商业白皮书

一流的 SD-WAN 和 SASE 以及零信任技术可为数字企业提供强大助力

aruba
a Hewlett Packard Enterprise company

目录

执行摘要

企业纷纷进行数字化转型，以期提高效率，增强客户满意度，寻求新的市场机遇，提升盈利能力，保持竞争优势。而将企业应用迁移到云端则是数字化转型方案走向成功所必须经历的步骤。为什么？时至今日，在云端运行的应用已多于在传统企业数据中心运行的应用，而且其中绝大多数应用均是以软件即服务 (SaaS) 的形式为企业所用。此外，在云优先的大环境下，企业必须确保用户可以随时随地通过任何设备直接且安全地访问应用。不仅如此，企业还需要确保网络能够始终如一地为员工和客户提供出色的体验。最后，企业中的移动和 IoT 设备数量暴增，极大增加了攻击面，使企业面临安全漏洞的威胁，而这些都有可能危及数据安全，导致网络停机时间。

今天的企业网络在设计之初并未考虑云优先的大环境，自然也无法有力应对数字化转型所带来的网络安全挑战。企业不仅需要保护云端的应用，还需要保护通过广域网 (WAN) 连接到这些应用的用户，这一点至关重要。与此同时，IoT 设备的大幅增加也极大地扩大了攻击面，导致企业面临愈发严峻的网络安全威胁。

因此，从策略上而言，当务之急是采用更智能、更安全、高度自动化的软件定义广域网 (SD-WAN)，以便无缝集成云交付安全性服务，从而形成最优的安全接入服务边缘 (SASE) 架构。SASE 必须辅以基于身份的零信任安全性来实施网络分段功能，以便用户和 IoT 设备只能访问与其业务角色相一致的网络目的地。

由于广域网和安全性转型相辅相成，但又不可能一蹴而就，企业可以先更新改造其中的一项，但要真正实现云投资的价值，这两项缺一不可。

今天的企业网络在设计之初并未考虑云优先的大环境，自然也无法有力应对数字化转型所带来的网络安全挑战。企业不仅需要保护云端的应用，还需要保护连接到这些应用的用户，这一点至关重要。与此同时，IoT 设备的大幅增加也极大地扩大了攻击面，导致企业面临愈发严峻的网络安全威胁

选择能够提供灵活性和自由选择的技术解决方案合作伙伴，也同等重要，因为这可以有效避免受供应商束缚。随着网络和安全架构的改造，企业可以及时采用创新成果，进而提高生产力，加快收入增长，增强盈利能力，控制成本。

应用在云端进行交付 — 安全保护也应如此

在传统实践中，所有来自分支机构地点的应用流量都会通过专用 MPLS 服务回传到企业数据中心进行安全检查和验证（请参阅图 1）。当应用完全托管于企业数据中心时，这种架构可以发挥作用。但随着应用和服务迁移到云端，这种传统的网络架构就显得力不从心了，这主要是因为前往互联网的流量在到达目的地之前需要首先经过数据中心和企业防火墙，由此便会导致应用性能受损，用户体验不一致。

此外，随着在企业网络之外工作并直接连接到云应用的员工越来越多，基于边界的传统安全性机制也愈加捉襟见肘。云和 SaaS 永久地改变了用户与应用建立连接和交互的方式。通过改造广域网和安全架构，企业可以确保在多云环境下，用户能够直接且安全地访问任何应用和服务，而无需考虑访问位置或设备。

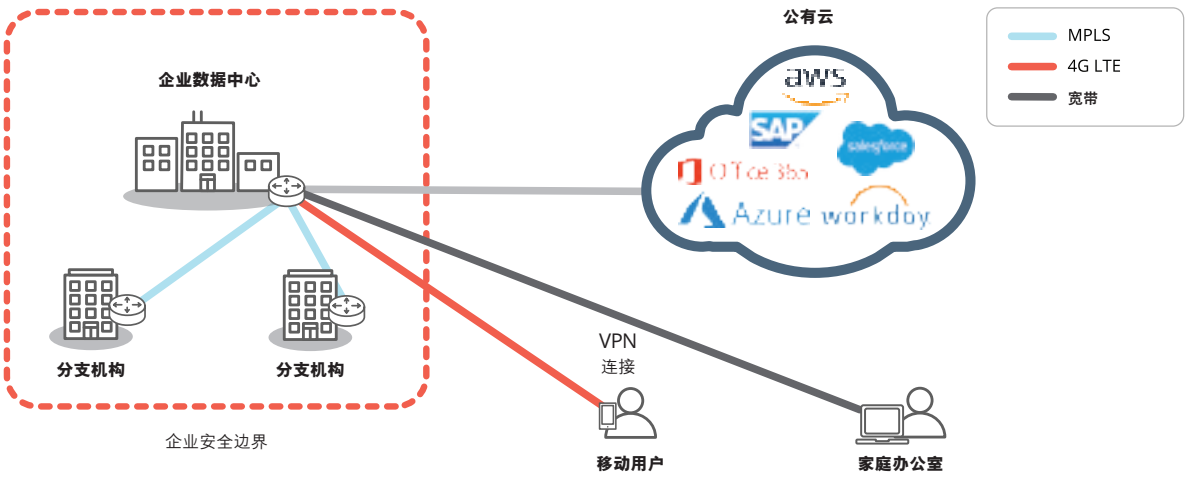

图 1：传统的企业广域网和基于边界的安全方法并不是为云而设计的。将所有来自分支机构地点的应用流量回传到数据中心会导致应用性能受损，用户体验不一致。

2019 年，Gartner 提出了新术语 SASE，即安全接入服务边缘。在这一框架下，企业可以将 SD-WAN 与云交付安全服务边缘 (SSE) 功能相结合，包括安全网络网关 (SWG)、防火墙即服务 (FWaaS)、云接入安全代理 (CASB) 和零信任网络接入 (ZTNA)。以前，这些都是相互独立的专用功能，但现在却可以通过云端统一交付，如图 2 所示。

SSE 解决方案的一些早期用户未能实施 SD-WAN，无法直接从分支机构站点应用自适应互联网分流，也因此无法直接将流量从分支机构站点定向到云。如果没有 SD-WAN 组件，前往云端的流量仍会被回传到数据中心，对应用性能产生负面影响。

安全服务边缘解决方案和 SD-WAN 可以消除管理多个本地防火墙所产生的成本和复杂操作，但为了阻止任何外来威胁，分支站点仍需要具备防火墙功能。如图 3 所示，借助先进的 SD-WAN 解决方案，企业便可以使用宽带互联网连接经自适应互联网分流直接连接到云端。智能识别白名单应用可以支持从分支机构到最近接入点 (PoP) 的本地分流，从而消除延迟，为可信的 SaaS 和云应用（如 Microsoft Office 365、8x8 和 RingCentral）提供最高质量的体验。应用感知功能还可以先将其他互联网流量发送给云交付安全提供商，以便在转发给 SaaS 提供商之前进行高级检查。先进的 SD-WAN 功能与现代云交付安全服务集成后，可以确保用户、设备、应用和 IoT 采取始终一致的执行策略和访问控制。这使企业能够落实合规性，避免停机时间，降低与安全漏洞有关的数据泄露风险。

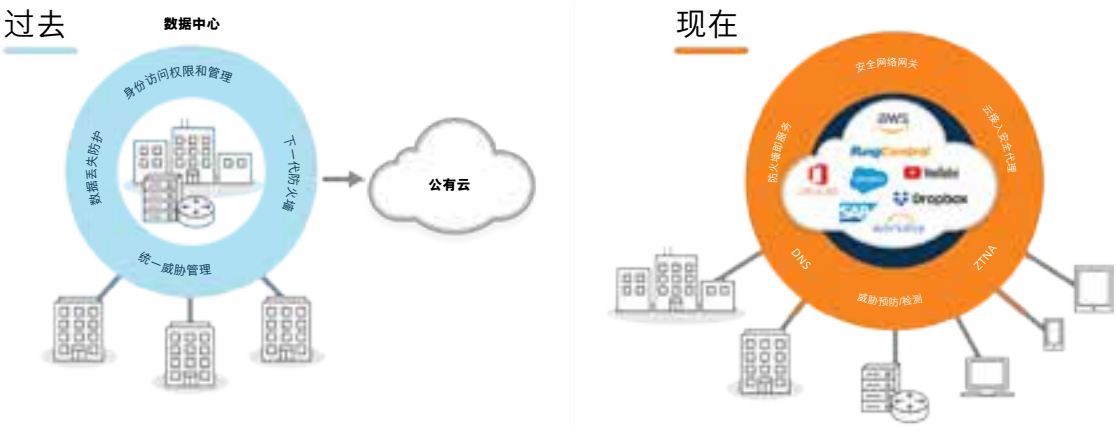

图 2：在以往的工作中，重点在于保护企业数据中心的安全，因为那是应用的唯一托管地。而现在，应用已经转移到云端并从云端交付，这无疑会让基于企业边界的安全性方法变得越来越找不到用武之地。当务之急是换一种思维，将安全性也转移到云端。

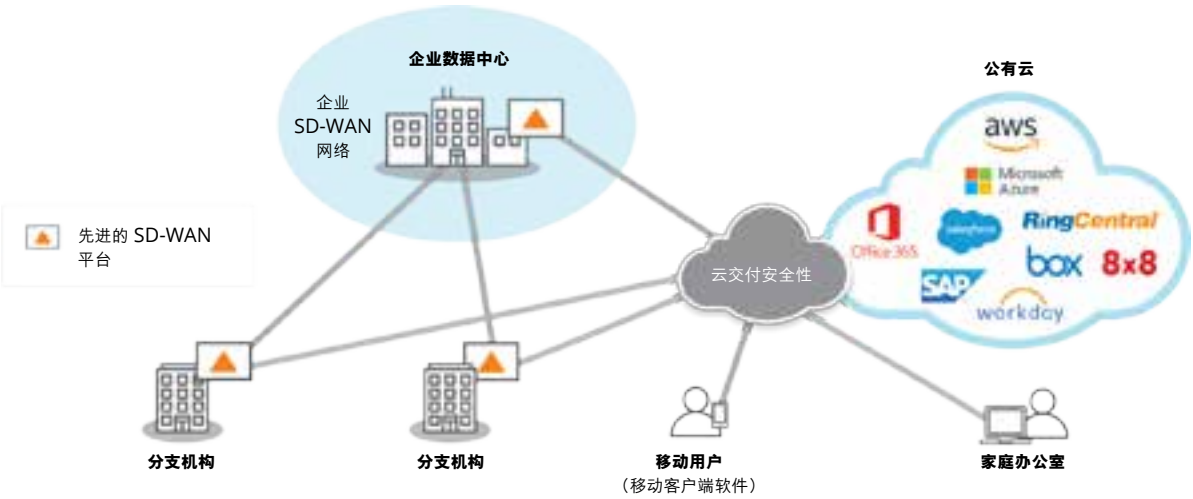

图 3：先进的 SD-WAN 为企业构筑安全的云基础。分支机构通过宽带连接和自适应互联网分流直接将用户与云应用连接起来，进而优化应用性能和用户体验。将先进的 SD-WAN 与云交付安全性合二为一，可以创建安全接入服务边缘 (SASE)，始终确保用户、设备和应用的安全。

一流的 SASE 为企业提供自由选择

随着网络安全方法的不断发展以及网络解决方案的日益复杂化，重要的是要选择经验丰富且有所侧重的供应商，以便评估出一流的安全性和网络解决方案。从现实角度来说，没有单一供应商能够兼备横跨两个领域的一流 SASE 能力，但这并不意味着企业必须降低对任一领域的要求，勉强使用基本功能。

随着威胁态势不断演变，安全性成为企业的首要顾虑，因此，企业必须保持敏捷性，才能以经济高效的方式快速采用新的安全性解决方案，而不必局限于单一供应商的解决方案。拥有独立的网络解决方案可以让企业放心地选择和部署最符合其业务发展和安全性要求的云安全解决方案。

先进的 SD-WAN 解决方案可以紧密集成多个 SSE 供应商，这意味着企业能够自由选择最优的供应商解决方案，以便利用自动编排统一 SD-WAN 和云交付安全性。借助最优 SASE，企业可以建立一致的安全架构，阻止网络攻击，同时提高业务敏捷性，降低业务复杂性。这最终将有助于企业在其现有的和进行中的云应用和服务投资上实现乘数效应。

利用零信任方法保护企业 IOT 的安全

企业中 IoT 设备的普及为业务流程的监控、报告、警报、自动化和优化带来了新的方式——从生产线的操作到 HVAC 及照明系统的节能自动化控制。借助自动化，IoT 让企业更加高效，但也使得系统的复杂程度达到了新高度，导致攻击面变大。面对日益增长的移动设备安全性挑战，IT 部门的应对方式是部署基于零信任模式的零信任网络接入 (ZTNA) 解决方案。ZTNA 解决方案的工作原理是在用户设备（如笔记本电脑、平板电脑或手机）上安装终端代理。

该软件代理可以确保来自设备的流量会先定向到云交付安全服务，之后再定向到 SaaS 应用或 IaaS 提供商。但与平板电脑和智能手机有所不同，IoT 设备是无代理设备，因此无法安装 ZTNA 软件代理，也不支持安装第三方软件代理。正因为如此，企业才需要一个适用于 IoT 设备的安全性解决方案，以便保护企业网络免受潜在漏洞的影响，避免可能的网络入侵以及对日常业务运营的干扰。

支持零信任架构的先进 SD-WAN 可以实现动态网络分段，应用最少特权访问原则，使企业能够在部署 IoT 设备的同时降低入侵相关的风险。根据身份、访问权限以及安全态势，SD-WAN 可以确保用户和设备只能与其角色一致的目的地进行通信。这个架构可以编排覆盖企业 LAN-WAN-LAN 和 LAN-WAN-数据中心/云的端到端网络分段，进而自动执行一致的安全性策略，确保更全面地了解情况。借助端到端网络分段，企业可以为 IoT 设备流量创建隔离的分段。每个分段均可定义独立的安全性策略，以定义设备流量执行的安全性策略。每个分段的流量均与其他分段的流量相互隔离，因此可以防止任何未经授权的访问。即使出现威胁，其影响也可以控制在威胁出现的分段。

我们来看一个示例。在安装了 PoS 和 HVAC 系统等无代理 IoT 设备的远程站点（如下图 4）中，先进的 SD-WAN 平台可以唯一地识别设备所使用的应用。而系统策略可以拦截 PoS 流量，并将其定向到信用卡交易处理应用所托管的企业数据中心。在该示例中，数据中心内部署的现有防火墙安全服务得到了应用。另一方面，HVAC 系统策略会先将 HVAC 流量进行分段，并将其定向到云交付安全服务进行额外的安全性检查，然后再将其传送到公有云托管的 IoT 控制中心。由于 IoT 流量根据业务策略进行了隔离，因此即便 HVAC 分段遭到入侵，也不会损害或威胁到 PoS 分段中的信用卡和个人数据。分段也有助于组织满足其业务的 PCI（或其他）合规性规定。如本例所示，采用先进的 SD-WAN 平台进行全面的安全部署，可以更好地保护当今不断变化中的企业，使其能够在尽享 IoT 好处的同时顺利踏上数字化转型历程。

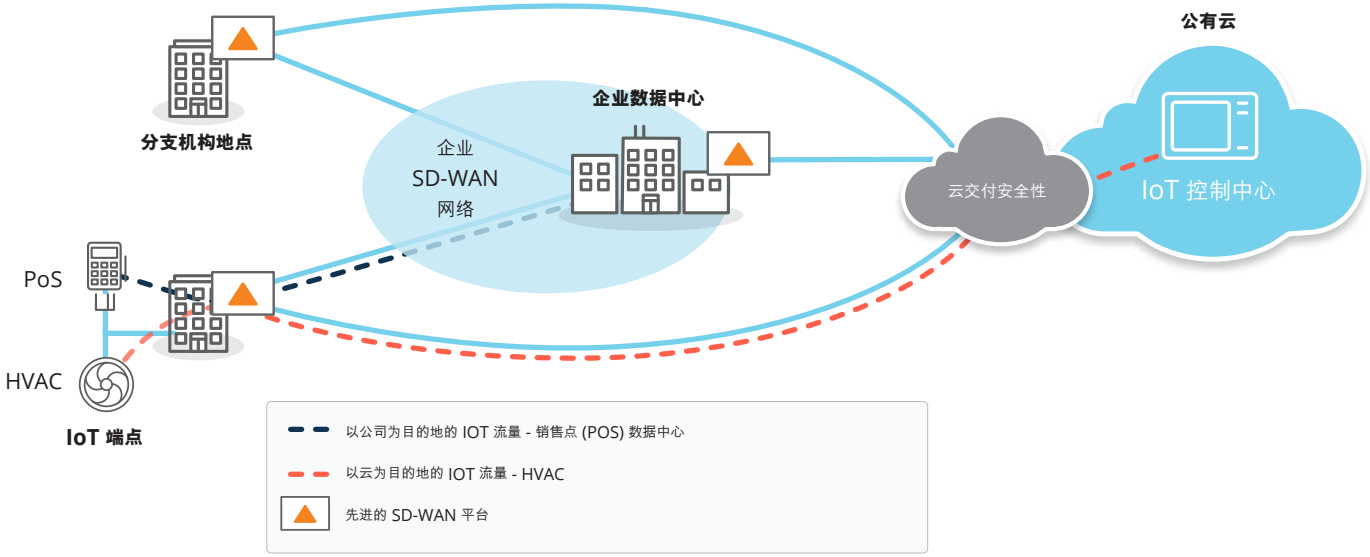

图 4：IoT 端点大量增加，带来了新的安全漏洞风险。借助先进的 SD-WAN 平台，企业可以实施零信任架构，实行网络动态分段，以此保护 IoT 设备。如图所示，分支机构的所有 PoS 交易数据全部流向企业数据中心，而 HVAC 流量则被送往云端的 IoT 控制中心。

利用先进的 SD-WAN 保护分支机构免受外部威胁

在过去十年间，随着企业数字化的发展，网络攻击的风险显著增加。在传统的基于路由器的网络环境中，分支机构堆积了大量的网络和安全设备，但这些设备很难配置、维护，也很难跟上最新的威胁发展趋势。远程站点还缺乏经验丰富的 IT 人员，导致面临潜在安全漏洞的威胁。

除了利用最优的 SASE 保护云运维以外，先进的 SD-WAN 解决方案还可以保护分支机构免受恶意威胁。SD-WAN 内置了下一代防火墙，设有入侵侦测和预防 (IDS/IPS) 及 DDoS 等威胁防御功能，可以保护分支机构免受恶意威胁。

基于特征的 IDS 系统可以始终监测网络流量，识别符合特定特征的攻击模式。在检测到入侵时，传感器会提供放弃、检查和允许流量等操作。入侵防御系统在运行时可以选择严格模式或性能模式。在严格模式下，流量须经过传感器，因此当有入侵发生时，流量会被立即阻断。在性能模式下，流量副本会被送去分析，从而在不影响网络性能的情况达到更高的效率。系统检测到入侵后会将其阻断。根据自身的安全性要求，企业可以自行选择严格模式或性能模式。

先进的 SD-WAN 还可以动态检测 DDoS 攻击，如协议攻击、ICMP 洪水攻击、SYN 洪水攻击和 IP 欺骗攻击等。在检测到异常网络行为后，该解决方案会使用快速老化、放弃过量和阻断来源等操作来限制请求数量。此外，在发生 DDoS 攻击时，SD-WAN 可以通过未受影响的网络链路继续路由流量，以此确保业务连续性。

将路由、广域网优化和下一代防火墙等先进的网络和安全性能力集成到单一的 SD-WAN 解决方案中，可以让企业极大地简化分支机构的网络运维。此外，安全策略还可以通过零接触配置从中心位置自动推送到所有分支机构，方便进行网络和安全策略的配置。这让企业可以快速轻松地设置新的分支机构，在短短几分钟内将安全策略的变更自动分发到数百或数千个分支机构，同时最大限度地减少错误。

广域网转型对于数字化转型的成功至关重要

除了迁移到现代云交付安全架构的所有好处之外，如今的云优先企业在进行广域网改造时还可以获得巨大的价值。传统的以路由器为中心的广域网从来就不是为云而设计的。企业必须更新改造广域网架构，重新思考如何以最优的方式构建分支机构网络，才能提高云应用的性能和安全性。企业不断加大云和 SaaS 的使用，同时着力优化用户体验。

广域网转型是指在用户和云之间提供更有效的路径和更好的体验。如前所述，直接从分支机构将自适应互联网分流应用于云托管的 SaaS 应用，不仅可以优化可用带宽，还可以减少任何可能对用户工作效率造成负面影响的延迟。

许多组织正在改造自己的网络边缘，也积极采用 SD-WAN，以便通过宽带互联网连接分支机构。基于统一定义的策略，SD-WAN 提供了支持多个广域网链接（MPLS、宽带互联网、LTE 等）的应用驱动型智能路径选择。SD-WAN 的优势包括:

- 交付具有成本效益的业务应用
- 提高应用性能、可用性和最终用户的体验质量
- 满足现代分支机构/远程站点或地点的要求
- 适应 SaaS 和基于云的应用和服务
- 通过自动服务配置提高分支机构的 IT 效率

满足应用服务等级协议的需求

这会直接提高企业生产力和业务敏捷性。企业需要的是基于高可用基础的高性能网络，以便为关键业务应用提供可靠支持。安全性决不能存有“亡羊补牢”的侥幸。对微分段和细粒度策略实施的支持，可以让企业有能力保护广域网，满足合规性要求，并防御漏洞。

企业必须保持敏捷，才能加快新分支机构的设置，动态调整策略和安全性规则。传播策略背景是分支机构自动化的重要需求。这使得先进的 SD-WAN 解决方案更具吸引力，因为采用此解决方案后，企业不再需要多个设备来分别执行专用安全功能，而是可以简化并巩固（或“精简”）分支机构的广域网边缘架构。通过先进的 SD-WAN 边缘平台，企业可以将 SD-WAN、路由、广域网优化、网络分段、分支机构安全性等功能统合于单一的集中管理平台，从而实现对广域网的改造。

集中化 SD-WAN 编排和针对特定应用的方法可以确保网络行为始终体现业务优先级。网络和安全策略的统一编排可以确保 QoS 和安全性始终如一地在应用（或应用类别）中得到应用和实施，无论以何种方式或在何处访问这些策略。应用性能和安全性可以由自上而下的业务策略决定，而不会受到自下而上的技术约束。先进的 SD-WAN 可以持续监控网络和应用的状态，检测不断变化的条件，并触发即时、自动的实时响应，从而消除欠压保护、停电和安全威胁活动的影响。此外，云平台与集成功能可以通过应用可编程接口 (API) 实现自动化连接，从而简化 IT 运维，使企业能够及时访问云交付安全性服务、IaaS 和 SaaS。如今的网络需要保持端到端可见性、可编程性和自动化，才能动态地保障多云环境所需的性能、安全性和最佳体验质量。采用最优 SD-WAN 和云交付安全性解决方案的智能广域网，可以推进数字化转型计划，使企业能够在不影响生产力和增长的情况下不断发展，及时采用新创新技术，同时最大限度地减少安全风险的影响。

结语

随着应用持续从数据中心迁移到云，现代云优先企业必须开展广域网和安全性转型，才能实现云投资的最大回报。而 SASE，即安全接入服务边缘，更是将该行业推向了新方向。如图 5 所示，企业在构建安全接入服务边缘时必须兼顾广域网和安全性转型，才能实现无缝体验。

先进的 SD-WAN 平台可以无缝连接各种一流的云安全服务，从而打造最优的 SASE 架构。归根结底，没有任何一家 SASE 供应商有能力通过单一平台同时提供一流的网络和安全性技术。随着威胁态势不断演变，企业必须保持敏捷，才能以经济高效的方式快速采用新的安全性解决方案。要想为企业提供更好的服务，则需要为他们提供自由的选择，协助他们评估平台是否可以整合最优 SASE。这样，企业才能避免被单一供应商的专有解决方案所裹挟，也能规避勉为其难只使用基础特性和功能的窘境。

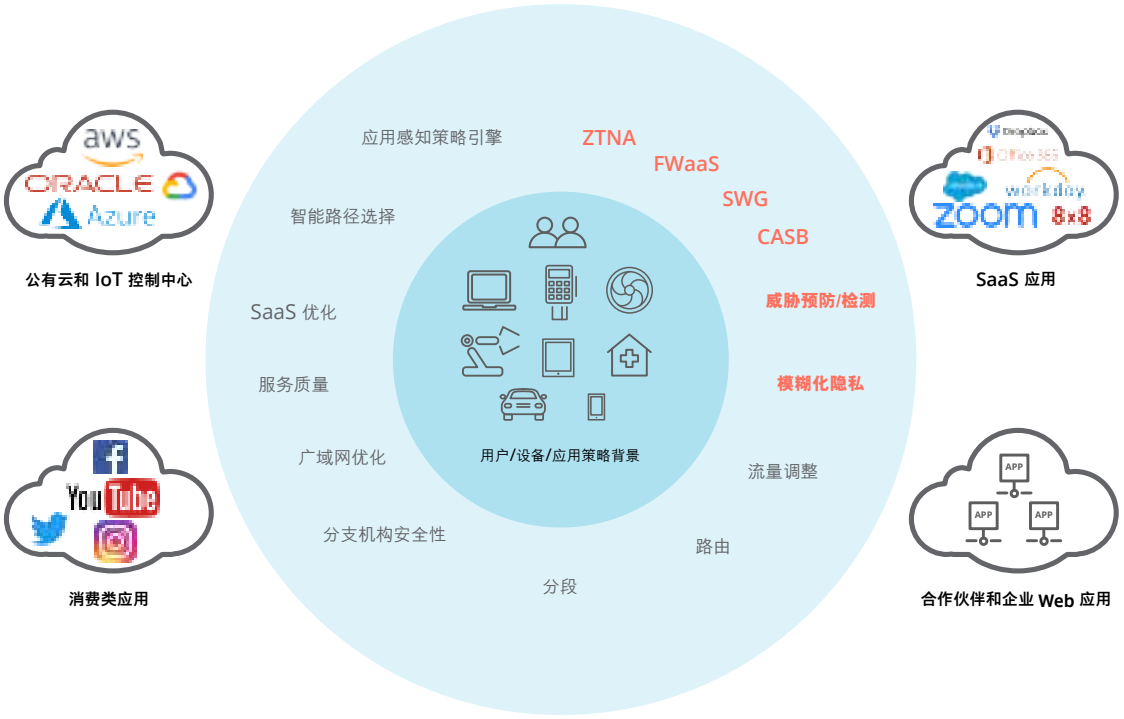

图 5：企业需要安全接入服务边缘来支持自己的数字化转型计划，即云优先策略和员工移动性需求。在强大的 SASE 架构中，齐备的广域网功能需要辅以全面的网络安全性功能，才能支持数字企业以动态方式安全地访问用户、设备和应用。

此外，随着 IoT 设备的激增，SASE 必须辅以根据身份对流量进行动态分段的零信任安全框架，以便用户和 IoT 设备只能访问与其业务角色相一致的网络目的地。

先进的 SD-WAN 可以在下一代防火墙中集成 IDS/IPS 功能，以便支持分支机构所需的基本安全功能；还可以加入云交付安全性作为补充，以此实现整个企业范围内端到端安全策略的无缝实施。这使企业有机会按照自己的节奏过渡到现代云优先的安全广域网架构，进而简化网络基础设施，而不需要作出任何妥协。

最后，有的企业可能还没准备好彻底放弃分支机构防火墙，无法完全转用云交付安全模式，但重要的是要找到一个能够提供自由选择的先进 SD-WAN 平台，并将其作为分支机构的集成解决方案，为领先的第三方统一威胁管理 (UTM) 软件解决方案提供支持。这不但可以消除采用单个专用防火墙时，往往会产生的额外成本和复杂管理工作，还可以为企业提供部署最优解决方案所需的灵活性，最终使企业能够顺利迁移到云交付安全模式。

随着企业不断加大对云的投资，为了兼顾广域网和安全性转型的要求，企业最终将走上这样一条道路：在提供最佳用户体验的同时，妥善应对当今网络安全挑战。企业在经过深谋远虑后，开启毫无妥协的广域网和安全性转型之路，最终将有能力保护自身数字资产，并在现有的和进行中的云投资上实现乘数效应。

aruba
a Hewlett Packard Enterprise company

BP_Successful-WAN-and-Security-Transformation_RVK_080422 a00110932chp

联系我们：www.arubanetworks.com/contact