动安全和隐私科技等方向的专业报告，

4 SASE 神兽方阵

4.1SASE 神兽方阵入选企业

CSA 大中华区综合考虑了企业的行业概况、商业模式、企业竞争力等因素，分别对应各神兽方阵数据模型的入选标准，筛选出一批在 SASE 领域具有一定市场规模，在业界有一定知名度和影响力，或者处于起步阶段但技术实力强和快速成长阶段的企业，作为 2024 年 SASE 神兽方阵评选的标杆企业。本次共 16 家，其中青龙神兽企业 4 家，朱雀神兽企业 4 家，白虎神兽企业 4 家，玄武神兽企业 4 家。

图 3 2024 SASE 神兽方阵

- **青龙神兽企业-综合领先型企业：**深信服科技股份有限公司、奇安信科技集团股份有限公司、网宿科技股份有限公司、天翼安全科技有限公司（4 家）
- **朱雀神兽企业-技术深耕型企业：**贵州白山云科技股份有限公司、杭州亿格云科技有限公司、中国电信股份有限公司上海研究院、北京火山引擎科技有限公司（4 家）
- **白虎神兽企业-快速进击型企业：**北京神州绿盟科技有限公司、新华三信息安全技术有限公司、联通（广东）产业互联网有限公司、启明星辰信息技术集团股份有限公司（4 家）
- **玄武神兽企业-新兴探索型企业：**江苏易安联网络技术有限公司、北京安数云信息技术有限公司、数篷科技（深圳）有限公司、锐西科技（北京）有限公司（4 家）

4.2SASE 神兽方阵入选企业介绍与点评

4.2.1 深信服科技股份有限公司

（一）简介

深信服科技股份有限公司是一家专注于企业级安全、云计算及 IT 基础设施的产品和服务供应商，其产品线涵盖安全运营、数据安全、终端安全、安全托管服务等领域。2020 年首次发布 SASE 的产品，基于容器和 K8S 编排技术的云原生架构，具备 SASE-ZTNA 零信任网络访问、SASE-SWG 互联网安全访问、SASE-XDLP 可扩展防泄密、SASE-GA 全球加速的安全能力，覆盖安全组网、混合办公、多分支上网安全等多种场景。

（二）点评

深信服基于多年安全领域的技术沉淀及行业实践，通过将零信任、SASE、SD-WAN 等产品能力整合，完成 SASE 产品的体系化解决方案落地，在 SASE 云原生架构、主动防御能力、策略一致性管理等方面均有较好表现。业务在国内及海外均有良好覆盖，在满足用户安全需求的同时，关注用户网络服务体验。产品及方案已在政府、金融、央企、能源在内的诸多行业全面落地，在技术研发和市场营收方面均表现突出，属于 SASE 安全领域的领军者之一。

4.2.2 奇安信科技集团股份有限公司

（一）简介

奇安信科技集团股份有限公司专注于网络空间安全市场，向政府、企业用户提供新一代企业级网络安全产品和服务，在人员规模、收入规模和产品覆盖度上均位居行业前列。2022 年 3 月 13 日，奇安信圆满完成了北京冬奥会和冬残奥会网络安全保障工作，兑现了北京冬奥会网络安全“零事故”的承诺。奇安信于 2021 年发布 SASE 产品，推出安全访问服务（Q-SASE），基于统一的安全防护与运营服务架构，以相对轻量化的投入、简易的部署，实现安全管理与运营的降

本增效，助力政企客户应对数字化转型的安全新挑战。

（二）点评

奇安信 SASE 解决方案主要基于一体化安全管理运营服务平台，集合 SD-WAN、云安全资源池（NGFW、IPS、SWG、DLP、WAF、终端安全等）、零信任等多维度能力，升级安全服务化模式，提供端网云协同的全程安全访问保障。奇安信具备完整的安全产品线，在 SASE 安全能力集成种类方面表现出色。此外，具备强大的生态能力和市场能力，在服务保障、品牌推广、国内外标准起草方面整体表现较好，总体属于 SASE 安全领域的领军者之一。

4.2.3 网宿科技股份有限公司

（一）简介

网宿科技股份有限公司是全球领先的信息基础设施平台服务提供商，专注于边缘计算、云分发、云安全、云计算、云服务及绿色数据中心业务，帮助企业技术创新实践。网宿 SASE 产品 SecureLink 发布于 2020 年，基于全球网络和计算平台，构建 SASE 一体化架构，实践全面零信任，帮助企业解决办公安全碎片化问题，为企业打造更安全、更高效、更便捷的办公访问体系，适用于远程办公安全、数据防泄露、威胁入侵防范、IT 效率增效等场景。

（二）点评

网宿科技基于已有的 CDN 网络及云服务新增安全服务，通过融合零信任访问 ZTNA、威胁检测与响应 XDR、数据安全治理 XDLP、IT 效率管理、安全 SD-WAN 和统一态势管理进行全流量的防护，形成 SASE 一体化的下一代办公安全访问体系。网宿通过端、平台、网深度融合，实现一体化网络及安全运营，基于其丰富的基础设施及成熟的网络管理技术，在能力覆盖、网络适配等方面表现优异，总体属于 SASE 安全领域的领军者之一。

4.2.4 天翼安全科技有限公司

（一）简介

天翼安全科技有限公司通过整合中国电信云网、安全、数据等优势资源和能力，为内外部客户提供云网安全、数据安全、信息安全等各类安全产品和服务。中国电信云脉 SASE 发布于 2023 年，面向办公场景提供办公安全一体化解决方案，以标准 SaaS/场景化定制等多元服务模式为全行业用户办公场景提供零信任网络访问、终端安全防护、上网行为管理、数据外发管控、网络加速、安全组网、身份识别与访问管理等多种安全能力，一站式解决企业办公全场景需求。

（二）点评

天翼安全云脉 SASE 产品采用云原生一体化安全架构，聚焦企业办公场景，提供零信任、数据防泄露、终端安全等安全防护能力，将安全以统一的服务化形式交付，满足企业数字时代混合办公安全管理需求。天翼安全依托运营商自身网络和安全技术优势，构建“云网安”一体化能力，在业务覆盖方面表现优秀。此外，凭借国有企业背景及强大的市场渠道优势，产品在多个行业全面落地，总体属于 SASE 安全领域的领军者之一。

4.2.5 贵州白山云科技股份有限公司

（一）简介

白山云是国内领先的边缘云服务提供商，建立了遍布全球的边缘网络，超过 1700 个边缘节点，储备带宽 80T+ ，海外防御能力 4.5T+，遍布海内外城市 300+，每日处理全球请求数 6000 亿+，已覆盖互联网、政府、电商、游戏、能源交通、金融、制造、医疗、地产等众多行业，在更靠近用户的互联网边缘端为 1000+家企业及其终端用户提供高速、安全及经济的数字体验。

（二）点评

白山云科技在 SASE 领域的表现令人瞩目，其以强大的技术创新能力和全球

服务网络为基础，提供了全面的 SASE 解决方案。公司不仅在边缘云服务领域积累了丰富的经验，而且在 SASE 产品的研发上展现了前瞻性。白山云的 SASE 产品通过整合零信任网络访问、数据防泄露、威胁检测与响应等关键安全技术，为企业提供了一个安全、高效、便捷的办公访问体系。白山云在产品研发和市场占有率的综合表现，使其成为 SASE 领域的佼佼者之一。

4.2.6 杭州亿格云科技有限公司

（一）简介

杭州亿格云科技有限公司是 SASE 安全服务商，通过自主研发的 SASE 服务平台—亿格云枢，产品提供包括零信任网络访问（ZTNA）、数据防泄漏（XDLP）、威胁检测响应（XDR）、防病毒（EPP）、上网行为管理（SWG）和统一端点管理（UEM）等功能，帮助企业以更低成本、更高效率建设更加安全、更好体验的下一代办公场景的安全体系，从而解决企业数字化转型过程中遇到的混合和分支办公安全、数据安全、终端安全等问题。

（二）点评

亿格云的 SASE 产品设计理念以人为中心，构建了一个零信任安全体系，这与传统基于边界的安全防护体系形成了鲜明对比。其安全数据的天然融合和无限云算力的深度挖掘，使得亿格云枢在安全融合、威胁处置闭环以及安全数据溯源方面展现出显著优势。在数字化转型的浪潮中，亿格云为企业提供了一个安全、高效、低成本的下一代办公场景安全解决方案，有效解决了混合和分支办公安全、数据安全、终端安全等挑战，是 SASE 领域的优秀企业。

4.2.7 中国电信股份有限公司上海研究院

（一）简介

中国电信股份有限公司研究院自成立以来致力于 5G 通信、网络安全、云网内生安全、Web 应用安全、网络攻防、量子密码等方向的研究，研发了 SASE、

深度威胁检测等在内的多个网络安全自研产品。科研成果和开发项目多次获得部级和上海市优秀科研成果奖，一大批拥有自主知识产权的科研成果在集团内得到广泛应用，并获得了良好的经济效益和社会效益。当前，上海研究院正以 SASE 架构为核心，结合软件定义广域网和零信任网络接入服务，致力打造云网安融合的架构体系。

（二）点评

电信上研院依托于强大的研发背景和专业团队，不仅在 5G 通信和云网安全领域取得了突破，更在 SASE 架构的实践中取得了显著成就。其自主研发的 SASE 产品，融合了软件定义广域网和零信任网络接入服务，为构建云网安融合的架构体系提供了有力支撑。电信上研院的 SASE 解决方案，以其深厚的技术积累和创新能力，在行业内树立了新的标杆，为推动网络安全技术的发展和应用做出了积极贡献。

4.2.8 北京火山引擎科技有限公司

（一）简介

北京火山引擎科技有限公司成功的 SASE 解决方案，旨在为企业提供更加安全、高效、智能的网络访问服务。通过一个集中化平台融合 IAM、ZTNA、CASB、SD-WAN 多项安全能力与全球化办公组网资源，在持续评估身份、网络、终端可信状态的基础上，通过智能动态引擎跨模块打通数据与控制点，真正实现落地。

（二）点评

火山引擎的 SASE 产品以其“All in One”的创新架构，实现了 IAM、ZTNA、CASB、SD-WAN 等多种安全能力的融合，展现了其在产品创新方面的领先地位。通过一个集中化平台，火山引擎不仅提升了数据的整合效率，还实现了管理的统一性，这在简化企业 IT 管理流程和提升办公效率方面具有显著优势。其 AI 大模型的应用，通过动态引擎的智能分析和推理能力，进一步增强了风险识别和处置的自动化水平。火山引擎的 SASE 产品在技术创新和市场应用方面均展现出强大

的竞争力，是 SASE 领域的重要参与者。

4.2.9 北京神州绿盟科技有限公司

（一）简介

绿盟科技自 2021 年发布 SASE 产品以来，积极布局该领域市场，为全球客户提供集成零信任、SD-WAN、安全网关（SWG）、防火墙即服务（FWaaS）等多重安全与网络融合能力的服务。绿盟科技的 SASE 产品专注于实时身份认证、动态权限调整和身份大数据分析，提供全方位的零信任安全控制，满足企业复杂环境下的多场景需求。其产品已在国内外设立了共计 53 个节点，确保国内外用户的网络访问速度和安全性，并且获得了不少奖项来证明其产品的实力。绿盟科技的 SASE 解决方案广泛应用于金融、能源、制造、医疗等多个行业，并通过灵活组网和跨国网络加速功能，助力企业实现安全合规的同时，提升业务效率。

（二）点评

绿盟科技在 SASE 领域具有显著的技术优势，其产品集成零信任、SD-WAN、SWG、FWaaS、CWPP、SOC 等多重安全功能，支持实时身份认证和动态权限调整，满足企业在多地域、多行业场景中的安全需求。凭借广泛的国内外节点布局，以及对各种应用场景增强配置，如云计算、工业互联网、物联网等，绿盟科技的 SASE 服务具备较强的可达性和可靠性，为客户提供灵活、安全的网络连接解决方案，也被市场及客户所接受和认可。

4.2.10 新华三信息安全技术有限公司

（一）简介

H3C 是新华三集团旗下的数字化解决方案提供商，以“云-网-安-算-存-端”一体化战略为基础，深入布局网络和安全业务。其 SASE 产品于 2022 年发布，包含零信任、SWG（安全网关）、FWaaS（防火墙即服务）等功能，支持全球 300 多个节点的广泛布局，为企业提供端到端的安全访问与管理服务。该产品通过支

持灵活组网、流量分析和跨国加速等功能，为政府、教育、金融等多个行业提供了定制化安全解决方案，满足复杂的数字化应用需求。

（二）点评

H3C 的 SASE 产品凭借广泛的全球节点覆盖和强大的集成能力，具备显著的行业竞争力。产品功能涵盖零信任安全、SD-WAN、SWG 等多种能力，提供一站式的网络安全服务，并通过 AI 和机器学习技术提升平台智能性。H3C 已获得行业协会奖项及第三方机构的专业推荐，显示出其技术方案在 SASE 市场中的认可度和领先地位，为企业数字化转型提供了稳固的安全支持。

4.2.11 联通（广东）产业互联网有限公司

（一）简介

广东联通产互成立于 2017 年，是中国联通集团旗下的产业互联网公司，专注于为各行业提供安全可靠的数字化解决方案。自 2022 年推出 SASE 产品以来，公司将零信任、FWaaS（防火墙即服务）、WAF（Web 应用防火墙）和安全沙箱等安全能力集成到统一平台中，帮助客户构建基于“云+数+安+AI”的安全体系。该 SASE 产品支持网络冗余、流量分析和统一管理功能，致力于提升政府、教育、金融、医疗等行业客户的网络安全防护能力，为超大城市安全运营提供了标杆示范。

（二）点评

广东联通产互凭借其运营商背景和广泛的行业实践经验，在 SASE 产品中融入了零信任和多维度的安全检测技术，特别适用于需要高安全性和灵活部署的行业。其 SASE 产品通过集成多项安全防护功能与强大的管理能力，帮助客户轻松应对复杂的网络安全挑战。其 SASE 产品拥有多种专利，获得了不同奖项，最终取得了不同行业客户及市场的认可。

4.2.12 启明星辰信息技术集团股份有限公司

（一）简介

启明星辰是国内资深的网络安全企业，近年来响应数字化需求拓展至 SASE 领域。其 SASE 产品于 2023 年推出，注重多层次的安全融合，涵盖零信任访问控制、SD-WAN、FWaaS（防火墙即服务）和 CWPP（容器工作负载保护）等多种功能，帮助企业实现安全与网络服务的有机结合。产品支持实时身份认证、终端环境感知、动态权限管理等核心功能，广泛适用于制造业、商贸、电子等行业场景，致力于提升企业网络访问的安全性和灵活性。

（二）点评

启明星辰在 SASE 解决方案上表现出深厚的技术积累，尤其是在实现多层次安全防护和融合架构方面具备优势。其 SASE 产品不仅满足企业在网络访问控制中的安全需求，还通过简化的部署和一体化的管理，为企业提供高效的访问体验。启明星辰在各行业的广泛应用表明其方案兼具适用性与高性价比，能够有效支持企业的数字化转型。

4.2.13 江苏易安联网络技术有限公司

（一）简介

江苏易安联网络技术有限公司是中国最早一批从事零信任体系研究和相关技术研发的企业，目前推出多款基于零信任架构之下的网络安全产品，以及 ZTNA 零信任解决方案和 EnSASE 安全访问服务边缘解决方案，提供包括实战攻防、应急演练等安全服务。易安联在零信任领域积累了丰富的项目实施、运维经验，深入理解零信任安全领域的技术和市场动态。在数字政府、教育、运营商、能源等行业有丰富的大型零信任项目实施交付经验。

（二）点评

易安联的 SASE 产品在技术上基于零信任理念，构建强大的安全防护体系。

在网络连接能力上表现出色，可满足企业多样化的组网需求，智能选路和负载均衡等功能保障网络的高效性。安全方面，涵盖多种安全技术，如防火墙即服务、云访问安全代理等，能有效应对各种网络威胁。产品还具有良好的兼容性，可与多种云环境和企业现有系统适配，相关产品已经在数字政府、教育、运营商、 能源等行业有丰富的大型零信任项目实施交付。

4.2.14 北京安数云信息技术有限公司

（一）简介

北京安数云信息技术有限公司应用云计算核心技术，深度融入 SDN 功能，在自主研发的“云安全资源池”基础上，加载“安全生态圈”、安全能力的自动化编排调度响应（SOAR）、云安全互联网应用（SASE）等功能模块，形成自主研发的智能安全调度管理平台、智能安全运营管理平台，业界首家达到运营商级别，首家支持云安全自适应技术，在中国移动、中国电信、中国联通、广电、政务云等行业积累了超过 1000 家的客户。

（二）点评

安数云 SASE 产品致力于为企业提供一站式安全访问服务边缘解决方案，其云管端架构将网络与安全功能整合到统一云服务中，提供高效的一体化防护。其自主研发的智能安全调度运营管理平台（DCS-SASE）是业界首家达到运营商级别支持云安全自适应技术的厂商，能够完全满足运营商、政府、金融、能源、军工、医疗、教育等各行业用户的需求。这种定制化的解决方案有助于各行业用户更好地应对云安全挑战，提升业务安全性。

4.2.15 数篷科技（深圳）有限公司

（一）简介

数篷科技是专注企业数据安全的技术创新公司，致力于数据安全平台（DSP）的研发，通过提供符合零信任架构标准的数据安全解决方案，帮助企业建立更加

灵活柔性的网络安全架构，保障从端到云的数据流动安全，彻底解决企业在开放环境中使用数据的后顾之忧，实现全球无边界的数据安全和业务连续性。依托先进的安全理念、强大的技术实力、创新的解决方案，数篷科技的产品赢得了业界的广泛认可。

（二）点评

数篷科技出色整合多种安全与网络技术，SASE 产品覆盖软件定义广域网（SD-WAN）、零信任网络访问（ZTNA）、防火墙即服务（FWaaS）等，提供网络接入、灵活组网、流量分析、统一管理、实时身份认证、终端环境感知、身份大数据分析、统一身份管理等能力。其产品已经在多个场景中得到了广泛应用，如商业智能（BI）、研发环境、IT 外包、跨组织协作、远程办公等，能够为企业提供高效、安全的数据安全保障，值得业界关注。

4.2.16 锐西科技（北京）有限公司

（一）简介

锐西科技是一家数字安全创新技术服务提供商，总部位于北京，在长沙和沈阳设有产品研发和运营中心，有着覆盖全国的营销渠道网络。锐西科技拥有零信盾、锐西智联两大自主业务品牌，自主研发了 SDP 零信任访问控制系统、Web 应用保护系统、零信盾 5G 智能接入终端产品、锐智一体化业务安全智能终端等产品；业务覆盖云安全、物联网安全、身份安全、业务安全、数据保护多个领域。

（二）点评

锐西科技聚焦零信任业务安全，其 SASE 产品具备网络接入、灵活组网、流量分析、统一身份管理等能力。锐西科技拥有零信盾、锐西智联两大自主业务品牌，并自主研发了多款产品，如 SDP 零信任访问控制系统、Web 应用保护系统、零信盾 5G 智能接入终端产品以及锐智一体化业务安全智能终端等。作为一家相对年轻的企业，锐西科技 SASE 产品在网络安全领域具有较大的发展潜力。

5 分析与总结

SASE 有三个明显的标签：安全、网络、云。本次调研揭示了 SASE 厂商的两种主要业务集成方式：47.06%的厂商本身是网络或云服务提供商，通过集成安全服务来组成 SASE 解决方案；而 41.18%的厂商在安全领域有成熟积累，通过新增组网与接入服务来实现 SASE。

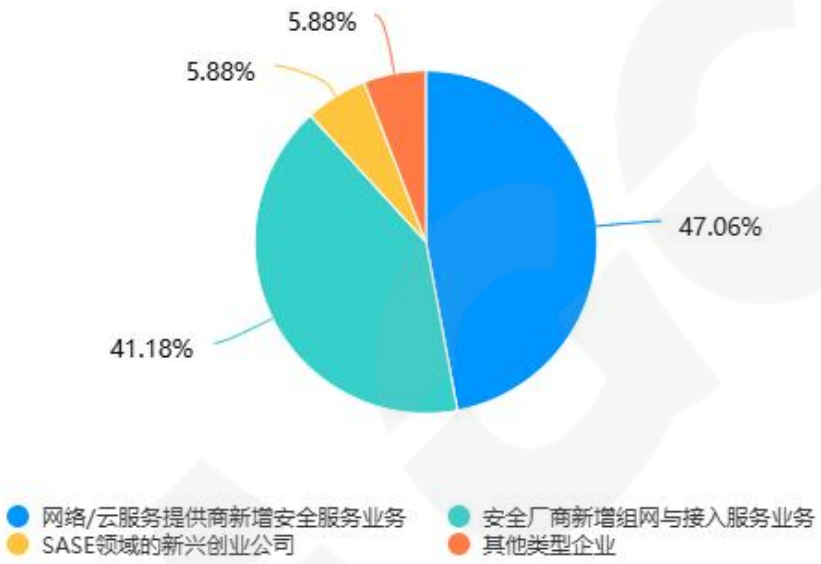


图 4 公司 SASE 业务路线

5.1 发现和结论

5.1.1 安全能力建设情况

根据调研结果，SASE 厂商普遍具备零信任基础能力，凸显了以身份为核心的管理在 SASE 技术中的重要性。然而，身份大数据分析支持的厂商比例较低，这表明在利用大数据技术进行身份认证和安全分析方面，SASE 市场仍有较大的发展空间和潜在需求。

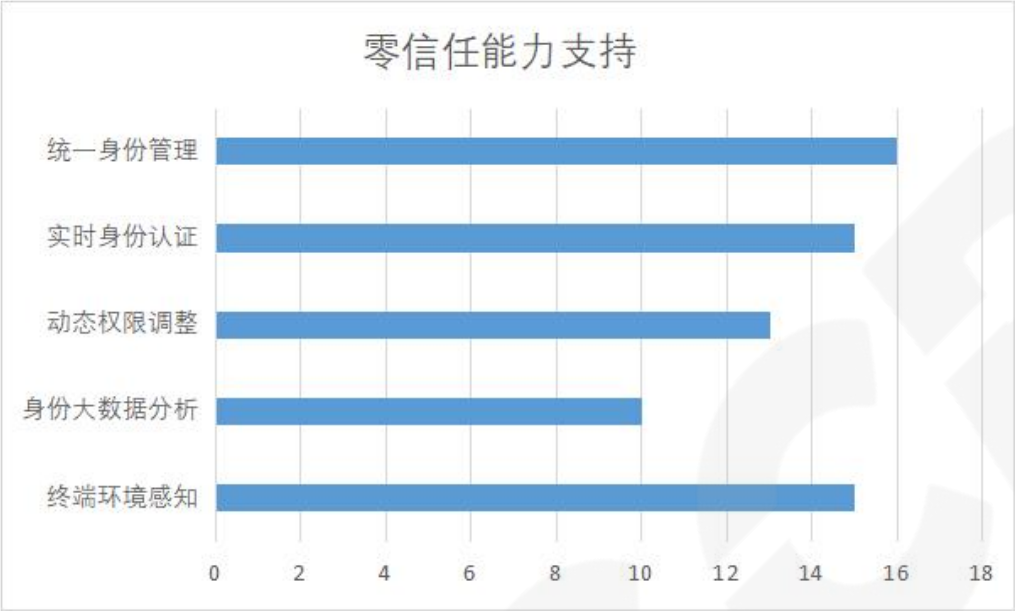


图 5 参选厂商零信任能力支持情况

在安全能力方面，SASE 厂商对防火墙即服务（FWaaS）、安全网关即服务（SWG）以及数据安全的支持较为深入，这些能力是构建 SASE 解决方案的关键组成部分。FWaaS 和 SWG 提供了网络层面的安全防护，而数据安全则关注数据在传输和存储过程中的保护。

国内市场中，SASE 产品的部署与云环境的关联性相对较低，这可能是由于国内企业对云服务的采用速度和模式与国际市场有所不同。因此，支持云访问安全代理（CASB）的厂商数量较少。

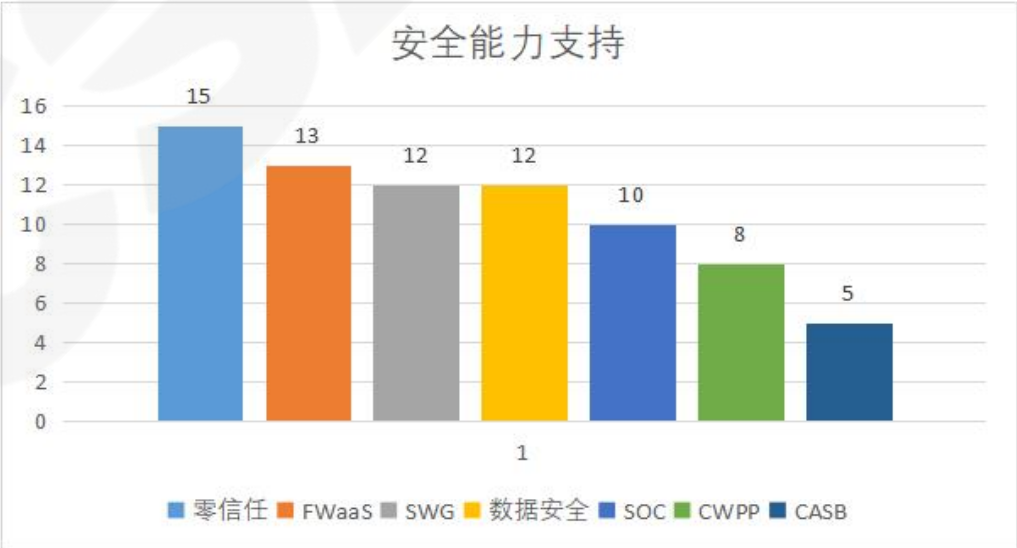


图 6 参选厂商安全能力支持情况

综上，可以看出安全访问服务边缘产品当前安全能力建设情况大致有以下几个特点：

- 零信任支持更加广泛：随着远程工作的普及和网络环境的复杂化，SASE 产品正越来越多地集成零信任服务，以确保所有访问点的安全性。
- 云安全服务需求较弱：当前 SASE 市场对云安全的需求和适配尚未达到预期水平，这可能与企业对云安全的认知和预算分配有关。
- 集成化的 SASE 服务：为了简化网络和安全管理，更多厂商开始提供集成化的 SASE 解决方案，将 SD-WAN 和网络安全服务合并，以提高效率和响应速度。

5.1.2 网络能力建设情况

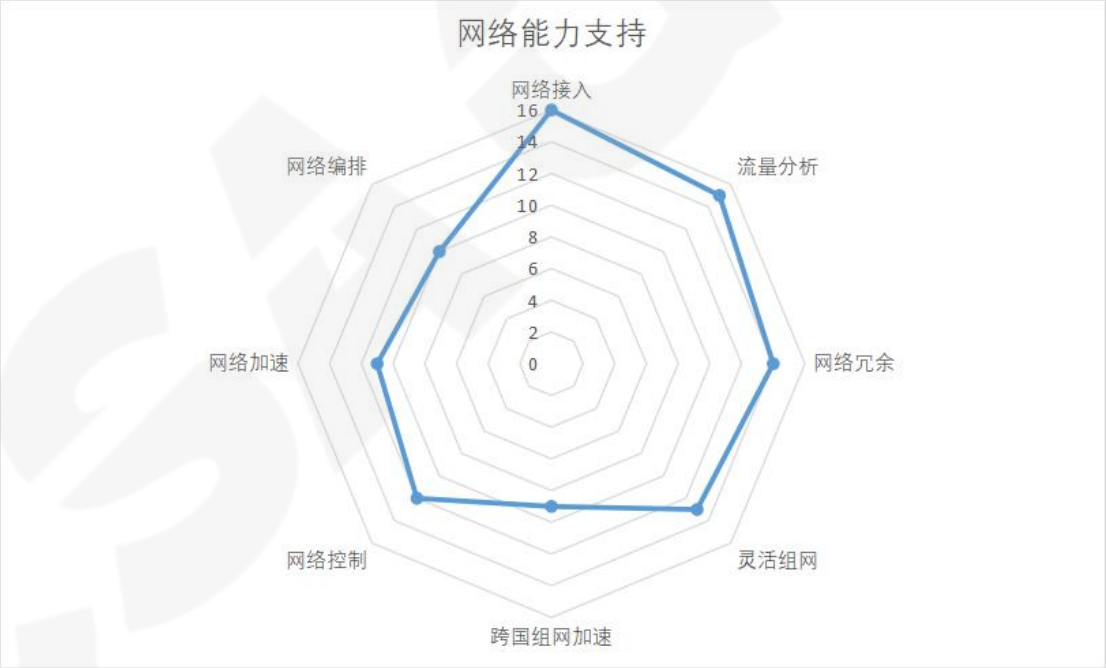


图 7 参选厂商网络能力支持情况

关于参选厂商 SD-WAN 部署情况，接受调查厂商基本具备 SD-WAN 基础能力，包括网络接入、流量分析、灵活组网并支持网络冗余，表明在 SASE 解决方案中，提供网络接入能力是相对成熟的解决方案。其中半数厂商支持网络加速、网络编排、控制等能力，证明市场对 SD-WAN 的高级功能需求可能还不够普遍，因此部分厂商根据目标市场和客户群体的不同，选择性地开发和提供特定的

SD-WAN 功能。

完全支持 SD-WAN 能力的厂商，也基本在海外部署大量节点和实体研发中心，以提供完整的海外接入支持和技术服务。

5.1.3 产品核心技术分析

本次参选的厂商中，网络/云服务厂商和安全厂商各占半壁江山，还有少数 SASE 的新创企业。不同服务商的能力支持各有差异，网络服务商强调通过 SD-WAN 组网构建一体化的网络架构，安全服务商更侧重于将安全能力进行整合，更方便地为用户提供服务。这表明当前的 SASE 产品多数基于供应商之前产品的积累，再进一步通过整合其他产品以达到 SASE 的“网络和安全融合一体化解决方案”的要求，因此能力侧重各有不同。

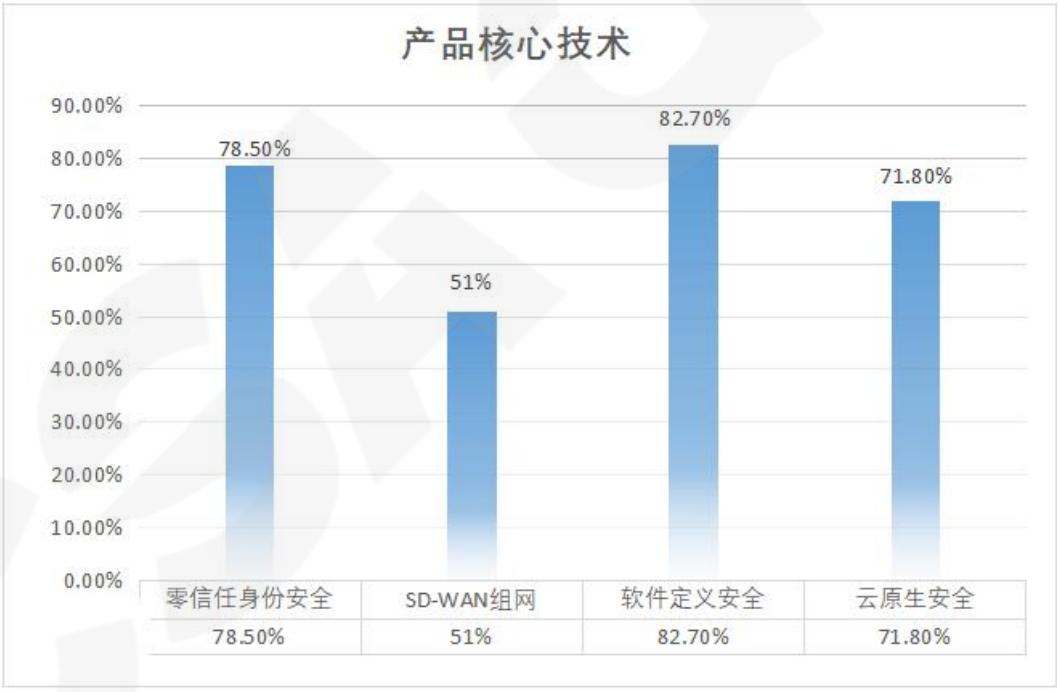


图 8 产品核心技术

本次接受调查的SASE厂商中，78.5% 厂商认为SASE是以零信任为基础的，基于零信任身份安全的安全与网络融合架构，通过强化了身份安全机制来适应复杂的网络威胁环境；51.26% 厂商将 SD-WAN 组网作为核心技术，对产品进行了安全升级，利用 SD-WAN 的智能选路、流量负载均衡、机密与隧道技术等技术，为 SASE 的网络部分发展提供强有力支持；82.70%厂商采用软件定义安全（SDS）

为核心的融合路线，SDS 将安全功能从传统的硬件设备中解耦出来，通过软件定义的方式实现安全策略的动态配置和管理，结合软件定义网络（SDN）实现网络流量的灵活调度和管理；71.8%厂商结合了云原生安全机制，根据业务需求弹性伸缩，自动化运维等功能提高资源利用率，加速创新与迭代。

5.1.4 用户画像

根据本次报告所有参选厂商的数据显示，目前使用 SASE 产品的用户覆盖广泛，涵盖了制造业、政府及事业单位、通信、金融、教育、医疗、互联网、食品交通、能源、服务、建筑、零售等行业。其中，由于制造业存在设备种类繁多、安全防护弱、实时性要求高等特点，需要通过 SASE 进行关键业务保障。同时，政府和事业单位由于数字政务的发展以及网络和数据安全的需求，也开始引入 SASE。

从产业链角度来看，SASE 行业的上游主要由提供安全产品、安全服务和集成解决方案的网络安全厂商构成；中游则包括网络服务和安全服务的提供商；下游为各行业的用户，包括政府、金融、电信、能源、教育等多个领域，用户范围广泛，主要集中在 B 端市场。

本次调查中客户案例的分布比例如下：

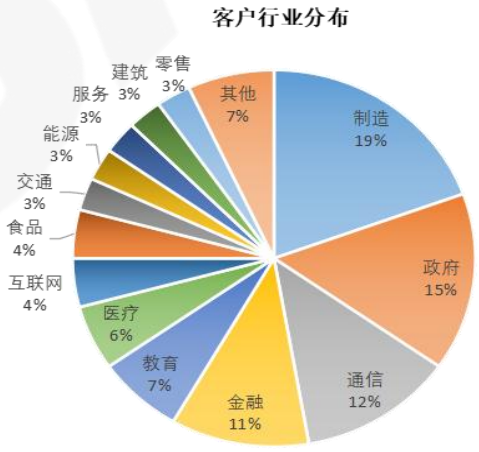


图 9 客户行业分布

以上用户在采用相关 SASE 产品或服务后，基于自身的实际情况和需求也对产品和服务本身提出了自身的理解与建议。

由于大多数用户自身业务与办公体量较大，要求 SASE 产品需要支持用户不同形态的操作系统、手机、便携式设备、PC 等多样化的设备。且在用户环境下进行本地化适配的过程中，与现有设施进行集成实际上是一个异常复杂的过程，需要基于用户本身的网络安全架构进行深入改造，因此对标品会提出相当的定制化需求。

部分用户涉及全球化业务，存在对客户端的海外下载需求。此外，用户关注的功能点还包含账号管理的透明度和追溯性，以及结合身份、终端、网络等策略进行全面安全策略匹配管理，实现网络安全多层防护覆盖等。

5.2SASE 产品分析

5.2.1 市场方面

从市场规模看，SASE 市场呈现了快速上升的发展趋势。Gartner、G2、Netskope CFO 的预测是整个 SASE 市场在未来 2～3 年达到 150 亿美元，30%左右的复合增速。Dell' Oro Group 的数据显示，2024 年第一季度 SASE 市场实现了 23%的收入增长，这是连续第 17 个季度实现超过 20%的增长，显示出 SASE 解决方案的持续强劲需求。

国内市场看，Gartner 预测，到 2024 年，大中华地区 SASE 市场规模为 7.69 亿美元，至少有 40%的大公司将采用 SASE 的模型。

从安全厂商布局来看，Palo Alto Network 在 23 年 12 月份用 10.25 亿美元先后收购数据安全态势管理初创公司 Dig Security 和企业安全浏览器公司 Talon Cyber Security，增强 SASE 能力。Cato Networks 凭借 CDN 的技术优势，通过全球分布式云服务，为所有边缘提供企业网络和安全能力，成为全球第一家 SASE 平台厂商。Zscaler 在过去几年中的成功取决于其作为 SASE 市场先行者的成功，其核心 SASE 业务（ZIA 和 ZPA）持续增长，Q2 业绩同比增长 32%。

相比国外，国内 SASE 市场正处在快速发展期。安全厂商、网络厂商以及云服务厂商都加入 SASE 的竞争中。顺应自动化、智能化趋势，SASE 提供商正在使用 AI 等相关技术，为用户提供体系化、智能化、一体化的 SASE 解决方案，

帮助用户实现“云网安”一体化架构。同时，根据中国云服务当前市场需求和私有化、混合部署的针对性需求，进行中国市场更多元的针对性 SASE 建设。

5.2.2 技术方面

SASE 不是单一技术，而是一套相互协同的解决方案，涵盖了网络接入能力、网络安全能力和安全统一管理能力。

1) 网络接入能力

SD-WAN 作为 SASE 的网络技术底座，融合软件定义网络（SDN）、网络功能虚拟化（NFV）、网络编排与探测等多种技术，能够以平台或托管方式提供基础网络连接、广域网加速、安全防御等多种 SASE 服务。

ZTNA（零信任）“以身份为基石、业务安全访问、持续信任评估、动态访问控制”四大关键能力，覆盖身份、设备、网络、应用、数据等维度，通过动态访问控制机制，持续优化访问策略，有效缓解各类访问风险，赋能 SASE 形成统一安全访问管控机制，切实保障了无边界、自适应、弹性访问、可持续安全评估的应用体验。

2) 网络安全能力

SASE 通过安全资源池按需集成了 FWaaS、SWG、WAF、ZTNA、网络审计、日志审计、云态势探针等多种安全组件，对访问流量进行安全防护和安全威胁检测分析。

FWaaS（防火墙即服务）为 SASE 提供防火墙安全防护服务，支持应用识别、威胁情报、入侵防御、病毒防护等功能，使企业轻松地管理网络安全，设置统一策略，及时发现异常并快速进行响应。

SWG（安全 Web 网关）通过过滤掉无用的 Web 流量内容和阻止存在风险或未经授权的用户在线行为，防范网络威胁和保护数据。支持网页过滤、用户认证、应用控制、内容审计、带宽管理、行为监控分析、防私接、数据防泄露等功能。

WAF（Web 应用防火墙）提供虚拟化 web 应用安全防 SWG 护能力，支持 Web 攻击行为拦截、敏感信息保护、暴力破解、Web 业务控制、威胁情报检测、资产探测、基于 URL 地址的外联检测等功能。

CASB（云访问安全代理）为多云管理提供了一个中心，用于跨多个云服务并发地执行策略和治理，以及对来自企业内外的用户活动和敏感数据（包括云到云访问）的精确可见性和控制。支持认证、单点登录、授权、凭据映射、设备建模、数据安全（内容检测、加密、混淆）、日志管理、告警，甚至恶意代码检测和防护。

3) 安全统一管理能力

SASE 通过一个安全管理平台实现安全与网络的统一配置与管理，收集和分析大量网络流量数据和安全日志，利用大数据分析技术挖掘潜在的网络访问安全风险和异常行为模式，基于威胁检测分析结果，为企业提供智能的安全策略决策建议，实现监测、分析到处置的闭环式托管运营服务，帮助企业优化安全基线和安全策略配置。安全管理平台还提供用户自服务门户，支持对运营中心承接的政企客户的安全防护能力和效果可视化展示，通过安全事件及安全运营报告定期进行服务交付。

5.3 SASE 落地部署建议

SASE 的部署方式通常是基于云的，将安全和网络能力虚拟化，通过统一的能力池对外进行输出，从而减轻多分支机构的 IT 建设与运维的投入和压力。SASE 通常由云服务提供商和网络安全公司联合提供，国内一些云公司由于自身安全能力较强，也进行一些相应服务的输出。SASE 与云环境存在多种集成方式，企业可以根据自身网络架构与业务特点选择适合自己的方式，常见的集成方式包括公有云、私有云、混合云、私有化部署、混合部署等方式。

企业还可以根据业务需求动态调整资源，如在公有云中扩展资源与服务、在私有云中保护敏感数据。通过多样化的部署方式使企业能够根据自身的安全需求、合规要求和技术基础设施，灵活选择最合适的 SASE 解决方案。此外，曾出现过整合不同供应商安全产品的 SASE 方案，但该方案很快被淘汰，由于不同产品耦合带来的巨大的复杂性及运维成本，导致此类解决方案难以很好地协同工作。

目前最受期待的解决方案是单一供应商的 SASE 集成方案，通过单一供应商提供 SASE，将所有 SASE 功能统一在同一套架构及管理台下，避免了复杂性和

适配成本。单一供应商往往也能对产品进行统筹性的调整与优化，这样更容易定位及排除问题。

根据 Gartner 的预测，到 2024 年底，将会有 5-10 家新的单一供应商进入市场，到 2025 年，单一供应商数量相较 2023 年增长 50%以上，大多数 SSE 供应商将会成为单一供应商 SASE。而 Cato 预计在 2025 年将会有三分之一的 SASE 建设由单一供应商提供，这个比例在 2022 年是 10%。到 2025 年，65%的企业将把单个 SASE 组件整合到一个或两个明确合作的 SASE 供应商中，而 2021 年这一比例为 15%。

5.4SASE 发展趋势

随着数字化转型的深入，企业对网络和安全的需求逐渐融合，SASE 作为一种全新的解决方案，正逐步走向成熟和普及。SASE 架构将“网络+安全”相融合，通过统一安全管理和运营服务平台，集成 SD-WAN、FWaaS、SWG、ZTNA 等多种安全防护能力，将原有安全产品建设交付模式转变为安全服务化模式，构筑“云网安”一体化防护体系。

为实现这一目标，不仅需要技术的进一步发展与整合，还需要在行业实践中逐步克服当前面临的挑战。以下是推动 SASE 一体化、安全智能化的几个关键方向：

1）全方位的身份整合

身份是 SASE 解决方案的核心。未来，SASE 需要将身份与设备、网络、应用等各个层面的安全策略无缝结合。通过 AI 和大数据分析等技术，进一步强化身份验证的精确度，并通过持续的行为分析和动态访问控制，确保用户在不断变化的网络环境中的每一次访问都能得到及时的安全评估与响应。

2）人工智能与自动化驱动的智能安全决策

随着 AI 和机器学习技术的发展，SASE 将能够实现更智能的流量分析和安全决策。AI 可以实时识别网络流量中的异常模式，并通过自动化响应减少人工干预。尤其是在应对高级持续威胁（APT）和零日攻击时，AI 能够发挥更大的作用，提前识别潜在的安全风险。此外，AI 还可以帮助 SASE 平台进行自我优

化，不断根据新的威胁情报调整安全策略，提升防护效率。

3）多云环境下的安全统一管理

随着多云和混合云架构的普及，SASE 需要能够提供跨多个云环境的统一安全管理。无论企业使用的是公有云、私有云，还是混合云，SASE 应确保一致的安全策略和合规性要求。未来，SASE 将更多依赖集成云服务和本地设备的能力，构建起一个无缝连接的全域安全防护网络，确保数据在不同云平台间流动时的安全性和可控性。

4）边缘计算与 5G 支持下的网络安全扩展

边缘计算和 5G 技术的快速发展将成为 SASE 架构进一步发展的催化剂。在支持远程工作、物联网（IoT）设备以及其他边缘设备的过程中，SASE 解决方案需要更深入地适配这些新的应用场景。例如，随着工业互联网的普及，制造业企业的关键资产和设备需要更多的实时监控和防护，SASE 平台必须能够灵活地支持这些端到端的安全需求，同时在保证安全性的同时不降低系统的性能。

5）标准化和跨域协同的推进

SASE 的发展不仅是技术层面的进步，也需要在行业标准化和跨域协同上取得突破。随着不同厂商提供的 SASE 解决方案逐渐趋同，未来的挑战在于如何建立统一的安全标准和接口，确保不同供应商之间的产品可以高效地协同工作。跨域的安全合作，尤其是在多国、跨地区的运营中，要求 SASE 平台能适应不同的法律、合规要求和网络环境，这对供应商提出了更高的技术和运营要求。

6）集中式与分布式架构的平衡

尽管单一供应商的 SASE 方案逐渐成为主流，企业在选择 SASE 产品时依然面临集中式和分布式架构的平衡问题。集中式架构能够简化管理和部署，但在应对跨地域、大规模用户时可能存在延迟和性能瓶颈。分布式架构则能提供更灵活的部署和更高的容错性，适用于复杂多变的网络环境。如何在这两者之间找到最佳的平衡点，提供更高效的运维体验，是未来 SASE 产品发展的关键。

SASE 的发展需要厂商在不断发展技术的同时，紧密结合企业的实际需求，推动安全与网络的深度融合。在未来的 SASE 架构中，安全性、灵活性、可扩展性和智能化将是其最重要的特征，最终将使 SASE 成为应对日益复杂的网络威胁

和业务挑战的核心解决方案。

6 SASE 实践案例

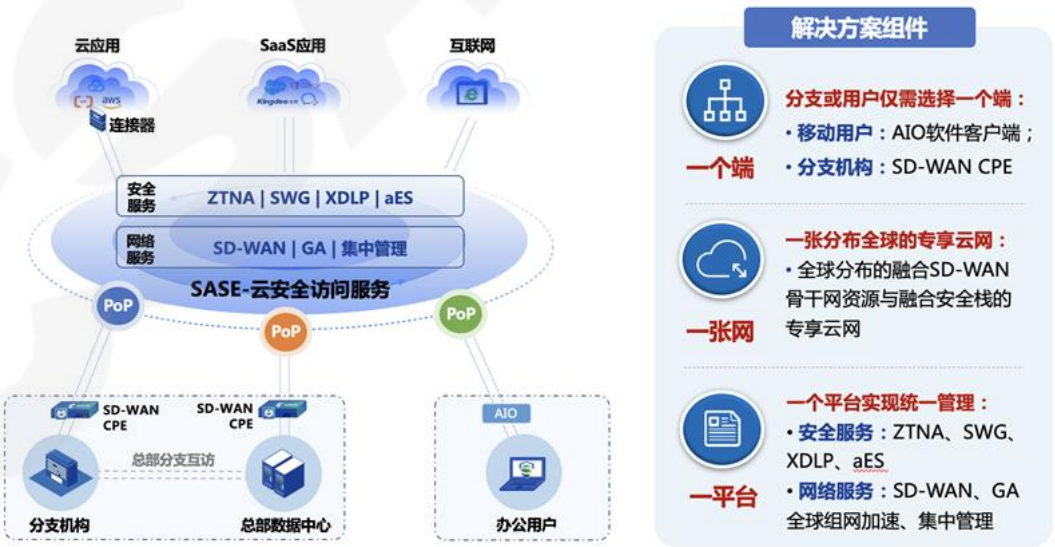
6.1深信服——云安全访问服务 SASE

6.1.1 产品简介

（一）能力描述

深信服 SASE 一体化办公安全解决方案，将深信服沉淀二十余年的安全功能与 SD-WAN 网络功能深度整合，基于 SASE 模型为核心，通过“一端一网一平台”的焕新架构，用户仅需要部署一个软件客户端或硬件 CPE 设备，即可就近接入全球分布的200+ POP 点，通过一个控制台按需获取ZTNA 零信任网络访问、SWG 互联网安全访问、XDLP 可扩展防泄密、GA 全球加速等安全与网络服务，为分支机构与远程办公用户提供一体化的安全与组网服务，快速提升全局安全水位，让用户以更好的体验、更优的路径，随时随地安全访问互联网、数据中心与多云应用。

（二）技术架构



深信服一体化办公安全解决方案通过“一端一网一平台”的架构为客户提供安全与网络服务：

1) 一端：灵活多样的端

对于分支机构，只需要部署一台深信服 SD-WAN 的 CPE 设备即可，通过智能引流的方式将互联网流量引流至 POP 点，在 POP 点提供安全服务后出局访问互联网；

对于远程用户，只需要部署一个 All in One 的软件客户端即可，融合了零信任接入、互联网安全访问、可扩展防泄密、统一终端安全的安全能力；

对于深信服的安全产品的老客户，比如全网行为管理 AC、零信任 aTrust 等产品，还支持通过客户端平滑升级的方式扩展数据防泄密等一体化办公安全能力。

2) 一网：全球分布的安全云网

一体化办公安全将安全与网络能力融合到就近接入的 POP 点上，深信服 POP 点采用全面的云原生架构，实现分钟级授权开通、秒级资源扩展，为用户提供 99.95%的 SLA 保障。

为了让用户获得 30ms 就近接入的极致体验，深信服在国内主要一二线城市，以及海外东南亚地区，均可提供安全 POP 服务，同时还深度融合 SD-WAN 骨干网资源，为中资出海客户提供全球加速服务，目前已在全球拥有 200+ POP 点。

3) 一平台：统一管理的控制台

管理员通过这一个控制台，就能实现策略统一配置、运维统一管理、数据统一分析。

（三）功能描述

SASE-ZTNA 零信任网络访问：通过云服务交付，以用户身份为中心，基于上下文感知、身份感知和设备感知等策略，允许授权用户安全地访问特定应用程序，同时隐藏企业资源，避免暴露在公共互联网上，让用户快速、安全、稳定地访问数据中心与多云应用。

SASE-XLDP 可扩展数据防泄密：基于数据来源的全新防泄密数据流转追踪技术，覆盖企业办公终端的各种数据外发通路，结合强大的防泄密数据分析能力与终端管控能力，实现敏感文件的全链路可视、可控、可溯源，全面满足固定场所办公、在外移动办公等场景的企业办公数据防泄密需求。

SASE-SWG 互联网安全访问：面向分支机构与办公终端的互联网安全访问服务，融合上网行为管理、下一代防火墙（含威胁管理）等一体化能力，通过分

支 CPE 引流或办公终端 AIO 客户端引流的模式，对网络流量的实时监控、过滤和控制，有效防御网络威胁，满足上网管控与合规要求，全面提升工作效率，让用户随时随地获得上网安全保护。

SASE-GA 全球加速：搭载 SD-WAN 技术和骨干网优化技术的解决方案，并支持组网与安全深度融合，能力覆盖全球 SD-WAN 骨干网络节点（PoP），确保您的网络服务实现全球就近接入，无缝跨区域部署，为用户打造快速稳定、简单易用、融合领先安全能力的安全组网解决方案。

SD-WAN 组网：深信服 SD-WAN 产品能够智能地调度网络流量，通过多链路负载均衡技术，有效利用多条网络线路，避免单点故障，提升网络的稳定性和可靠性，在安全方面，集成了防火墙，同时可灵活订阅 SASE 安全服务，实现分支组网与安全的一体化交付，企业能够方便地对分布在不同地点的分支机构网络进行管控，大大降低管理成本，助力企业实现高效、安全的广域网连接。

6.1.2 实践案例：制造业一体化办公安全解决方案

（一）项目背景

某国内服饰集团公司创始于 1976 年，是国内兼具大规模及先进生产设备的品牌羽绒服生产商。该公司早在 2014 年提出了“智改数转”战略，打造了“智慧门店+线上云店”的全域零售新模式，构建了以 SAP ERP 为核心的信息平台，波司登在各地存在 25 家分公司，员工两万余人，目前在 IT 组网方面遇到的新挑战如下：

a) 互联网暴露面大；

b) 应用访问安全与体验差；

c) 分支互联网安全有风险。

（二）项目内容

为该公司全国 25 个分支，2000 多远程办公用户提供 SASE 一体化办公安全解决方案：

a) 助力网络扁平化构架升级，实现业务安全高效访问：一种基于“智能、管理、控制、分析、安全”为一体的广域网管理方案，突破了传统广域网的瓶颈，实现了广域网的网络扁平化，降低了广域网管理的复杂性，在数据传输方面实现了低延迟、高速率。分支仅需一个端（安全 SD-WAN 设备），即可融合 SD-WAN 组网与安全功能，并能弹性订阅云上安全服务，极大简化了分支的组网架构；

b）网络、安全全局统一管控：通过 SASE 可以轻松为零售公司构建一个全局的分支上网安全策略与防护体系，实现分支安全的可管可控；

c）建设成效超预期，全面实现多赢：相比传统的单点产品组合的解决方案，深信服安全组网能大幅降低整体硬件产品投资，减少运维工作量。

（三）项目成效

a）提升体验保障安全：通过安全 SD-WAN 加密，零售公司访问业务系统的数据传输安全得到了充分保障，总部业务系统将暴露于公网的端口全部收回，仅保留 VPN 端口，大大减少安全风险；同时通过 SD-WAN 技术，链路和设备故障实现自动快速切换，保障业务可靠性；

b）全网设备集中管理：通过集中管理平台统一远程运维分公司 SD-WAN 设

备，实时展示分支组网情况，提高运维效率，降低运维成本；

c）分支安全一体防护：SASE-AC 对企业终端违规上网行为、文件外发和信息泄露途径等进行管控，有效保障企业信息安全；同时通过云情报网关，实现失陷终端外联实时检测与拦截，有效应对挖矿、恶意软件、APT 等新型威胁，及时发现问题、阻断攻击、溯源闭环；

d）安全能力弹性扩展：按需订阅 SASE 云安全能力，将来动态扩展，避免投资浪费。低成本地应对不断发展的 IT 变化。

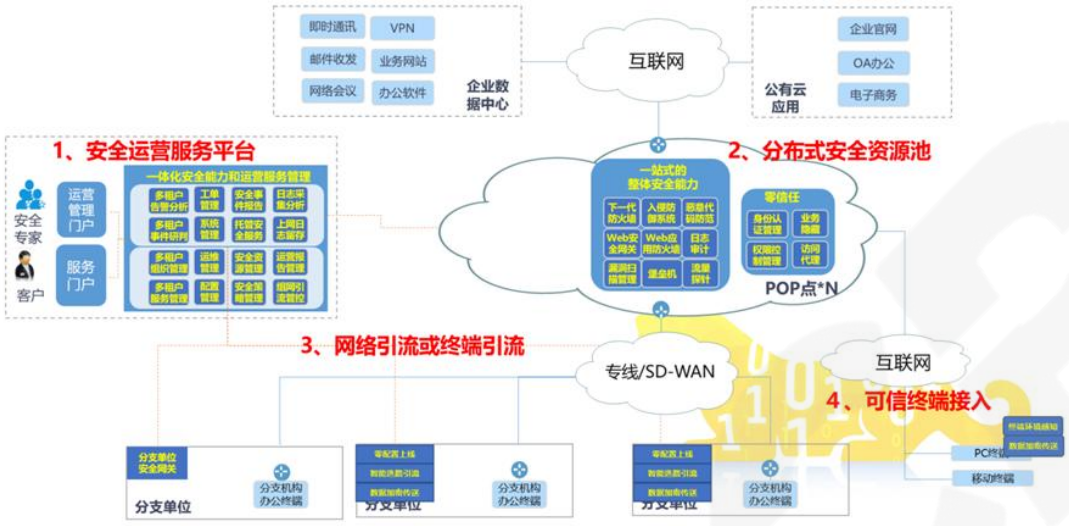
6.2 奇安信——安全访问服务 Q-SASE

6.2.1 产品简介

（一）能力描述

奇安信 Q-SASE 以 Gartner 定义的 SASE 架构为基础，采用软件定义安全（SD-Sec）+软件定义网络（SD-WAN）相结合的技术路线，集成 SD-WAN、NGFW、SWG、DLP、主机安全、零信任等多种安全防护能力，构筑“云网边端”安全防护体系，将原有的安全产品建设交付模式转变为安全服务化模式，帮助众多的企业和政府客户实现互联网访问、内网应用访问、远程办公等多场景下的全面安全防护及统一管理和运营，打造一体化安全运营体系标准，且在多个大型央国企、政府、教育、能源等多个重要行业落地运营。

（二）技术架构



（三）功能描述

（1）运营管理服务平台

安全访问服务的统一运营管理服务平台（包括安全运营管理系统、客户服务系统、上网行为分析系统等）提供对整个 Q-SASE 架构中的各系统模块的接入、配置、持续运行监测，保障整个系统的稳定持续运行。支持对运营人员的权限和工作进行管理，提供对安全告警日志和安全事件的持续跟踪和管理，并基于客户需求针对安全资源池和安全网关中的组网策略和安全策略进行持续优化。支持对客户关心的网络使用、应用访问、安全事件等信息进行可视化展示。

（2）安全资源池

Q-SASE 安全资源池采用虚拟化镜像的方式部署不同安全组件，安全资源池的安全组件按需配置，包括虚拟化防火墙安全组件、上网行为审计安全组件、零信任接入安全组件、虚拟化 WAF 安全组件、态势感知云探针安全组件等，也可以部署日志审计、堡垒机、数据库审计、漏扫等等保组件，具有安全能力弹性扩容特点，支持安全组件单点登录，安全组件和特征库统一升级，

（3）组网引流

安全网关采用 SD-WAN 组网技术与安全资源池实现快速灵活的接入，支持将分支访问流量按需引流到安全资源池进行安全防护和上网审计。安全网关不仅支持多种 VPN 协议，同时集成了基础防火墙、应用与身份识别、应用层安全防护等综合安全防御功能，实现组网与安全策略一体化，能够为电子政务外网、新

关基基础设施建设提供全面的接入方案。ASE 安全网关支持针对业务数据的隧道隔离以及数据传送的加密，包括多种加密方式，如 IPSecVPN、SSLVPN、PPTPVPN。安全网关设备支持多种国际算法以及国密算法。可基于应用识别技术，将各种上网流量区分成不同应用，并依据配置的策略，对不同应用设置不同的引流规则。

（4）可信终端接入

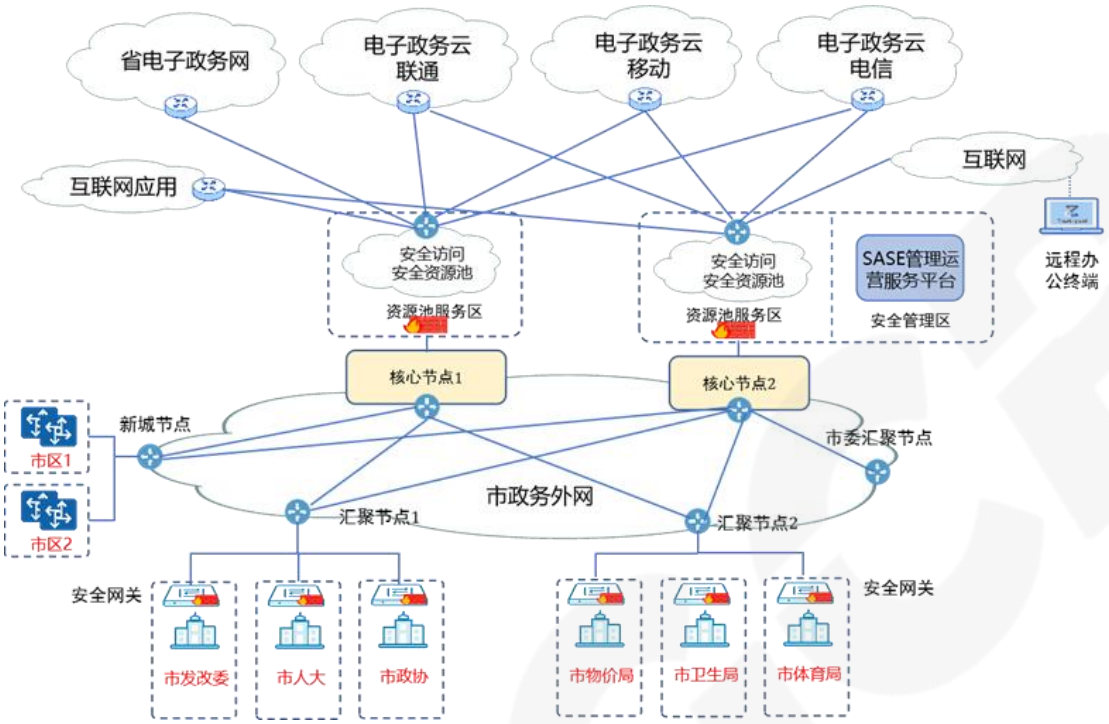
基于零信任可信客户端的接入方式，通过零信任可信访问控制台和零信任可信应用代理，从身份风险、终端风险、网络风险、权限和数据风险 5 个维度，全面构建从终端到应用访问的端到端安全防护能力，通过便捷的运维管理能力和动态访问控制机制，确保零信任的防护效果落实在业务访问的各个阶段。

6.2.2 实践案例：政务外网一体化安全防护方案

（一）项目背景

随着政府行业数字化转型的不断深入，安全暴露面和被攻击风险快速增加，网络安全形势不容乐观。基于数字政府改革建设“十四五”规划，为数字政府建设全要素、多层次的安全防护体系，打造自主可控、安全高效的数字政府技术路线。同时，从网络安全监测预警、攻防演练和现场检查中发现，该省政数局政务网信息系统不同程度地存在安全隐患及问题，受人员和技术等方面的限制，无法全面掌握各委办局实际安全防护效果，缺少对安全服务商监督手段，对网络安全风险把控不足；因此，以奇安信 Q-SASE 安全访问服务架构为核心，实现网络内生安全的云、网、边、端“全栈式”安全防护能力，以威胁检测+安全防护能力为基础，结合智能安全事件分析和溯源，打造“安全无界、资产无忧”的一体化安全防护和安全运营解决方案。

（二）项目内容



本项目的整体建设内容包括：

1)SASE 管理运营服务平台：在电子政务网的安全管理区部署 Q-SASE 的管理运营服务系统，实现对整个安全防护系统的管理、资源调度、安全运营和客户服务。

2）安全资源池（POP 点）：通过在政务外网的两个核心节点部署安全资源池承载各种安全防护组件和威胁检测组件，提供给各委办局的互联网访问、政务云访问的安全防护及安全运营服务。

3）办公机构安全网关：通过汇聚节点接入到政务外网的市政数局、各委办局直属单位通过安全网关引流至安全资源池。

4）远程办公终端：通过零信任客户端接入到政务外网互联网出口的安全资源池的零信任代理网关，通过安全资源池的身份认证及业务访问防护能力后，再访问政务云平台的业务系统。

（三）项目成效

本项目作为国内首次在政务外网建设的 SASE 一体化安全防护和运营体系的案例，借鉴了国际领先的 SASE 和零信任架构，依托 SDN、SDS 等创新技术，打造了云边端一体化的安全协同防护系统，为市级委办局各单位访问互联网、访问政务云业务系统保驾护航。本项目为全市电子政务网络、云平台、办公终端提

供信息系统安全防护效果评估，网络威胁实时监测，安全事件处置闭环等服务，并对政数局统筹建设的安全设施提供统一的日常运维管理服务，全面提升安全保障能力。同时也通过集约化建设的安全防护系统，统筹建立的一体化安全管理运营中心，极大降低了传统分散建设的安全防护设备和态势分析系统的投资，经过测算，预计减少市级委办局安全系统建设投资及运营成本 40%。

6.3 网宿科技——SASE 一体化办公安全产品

6.3.1 产品简介

（一）能力描述

网宿 SASE 一体化办公安全基于网宿全球领先的网络和计算平台，构建 SASE 一体化架构，实践全面零信任，帮助企业解决办公安全碎片化问题，为企业打造更安全、更高效、更便捷的办公访问体系，适用于远程办公安全、数据防泄露、威胁入侵防范、IT 效率增效等场景。

（二）技术架构

（三）功能描述

网宿 SASE 产品主要由五大功能模块、统一管理平台和安全及网络底座构成：

1) 安全 SD-WAN：依托网宿全球丰富的 PoP 骨干节点，基于智能 QoS、协议优化等能力提供加速访问，助力企业快速组网，实现降本增效。全程链路提供端到端加密，PoP 骨干节点具备发现及阻断内网流量威胁的能力，能够更好地保

障企业内网传输安全。

2) 零信任访问 ZTNA：采用“持续认证、永不信任”的零信任理念，以身份驱动为核心，持续评估访问过程中的行为可信，实现动态访问授权，有效解决企业数字化办公带来的无边界安全问题。

3) 数据安全治理 XLDP：结合领先的数据安全治理理念，提供由浅到深的多级数据安全方案，集成端点数据防泄露（EDLP）、WEB 数据防泄露（SWG、RBI）、安全工作空间等能力，一体化解决企业面临的数据泄露风险，为企业构建全域数据安全的治理体系，保护企业敏感数据。

4) 威胁检测与响应 XDR：集安全基线、终端杀毒、漏洞检测、网络入侵检测、主机安全检测为一体，覆盖终端、网络、主机各个环节安全防护，确保入网终端的安全合规。

5) IT 效率管理：提供一站式企业 IT 资产管理与监控平台，帮助客户发现并梳理企业内的软硬件资产，功能包括终端资产梳理、桌面管理、网络准入、上网行为管理等，实现资产统一可视化运营管理。

6) 统一管理平台：对用户操作行为进行全面追踪审计，通过平台实现全网业务态势实时感知，支持威胁探测和告警，满足企业运维及安全需求，提高管理效率。

7) 安全及网络底座：基于网宿丰富的基础设施底蕴和成熟的网络管理技术，构筑先进的网络及安全底座，全方位保障企业网络安全，实现高质量访问。

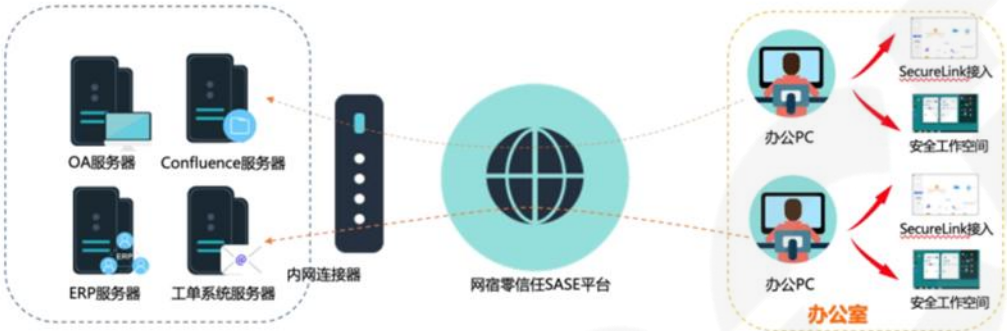
6.3.2 实践案例：云客服安全实践项目

（一）项目背景

客户主要业务系统部署在公有云上，业务系统存有大量敏感数据，员工原先通过传统 VPN 访问，无法根据终端安全状态及用户访问行为实时动态权限调整，终端若遭病毒、恶意软件感染，攻击者可借此对云上业务发动横向攻击，严重威胁数据安全与业务连续性。同时，客户业务系统含有大量敏感数据，这些数据的安全直接关系到企业的竞争力和市场地位，对于财务、研发等关键岗位的员工，其访问和操作数据的行为需要得到严格管控，以避免敏感信息的无授权外发。基

于此，客户携手网宿共同落地 SASE 一体化办公安全方案，全面提升办公安全水位线。

（二）项目内容



基于网宿 SASE 一体化办公安全的建设思路，联动包含 ZTNA 安全办公、流量威胁检测、数据防泄露等多项安全能力，全面提升办公安全水位线。通过员工访问权限的统一管控和终端的准入安全，当检测到病毒、蠕虫、SQL 注入等网络攻击时，将隔离阻断攻击流量，确保流量的合法性；同时，实时监测员工的登录及操作行为，一旦发现暴力破解、扫描探测、越权访问等异常操作，将动态调整访问权限，限制员工访问并审计，保障员工行为合法合规；从员工访问应用、下载数据、外发等环节进行全链路跟踪，降低数据泄露风险，让云端办公更安全、更高效。

（三）项目成效

通过使用网宿 SASE 一体化办公安全解决方案，轻松实现安全上办公，目前已经覆盖内部业务系统多达 100 多个，客户价值包括：

1) 通过 ZTNA 实现对员工访问权限的统一管控，结合流量威胁检测能力，及时识别并阻断病毒、蠕虫、SQL 注入等网络攻击，快速响应安全事件，并动态调整访问权限，减少潜在的损害，显著提升企业网络安全防护水平。

2) 全链路跟踪员工对应用的访问、数据的下载和外发行为，通过数据防泄露措施，帮助企业及时快速发现风险用户、处置数据泄露事件，并提供外发截屏取证，方便溯源定责，有效降低数据泄露的可能性。

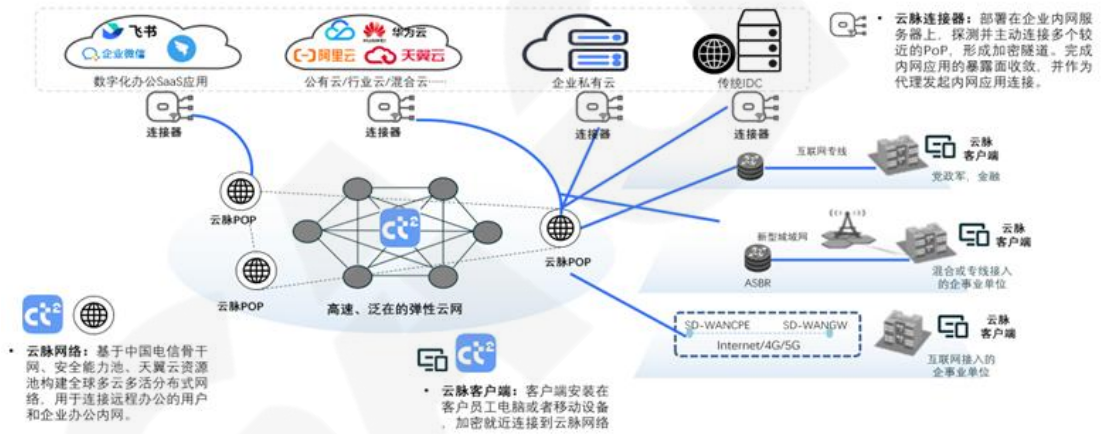
3) 通过一体化的安全架构简化安全管理，无需部署多套产品，降低终端性能消耗，提升 IT 管理效率 30%以上。

6.4天翼安全——云脉 SASE

6.4.1 产品简介

（一）能力描述

云脉 SASE 是一套遵循 Gartner SASE 技术模型，融合了中国电信优质网络与中国电信安全公司核心安全能力的新型办公安全服务平台。通过云脉客户端、云脉 Mesh 网络、云脉连接器三大核心组件，为用户提供零信任网络接入、数据外发管控、终端安全、IT 效能管理一体化能力，解决当前企业内部署多个安全产品缺少联动且存在安全管理盲区的问题，使用户在任何位置、通过任意终端均能高效、安全接入企业内网。



（二）技术架构

（三）功能描述

中国电信云脉 SASE 作为一个融合网络与安全，办公全场景覆盖，兼顾安全、体验、效率的下一代一体化办公安全平台，旨在为全行业数字化转型用户提供零信任网络接入、数据外发管控、终端安全、IT 效能管理四大办公安全技术支撑能力，全面助力用户增强办公网络与办公应用安全性，提升员工日常办公体验，简化 IT 人员运维管理工作内容、提升效能，并降低企业整体安全投资。

1) 零信任网络访问

通过应用 ZTNA 技术严格落实“永不信任、持续验证”的零信任原则，为用户提供基于身份权限的细粒度访问控制。同时，通过网络、终端安全策略直接打通，云脉 SASE 能够动态监测实时调整用户/终端对应用的访问权限、记录 4-7 层访问日志，实现随时随地安全接入、访问行为可管可查。

2) 数据外发管控

打造人、数据、通道三位一体的办公敏感数据安全治理体系，提供“全链路闭环”的敏感办公文件外发管控，基于对用户敏感数据的分类分级，持续跟踪分析异常数据外发行为，并告警/拦截；同时，支持为用户生成专属的敏感数据地图，提供更直观的敏感数据分布视图，便于灵活开展基于组织架构、用户、办公终端等多维度的数据安全管理。另外，提供屏幕水印、截图存证、文件追踪等调查溯源方式。

3) 终端安全

提供病毒查杀、漏洞修复、上网管控、威胁情报、扩展威胁检测与响应、网络隔离等面向 Windows、MacOS 等办公终端的安全防护服务，并将终端安全现状与整体零信任网络接入做了结合，使得用户对办公终端入网的安全管理更加全面。

4) IT 效能管理

统一管理各类办公终端，一站实现盗版检测、软件分发、有线/Wi-Fi 网络准入，检测-决策全链条自动化处置，提高用户 IT 管理效能。

6.4.2 实践案例：多分支国企安全接入方案

（一）项目背景

该单位为方便各分支机构人员访问集团 OA ，将 OA 系统发布至互联网且未做安全防护。然而，鉴于该企业为省属国企，监管单位在对企业 IT 资产进行常态化安全扫描检查时发现，OA 系统存在登录绕过高危漏洞，要求一周内完成整改。

因此，该企业迫切需要对 OA 系统进行安全加固，一方面满足分支人员高效、便捷接入系统，另一方面需要收敛 OA 系统互联网暴露面，做到应用隐身，降低漏洞被黑客利用的可能性。

（二）项目内容

针对该用户远程应用接入、应用互联网暴露面收敛、分支-总部高效互访等业务需求，中国电信为用户提供了云脉 SASE 标准解决方案，在不改变用户原有网络架构的前提下， 24 小时内完成互联网暴露面收敛与应用迁移，为用户提供 OA 系统的零信任网络接入能力。

云脉 SASE 上线后，整体为用户提供基于身份的细粒度应用访问控制，为用户设置基于终端安全、网络位置、系统配置、可信进程等条件的动态策略，使得内网应用全面隐身，并通过一体化客户端整合的终端桌面统一管理、软件统计、软件分发管理和盗版软件的检测能力，协助用户 IT 管理员更方便地开展企业办公资产安全管理。

（三）项目成效

暴露面收敛：使用云脉 SASE 收敛了 OA 系统互联网暴露面，使攻击者无法

通过扫描工具检测到业务系统存在，实现业务系统“隐身”，极大提升业务系统安全性。

访问安全加强：相比较传统 VPN 提供了基于身份的细粒度访问控制，对用户登录接口进行多重身份验证、并提供动态授权，进一步提升企业对人员入网、办公/BYOD 设备访问内网应用的安全管控能力。

用户体验提升：云脉 SASE 一体化客户端除提供零信任网络访问能力外，还具备 IT 设备管理、合规检测、外设管控、软件管理、日志审计等办公安全管理支撑能力，一方面减少企业员工办公终端上 Agent 的数量、提升员工办公体验；另一方面，通过一体化平台为 IT 管理员提供强大管理后台，提升安全可管、可控、可视能力，全面提升安全运维成效与水平。

6.5亿格云——亿格云枢

6.5.1 产品简介

（一）能力描述

SASE 一体化办公安全平台——亿格云枢，提供包括零信任网络访问（ZTNA）、数据防泄漏（XDLP）、威胁监测响应（XDR）、防病毒（EPP）、上网行为管理（SWG）和统一端点管理（UEM）等功能，帮助企业以更低成本、更高效率建设更加安全、更好体验的下一代办公场景的安全体系，从而解决企业数字化转型过程中遇到的混合和分支办公安全、数据安全、终端安全等问题。

（二）技术架构

（三）技术架构

「亿格云枢™」是亿格云基于云原生安全技术构建在阿里云、腾讯云、AWS、GCP 上的全球多云多活的 SASE 平台，通过 SASE 理念实现的全新网络和安全架构，全平台以身份为边界，构建了一朵集中管控安全的“云”、一张全球办公加速的“网”和一个安全能力合一的“端”，形成云网端融合的云原生安全体系，以 SaaS 化的服务提供零信任网络访问（ZTNA）、数据防泄漏（XDLP）、威胁检测响应（XDR）、防病毒（EPP）、上网行为管理（SWG）、统一端点管理（UEM）等安全能力，打破了企业建设办公网安全需要部署 10 多个办公安全产品且安全产品间烟囱化的现状，崭新的架构和安全服务为企业带来如下收益：

1）对企业网络架构 0 调整和现有应用 0 改造，即可收敛互联网暴露面，快速落地零信任安全体系，实现基于身份、持续验证的动态访问控制能力的企业安全新边界；

2）让企业客户能够实现统一管控办公网的网络和配置安全策略；

3）实现总部、分支、居家办公、移动办公等不同场景全场景一致高安全水位；

4）SaaS 部署，15 分钟极速启用，高效运维；

5）全平台、全功能的客户端 SDK，可无缝集成到企业自有的办公应用里，极大减轻管理员推广安全产品的阻力和落地工作的负担；

6）利用就近接入的全球加速网络，显著优化移动与远程办公网络质量，提升跨运营商和跨境链路访问速度与体验。

7）采用轻端重云架构，打造轻量化、稳定、安全功能合一的客户端，以少量资源占用实现终端用户的无干扰网络访问和安全防护，确保极佳的办公体验。

6.5.2 实践案例：全球制造企业办公安全实践

（一）项目背景

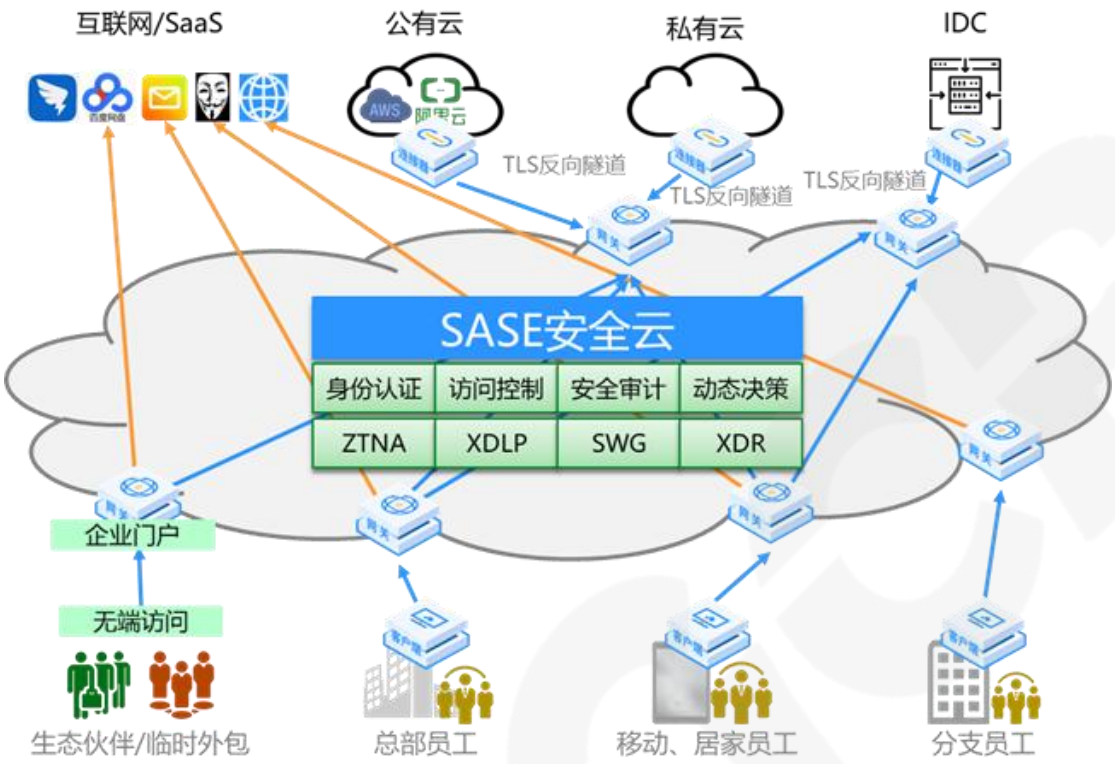
某世界 500 强集团，总部位于国内。现有员工超 2 万名，产业布局 10+国家和地区，营销网络辐射全球。旗下业务分布亚洲、欧洲等地、是全球某制造领域行业的标杆和领袖级企业。

随着业务数字化转型，该集团积极采用云计算、大数据、物联网、移动互联网等新兴技术，IT 建设不断演进。此背景下，业务系统愈发开放、终端类型逐渐多样、任意地点均可办公。新技术带来新生产力的同时，逐步瓦解传统的物理网络安全边界，开放协同、移动办公等新型办公场景成为常态。

从外部威胁看，0day 漏洞、近源攻击、社会工程学、APT 等高级攻击手段层出不穷，黑客攻击能轻松突破互联网边界进入内网，攻防对抗已经常态化；从内部威胁看，内部员工非授权访问业务系统，违规、有意的数据窃取，无意识的数据泄露等情况也愈演愈烈。

（二）项目内容

为该集团推出一套全面的安全解决方案，包括基础功能（身份认证、访问控制、日志审计、终端管理）和零信任网络访问、网络准入控制、数据防泄漏等高级功能。实施 SASE 一体化办公安全解决方案，借助零信任 SASE 架构，隔离办公内网与互联网，满足远程办公的安全需求，同时降低用户体验损害，有效阻断终端风险。通过网络准入控制系统，对终端设备实施严格的身份验证和访问控制，防止未授权用户或设备进入企业网络，减少安全漏洞和网络攻击风险。结合零信任和数据防泄漏技术，实现从数据下载到流转到外发的全链路保护，降低机密信息泄露风险。SASE 架构认证方便、访问速度快、性能好，支持高并发场景，全天候无间断工作，确保数字化办公的高效、稳定、可靠。同时，结合企业流程自动化系统，降低运维管理成本，提升整体办公效率和安全性。



（三）项目成效

SASE 安全架构以低运营成本、高便捷性助力该集团实现数字化安全运维。应用自动发现和权限智能梳理功能，基于访问流量自动识别应用并推荐访问控制策略，有效降低安全运营的难度。SASE 基于用户身份和访问行为动态下发访问控制策略，避免因策略固化带来的安全风险。通过记录终端环境信息和访问日志，使得内网访问行为可视化，员工体验数字化体现在网络质量和设备健康状态的实时监控上，通过采集 CPU、内存占用、WIFI 信号、网络速度等数据，以时序图形式展示，帮助快速发现并定位问题，从而优化终端性能和网络状况。

目前集团内部已铺设安全平台超 10000 个终端，实现办公安全数智化，集团应用全景可视，办公资产清晰可管，企业数据链路可溯等。高效落地 10+海内外分支地区或公司，实现全球办公一张网，随时随地安全办公，有效提升员工入网体验。同时利用大模型生成专有审计小模型，实现 DLP 高效运营、有效闭环，审计时效提升至 1 小时审计 30 人，效率提升 10 倍。

7 评价方法论

云安全联盟大中华区发布的神兽方阵系列遵循相对客观的方法论与评价体

制，在本次发布的 SASE 神兽方阵中，CSA 大中华区参考了众多较为成熟的评价方法，同时结合 SASE 产业在中国国内的实际情况，围绕企业真实数据讨论出客观的评价指标体系，并在此基础上运用模糊综合评价法，建立了综合评价模型。

7.1 公司选择

神兽方阵系列是一套综合企业产品发展路径的体系模型，包括规则分类、象限模型、细分权重等，对企业及企业产品进行发展路径的分级定位，客观评价该企业产品在行业内的状态。

CSA 大中华区综合考虑了企业的行业概况、商业模式、企业竞争力等因素，分别对应各神兽方阵数据模型的入选标准，筛选出具有一定规模，知名度和影响力，或者处于起步阶段但技术实力强和快速成长阶段的企业，进而通过访谈评价分析进一步筛选推荐上榜。

7.2 评价维度

在评价指标上，CSA 大中华区经过多轮筛选，确定了 SASE 神兽方阵的两个评价维度，多项分类数据模型，并根据分类数据模型下的各个指标因素的重要性，构建了指标判断矩阵。

7.2.1 技术研发评价维度

技术研发能力是 SASE 领域最主要的竞争因素之一，通过该维度可以反映不同企业对于 SASE 技术创新的战略趋势，同时也体现了企业的核心技术研发投入程度和产品更新速度，而将技术研发能力作为核心能力的企业，往往具有较强的技术实力，其产品在市场中不断迭代趋于成熟。神兽方阵在技术研发评价维度中从研发能力、知识产权与认证、产品成熟度等具有代表性的量化指标进行综合评价。

1) 研发能力

这一数据模型主要体现企业独立研发的能力以及对 SASE 产品研发的投入

能力，包括研发团队的技术能力、企业在 SASE 领域的研发投入情况、SASE 产品在公司产品组合中所处的位置，以及产品功能的开发能力。此外，我们综合考虑产品国产化适配情况、SASE 产品的技术路线（基于零信任身份安全的安全与网络融合架构、基于 SD-WAN 组网的安全架构、多种安全能力集成等）。

2) 知识产权与认证

这一数据模型主要体现企业在该类产品研发中的技术积累，对于核心技术的掌握程度。知识产权主要包括了专利权、著作权以及销售许可的拥有量。已获得的测评认证资质包括其 SASE 产品获得 Zero Trust Ready、SD-WAN Ready 2.0 等第三方测评资质的情况。此外企业对于 SASE 产品研发的专注程度也体现在知识产权与企业的产品（服务）的是否具有强关联性，以及第三方测评认证的数量。

3) 产品成熟度

这一数据模型主要体现产品与目前市场的契合程度，包括了企业对 SASE 产品投入研究的年限、上市时间、全球 SASE 节点部署数量。另外对于 SASE 产品后续规划的自述，CSA 将其与企业对于 SASE 相关产品方案规划、技术支持覆盖范围、与新兴技术的融合和产业发展的预测相结合，作为判断企业 SASE 产品发展潜力的参考依据之一。

7.2.2 市场营销评价维度

SASE 产品具有快速迭代的特性，对企业产品更新换代能力提出了更高的要求，能够敏锐察觉市场需求并及时推出新产品。所以企业在进行技术研发和产品创新的同时，应重视 SASE 产品的营销管理，建立完整的产品销售管理体系，并与客户建立长期的战略合作计划，帮助 SASE 产品适应市场环境，不断提高产品质量和市场竞争力。

1) 产品营收

这一数据模型主要体现企业 SASE 产品上的销售情况，销售数据是最有力证明企业在 SASE 产品竞争力的指标。盈利能力作为市场营销的主要目标之一，企业在 SASE 产品上的盈利能力与其产品在市场中的竞争水平是强相关的，同样企业 SASE 产品营收占整体市场的比重以及其所处上下游位置，往往体现了该产品

综合能力与市场认可度，另外企业在 SASE 产品在市场中变化情况作为产品的动态评价能力。

2) 用户情况

这一数据模型主要体现企业在 SASE 产品上的客户管理，主要包括客户满意度、服务能力、新客户开发率、终端持有率等因素。该数据模型主要以使用的组织和用户数两个方面评估企业 SASE 产品的使用情况，并根据客户的复购率评估产品满足客户需求的程度。此外，我们收集了调研单位最近收到关于 SASE 产品的用户反馈，以及他们如何回应解决的，这一点作为辅助参考依据。

3) 营销能力

这一数据模型侧面反映企业在 SASE 产品上的市场投入和重视程度，并结合其他指标反映营销活动的效果。该模型主要包含了企业在 SASE 产品中的营销投入、营销模式、营销计划等要素反映了企业在 SASE 产品品牌建设、产品质量、渠道建设等方面的综合实力。这一模型可以作为分析其他数据指标之间的相互影响的参考依据，进而分析各指标之间的内在相互作用和长期趋势。

7.3 入选标准

根据上述的评价维度，CSA 大中华区首先确立 SASE 领域中在技术研究、市场产品的被普遍认可的领跑者，以这些头部企业的产品为最高标准，然后建立分级评价体系，将该分级评分纳入四大神兽方阵的入选标准与评价中。该评价体系将每个维度下的不同数据模型赋予不同分值予以评价。

7.4 评价流程和要求

CSA 大中华区在本次 SASE 神兽方阵评价过程中遵循严谨、客观的评价流程，以公平、公正、诚信为原则，确保评定结果的合情合理。

7.4.1 专家访谈

为确保问卷质量，由 CSA 专家组与部分头部企业沟通，访谈各企业的管理

层、核心技术人员、相关业务人员。从访谈中获取目前企业在 SASE 产品研发、销售、运维等方面的关注重点，并根据企业对于 SASA 产品市场的认知与长远认知设计问卷大纲，大纲维度设计由多位行业专家多次讨论最终通过。

7.4.2 问卷设计

问卷设计根据大纲要求进行具体问题的设计与排版，并将不同的问题分开排列，以确保相关问卷结果与相关维度的关联。问卷经过多个企业的先行设计测验，CSA 根据测验的反馈与收集的结果对问卷维度包括比较倾向、比较方向、比较动机、比较效果等方面进行了相应的微调，确保数据建模时能够综合体现企业在 SASE 产品的能力。在上述基础上，采用专家评定法、问卷调查法、内部一致性信度等方法对问卷进行审校，发布最终问卷。

7.4.3 数据收集与评价

通过企业调查和问卷调查，及经过专家讨论分析，将问卷各分指标数据化为数据模型的隶属度，然后利用数据模型对两个评价维度进行综合评价。同时根据相关企业的实际行业情况对比，结合原始数据验证了模型的可靠性，并对各模型的分类精度进行了比较分析。

7.4.4 情况核实

对所有问卷的结果进行严格复核后，采用双录入的方式将数据（包括数据表与验证文件）录入神兽方阵的计算模型中，形成企业的神兽方阵的初步定位。CSA 根据初步的入选情况对每一家入选企业对数据进行核对与材料的补齐，对未入选企业实际情况的数据及时提出调整意见，并按程序重新提报、修改，确保数据可靠、准确、完整。

8 展望

随着企业数字化转型的加速，对于能够提供灵活、高效、安全的网络安全访问服务的需求日益增长。SASE 不仅仅是一项网络安全解决方案，更是一次理念变革。借助 SASE，我们可以集成多种网络和安全能力，迈向构建云网安融合架构的新篇章。构建 SASE 安全并不容易，但它已成为安全技术未来发展的主流方向之一，越来越多的厂商加入 SASE 市场中，并基于不同的技术积累衍生出各具特色的产品形态。

此次调研结果揭示了 SASE 产品在当前网络安全市场中的巨大潜力和广阔前景。SASE 架构通过将网络功能与安全服务相结合，为分布式企业提供了一种创新的解决方案，能够有效应对复杂多变的网络威胁和挑战。

为了推动 SASE 产品的发展，我们鼓励更多的厂商加入这一领域，共同探索和创新，一起提升 SASE 产品的性能、可靠性和用户体验，拓展 SASE 的知名度，使更多用户能够享受到 SASE 带来的安全与便利，更有助于形成统一的行业标准，为 SASE 技术的长远发展奠定坚实基础。

由于本研究报告是云安全联盟大中华区在 SASE 领域的首次尝试，瑕疵不可避免。我们的研究团队在今后会持续优化，进一步改善。同样，我们欢迎广大读者给予反馈以更好地提升我们的工作。

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