

某头部金融保险公司OneWAN安全组网案例

随着金融行业的快速发展和数字化转型的推进，某头部保险公司面临着分支机构遍布全国各地、网络环境复杂多变、数据安全要求高等挑战。为提升各个分支机构间的网络协同效率、确保数据安全传输，并降低运维成本该银行决定构建一个高效、安全的网络架构。

用户痛点



缺乏灵活网络解决方案 应对复杂分支结构

分支结构遍布全国各大城市，网络环境复杂多样，因此需要支持灵活接入各种线路类型的网络解决方案。



小型分支缺乏有效 安全防护

各级城市的小型分支和网点因人数较少，投入安全硬件的成本较高导致暂时未能实施有效的安全防护。



用户体验保障与安全 架构受限制

为保障用户体验，安全防护未通过总部进行，但传统的本地硬件安全架构受到本地政策和硬件设备性能的限制，无法实现全局统一和弹性伸缩。



复杂网络需统一运维 与技术支持

由于分支节点众多，网络拓扑复杂，迫切需要统一的可视化运维管理以及7x24x365的技术支持。

赛柏特解决方案

OneWAN

+

SASE

用户效益

网络使用效率提升

通过OneWAN的智能化管理和链路优化功能，实现了分支机构间的高效、可靠连接业务处理速度大幅度提升。

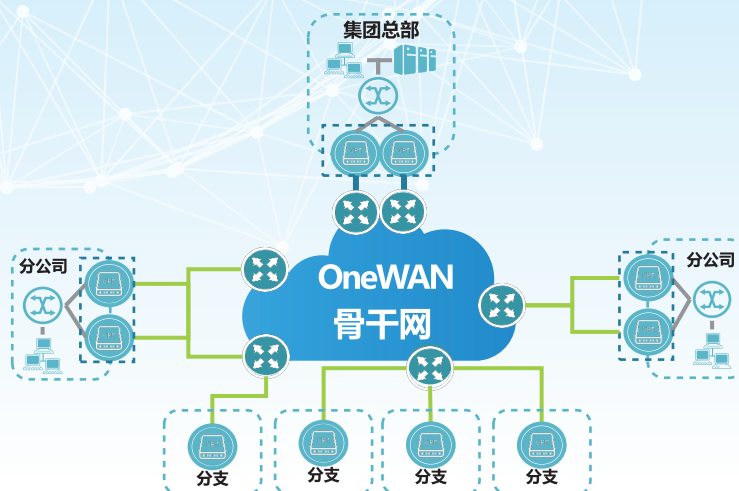
数据安全得到加强

轻资产化SASE安全方案，不但为客户节省安全建设成本，还实现了全局统一安全策略，不再依赖单点设备安全性能，实现弹性伸缩。

专业的售后运维服务

主动式自动化运维平台，及时高效响应。智能化网络故障分析、处理，提升网络服务质量。全天候7*24*365专业技术服务团队，保障网络稳定运行。

方案部署



OneWAN SASE 能力全覆盖

All in One 终端安全服务

SASE-ZTNA(零信任)

- 移动终端业务访问认证、传输加密
- 业务访问权限管控、访问审计
- 单包授权，业务隐身

SASE-XDLP (可扩展数据防泄密服务)

- 基于数据源的全新防泄密数据流转追踪
- 泄密事件预警、风险用户分析、敏感数据地图、泄密事件追溯
- 文件流转全链路图

上网管控及安全防护

SASE-SWG

- 上网认证
- 互联网访问管控
- 互联网访问审计
- IPS入侵防御
- 内容安全-防病毒
- 恶意URL过滤

安全组网服务

服务化组网

- OneWAN订阅 / 硬件AF
- 组网 + SASE安全组件

SASE-BBC

- 分支设备管理BBC
- 业务访问体验管理DEM

SASE-DNS安全

- 分支威胁云查(DNS安全)
- SDW网关联动处置

SASE-aES (终端安全管理)

- 终端病毒查杀
- 终端资产管理、外设管理、数据保护
- 漏洞扫描、补丁修复、终端基线检查

SASE能力全景图

为何选择赛柏特

全球资源 (自建骨干)

全球POP节点已升级为SASE POP，以“物理升级为云POP+云连接联动公有云”为平台，无缝连接、灵活部署SSE网。

全球交付

将安全能力部署至算力POP节点，实现多类安全能力 (FWaaS、AC、ZTNA、SWG)、同时支持自研及多品牌交付(华为、深信服、Fortinet等)交付；覆盖全类型网络，具备CPE设备全流程落地交付能力。

AI+

AI运维

AI ChatOps智能运维支持智能巡检、自动化作业、监控、自动化故障处置、故障影响可视化和自动报表监控处置能力，实现99.99%稳定性。

自主创新

携手华为共建SD-WAN联合创新实验室、开展MSSP服务模式创新，与深信服共创SASE全球一张网，获广东省科技厅“网安智算工程技术研究中心”认定，曾参编SD-WAN等多个行业标准及白皮书。

赛柏特通信技术有限公司
Cypress Telecom Limited

T: 400 6333 699
W: www.cypresstel.com
E: marketing@cypresstel.com

香港·深圳·上海·北京·西安·澳门·新加坡·东京·纽约



赛柏特微信公众号



赛柏特领英