解决方案简介

基于英特尔® 至强® 可扩展处理器的深信服 SASE 提供网络与安全融合的服务能力

SANGFOR 深信服科技

“数字化转型驱动着算力与网络的深度融合，安全是算网融合的重要保障，SASE 将成为用户优化组网成本、保障体验、简化运维的重要方式。基于英特尔® 处理器架构的深信服 SASE 服务满足了多分支机构、中小企业用户、移动办公用户等对于互联网、泛云应用安全访问能力的迫切需求，从而让用户无论在任何时间、任何场所，都能安全、快速、稳定地访问任何应用。双方将进一步深化合作，共同助力用户数字化转型，共建云网安融合新生态。”

— 深信服 SASE 产品线

概述

在数字化转型的驱动下，企业的应用与服务正在突破物理边界，这在催生了企业办公与商业模式创新的同时，也带来了更加复杂的网络安全风险。基于物理边界的网络安全防护模式难以有效保护企业应用与数据的安全，企业需要既能满足网络安全防护需求，又能够加速多云、多地应用网络访问的方案。在此背景下，安全访问服务边缘（SASE）服务解决方案应运而生，SASE 融合 SD-WAN 广域网能力与全栈的网络安全能力（如 SWG、CASB、FWaaS 和 ZTNA），将安全和网络能力上移，通过统一的云交付形式交付给用户，以满足企业数字化转型的动态安全接入需求。

深信服科技股份有限公司（以下简称：深信服）推出了基于英特尔® 处理器架构的 SASE 服务解决方案。该方案依托于零信任理念，包括 SD-WAN 组网、零信任网络访问、云上网行为管理、云下一代防火墙、云威胁情报网关、下一代数据防泄密等核心组件，通过云化、订阅化方式，可以将企业原有基于物理边界的网络安全防护模式，转化为基于边缘安全服务的网络安全防护模式，解决企业在云化和数字化过程中，企业办公安全上网和远程接入的问题。

深信服 SASE 服务采用了第四代英特尔® 至强® 可扩展处理器，在利用处理器强大的性能加速安全访问等负载的同时，采用处理器内置的英特尔® 高级矩阵扩展（英特尔® AMX）、英特尔® Data Streaming Accelerator（英特尔® DSA）、英特尔® QuickAssist 技术（英特尔® QAT）、英特尔® Software Guard Extensions（英特尔® SGX）等高级硬件能力，满足数据加解密、可信计算等方面的需求。

挑战：网络安全物理边界模糊化，安全访问成为重要痛点

随着数字化转型进程的加快，企业的 IT 架构逐步云化、互联网化、移动化，对于那些业务分散程度较高、分支众多的机构而言，企业数据与应用常常分散在不同的公有云、私有云和混合云上，这让跨云访问与管理变得日趋复杂。在中国，另一个值得关注的趋势是企业出海的热潮，据商务部、外汇局统计，2023 年 1-11 月，中国境内投资者共对全球 154 个国家和地区的 7149 家境外企业进行了非金融类直接投资，累计投资 8145.4 亿元人民币，同比增长 18.4%[1]。

[1] http://www.mofcom.gov.cn/article/tongjiziliao/dgzz/202312/20231203462796.shtml

同时，远程办公、移动办公的广泛盛行意味着，办公已经日渐脱离原有的物理空间限制，员工需要通过跨网络来访问企业数据与应用，以获得更高的敏捷性，提升工作效率。《中国互联网络发展状况统计报告》显示，截至 2022 年 12 月，中国线上办公用户规模达 5.40 亿，较 2021 年 12 月增长 7078 万，占网民整体的 50.6%[2]。

上述趋势意味着，企业原有以数据中心为核心的网络安全边界向以泛云、分支、移动用户等为核心的多中心、离散化访问方向发展，网络安全边界变得模糊不清，这带来了巨大的安全挑战，传统方案难以有效应对：

- **威胁挑战指数级增长，传统安全产品难以构建防御体系：**分支数量增多、多云数据中心、接入设备多样化，导致了网络边界模糊化，威胁挑战呈指数级提升，传统安全设备很难落地，以云平台交付安全能力成为必然趋势。
- **传统方案难以防御针对分支、移动终端的高级威胁攻击：**随着针对分支、移动终端的高级威胁攻击的常态化，传统方案暴露出无法覆盖离网终端、微分支，分支组网与运维困难等风险，导致高级威胁乘虚而入。
- **安全投入高：**在传统方案中，为了提升防护效果，多分支机构的每个分支都需要购入安全设备，这会带来较高的安全投入成本。
- **安全运维负担重：**传统方案通常只能覆盖特定的机构，随着分支机构的扩展，企业需要在每一条分支上部署安全方案，这将导致企业承担巨大的安全部署与运维负担。

为了解决上述问题，网络安全访问服务架构 SASE 应运而生。Gartner 于 2019 年提出了 SASE 的概念，Gartner 对 SASE 的定义是：一种结合了广域网功能和全面的网络安全功能的新兴服务产品，用于满足数字化企业的动态安全访问需求。SASE 具备云原生、身份驱动、全安全栈融合、PoP 全球分布等特点，客户不需要投入大量资金去建设、运维和管理自己的硬件防火墙等基础设施，只需要为安全服务付费，即按需购买服务，即可获得高效的安全服务能力。

根据 Gartner 和 IDC 关于网络安全市场空间的预测，2025 年全球 SASE 规模（包括SD-WAN、FWaaS 防火墙及服务、SWG、云安全访问代理和零信任）可达到 147 亿美元，其中北美市场占比 45%，亚太和欧洲超过 15%，SASE 复合年均增长率 CAGR 预计达到 36.3%；2024 年大中华地区市场规模大约为 7.69 亿美元，折合 49.22 亿元，存在广阔的市场空间。

SASE 采用了零信任访问网络、云原生架构、流量接入处理、安全服务编排、统一网络调度、全局配置一致性等关键技术，并利用人工智能（AI）、硬件加速等技术，在流量分析、加解密等方面实现了新的突破，这也对于 SASE 基础设施的算力带来了挑战。

- 在 AI 方面，安全大模型等 AI 应用在安全防护中扮演着愈发重要的作用，通过 AI 模型进行用户实体行为分析（UEBA）、流量分析、文件相似度分析等流程，有助于提升安全防护的效果，封堵更多未知威胁。在 SASE 服务中，SASE 平台需要采用训练好的模型进行模型推理，对于基础设施的 AI 算力带来了较高要求。
- 在加解密方面，当今的互联网上的流量，大部分已经转成加密流量，基于流内容的识别不仅低效，而且随着 QUIC 等协议的出现，解密再识别处理越来越困难，这就需要 SASE 平台提供强大的加解密能力支持。另外，加解密能力的提供有助于对边缘接入网关到 PoP 的 IPSec VPN 进行加解密卸载，从而大幅提升接入组件的性能吞吐。
- 在解压缩方面，在数据安全领域泄密分析场景，需要高效地对压缩文件进行分析，以实现实时的防泄密封堵。基于硬件的加速方案能够加速 SASE 平台的文件的压缩和解压，从而提升泄密分析场景的性能和体验效果。

解决方案：基于英特尔® 处理器架构的深信服 SASE 服务

深信服 SASE 服务解决方案基于零信任理念，采用云化、订阅化方式，通过全新边缘安全服务取代企业原有基于物理边界的网络安全防护模式，解决企业在云化和数字化过程中，企业办公安全上网和远程接入的问题。

深信服 SASE 服务包括 SD-WAN 组网、零信任网络访问、云上网行为管理、云下一代防火墙、云威胁情报网关、下一代数据防泄密等核心组件，将原来基于本地的行为管理、上网安全、零信任接入能力和组网的能力，通过云原生的方式，在全国网络接入点（POP 节点）上重构安全便捷的安全服务能力，为企业用户提供可按需订阅的办公安全组网和安全能力，解决企业网络访问体验、安全管理、数据安全保护等问题。

[2] 数据援引自：中国互联网络信息中心（CNNIC）：第 51 次《中国互联网络发展状况统计报告》

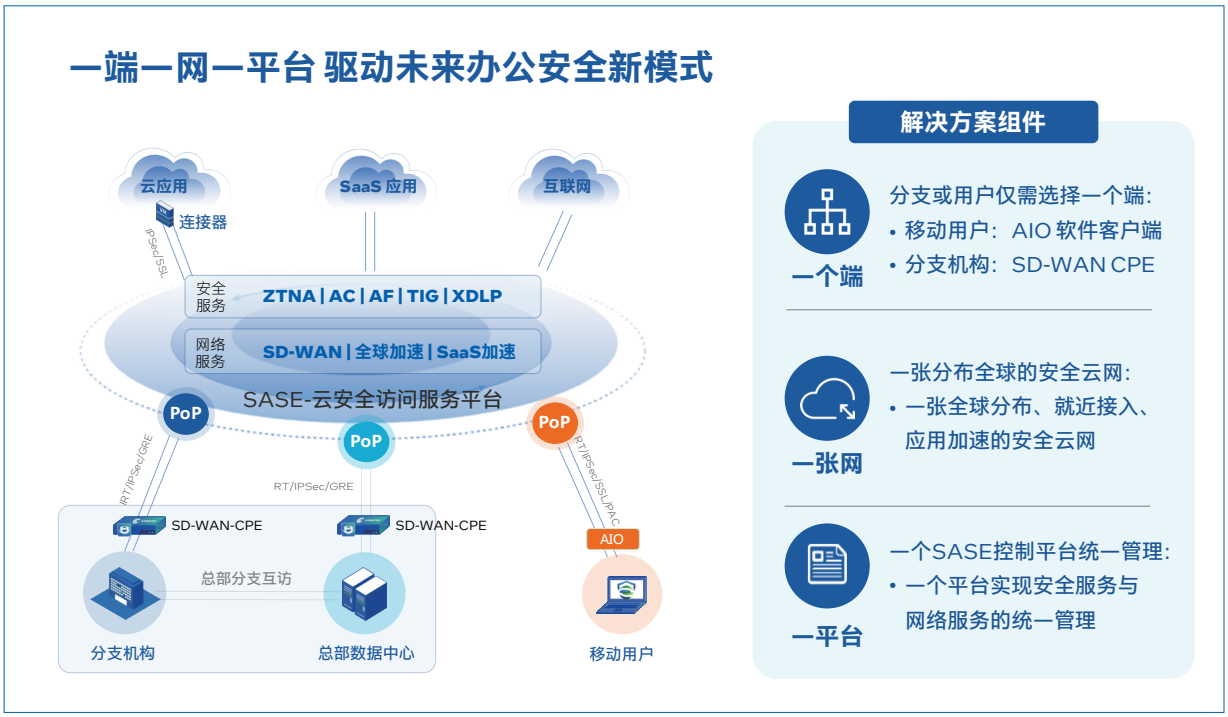

图 1. 深信服 SASE 服务架构

深信服 SASE 服务具备以下特点:

云原生多租户架构

深信服 SASE 服务完全以云服务的形式交付网络安全，其云原生架构更具灵活性且可扩展，为用户提供了一个成本更低、匹配度更高、效率更高的平台，可以快速适应新兴业务需求，实现用户就近接入，保障更好的体验。

兼容更多网络边缘，实现总部、分支和移动办公接入

深信服 SASE 服务支持多种接入方式，企业网络通过在出口部署的 SD-WAN 引流器 定向引流至 SASE；远程用户使用 All in One (AIO) 客户端连接到 SASE 作为访问互联网、SaaS 应用、数据中心及云端应用的统一访问入口，提供了无缝的用户体验，实现企业全场景接入。

拥有大量全球发布的 PoP 节点，提供更好的访问体验

深信服 SASE 服务在国内拥有 40+ 个 PoP 点，并拥有多个海外 PoP 点，可以满足用户在国内业务拓展以及出海的要求。数据中心对远程用户进行身份认证后，根据其地理位置信息将用户接入当前最近的节点，减少达到目的应用的路由跳数，进而实现加速访问。

一致性安全能力

深信服 SASE 服务基于零信任理念，将原来基于网络安全访问控制转变为身份访问控制方式，基于云端身份认证技术强化安全防护，为企业总部、分支和移动提供一致的安全体验。

在 SASE 的跨云网络安全访问过程中，由于企业网络访问规模在不断扩大，广域网流量随之持续增长，应用传输过程中存在很多冗余重复流量，造成了不必要的带宽浪费。为了解决此问题，深信服 SASE 服务采用了智能引流技术，可通过 DPI 或自定义五元组识别应用流量，高频率检测链路体验质量 (QoE) 及带宽利用率，将应用流量调度在最优链路上传输，也可指定应用在指定链路上传输。这有助于大幅度削减上云流量，带宽利用率获得了进一步提升，节省了大量的带宽扩容费用支出。

深信服 SASE 服务还集成了云情报网关服务，支持恶意 IP 过滤、恶意域名检测、威胁情报云查功能，支持全部未知 DNS、IP 流量云端检测，提供云端海量威胁情报、海量的规则 +AI 智能号引擎检测能力，100 ms 内实现云端已知威胁拦截，未知威胁 5 分钟全网情报同步[3]。

[3] 数据援引自深信服内部测试数据。英特尔并不控制或审计第三方数据。请您审查该内容，咨询其他来源，并确认提及数据是否准确。

深信服 SASE 云下一代防火墙服务基于深度应用识别技术，能够对流经防火墙的数据报文进行深度应用层分析和检测，通过对数据报文进行协议分析和重组，并根据检测结果对数据报文做出响应动作。深信服 SASE 云下一代防火墙服务 内置 8000+ 主流入侵防御系统（IPS）特征库，正常每两周例行更新，重大事件 24 小时更新响应。由于 IPS 攻击检测主要依赖攻击特征匹配，IPS 模块检测的精准度依靠规则库的数量和规则库更新的及时性，这种检测方式的劣势是无法针对复杂漏洞、未知漏洞进行防御。深信服自研的 IPS 反逃逸漏洞防御引擎在漏洞特征库的基础上，增加了行为分析检测技术，基于攻击泛化的漏洞覆盖技术，从漏洞共性攻击与利用方式，泛化出通用漏洞特征，利用最少规则检测更多的安全漏洞的能力。

采用第四代英特尔® 至强® 可扩展处理器加速 SASE 安全访问

在 SASE 的分布式边缘节点中，深信服采用了第四代英特尔® 至强® 可扩展处理器。该处理器通过创新架构增加了每个时钟周期的指令，每个插槽多达 60 个核心，支持 8 通道 DDR5 内存，有效提升了内存带宽与速度，并通过 PCIe 5.0（80 个通道）实现了更高的 PCIe 带宽提升。第四代英特尔® 至强® 可扩展处理器提供了出色性能和安全性，可根据用户的业务需求进行扩展，为 SASE 运行在分布式边缘拓扑点的各类应用提供了强大的性能基础。

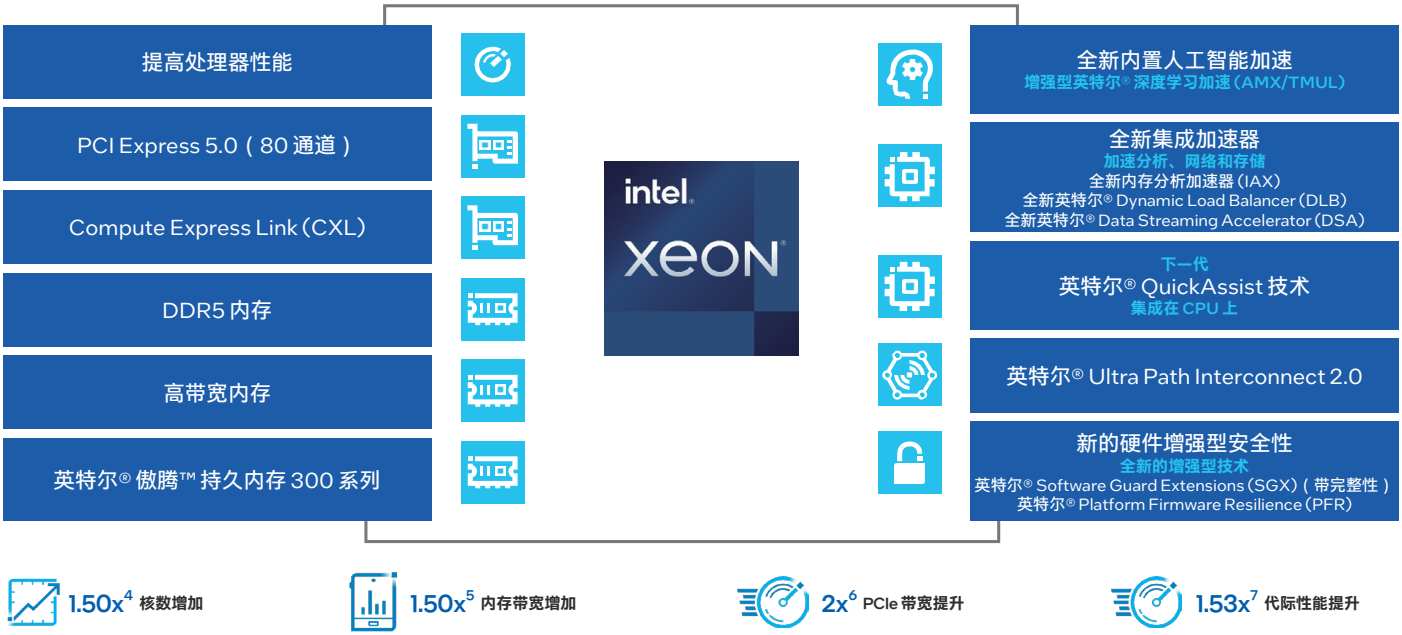

图 2. 第四代英特尔® 至强® 可扩展处理器为数据中心提供多种优势

深信服 SASE 服务需要处理广泛的加解密负载。例如，SASE 通过零信任访问控制模式，在客户端和 POP 点之前采用加密隧道传输保障安全；在安全套接层（SSL）内容管理中，通过数据加密技术，可确保数据在网络上之传输过程中不会被截取及窃听，深信服 SASE 具有对 SSL 加密内容的完全管控能力，通过中间人解密技术，解决网络加密流量解决识别和处理问题，从而支持识别、管控、审计经由 SSL 加密的内容。分布式边缘拓扑点的加解密性能将在很大程度上影响 SASE 性能。

深信服 SASE 方案采用了第四代英特尔® 至强® 可扩展处理器内置的英特尔® QAT 技术加速加密和压缩，以减少 SASE 在数据加解密负载中的开销。英特尔® QAT 是英特尔针对网络安全和数据存储推出的一个硬件加速技术，专注数据安全和压缩加速，助力应用程序和平台的性能提升。英特尔® QAT 技术有助于加速深信服 SASE 服务中的安全负载，提供更佳的性能表现。

[4] 数据来源自第四代英特尔® 至强® 可扩展处理器的最大核数（60 核）与第三代英特尔® 至强® 可扩展处理器的最大核数（40 核）的比较。

[5] 详细配置信息请访问 intel.com/processorclaims，选择“第四代英特尔® 至强® 可扩展处理器”，查看编号“G2”。实际性能受使用情况、配置和其他因素的差异影响。

[6] 数据来源自第四代英特尔® 至强® 可扩展处理器（80 条 PCIe 5.0 通道）与第三代英特尔® 至强® 可扩展处理器（64 条 PCIe 4.0 通道）的比较。

[7] 详细配置信息请访问 intel.com/processorclaims，选择“第四代英特尔® 至强® 可扩展处理器”，查看编号“G1”。实际性能受使用情况、配置和其他因素的差异影响。

深信服 SASE 还深度融合了人工智能（AI）技术，搭载了基于 AI 的网页智能分析系统（Intelligent Webpage Analysis System，IWAS），能够根据已知网址、正文内容、关键字、代码特征等对网进行学习和智能分类，帮助组织完善网页访问行为的管理。IWAS 利用第四代英特尔® 至强® 可扩展处理器内置的英特尔® AMX 来进行 AI 推理加速。英特尔® AMX 针对广泛的硬件和软件优化，它进一步增强了前代技术 - 矢量神经网络指令（VNNI）和 BF16，从一维向量发展为二维矩阵，以便最大限度地利用计算资源，提高高速缓存利用率，以及避免潜在的带宽瓶颈，从而支持深信服 SASE 方案进行高效的网页访问行为管理。

此外，第四代英特尔® 至强® 可扩展处理器还提供了包括英特尔® SGX 在内的平台级安全增强功能，有助于保护高度分布的使用中的数据。结合深信服在安全防护技术领域的深厚积累，能够更好地提供安全网络能力。

收益：助力用户安全拥抱数字化转型

基于英特尔® 处理器架构的深信服 SASE 方案能够帮助用户缓解多分支机构、移动办公、远程协作过程中的安全网络访问难题，构建高安全、易运维、高敏捷性的安全管理平台。在以下场景，其能够为用户带来重要价值：

- **多分支机构安全建设：**针对多分支机构安全建设中出现的安全投入高、统一管控难度大等问题，深信服 SASE 服务提供了高适用性的方案，分支机构只需部署 SD-WAN 设备，按需订阅安全服务，即可在云端对所有分支机构进行统一安全管控；当分支机构人员增加或带宽规模扩大，可直接弹性扩容，满足企业发展需求。
- **中小企业一体化办公安全：**在深信服 SASE 服务的支撑下，中小企业无需购买大量传统安全设备，按需订阅安全服务，即可实现违规上网行为管理、终端安全检测与响应等全面防护，企业安全无需投入专人维护，深信服云端安全专家全程助用户管理安全策略，全面保障企业办公安全。
- **移动办公安全管理：**深信服 SASE 服务可助力用户构建基于网络、设备的安全防护边界，企业只需安装轻量级客户端软件，即可对移动办公终端进行统一违规上网行为管控、信息文件防泄密、终端威胁检测等安全防护。

展望

通过深信服 SASE 服务赋能的 SD-WAN 生态，用户仅需一个登陆门户、一个运维平台，即可获得全网统一的策略和可持续生长的安全服务，实现总部和分支、客户端统一运维、成本可控、体验顺滑、安全无忧、简单运维。深信服 SASE 服务还可以与 SD-WAN 骨干网无缝融合，将深信服的软件安全和运营能力通过安全订阅、线上服务的方式一站式提供给用户，打造网安融合的新模式。在 Gartner 报告中，深信服被列为单一供应商 SASE 的代表厂商[8]，Frost & Sullivan 则在报告中将深信服评为 SASE 市场的领导者[9]。

英特尔在云计算、网络、数据中心服务器架构、企业工作站和嵌入式计算等方面拥有领先的技术积累，能够支持用户构建基于英特尔® 架构，从边缘到云的 SASE 基础设施。面向 SASE 的未来市场需求，英特尔正在与深信服深化合作，优化 SASE 服务在性能、安全性等方面的表现，帮助企业客户从其 SASE 投资中获得出色价值。

[8] 数据来源：2023 年 6 月 Gartner® 发布的《新兴技术：在三重挤压中蓬勃发展——对云安全风险投资的关键洞察》报告

[9] 数据来源：Frost & Sullivan：《Frost RadarTM：2023 年全球安全访问服务边缘 SASE 市场》

关于深信服

深信服科技股份有限公司是一家专注于企业级网络安全、云计算、IT 基础设施与物联网的产品和服务供应商，拥有深信服智安全、信服云两大业务品牌，与子公司信锐技术，致力于承载各行业用户数字化转型过程中的基石性工作，从而让每个用户的数字化更简单、更安全。一直以来，深信服十分重视研发和创新，并坚持以“持续创新”的理念，全情投入为用户打造省心便捷的产品，获得了市场的广泛认可。目前，超过 10 万家企业级用户正在使用深信服的产品。

关于英特尔

英特尔（NASDAQ: INTC）作为行业引领者，创造改变世界的技术，推动全球进步并让生活丰富多彩。在摩尔定律的启迪下，我们不断致力于推进半导体设计与制造，帮助我们的客户应对最重大的挑战。通过将智能融入云、网络、边缘和各种计算设备，我们释放数据潜能，助力商业和社会变得更美好。如需了解英特尔创新的更多信息，请访问英特尔中国新闻中心 newsroom.intel.cn 以及官方网站 intel.cn。

intel®

实际性能受使用情况、配置和其他因素的差异影响。更多信息请见 www.Intel.com/PerformanceIndex

性能测试结果基于配置信息中显示的日期进行测试，且可能并未反映所有公开可用的安全更新。详情请参阅配置信息披露。没有任何产品或组件是绝对安全的。

具体成本和结果可能不同。

英特尔技术可能需要启用硬件、软件或激活服务。

英特尔未做出任何明示和默示的保证，包括但不限于，关于适销性、适合特定目的及不侵权的默示保证，以及在履约过程、交易过程或贸易惯例中引起的任何保证。

英特尔并不控制或审计第三方数据。请您审查该内容，咨询其他来源，并确认提及数据是否准确。