网宿科技 | 网宿安全

网宿安全 · 2023版

SASE安全访问服务边缘白皮书

目录 CONTENTS

第一章 严峻的网络威胁态势

1.1. 企业IT架构演进挑战

当今高速发展的信息时代，网络和数据化经济占有关键地位，随之在网络空间的风险也急剧扩张，地缘政治对峙、区域战争爆发和全球经济低迷又添加了更多的不确定性，这一切造成了某些混乱失控的局面，网络犯罪分子则有了可乘之机。当下，全球Covid-19疫情虽然已经宣告结束，然而疫情所带来的企业可持续业务流的潜在风险则带来更多压力，对于所有依赖IT网络的组织，迫切需要前瞻性的布局，以增进全局业务和网络的可达性、柔性和安全性进而保持商业可持续性，这是所有组织面对的考验。

随着金融、电信、政府、能源、制造业等行业数字化转型加快，其原本封闭的网络和业务系统更加开放。大量信息、数据流转互通，网络互联、新的业务生态正在构建、合作模式加速供应链整合与效率提升追求，企业云化业务加快，预计2025年全球云计算市场容量超过1.3万亿美元，中国超万亿人民币，预期至2024年55%组织将采用云服务。由于云服务与原IDC模式的部署和管理完全变更，企业原来护城河式边界防御无法应对。

1.2. 组织内外攻击风险

网络空间的攻击形势近年来变得更加严峻，已经对全球制造、金融、能源、医疗、政府组织等关键领域造成严重影响。在某些事件中，攻击者挟持关键基础设施进而索要高额赎金，甚至可能影响国家的正常运作能力，如2021年Darkside对燃油管道运营商科洛尼尔的勒索攻击导致美国于5月9日宣布18个州进入国家紧急状态，最终以支付赎金了结，而2022年5月8日，受到Conti勒索攻击的哥斯达黎加政府多个机构陷入瘫痪，新当选总统宣布全国进入紧急状态。网络不分国界，网络攻击事件中往往导致被攻击目标的关键信息系统无法正常运转，并且攻击来源难以追踪，敏感信息的窃取和泄露导致组织极大的法律合规和业务经营风险。

1.2.1. 近期重大网络攻击事件

网络犯罪分子团队式紧密合作，逐渐向组织紧密、技术性高、目标针对性强、团伙间密切配合方向演变，而各组织内部防御措施不到位，2022年网络攻击事件频频发生。有组织的黑客组织化攻击愈发频繁，备受瞩目的攻击事件造成了巨大的金钱损失和负面社会影响。以下回顾近期发生的典型的网络攻击安全事件，通过这些事件，可见网络攻击导致的巨大风险何等惊人。

- 2022 年 12 月，蔚来汽车公司收到外部邮件，发件人表示拥有大量蔚来内部数据，并以泄露数据勒索 225 万美元（当前约 1570.5 万元人民币）等额比特币。经初步调查，被窃取数据为 2021 年 8 月之前的部分用户基本信息和车辆销售信息。

- 2022年10月，中国台湾省全岛个人信息被放在网上兜售，经调查至少20万条真实，某黑客在国外论坛“BreachForums”上出售20万条中国台湾省民众的个人资料，并声称拥有台湾省2300万民众的详细信息。
- 2022年6月，澳大利亚交易巨头 ACY 证券暴露了 60GB 的用户数据，总部位于澳大利亚悉尼的贸易公司ACY Securities (acy.com) 在网上公开了大量用户和企业的个人和财务数据供公众访问。
- 2022年6月，富士康证实其墨西哥一家工厂在5月底遭遇了勒索攻击，黑客窃取了100GB的未加密文件，并删除了20TB至30TB的备份内容，并索取1804比特币（约合人民币2.3亿元）赎金。该事件极大程度上干扰了富士康的生产节奏，其影响波及富士康整体上下游产业链。
- 2022年6月，希尔兹医疗集团因数据安全漏洞数据泄露，影响200万人。总部位于美国马萨诸塞州昆西的希尔兹医疗集团（Shields Health Care Group）报告称，集团正在调查一个数据安全漏洞，该漏洞可能影响数十个地区医疗机构约200万人。
- 2022年4月，哥斯达黎加多个政府机构遭到Conti组织的勒索网络攻击，政府程序、签名和邮票系统被破坏，财政部的数字服务无法使用，这影响了整个生产部门，总统罗德里戈·查韦斯（Rodrigo Chaves）宣布全国进入紧急状态。
- 2022年3月8日，三星证实源代码被窃取，科技巨头频陷勒索软件泥潭，黑客组织声称对芯片制造巨头英伟达进行了网络攻击，表示已窃取近1TB数据，并公开索要赎金。由于英伟达未满足其勒索要求，入侵者公布了包含英伟达GPU驱动、挖矿锁算力软件源代码等高度机密数据。
- 2022年3月1日，日本丰田汽车公司因零部件供应商受到勒索软件攻击，决定停止日本全国所有工厂运行，此次攻击导致丰田中断了约三分之一的全球生产。
- 2022年2月底，全球最大的轮胎制造商之一普利司通遭受LockBit勒索攻击，普利司通公司承认其一家子公司在2月份遭遇勒索软件攻击，导致其在北美和中美地区的计算机网络和生产中断了约一周时间，攻击者威胁从普利司通公司系统中删除信息，并将这些信息予以公布，该组织提供给被勒索的公司一个在发布数据之前付款窗口，并添加了一个倒计时器，以此产生戏剧性效果。
- 2022年02月20日，全球十大物流公司之一的Expeditors遭勒索软件攻击，致全球业务受损。

这些严重的内外网络安全一系列事件加剧了人们对于数据和网络安全性的忧虑，从科研院校到疫情防控数字化工具，从个人用户到办公软件、实体制造业，网络攻击的覆盖范围愈加广泛，且对不同行业、组织衍生出各类具有针对性的攻击形式。在此情势下，业界迫切需要追踪掌握各行业面对的各层面网络风险，分析预见网络威胁的演变和发展趋势，以采取有效应对措施保障企业和组织的信息网络安全。

1.2.2. 网络失陷造成严重损失

全球范围内的网络攻击正在急剧增加，与2021年相比，2022年企业网络遭受的网络攻击量级增加38%。黑客入侵几乎总是以金钱为动机，其中对数据的摧毁、窃取造成企业运营安全极大风险。一般而言，个人事务及隐私如果泄露可能会引起焦虑和纠纷，但对于企业而言，被窃取的内容可能包括专有信息、客户信息、账户和支付详细信息或其他极高价值的企业机密数据，一旦被攻击造成企业的业务无法运行，敏感数据被泄露公布，将对企业造成巨大伤害，企业受到网络攻击会遭受多个层面的损失。

表 1网络攻击对企业造成的损失

短期		长期	
业务服务中断	抢救修复的中断时间	声誉受损	资金损失
数据泄露	恶意软件和勒索软件感染	违规罚金	法律费用
帐户入侵	巨额应对和修复成本	客户流失	品牌信誉受损

2022年，在所有网络攻击中，恶意软件注入后门程序是最多的攻击行为，而这种攻击的后续恶意行为中约三分之二为勒索攻击。综合来看，勒索软件攻击是数量占比最多的威胁类型。勒索软件是一种极具传播性、破坏性的恶意软件，黑客用来劫持用户资产或资源、数据，旨在加密和盗窃数据以勒索钱财。勒索软件利用多种密码算法加密用户数据、更改系统配置等方式，使用户资产或资源无法正常使用，受害者必须向攻击者付费，才能获得解密密钥，重新获得数据，恢复系统正常运行。当然，即使受害者按照攻击者要求付款，仍然面临拿不到解密密钥、长时间无法恢复业务的风险。

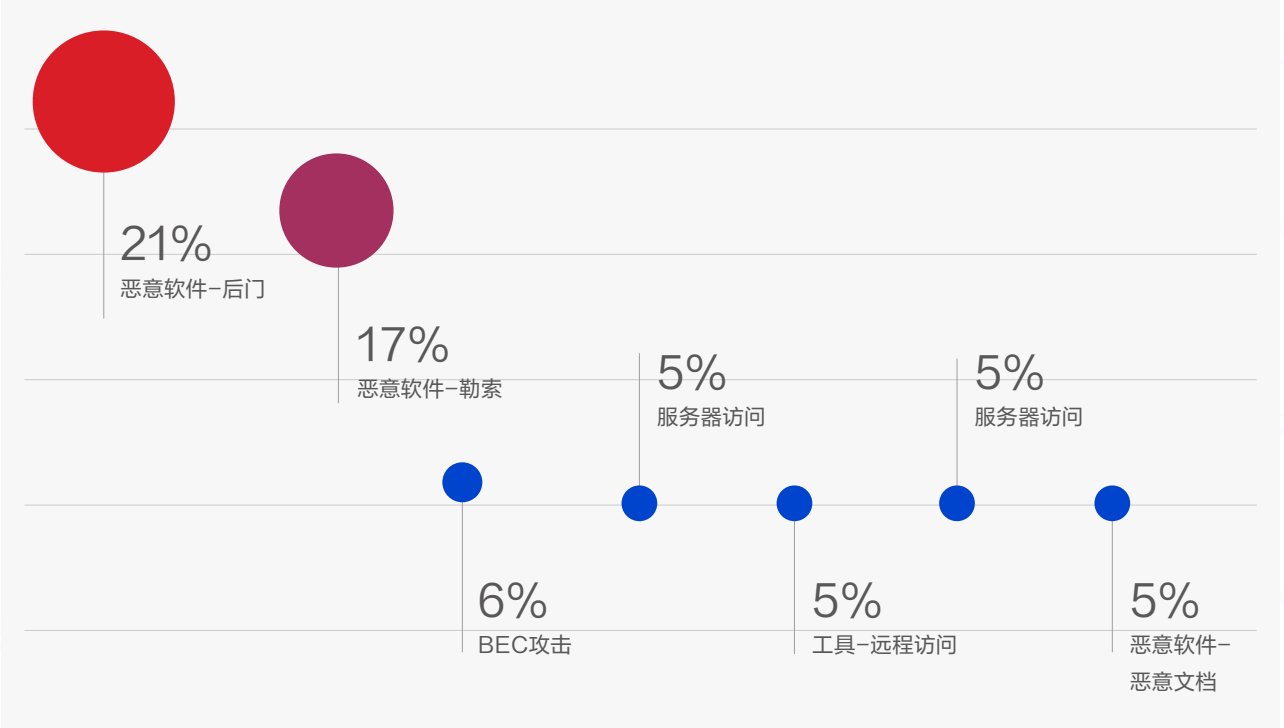

图 1 网络攻击实施动作

由于勒索攻击事件中被加密信息难以恢复，直接导致作为攻击目标的关键信息系统无法正常运转，攻击来源难以追踪，敏感信息的窃取和泄露导致极大的法律合规和业务经营风险。勒索软件对现实世界的威胁加剧，已经成为全球广泛关注的网络安全难题。如今，随着暗网、虚拟加密货币的兴起，受害者通常需要支付无法追踪的加密货币，攻击者的行踪更加隐匿，使得这种网络犯罪更加猖獗。勒索软件导致的数据泄露的规模、攻击的破坏效果都呈现扩大趋势，且在许多情况下直接攻击受害者关键设施组件致使业务中断，勒索软件攻击者对赎金的要求也越来越高。2017年在全球150多个国家和地区迅速蔓延的WannaCry勒索软件赎金仅为300美元，4年后勒索软件要求企业支付的赎金则动辄在几百万美元，REvil勒索软件在2019年前后出现在中国时，索要金额仅7000元人民币，到了2020年，该团伙的勒索金额已动辄千万美元以上。

除不可预测的赎金费用外，平均估算，受到勒索软件攻击的企业还需要付出462万美元成本用于支付检测评估、多方通告、业务损失和响应成本。尽管近年许多企业采购了网络保险，但是仅能覆盖小部分损失。从整体整体趋势来看，网络攻击导致的数据泄露的成本和影响力已远超以往。2022年，美国数据泄露的平均成本已达到944万美元，是全球平均水平（435万美元）的两倍以上。攻击抑制在当下的困难也显而易见，根据IBM和Ponemon Institute发布的一份报告“2022年数据泄露成本”，安全团队平均需要277天才能识别和控制数据泄露。

1.2.3. 网络攻击手段发展特点

网络威胁实施者利用不断变化的局面，抓住机会采用各种手段和方法，成功渗透进世界各地的组织和企业中，攻击者已经逐渐从“广撒网”误打误撞的手法转向定向攻击，表现出更强的针对性。攻击者瞄准政府、金融、能源、医疗等承载重要数据资源的行业信息系统作为实施攻击的“高价值”目标，逐渐摒弃了传统利用钓鱼邮件、网页挂马等“广散网”无特定目标的传播模式，其攻击目标转向大型高价值机构。

网络攻击导致的数据泄露事件愈演愈烈，传统防火墙、反病毒软件、入侵检测技术等信息安全防护措施已难以独立应对。此外，网络安全人员不仅要应对网络犯罪分子，还要与“内鬼”斗智斗勇。从2022年发生的各类数据泄露案件来看，涉及到内鬼占有相当一部分比例。随着黑客攻击手段不断优化，攻击方法持续迭代，再加上逐步形成的上下游产业化，围绕数据泄露进行攻击的成本不断降低，社会各团体面临的数据安全形势日渐严峻。

此外，攻击技术呈现快速升级趋势，黑客利用系统漏洞入侵以及随后的内网横向移动过程达到自动化、集成化、模块化、组织化的特点愈发明显。具体手段和策略也持续升级，如网络勒索攻击团伙往往在加密敏感数据同时将目标数据文件窃取回传，并在互联网上或暗网的数据泄露站点上公布部分或全部文件，以施加压力胁迫受害者缴纳赎金。

（1）攻击技术快速更新

混合的多媒介威胁，结合电子邮件诈骗、动态URL和偷渡式下载，从而在攻击初始阶段绕过传统的防御措施。混合攻击的后续阶段涵盖恶意软件出站通信、二进制下载和数据泄露、勒索攻击。定向攻击广泛利用浏览器、插件和桌面应用程序中的零日漏洞破坏系统。精心设计的网络钓鱼电子邮件威胁通常针对具体目标企业，攻击方式不仅具有个性化和针对性，而且随附的恶意软件、链接也很独特。由于这些恶意软件的特征码从未出现过，与网络常见的、大批量传播的垃圾邮件明显不同，因此传统的反垃圾邮件和防病毒系统很难捕获，传统的

信誉工具和垃圾邮件过滤器通常会漏掉这些信息，从而使传统的基于情报的保护手段失效。

（2）定向APT攻击

传统勒索软件攻击者使用广撒网无差别攻击，这种方式很难预测受害者是谁，哪些受害者有价值。同时，普通用户的数据价值相对不高，且缴纳赎金的意愿并不强烈。如今，勒索攻击定向精准攻击的趋势愈发明显，主要针对掌握大量数据的企业组织发起定向攻击，植入勒索软件并勒索超高额赎金。其攻击手段日趋APT化，形成涵盖探测侦察、攻击入侵、病毒植入等的精准化攻击链，如嗅探网络发现攻击入口、利用漏洞攻击入侵、精心设计的社会工程入侵等，攻击不计成本、不择手段，从低权限帐号入手，持续渗透攻击，直到控制企业核心服务器，渗透全面释放恶意软件，使受害者企业彻底瘫痪以有效勒索赎金。

（3）双重/多重勒索攻击

双重/多重勒索成为犯罪分子胁迫受害用户屈服的有效手段，一半以上的勒索软件采用双重勒索手段。勒索攻击从单纯的支付赎金即可恢复被加密的数据，逐渐演变成先窃取商业信息和内部机密，攻击者通过甄别和窃取用户重要数据，以公开重要数据胁迫用户支付勒索赎金，这种新模式也被称为“双重勒索”。这样一来，不仅使得勒索攻击杀伤性增强，被勒索企业缴纳赎金的可能性变大，即使企业使用备份恢复系统，核心机密泄露也会导致极其严重的损失，使得受害企业同时承受数据公开、声誉受损、法律处罚等多重压力。此外，在攻击者加密之前通过在受害者目标环境中安装具有DDoS攻击能力的后门程序，以“拒绝支付赎金则外泄数据或发动DDoS攻击”为威胁筹码，形成多重勒索，逼迫受害方支付赎金。

（4）供应链攻击

不同于攻击单一目标，供应链攻击指数级扩大入侵范围，通过入侵上游供应商，如通过软件补丁方式分布到众多使用该软件的企业IT设施内部。对于企业而言，其网络节点和上下游关联企业、供应商都成为潜在的攻击漏洞，产业链中安全薄弱环节均成为攻击者实现突破的关键点。

（5）攻击产业平台化

各类网络黑客生态系统正在不断发展壮大，形成了更小、更灵活的犯罪团伙。不断扩大的市场规模触发了新的盈利模式，部分网络勒索软件攻击组织开发了RaaS（勒索软件即服务）平台，面向“会员”提供开箱即用的勒索软件攻击服务。开发者可以提供一整套解决方案，如购买勒索软件程序、靶标系统访问权限，或订购针对特定目标的勒索软件攻击服务，甚至包括利用加密货币进行赎金支付等。同时，在社工信息、病毒开发、攻击入侵等环节招募合作伙伴，分工协作增加勒索软件攻击成功率。依赖这种平台化模式，攻击者甚至不需要任何编程技术就可以开展违法犯罪活动，网络攻击的门槛大幅降低，理论上任何人只要支付少量费用就可以通过这类服务平台开展勒索攻击。依靠这种黑产模式，某勒索攻击软件仅用一年多时间就敛财20亿美元。

1.3. 网络风险分布和管控框架

网络黑客和攻击者有许多可行的途径入侵企业内部，网络犯罪分子在利用网络渗透入侵的技术手段、社会工程和系统漏洞利用方面非常有“创意”。常见攻击手段如钓鱼邮件传播、水坑网站挂马传播、垃圾邮件、漏洞入侵、远程登录入侵传播、供应链传播和移动介质传播等。在常见的网络攻击事件中，攻击者往往首先利用系统、流程、人员的弱点进占入口，进而实施后续各类设施破坏、数据窃取和勒索行动。

1.3.1. 网络攻击事件的利用入口

在整个2022年，网络入侵事件中，利用网络钓鱼发起攻击占据了41%的比例，包括使用附件、链接、服务三种具体方式的钓鱼攻击。反网络钓鱼工作组(APWG)报告称，在2022年第三季度总共观察到300万次网络钓鱼攻击，这是该组织观察到的最糟糕的一个季度。尽管企业对员工进行多年的安全意识培训，但危险的用户行为仍以极高的比率持续存在，导致各种包括对可疑链接的点击和考虑不周的恶意应用程序/文件下载等失误行为。

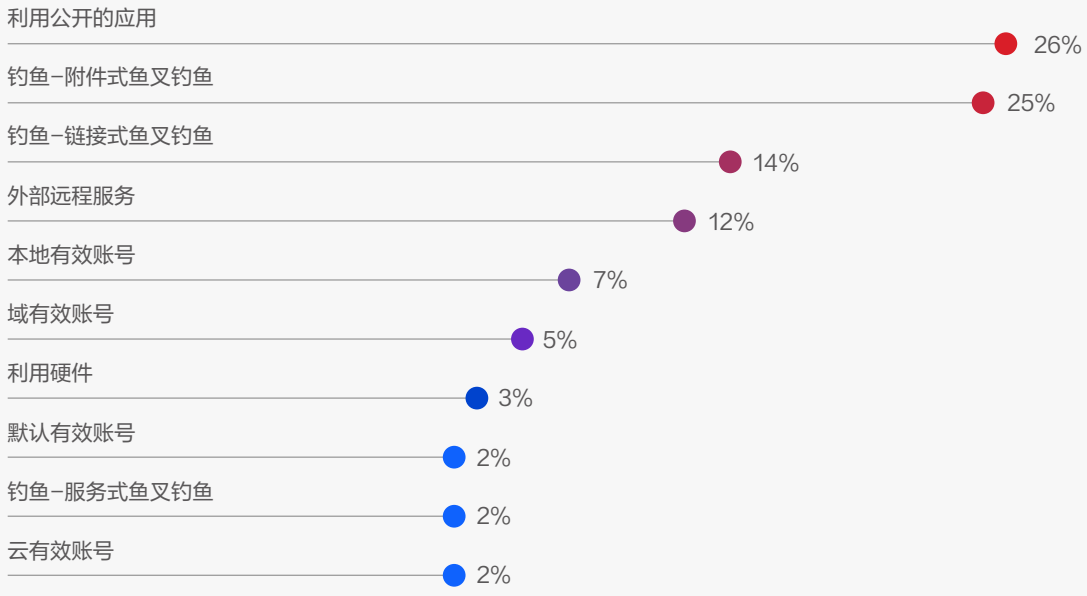

图 2 网络攻击起始接入方式分布

网络钓鱼是指企图窃取敏感信息以利用或出售的一种网络攻击行为，敏感信息的形式包括用户名、密码、信用卡号、银行帐户信息、商业机密或其他重要数据。攻击者伪装成信誉良好的来源，诱使受害者受骗上当，类似于渔夫使用诱饵来捕鱼。钓鱼（包括钓鱼邮件、钓鱼网站、诱饵文档或程序伪装等）作为低成本的攻击方式一直被网络攻击者大量使用，犯罪分子精心设计社会工程实施钓鱼攻击，诱使受害者点击链接访问恶意网站地址、打开附件中恶意文档、点击恶意链接从而触发后续入侵和恶意软件植入。

网络钓鱼攻击几乎为全球所有行业都带来了损害，任何企业都可能成为网络钓鱼的目标，据估计32%的数据泄露与钓鱼攻击有关，应对钓鱼攻击已经成为当今企业组织网络安全亟需应对的高优先事项。钓鱼攻击者的一般动机包括：

1、窃取银行账户、交易平台账户等信息
2、获取个人信息，地址、电话、身份ID等敏感信息
3、窃取企业组织的机密文件
4、进一步实施勒索软件攻击
5、获取立足点，寻找有价值目标，实施后续的攻击或组织内放大攻击

钓鱼网络攻击中，攻击者发送含有恶意链接、恶意附件的邮件给受害目标，一旦收件者打开邮件中携带的恶意链接，访问攻击者事先部署的钓鱼网站，输入敏感账户信息后，攻击者即可在后台收集到用户的敏感应用访问凭证，冒充受害者登入敏感系统，进行数据、资金等窃取和破坏活动。

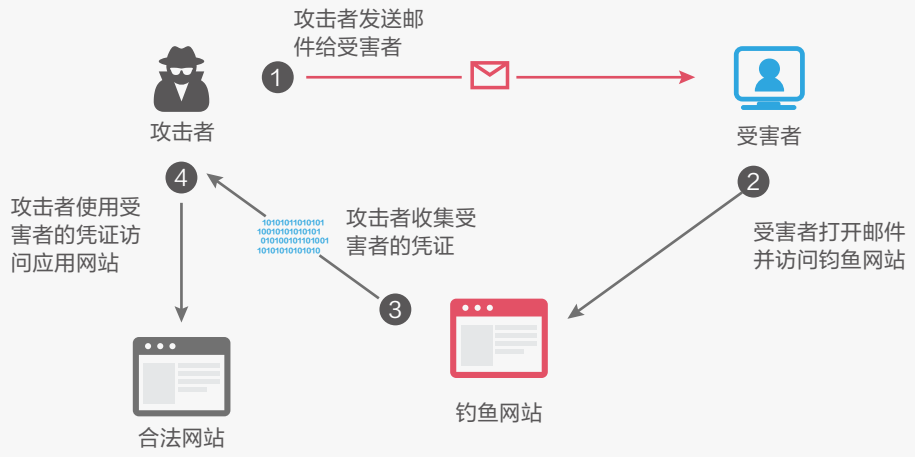

图 3 典型钓鱼攻击过程

此外，攻击者还会利用邮件附件/恶意网站中的木马病毒、间谍软件进行通信窃听、入侵企业内网、盗取敏感数据的钓鱼攻击后续行动。

排名第二位、第三位的则是面向外部互联网的应用和外部服务。攻击者扫描、探测、开发利用这类对公服务的脆弱性，例如各类层出不穷的0day漏洞，一旦渗透成功即在组织内部网络中横向移动的立足点展开内部的扩展攻击。例如，在2021年12月才被披露的Log4j漏洞，在短期内即在“被利用最多的漏洞”排行中快速上升到第二位。在其被公开后48小时，攻击量即达到10万，3天内有超过100万次攻击。截止2022年1月31日，SonicWall组织记录到1.422亿针对Log4j的尝试攻击。这种波及面非常广泛的漏洞如果被成功应用到犯罪分子的攻击行动中，就可能会带来新的波及全球的大规模企业网络攻击冲击波。

此外，攻击者有相当一部分即利用各类账号、凭证实施爆破、入侵，冒充合法用户身份在企业网络中放大攻击面，伪装成正常操作窃取企业核心敏感数据，恶意攻击软件一般的传播途径包括如下方面：

1、利用钓鱼邮件传播。攻击者发送带有恶意链接和恶意文件附件的针对性的网络钓鱼邮件，一旦用户打开邮件附件，或点击恶意链接，恶意软件将自动加载、安装和运行，实现实施恶意软件攻击的目的。

2、利用安全漏洞传播。漏洞利用仍是攻击关键手段，引发恶意软件传播一点突破、全面扩散。攻击者主要利用已公布漏洞，通过漏洞扫描、端口扫描等方式主动发现未及时修补漏洞的设备，利用弱口令、远程代码执行等网络产品安全漏洞，对用户内部网络实施远程攻击入侵，获取管理员权限并在攻击目标内部网络横向移动，扩大恶意软件感染范围，实施更多入侵行动。同时，一些零日漏洞一直在被威胁实施者利用。

3、利用远程桌面入侵传播。攻击者通常利用弱口令、暴力破解等方式获取攻击目标服务器远程登录用户名和密码，进而通过远程桌面协议登录服务器并植入恶意软件。同时，攻击者一旦成功登录服务器，获得服务器控制权限，可以服务器为攻击跳板，在用户内部网络进一步传播恶意软件。

4、利用网站挂马传播。攻击者通过网络攻击网站，以在网站植入恶意代码的方式挂马，或通过主动搭建包含恶意代码的网站，诱导用户访问网站并触发恶意代码，劫持用户当前访问页面至恶意软件下载链接并执行，进而向用户设备植入恶意软件，攻击并且可以从浏览器发起内存空间无文件攻击，无需落地文件到磁盘驱动器，规避安全检测。

5、伪造正规软件传播。仿冒或者篡改正常软件应用程序，通过虚假软件和虚假产品更新，诱导用户下载执行，隐藏在程序/可执行文件中的恶意程序加载勒索攻击病毒。

6、利用移动介质传播。攻击者通过隐藏U盘、移动硬盘等移动存储介质原有文件，创建与移动存储介质盘符、图标等相同的快捷方式，一旦用户点击，自动运行恶意软件，或运行专门用于收集和回传设备信息的木马程序，便于未来实施针对性的恶意软件攻击行为。

7、网络文件共享传播。攻击者将恶意攻击病毒植入PDF、DOC等文件中，利用网络共享平台、各类网盘等分发，用户下载后打开文档即触发恶意软件攻击，此类外表正常的文档隐含攻击代码，极具欺骗性。

8、利用软件供应链传播。攻击者利用软件供应商与软件用户间的信任关系，通过攻击入侵软件供应商相关服务器设备，利用软件供应链分发、更新等机制，在合法软件正常传播、升级等过程中，对合法软件进行劫持或篡改，规避用户网络安全防护机制，传播恶意软件。

1.3.2. 网络安全防御管理机制

根据NIST计算机安全事件处理指南，对网络攻击事件处理生命周期涵盖早期预防、探测事件和分析、遏制攻击和消除及恢复、事后复盘整改四个阶段。

图 4 安全管理阶段

全面的针对网络和数据的防护需要同时在多个方面保持主动和警惕，安全必须涵盖在企业运作的每个方面。下面以当下造成严重网络安全威胁的勒索软件攻击防御为例，说明企业体系化安全全局建设的多阶段关键要点。

事前预备：

1、员工培训教育，企业分部门、角色进行定期网络安全培训，提升网络管理员和普通用户的安全意识。普通用户是各类钓鱼邮件、恶意软件攻击的入口，需要经常进行网络安全日常培训，包括内部通过模拟方式进行演习强化。

2、修复薄弱策略，针对文档宏的风险进行组策略安全配置，如封禁互联网获取文件中宏的运行，去除邮件中可执行文件，限制temp目录中程序的执行，全局禁用adobe Flash，限制 Windows Scripting Host脚本执行，AD管理入口不应直接暴露在互联网提供访问。

3、登录密码加固，用户应当及时修改默认密码，修改企业中重要资产、系统、组件和接口的默认密码，同时增加密码强度。

4、采用MFA机制，密码可能失窃或被暴力破解，企业应在尽可能多的登录入口采用多因子认证，保证攻击者即使获取密码也无法轻易突破系统。

5、激进补丁政策，攻击者大量利用已经公布的漏洞和0DAY漏洞，主动和定期修复操作系统、第三方程序的漏洞，维持快速和自动化的补丁机制，这些措施有助于保护企业免受恶意攻击者进行漏洞利用入侵。

6、减少网络暴露面，避免关键信息系统在互联网上暴露，尽可能减少资产在互联网上暴露，特别是避免重要业务系统、数据库等核心信息系统在互联网上暴露。

7、DNS和流量过滤，增加DNS可见性，识别网络访问中恶意目标域名、IP并进行封禁和告警，判断DGA形态可疑的DNS请求并进行处置，阻断连接攻击者的C&C服务器。

8、最小权限原则，对组织内的关键业务系统设置严格的访问权限和维护变更，限制用户仅访问所需要的网络、系统和数据，限制其数据读写权限，限制用户本地设备admin权限。

9、程序和设备控制，监控终端环境情况，只允许运行所需的应用程序，只允许必要的 USB 连接系统，关闭自动播放功能，关闭或者修改默认的135～139、445等高危端口。

10、执行安全域控制，对内网的安全域进行合理的划分，域之间通过访问控制列表（Access Control Lists，ACL）限制，阻止横向移动，对于域管理员账户和设备加固防护。

11、严格备份计划，建立关键数据、系统的周期备份计划，创建勒索软件类攻击无法访问的防篡改备份副本，包括本地网络备份、离线备份、云备份。

12、部署EDR工具，EDR有助于尽早发现攻击并进行隔离，避免成为攻击跳板，帮忙IT人员观察感染设备情况和进一步的分析。

13、制订响应计划，考虑周全的事件响应计划使企业在面对灾难级局面时，在处于极度紧张的局面下，在各个层面、组织上进行协同和处置，减少最终损失。

检测响应和分析：

1、网络恶意攻击企业网络共享设施，用户工作中发现网络共享文件被加密不可用，应定位受感染用户设备并阻断其访问，抑制进一步对网络共享设施中数据的加密。

2、网络恶意攻击用户本地设备，用户工作中发现本地文件被加密不可用，应立即将设备关机以阻止恶意软件进一步的攻击和内部扩散，交由IT专业人员处理。

3、企业SIEM系统发出文件大规模操作告警，对于部署SIEM监测的企业，有可能发出超出日常文件操作量的告警，从而引起IT人员注意，定位到已经发生恶意攻击。

4、网络恶意攻击者发出提示信息，攻击者在已经执行完对本地和网络文件的加密后，会在感染设备的界面中留下网页或者文档，告知受害者数据已经被加密，应当立即拍照以提供给安全专业人士进行分析，这有助于确定恶意攻击软件类型以寻找应对经验。

5、分析恶意软件的变种类型，根据恶意软件的消息、攻击表现和路径，研判恶意软件的变种类型。
追踪定位攻击者初始入口，如果是通过邮件钓鱼则需要扫描公司内邮件库以清除所有可能未被打开的攻击邮件，如果是访问恶意网站则立即进行防火墙屏蔽，如果是经由系统漏洞的攻击则需要立即进行补丁修复。

抑制、清除和恢复：

1、一旦发现攻击发生，应当立即隔离受感染设备，断开其网络连接或者关机，以防止攻击在内部的进一步扩散。
2、下线共享文件和数据，在无法明确定位到感染根因时，快速将已经部分加密的共享设备下线以阻止进一步数据破坏，包括各类开启CIFS/SMB协议的装置都应当进行检查。
3、清除网络设备中感染的恶意软件，包括各类本地设备和其它关键设备及服务，同时应当清除所有钓鱼邮件、屏蔽恶意网站，有策略地修改受影响的用户密码以阻断攻击者利用。
4、对于定位到是由系统漏洞攻入，则应当进行打补丁操作，阻止后续可能的再利用攻击，对于无法打补丁的情况则需要进行隔离，消除暴露面风险。
5、恢复遭到时破坏的数据，如果系统备份机制运行正常且备份数据未被加密、删除，则可以从备份库中恢复数据，应当检查确认备份库未被植入恶意攻击文档、代码。
6、由专业人士分析，寻求是否可能破解加密，或者从感染设备中打到解密密钥，当然，根据既往攻击事例，这些措施成功可能性较低。
7、按照合规和法律要求向相关机构报告恶意网络攻击事件。
8、决策是否支付赎金，寻求专家建议，评估系统和数据的破坏程度、法律合规的要求、支付后是否保障恢复、获取到解密密钥进行恢复的时长成本等。

复盘和加固：

1、会议检讨事件处理过程，评估应急预案各项措施的执行情况，进而对事件响应预案进行修订优化。
2、系统检视和加固，由安全专家组织检视内部网络、安全架构的合理性，修补其中的漏洞，规划演进组织的安全机制、提高安全成熟度。

而整合的SASE，可以很好地在边缘侧，包括接入用户、设备侧和接入通道网关侧，在此前沿地带即可隐藏内部脆弱性，以强认证措施对接入方进行身份核实，且严格实施最小权限原则，动态评估和细粒度调整，在安全PoP上即对流量即时进行威胁检视和阻止，保护企业的资产、人员和数据安全。

第二章 SASE安全体系

2.1. SASE架构和能力

2.1.1. SASE的定义

云、大数据、物联网、边缘计算以及移动办公的发展已经从根本上改变了访问和连接网络的要求，对于大多数组织来说，现在有更多的用户、设备、应用程序、服务和数据位于企业外部，而不是在企业内部。企业广泛的云服务的发展，需要提供来自世界任何地方的最佳连接，而不仅仅是来自数据中心的连接。地理位置不同的分支、需要以可靠的传输来连接到物理和云数据中心，这些数据中心必须比公共互联网更安全可靠。尝试使用传统的基于边界的方法随时随地保护安全访问，导致供应商、策略、控制台和复杂流量的路由管理、安全控制，增加了复杂性和成本，并降低了敏捷性。由于缺少统一的工具支持访问响应速度和安全控制能力，给安全管理员和用户带来复杂性倍增的压力，当下组织需要的是能够基于身份感知和上下文感知的网络和安全访问新模式，可以将用户、设备和分支连接到任何位置、任何资源，随时随地高效为企业数字资源服务提供安全支撑，高效和敏捷的网络、安全防护的诉求，移动办公、三方合作接入等更加普及发展，成为组织必需品。

企业需要同时满足安全性、云、远程访问和连接要求。SASE将SD-WAN组网、安全性和远程访问融合到统一的云服务中，减少了以往单点解决方案的数量、复杂性、成本和繁重的运维工作，从而获得一致性、敏捷性、安全性及对组织业务支持的速度和效率。

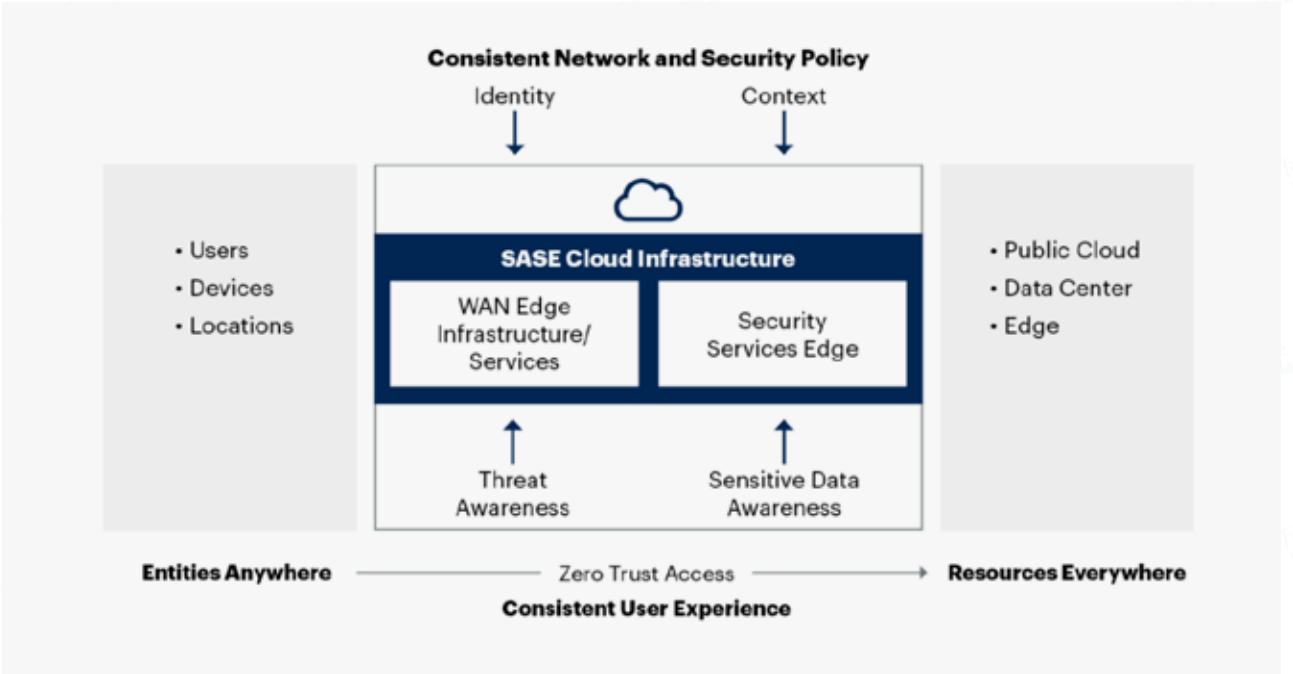

图 5 Gartner SASE框架定义

2019年，Gartner定义了安全访问服务边缘(SASE)的概念，SASE将全面的网络即服务功能与全面的网络安全功能相结合，以支持数字化企业的动态安全访问需求。

SASE方案提供多种融合网络即服务、安全即服务功能，包括软件定义广域网（SD-WAN）、安全Web网关（SWG）、云访问安全代理（CASB）、网络防火墙（FW）和零信任网络访问（ZTNA），使用以云服务为中心的架构。SASE支持企业各分支机构互联、远程工作人员访问和本地通用互联网访问、云资源访问的安全。基于用户的身份启用零信任访问，以设备或其他主体结合实时上下文控制边缘访问的所有流量，管理全面的安全性和实施统一合规性策略。SASE产品具有跨所有功能的通用管理平面，保持数据、网络的一致控制。可以随时随地向任何用户、任意设备、任意位置提供访问能力，是集安全、网络为一体的服务平台。

2.1.2. SASE的核心组件

SASE目前是方兴未艾的IT市场新技术类别，它将组网SD-WAN、安全性和访问控制在云中进行融合，通过新的融合云原生架构提供对现有分散网络的组合和安全控制功能。它帮助IT化组织变得更快、敏捷和高效，同时保持高性能和安全的网络。SASE融合各类网络、安全能力组件，呈现能力整合、统一管理、策略控制的体系化服务。

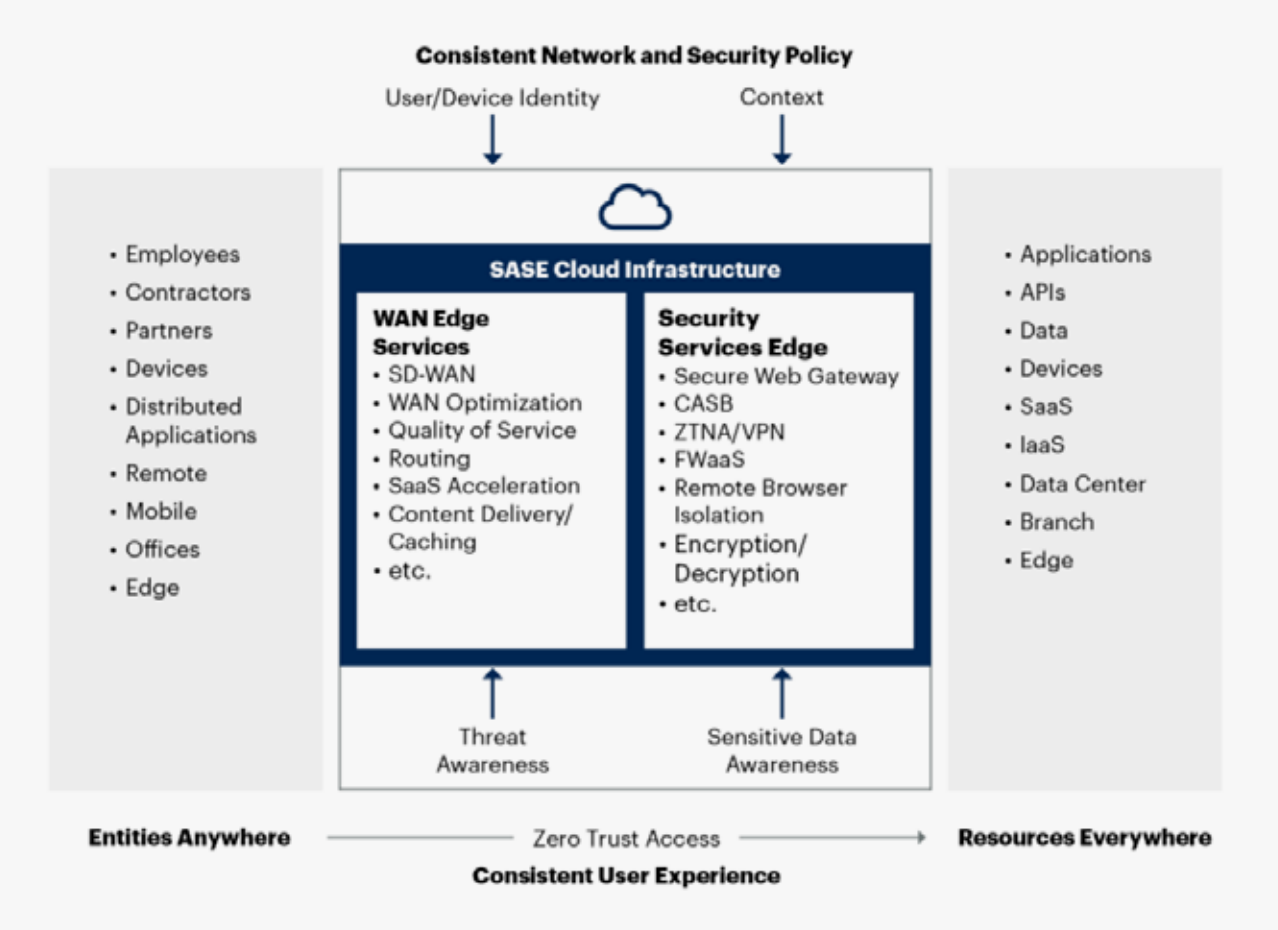

图 6 Gartner SASE标准组件框架

1、SD-WAN软件定义广域网，使用软件来管理企业的广域网连接，利用虚拟化技术，根据业务流量和链接需要进行不同的叠加网络连接和管理，提供分布式企业组织之间的网络连接，其位置和资源以私有方式托管，保障灵活的数据中心底层连接，其允许企业使用任意组合的底层连接服务，如MPLS、互联网或移动（例如5G）互连网，此功能使企业能够选择最高效的用于传输流量、同时降低成本的连接方法，并且简化管理，提供广域网优化，侧重于最大限度地提高数据业务效率，在不同位置如数据中心、分支机构和云之间保障高效传输能力，使用如TCP加速、网络缓存、压缩技术和具有前向纠错技术保障网络的效率和完整性。

2、ZTNA零信任网络访问，将网络空间的网络元素身份化，通过身份定义访问边界，为远程用户和第三方提供了一种访问组织的本地和云应用程序的安全方式，通过动态评估访问请求的置信度，对访问行为进行持续干预，使用基于最小权限原则控制对网络业务、数据的访问权限，无论用户位于何处，均需要对用户、设备进行严格的识别和验证，在用户、设备、网络、应用和数据的访问过程中建立持续适应性的信任评估控制，以增强安全策略执行可信度。

3、FWaaS防火墙即服务，云化的防火墙服务，将下一代防火墙（NGFW）功能扩展到任意位置和用户，取决于具体地点要求，它可以控制VLAN和子网之间的访问，无需现场使用物理硬件式的NGFW设备。FWaaS实施应用程序感知访问，控制资源站点和用户之间的连接和安全控制策略，同时将IPS策略应用于所有流量，识别和抵御威胁攻击。

4、SWG安全Web网关，基于云的SWG消除了对本地UTM设备的需求，SWG保护用户对互联网网络资源的访问，利用威胁情报，通过URL过滤和反恶意软件检测以保护互联网流量安全，提供流量解密和深度数据包检测来感知威胁并防护企业内部网络和用户、设备的安全性。

5、CASB云访问服务代理，用于发现业务中使用的基于云的应用程序，通过检测流量分析它们的使用方式以及由谁在使用，并控制对这些访问执行什么样的操作。CASB功能还扩展到检测敏感数据类型，并在此类流量或文件尝试离开组织时执行干预动作以保障安全合规性。

6、RBI远程浏览器隔离，为用户提供安全访问网络资源的隔离化方式，消除恶意站点、恶意软件、零日漏洞利用和网络钓鱼的威胁。一般通过在远程虚拟容器中呈现有风险的站点和业务，确保恶意代码不会感染到访问者端点设备。

2.1.3. SASE的关键能力

SASE是在当下新的IT发展态势下，因应各类网络和安全挑战的新技术类别和解决方案，它不是某个特定的最新创新小部件。相反，它通过崭新的融合云原生架构为客户提供统一的网络和安全功能，SASE所具备的集成特性和架构能力灵活构建的新属性，将SD-WAN和网络安全融合到全球化、云原生的服务中，为所有地区的用户提供安全的应用访问，优化云和企业内的应用连接性，为任意地区的分支提供安全网络访问，使用零信任架构无缝地将云、数据中心及移动用户集成到一张安全网络中，提供全套安全服务以持续保护访问流量，帮助IT组织变得更快、敏捷和高效，同时保持高性能和安全的网络。

1、集成收敛

SASE将SD-WAN、零信任网络访问（ZTNA）、防火墙即服务（FWaaS）、云访问安全代理（CASB）、数据防泄露（DLP）等多种功能融合到单体平台和一个直通安全引擎中。这种高度集成化的SASE平台无需用户再选择、测试、部署和管理离散化的单点解决方案，而是能够在世界任何位置为用户使用同一平台逐步部署各种功能，直通安全引擎消除了反复链接多个独立产品的开销，避免流量回环，高效实现所需的网络优化和安全保障效果。

2、云原生架构

传统架构迫使IT部门需要设计为业务提供的各种功能的定制，这是一项复杂且昂贵的工作，并且使维护和故障排除都复杂化，并可能影响远程位置的连接安全性和连接速度。SASE基于云原生架构进行构建，从底层即具备深度安全性和高可用性措施，以确保服务连续性。云原生安全性有助于减少分支机构本地占用空间，并为所有边缘提供统一的可靠保护，从云、数据中心一直到世界任何地方的用户、设备。SASE服务无需单独构建托管网络和安全功能集中区域，也无需预先进行复杂的容量规划和高可用性设计，融合的骨干网全球节点为网络和云流量提供安全可靠的连接和传输。云提供商负责维护平台，从而能够更快地进行集中修复和增强，企业无需承揽扩展和调整基础架构的额外负担，即可依靠合作方的服务适应新的增长的挑战。与维护基于传统硬件设备的解决方案不同，通过云交付的模型简化了关键网络和网络安全服务的交付和运营，云原生架构减少了繁重的上线工作和基础架构维护，具备高度弹性，支持快速缩扩容，提高安全运营和维护的敏捷性。

3、智能高速连接

SASE云化的服务可以在所有位置扩展其所有功能，同时保持最佳性能。针对WAN和云流量优化连接私有骨干网，为企业内部分支网络和互联网流量提供可靠的传输。它可以处理从所有边缘（物理设施、云和用户）到任何目标（本地、云）的流量，以使所有流量都得到优化和加速，而无需部署特定于边缘的加速解决方案。当然，这一点也取决于供应厂商实际可以提供SASE功能的PoP节点的数量和分布位置。

4、安全即服务

SASE应用于所有位置和用户的安全栈的高效能集中控制，当分支机构和用户连接到互联网络时，必须保护所有流量免受威胁。针对整个企业的云规模远程访问，移动办公、三方接入、共享办公、居家工作等场景，迫切需要将企业安全和优化功能扩展到办公室以外的用户。传统方式当大多数流量都在MPLS网络内时，这种对普遍安全性的要求不那么重要，而当今的流量通常需要进出云和互联网，这就需要扩展旧式基础架构，以便始终支持所有用户的此类访问。SASE则在云中放置了广泛的安全控制措施，跟随用户访问需要，并在办公室内外提供相同的连接能力和一致的安全性保护。在办公室，用户可以通过SD-WAN设备连接到SASE云，在办公室外，可就近持续将用户连接到SASE服务，其流量受同等的安全防护和连接优化功能。SASE一致保护所有流量（包括WAN和互联网）免受网络钓鱼、恶意软件和其他互联网传播的攻击。

5、可见性和控制

SASE作为企业资源的统一访问边缘，所有网络连接请求和数据流动均经由其安全网关，对网络空间中主、客体各方提供分析透视、画像和控制能力。包括对用户账号、终端设备的安全状态持续监测和分析，对用户风险汇聚进行信任画像和历史行为趋势预测。同时支持对所有连接过程中传输通道进行控制，对数据流向进行管控，基于数据分级分类的识别模型深度分析识别流量中敏感数据，对各类通道中数据外流进行实时感知和阻断，防止关键数据的泄露。针对云上资产和服务的使用，以CASB有效识别云服务资产和数据上传下载的监测和控制。此外，在终端安全管控全面覆盖情况下，可有效对用户侧存储和使用的数据进行管理，防止分散化存储在设备端点的敏感数据脱管泄露，从云、管、端、边整体化对数据资产和流动提供全局可见和追溯控制。

6、统一边缘访问

SASE架构是从开始其定义设计即是为全局企业流量提供连接的可控制边界，旨在服务于所有边缘，包括站点、云、数据中心和各方人员、物联设备。使用传统方法实现这一目标的唯一方法是为每个类型的边缘部署单独的单点解决方案，如用于分支机构的SD-WAN，用于远程访问的ZTNA，以及用于最佳云访问的云加速组件和CASB控制。而SASE提供对云和数据中心的应用和数据的强大且有弹性的最后一公里访问，完整的SASE架构包括完整的边缘SD-WAN解决方案。

SASE边缘的目标即确保分支机构流量以最佳方式流向SASE云PoP网络，然后从那里流向互联网、云数据中心和云应用程序以及托管在物理数据中心中的目标应用程序。SD-WAN流量控制使用多个分支链路连通、按应用程序控制QoS流量优先级，并且缓解对损耗敏感的应用程序（即语音）的链路退化来实现的。组网的策略管理和链路优选，及安全性、云和远程访问一起通过SASE控制台进行全面管理和分析，随时随地提供混合工作通道。

2.2. SASE典型应用场景

SASE云平台是一项集多种功能于一身的云原生的网络与安全服务，它将SD-WAN、零信任ZTNA、防火墙、安全网关、云访问安全代理CASB和威胁情报整合到统一的解决方案中，帮助各种规模的企业保护用户、应用和数据安全。随着越来越多的组织采用互联网直接接入式的访问模式，SASE平台可以帮助企业轻松将保护扩展到移动用户和分支机构，围绕企业分布在云上、私有IDC中的业务和数据构建软件定义柔性的安全屏障，所有访问者获得一致性的安全高效访问。

SASE致力于保持与组织业务驱动因素一致，例如远程访问、安全应用程序访问、合并和收购场景以及云迁移转型，支持端到端的访问安全控制以保障网络安全。

1、混合型办公

构建零信任网络访问解决方案，该解决方案将替换过时的VPN连接，增强保护更快、无缝的用户体验。远程用户可以访问多云中的应用程序和数据环境，并将数据泄露风险降至最低。访问时更快、更无缝的用户体验，随时随地支持主体接入所需要的应用程序和资源。

2、三方访问

组织将内部劳动力政策扩展到承包商和第三方用户，提供安全交互协作和资源接入。可为承包商和第三方提供同等级别身份验证，保护跨公司协作的业务和数据安全，支持大规模管理和运营，为每个用户、组和应用程序制定细粒度单独策略。

3、兼并和收购

使用组织的现有身份服务提供商，支持利用两家或者多家供应商的现有身份体系进行访问管理，保障供应商解决方案进行平稳过渡和切换，提供更快的访问和轻松的网络集成，支持各类合并企业、连锁和加盟机构跨地域网络高速安全互通。

4、网络转型

帮助组织从传统网络边界转型到基于云的安全边缘框架。作为整体SASE的实施战略，从边缘到云的端到端网络安全，实现基于云的无缝网络集成，以SD-WAN连接分支，提供防火墙保护网络和业务，提升跨广域网的企业办公效率、数据传输质量和业务接入安全度。

5、边缘保护

组织可以使用集成的边缘计算算力。完整的SASE解决方案带来的边缘可用的安全性，边缘的安全能力组件易于根据需要弹性启用，包括分支机构、移动人员到云接入的保护，集成的边缘计算安全性同时支持实现更多边缘接入保护，包括物联网的连接和安全访问。

2.3. SASE核心价值

2.3.1. 支撑CIA原则

广义而言，信息安全是指保护业务所涉及的IT过程、信息和底层系统免受不当访问、使用、修改或破坏。这通常由三个关键安全概念来描述：机密性、完整性和可用性。这三个原则共同构成了信息的支柱，被称网络安全CIA三原则。尽管不同类型的系统和数据可能优先考虑一个原则，但是这三个安全概念协同工作并相互依赖才能成功地全面维护信息安全。

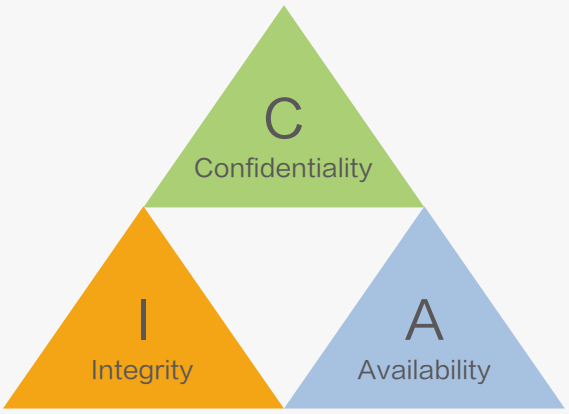

图 7 信息安全CIA三原则

机密性、完整性和可用性是信息安全提供的最关键特征，其主要定义如下

1、机密性，CIA三原则的首要原则是保密。机密性是限制授权用户和系统访问数据，并阻止来自未授权的访问，机密性保证只有预期的人员才能够访问授权范围的信息和资源。机密的目标是预先禁止未经授权访问数据，限制非预期的查看、复制或移动数据，数据的泄露是当下网络攻击的主要方面，对企业的正常营运影响巨大，机密性的保障至关重要。

2、完整性，完整性是维护数据和系统的准确性、有效性和完整性。它确保数据不被合法授权以外的任何人操纵和篡改破坏，完整性是为了确保所有数据保持完整、正确和可靠。未能正确保护数据完整性可能会对业务流程产生负面影响，包括可能做出不当决定或潜在错误有害行为。

3、可用性，确保授权用户可以在需要时访问数据。在企业运营环境下，可用性的必须得到保证，即合法各方可以及时、不间断地访问所需的系统和数据，以各自支持做好自己的工作，支持企业经营业务流程顺利进展。对可用性的威胁可能会干扰甚至阻止组织的业务运营，关键系统和数据的长期中断必然会导致客户利益损害和收入损失。

当下，企业的受攻击的暴露面正在不断扩大，信息物理系统和物联网的使用、开源组件和代码、云应用、复杂的数字供应链、社交媒体等引发的风险使企业暴露出的受攻击面超出了其可控范围。数据窃取、损毁和业务中断导致CIA原则在当下需要有更全局层面的防护，企业必须采用比传统的安全护城河式监控、检测和响应更先进的方法，来管理更大范围的安全风险。而SASE则可以从多个方面来对CIA原则进行确保支持，它将网络和安全功能集成到一起，帮助企业应对各种变化和安全性风险。

SASE围绕企业的资产构筑一道灵活自适应的边缘，提供所有接入者对资产的安全连接，并通过各种技术手段确保其保密性、可用性和完整性，保障安全访问服务边缘上的主、客体的互联可用且受控，保护企业的资产和业务数据的安全，支持位于企业内部、外部的用户、设备、应用程序、数据和服务的交互，从而支撑实现新的数字化业务场景。

表 2 SASE对CIA原则支持要素

可用性	SD-WAN分支组网和传输保护，更高效地保护网络，从而提高网络以及网络安全人员的效率
	通过SD-WAN结构动态化选择路由路径，智能全球网络互联互通
	多云互通，安全访问和可见性增强，跨云连接
	互联网直接访问，避免回环流量到企业总部，同时提供安全保护
	通过整合供应商来改善监测能力和易管理性，减少供应南管理复杂性和成本
	单通道体系，消除典型安全栈串接式检查引擎增加的延迟
	对用户、设备和服务提供低延迟访问，改进全球规模和运营复原力
机密性	使用多种威胁信号和上下文信号来建立信任关系，以零信任机制确保对内部资源和互联网的安全
	保护分支机构和远程用户到出站流量，防火墙过滤威胁流量
	保护端点设备，反恶意软件
	保护账户安全，启用NFA校验合法身份，身份生命周期治理
	严格的最小权限原则，限制非法访问
	通过在尽可能靠近用户的位置交付安全控制措施来提高安全性，使攻击者更难发现和
	SD-WAN组网和优化，提升连接服务的质量
完整性	提供多种隔离和加密措施，保障用户侧和企业侧数据资产的完整性
	全传统通道加密传输，防篡改和抗重放攻击

2.3.2. 边缘的可控可视

近年来各行业的移动技术、云计算、物联网不断发展，行业合作伙伴间协作关系的日益密切，原来基于安全IT设施组建的内网边界的安全假设已经不再适用。传统的护城河模式下，攻击者在成功突破一个防御点之后便能利用网络固有的默认信任弱点，在网络、应用环境中横向移动来寻找和窃取敏感数据目标。在受信任区域内发起攻击的内部威胁往往可以获得更高的权限，针对那些想方设法绕过防火墙，分别通过遭泄露的用户凭据或易被攻击的面向互联网的应用程序、或在企业内部“受信任”网络中发起的威胁，需要一种柔性而非固化的边界，检测并防止威胁入侵、横向移动，以额外的安全控制措施对其加以阻止，从而将恶意攻击所产生的影响降到最低。

网络边界，与其将它视为网络可见“边缘”的一种访问控制方法，倒不如把它看作能够实施访问控制决策的任何位置，这道边界仍然可以是防火墙和其他安全设施，围绕企业资产动态构筑防御边界，软件定义边缘的能力集合和分布位置，在所有访问路径上实施企业的安全策略。这道可柔性定义的边缘决定了哪些安全策略适用，针对任意访问请求，其零信任安全模型都会重复确认原有的信任假设的要求条件的持续维持确认。SASE基于云的聚合能力，当企业需要的时候可以动态创建基于策略的安全访问服务边缘。

1、可见性指导策略。为技术、运维、管理人员提供尽可能丰富的流量可见性、分析、和情报资源，管理分布在数据中心、云上各类资源，以支持在制定策略时有理有据，通过合理的自动化、编排、集成来尽可能降低管理压力。

2、柔性边界为访问控制决策提供空间。选择最适合企业网络环境的层面和流程点，包括网络层、应用层、身份验证点、策略校验点以及执行控制处理工作流。

3、动态的信任，持续评估。边缘安全组件持续不断地对用户、设备和应用程序的状态进行反复评估，并对信任度做出相应的调整。这种模式有助于即时通过新发现的威胁和漏洞，随时做好准备进行遏制，以应对那些使网络风险级别升高的安全事件，保障访问连接的安全。

4、所有权不等于控制权。从BYOD设备和IoT（物联网）设备到SaaS和公有云，验证所有的接入，将信任扩展到所有权或管理权并不掌握在企业手中的人员、设备、应用和网络。

5、连接控制中进行访问决策。网络资源的连接过程中，针对主客体的访问控制，组内成员资格、层内应用服务、从某个网络位置连接的设备，单项信息本身都不足以对活动进行授权，必须在连接中即经过综合的、策略基线性的安全性核验。

6、有效遏制威胁。将最小权限控制和各种响应能力结合起来，零信任默认的系统不相信所有的访问者，将所有访问请求视为具有潜在的威胁可能性，实时对访问者身份和权限进行检测和认证，然后才可接入内容或调用相应的系统功能。全局层面及时监控威胁活动，自动化策略处置业务流程，共同限制威胁活动的蔓延。

SASE为远程员工、固定场所、任何需要连接的设备以及工作负载提供可靠连接，确保其安全地访问应用、数据和互联网资源。针对任何网络或云环境，获得从用户到应用的全面端到端可视性，提供快速可靠的安全云通道，采用零信任机制验证用户身份及设备健康状况，确保基于每次会话的对应用、数据的访问都是安全的，其基于云的简化基础设施支持快速的扩展，帮助企业提高业务敏捷性。

2.3.3. 云原生安全收益

SASE有效管理分布在全球的员工、合作伙伴间的网络通信和协作，排除阻碍高效办公的因素，是提高生产率的重要手段，它同时确保安全的接入和安全的远程工作会话，并使用个性化和场景化的管理工具，帮助组织简化工作流程、降低复杂性，兼顾统一访问和统一安全，提供业务敏捷性，其基础设施和服务具备高度弹性，容量规模易变更、位置易部署，新的服务和应用易于启用。

用户体验与控制的收益：

1、用户体验佳，无论用户位置和使用设备如何，都获得一致的可预期访问效果
2、位置无关，应用访问与底层网络分开，应用可以迁移，但是用户访问过程不用变化
3、提供更多访问选项，不再是非黑即白，而是能够提供有条件、灰度控制的访问
4、对供应商和合作伙伴提供协同方法，不强制环境的安全远程访问
5、支持更多应用上线而不用在防火墙打洞，建立安全措施可即刻开始审计追溯应用访问

消除网络和数据风险：

1、资源隐身，不再暴露于公共互联网，对缺乏访问凭证或者可信度的主体不可见
2、所有访问均被约束在授权范围内，减少失陷账户的爆炸半径
3、对数据的类型、位置、流向增强可见性和一致性管理
4、提供用户行为的全景分析，更快发现风险和威胁，无论是恶意攻击还是异常行为，都可以快速进行抑制处置或者策略调整
5、安全状态全局提升，从云底层开始构建安全能力

流畅的产品部署和维护：

1、云原生安全服务，随着组织的业务需求而扩展，消除传统硬件安全设备的部署复杂性和容量限制问题
2、统一的云平台，单通道架构进行安全检测（仅需将加密数据包打开并检查一次，即可进行恶意软件检测及数据丢失引擎完成分析）和统一的策略执行点，统一的管理台与策略引擎，保障全局安全策略控制的一致性
3、独一供应商，消除多方对接、调试、故障分析和修复产品、升级导致的上线延期
4、先进的编排、自动化、监控和故障排除功能，提供优化性能、可扩展性和弹性、全局安全策略，获得对用户、行为及环境性能的更全面洞察和可视化管理。

2.4. SASE市场发展

2.4.1. 市场发展空间预期

自2019年Gartner首次推出SASE市场定义以来，行业和客户对SASE的兴趣出现爆炸式增长，这主要是由于现有供应商无法满足企业需求导致。与2020年相比，2021年最终用户对SASE的查询量增长了89%，这一趋势持续到2022年第一季度。在2022年的Gartner首席信息官和技术高管调查报告中，SASE是第三大最常被引用的技术投资，进一步证明SASE的势头在企业中正在增长。

根据Gartner的预测，到2025年，更多企业将采用SASE架构来统合云服务和私有应用及互联网的访问，这一比例将从2021年的20%升至80%。其中核心的零信任网络接入（ZTNA）将成为全球增长最快的网络安全细分市场，预计2022年将增长36%，2023年将增长31%。在2025年前60%组织将采用零信任作为安全新体系构建的起点。中国区域，根据IDC预测，2024年中国网络安全市场总体支出将达167.2亿美元，其中零信任安全市场占比将达到10%，约为百亿人民币规模。

此外，在2021年，Gartner定义了一个新的术语SSE（Security Service Edge，安全服务边缘）。简单来说，SSE就是SASE中的安全部分，Gartner将SWG、CASB和ZTNA定义为完整的SSE产品的必要组成部分。据Gartner统计，2020财年SSE市场的收入在24亿至26亿美元之间，同比增长了19% −21%。预计到2025年，70%部署ZTNA的组织将选择SSE（2021年这一比例为20%）。同时，相较于独立的CASB、SWG和ZTNA产品，80%的组织将选择购买SSE整体解决方案（2021年这一比例为15%）

2.4.2. 市场驱动关键要素

随着云计算、大数据、人工智能、物联网等新一代信息技术与制造技术的加速融合，近年来，数字经济如今成为经济发展的重要引擎。但也需要注意到，产业数字化在极大提升产业链协同能力和生产效率的同时，也使得原本大多局限于网络空间中的安全问题更加蔓延到现实生产中，数字化安全基底亟待进一步筑牢。

1、行业数字化转型

云迁移加速，在亚太区那些声称将平台化使用视为企业最高优先级事项的业务与技术专业人士中，43%都采用了行业特定的云解决方案。亚太区的制造业、建筑业、公用事业和其他行业的企业贡献了全球工业增加值的45%。这些企业将通过数字产业平台采用云技术引领行业转型，创造与提供可持续的客户价值。

亚太区跨境商务急速增长，Forrester预测这一方向在2022将增长20%，亚太地区的主要经济体，如中国、印度和东南亚国家，正在积极推广现代化支付网络，《区域全面经济伙伴关系协定》也将进一步促进跨境商务的发展。

数字化转型后，各类核心的数据从原本的零散数据、离线数据、甚至纸质数据都云端化汇总到数字平台，一旦被黑客攻破或者释放勒索病毒勒索，不但失去了所有商业秘密，严重影响企业营运，还将面临极大的法律、合规风险。企业云化战略的进行，云上数据中心和云服务的广泛使用带来了随时随地接入的便利性，但是由于脆弱的安全实践也暴露了基础设施和凭证，从而带来严重攻击后果，攻击者开始针对开源软件、无服务架构、IaC（基础设施即代码）着手入侵，对于开源软件供应链的攻击在2021年上升了650%。

另一方面，物联网的快速发展，工业控制系统逐步走向链接化、自动化与智能化，但也由此产生了一系列安全隐患。且由于被攻击的可能性高，其重要性涉及企业生产乃至基础设施建设，一旦被破坏，对社会生活或将产生破坏性影响。

数据化转型是几乎所有行业的发展战略，SASE云服务则充当互连高速通道，优化从分支机构和用户到云应用程序和数据中心的流量，同时实现持续访问的零信任安全控制，使用身份和关键上下文背景的其他元素进行评估，它改进并确保一致的应用程序和安全访问策略和用户体验，无论用户的位置和设备如何，SASE通过在云中放置尽可能多的功能，可以均衡地将这些功能扩展到所有边缘，统一进行控制和连接，从而降低复杂性和成本。

2、安全风险的日益升高

随着生产流程的数字化程度逐渐提高，安全风险对显示生产的威胁亦愈加深入，深入具体业务机理、渗透供应链与工控系统是企业、尤其是制造业企业在面对勒索软件时易被“牵一发而动全身”的主要原因。

安全风险的蔓延亦并不局限于生产端，随着各类穿戴式设备、智能汽车、家用电器联网比例的提升以及边缘计算的快速发展，除PC、智能手机等设备外，对其他个人设备的攻击和控制亦是需要重点防范的安全风险。以智能汽车为例，相较于手机、PC直接与服务器进行点对点通信的形式，从网络安全角度看，智能车主要的特点在于除了用户手机APP和云端服务器，还多了车辆本身的一端，一旦黑产实现了对云平台防御的突破，是有可能利用内置好的通信控制协议实现对车辆的单点控制的。

互联设备和服务的激增也扩大了攻击面。据专家预测，到2022年底，活跃的物联网(IoT)设备数量将增长至144亿，年同比增长率为18%。仅在2022年，与物联网设备相关的漏洞数量就增长了16%，而所有漏洞的增长率仅为0.4%。

国际安全服务提供商Check Point Research发布的数据显示，2022年第二季度全球网络攻击次数已创历史新高，较2021年同期增长32%，第三季度亦较去年同期增长28%，这一年，勒索软件攻击、DDoS攻击等网络攻击形式愈加多变与频繁，工控安全、数据安全等领域的防护要求较之以往也更加严格，传统的安全解决方案已无法完全覆盖当前的防护需求，无论是传统行业还是新兴产业，均需根据实际业务情况构建更具针对性的安全能力。

值得注意的是，除攻击次数显著增加外，攻击范围的扩大亦是近年来网络防护形势重要的变化趋势。除政府机构、大型企业等传统重点攻击目标外，医疗机构、中小企业、数字化基础设施等愈加受到不法分子的关注。

对于所有依赖数字化的组织而言，随着资产数量的增加，安全威胁的攻击面也随之扩大，在日常运维过程中，由于运维人员能力的参差不齐，任何如补丁更新的及时性、基线配置问题、安全产品应用等方面的工作疏忽，都可能极大提升数字基础设施的安全风险。为了有效控制风险，企业需要探索新的网络安全方法。SASE提供的配套边缘防护机制，在保障业务和网络连接支持的能力层上，以ZTNA为核心控制引擎，灵活的接入控制机制保障各类场景下数据化场景下安全地互连互通。据Forrester公司的研究，采用某些零信任解决方案的企业可获得高达92%的投资回报率，并将数据泄露的几率降低50%。

3、供应链组合重整

2022年，面对地缘政治冲突、劳动力短缺和自然灾害频发，各行各业的企业都严重依赖于供应链组合、控制、协作的能力。企业迫切需要构建强柔韧性供应链能力，确保可靠地采购长期供不应求的产品和原材料，从半导体、药品到食品，全面保障一切物资的可靠供应。在各种政策管控风险、自然灾害的驱动下，许多企业领导者已经开始重新思考其供应链模式。各类突发事件可以摧毁供应链中的关键环节，从而对依赖于供应链的企业经营产生严重影响。地缘政治冲突带来的中断也是如此，2022年，乌克兰危机促使全球范围内的企业开始重新思考其合作伙伴生态系统。据IBM估计，多达三分之一的组织在过去三年中已经开始与新的国家或地区的供应商开展合作，并在这些不断发展的业务生态系统中引入数字协作和自动化。

中国地区，近年来，制造业出现向东南亚迁移现象加快，这种转移的趋势已经存在多年。将产业链转移到东南亚的不仅是欧美企业，还包括中国本土企业。中国工业制造基地在东南亚快速设立各类工厂，这中间涉及一许多复杂的经营流程整合、涉及高效收购/合并/拆分企业组织，这一切需要有效的IT整合能力，将全球化分布的工厂、总/分部高速连接，以智能工作流支持业务，并与生态系统合作伙伴通过数字化平台进行供应链协同。

全球覆盖的SASE平台通过云化部署，可以快速应对业务扩张所需的组网、多地安全连接、移动办公访问的诉求，在组织剧烈的业务变动中，更好地提供网络连接的高效通道和数据、业务访问的可控安全性。

4、远程办公和混合办公

企业在运营中的各个阶段中，广泛需要远程办公对员工、合作伙伴进行支持，灵活性地实现混合办公，以降低通勤成本。企业合作生态和外包模式等有效扩大合作范围并降低成本，与生态系统合作伙伴共享技能和资源，并将一些工作流外包给合作伙伴，从而实现降本增效的组织目标。

疫情之下，2022有年高达60%的组织进入大规模远程办公模式，如今仍然有78%的企业持续保有大量员工居家办公或某种形态的远程工作。如今疫情虽已经线束，然而潜在风险下，企业需要提升IT设施风险应急能力，以在突发威胁场景下有效支撑业务运行。

当下，远程接入企业网络、云环境已经对业务的持续性起支撑作用，而居于供应链各方的三方伙伴、服务商、供应者同样会接入企业网络资源，甚至包括各种敏感程度的业务应用、服务器和数据库。远程办公，需要企业资产在互联网上的开放，这当然增加了企业暴露的网络攻击面（无论是资产量级还是曝露时间）和安全风险升高。而传统的VPN暴露网络和服务，且经常出现未修复的漏洞，易受攻击，大多数开放网络暴露面过大，攻击者则利用各种漏洞和薄弱点来发起攻击，例如通过员工自带设备、供应链合作伙伴、脆弱的云安全措施保障来进行攻击行动，并轻松横向移动攻击关键系统和窃取企业内部机密数据。没有有效安全远程接入防护则带来风险上升，2021年平均的供应链攻击财务损失高达140万美金。SASE通过零信任ZTNA安全访问控制，为各方不同角色提供安全接入，保护企业核心资产和数据。

第三章 SASE实施路径

3.1. SASE成熟度模型

SASE作为组织IT的柔性边界，连接性和安全性是其能力范畴核心，好的SASE架构一定实施零信任原则，访问必须得到授权、信任需要基于条件集合持续评估，实现安全防护的前提是要消除隐性信任，为了保障敏感资源的访问安全，应明确验证主体请求的各个方面，这是企业保护数据资产的根本原则变化。落实零信任是SASE架构实施的良好基础，以保护混合环境中在任何位置的用户、应用和数据。同时，SASE遍布全球的骨干网为任意位置提供可预期的连接，SD-WAN管理最后一公里链接和服务质量，安全即服务的栈式接口安全组件为来自所有位置和用户的流量提供保护，针对移动用户对云、IDC中资源的访问提供安全保障和链路优化，且以集成的自助服务式的管理平台支撑高效运营。

按照SASE框架的设计目标，SASE能力应得到全部的落实，其理想形态应覆盖组织IT的关于访问控制的各个层面，包括连接性、安全性和策略控制一致性和高标准的服务能力：

1、保护用户、设备、应用、服务、数据、接口和基础设施，提供零信任网络安全能力，基于身份、行为、环境信息持续评估风险和信任等级，动态控制资源访问过程；
2、简易的终端用户体验，提供各平台统一客户端，屏蔽各类接入实现和安全检测、修复的复杂性，为用户访问提供一致体验；

3、确保从用户到云的安全连接，所有传输数据保障加密；
4、对于敏感数据提供可见性和控制机制，同时检测、呈现和抵御恶意内容和网络攻击；
5、一致化的策略执行，无论访问主体形态和位置，支持分析决策单一引擎计算；
6、易管理，提供聚合的策略控制和编排面板，通过集中管理和分析，综合应用来自不同来源的威胁情报，应用一致性的安全策略；
7、对所有访问类型提供策略实施手段，如敏感数据和恶意软件检测，安全策略应用到SWG、CASB、ZTNA等全部安全组件中，可选提供WAF和API安全保护（WAAP）；
8、所有类型组织实体覆盖，包括分支、总部和边缘位置的用户和设备，SD-WAN支持为分支内部不安装agent的网络设备（如打印机）提供连接和安全保护；
9、直通加解密安全检查，一次性检测加密流量和内容，解密一次进行恶意软件、攻击检查，并进行敏感数据核查，一次通过的云化组件式架构从而保障处理效率；
10、通过将可见性、情报和安全策略实施扩展到网络上的每个连接点，启用fullmesh的威胁感知网络；
11、高可用、低时延的网络服务，云原生架构弹性易扩展，提供高效、可靠、动态的服务，多地区分布式PoP边缘确保提供符合预期的SLAs质量。

SASE针对企业发展各阶段提供相应进阶选项，建议可对照如下成熟度模型表格进行核验，通过定义了SASE的关键能力范畴，针对每个类别的状态提出了相应精细化的描述参考指标。实施组织可以判断当前评估的SASE方案是否符合企业的实际状况和提升目标，如果供应厂商提供的SASE安全产品与该表中的三阶段指标要求保持一致，具备高级或理想型供应能力，那么可以认为该方案和产品有助于帮助企业实现全面的SASE安全架构转型。

表 3 SASE成熟度能力阶段

	起始阶段	发展阶段	最佳阶段
身份	使用弱凭证如密码进行认证	使用MFA等强身份认证机制	启用无密码验证和钓鱼抵御
	云端和本地应用间无SSO	大多应用进行云化或统一的身份认证和授权并进行SSO	全部具备统一云化身份服务并SSO登录
	身份风险的可见性、管理能力非常有限	具备身份和会话的可见性	具备组用户、接入和角色的管理及自动化检查
设备	使用EPP管理内部端点设备	内部设备向云上统一注册和由云MDM提供商进行安全配置和管理	设备健康、反恶意软件和安全性持续监测和校验
	设备已加入域并通过组策略对象或配置管理器之类的方案进行管理	对设备初次接入进行合规性检查	对企业设备和自带设备均进行统一全基线风险访问控制
	有限的合规可见性	EPP+EDR组合监测入侵并响应处置，基础的自动修复剧本	使用EPP+EDR+TVM用于状态管理，高级自动剧本修复和XDR集成

网络	人工的和静态的权限管理	使用策略管理权限并基于推荐进行调整	基于风险与使用情况自动化自适应策略控制资源访问
	一些网络资源直接对用户开放，VPN和开放的网络为大多数资源提供接入	会话级隔离对敏感工作负载的接入，云应用、互联网和私有应用不再假设位置可信而接入	基于数据信号由云服务对所有会话持续评估，检查策略违反事件并进行动态的接入撤销
	基于威胁监测工作负载和进行静态流量过滤，部分内外部流量经过加密	监测流量，大部分内外部流量加密	监测流量检查潜在威胁并且动态化反应，所有数据和网络流量端到端加密
	通过防火墙IPSEC连接分支	通过专线连接机构并提供IDC与云高速连接	SD-WAN连接分支机构，混合云高速连接
	网络流量通过互联网传输	网络流量通过区域专线传输	网络流量通过高速网络传输，具体全球可达性
应用	本地Web应用配置SSO	本地Web应用和客户端应用使用零信任接入控制	所有内部应用零信任接入控制和隔离保护，全部配置SSO登录
	评估云影子IT风险，监测控制关键应用	本地应用面向互联网	所有应用都可使用最低特权访问并具有持续验证
	用户可以访问一些关键的云应用	云应用配置具备SSO	监视和响应会话期间的所有应用程序并进行动态控制
数据	使用基于规则和关键词的方法在所有位置、应用和服务发现并分级敏感数据	自动化地发现所有位置、应用和服务的数据并进行分类和标记，包括异构数据	通过智能机器学习模型持续发现和进行信息关联来定位数据泄露风险
	访问过程受边界控制，而非受数据敏感度控制	不受限于物理边界的接入控制	访问决策由云安全策略引擎控制
	基础数据DLP网络层检测	绝大部分数据经过网络DLP分析和端点数据DLP保护，使用RBI隔离	全局数据经过网络DLP分析，所有端点数据DLP保护，使用RBI隔离和沙箱保护
	敏感度标签是人为标记的，数据分类不一致	限制敏感数据流转	主动数据治理和风险评估
基础架构	跨环境的权限需要人工接入	监视工作负载并对异常行为产生告警	阻止未经授权的部署并触发警报
	虚拟机和服务器的配置管理运行工作负载	每个工作负载都分配有应用程序标识	粒度可见性和访问控制可用于所有工作负载
		提供访问主体对资源的访问请JIT保障	用户和资源访问按工作负载细分

威胁保护	响应式的威胁和漏洞检测	主动的威胁和漏洞检测，及入侵响应	针对全局的威胁自动化告警调查和修复
	为端点设备提供入侵前保护工具如AV，为邮件提供安全网关保护	针对基础威胁自动化告警调查和修复	积极使用风险分析、威胁情报和最佳缓解措施进行漏洞和错误配置的修复
	隔离式的安全和响应	XDR能力初步和部分SIEM集成	XDR能力贯穿全局，和SIEM完整的集成，具备高级风险捕获，检测、响应和阻止能力
策略实施	基于有限数据感知的访问决策	基于扩大的安全感知源的访问决策	基于全局的安全感知讯号源的访问决策
	非中心化的访问决策	使用中心化策略引擎进行访问决策	持续评估的决策，实时策略执行
	仅在访问时作出决策，不具备持续性	访问决策近实时风险评估	访问决策实时风险评估

3.2. SASE应用实施准则

SASE的目标是将组织的网络与安全功能整合到一起，作为完整的一体化云服务提供。它是一种架构、一种策略和一个持续的安全防护目标，而不是可以用一个单体软件包就能实现的东西。有很多工具可以帮助组织开启这个概念，包括身份安全、访问管理和网络分段，但目前还没有一个各种场景都通用的独特产品可以提供SASE的完整功能。大多数组织都处于实现这一新型安全架构的早期阶段，企业和安全风险管理领导者应制订SASE迁移计划，从传统边界和硬件中心的架构转变为基于SASE的架构。

SASE实施涉及组织中网络、安全和业务等各部门，通常决策来自首席信息官，只有这些角色有相应有能力拆除组织孤岛，以实现SASE架构的愿景。常见的SASE项目是以简化策略管理和实施并改进组织的安全状况为目标。一些项目由网络和分支机构主导和发起的转型计划，有些则是由安全性和支持混合办公的需求主导的。由于SASE产品同时面向网络和网络安全功能，因此有效的方法是组建横跨网络与安全的团队，负责SASE整体的设计、控制和运营，拟定企业采用SASE的战略路线图。根据企业当前所处IT建设的现状，分步骤充分评估后选择合适起点来开始实施SASE，关键措施包括如下步骤：

1、定义边缘

边缘是两种差异部分的接触交互点，传统是由内网、外网概念在IT领域中呈现。在SASE的这一阶段，需要梳理所有私有和SaaS应用、所有数据资产，搞清楚部署在办公场所中的系统、这些系统的用户及相关应用程序，包括IoT和OT，并确定其在企业组织中的功能及其在网络上的操作范围，进而明确SASE安全方案的适用范围。根据组织IT具体架构，可能仍然需要基于私有数据中心的网络基础架构，但大多数企业正在过渡到边缘计算。有些公司可能采用总分连接，另一些公司则采用依赖云的结构。组织需要定义业务所在，进而确定边缘构建，一些服务可能仍然需要在本地交付，但趋势是转向成熟的SASE产品统一边缘托管，边缘定义决定了后续可能功能组件的选择。

2、安全整体视角

企业通常已经拥有战略所需的部分网络和安全系统，应分析这些已有系统的成熟度和有效性，有些工具可能是为了解决某个特定问题而购买的，但还没有经过优化或没有与其他系统集成。碎片化的方式部署和使用，这可能会降低整体安全防护能力，从而出现防护效果不理想的现象。但如果因实施SASE而全部立即放弃传统安全产品，也可能会引发意想不到的安全风险。因此SASE实施部署需要与复杂的原有产品体系相互联动配合才能成功，避免导致产生在全局安全风险上的能力缺失，以减少攻击和数据泄露的几率。组织需要清点实施多年的本地边界和分支硬件设备、合同，为基于云交付的SASE能力做准备，深入分析办公场所网络环境中用户、设备和应用程序的通信以及网络流量、访问模式，从而规划适用范围内的网络功能及要求，并需要在设计初期即详细考虑后续的集成对接，以获取深层全局关联的威胁进而更优化抑制潜在的网络风险。

3、确定业务覆盖范围

有效实施SASE模式需从业务需求入手。询问要保护什么资产、为何保护，来确定哪些方面采用SASE技术能更有效提高安全能力，这最终将支持企业的整体战略转型。需要确认SASE构建所覆盖的业务范围，通常围绕各类访问连接来考虑，如移动办公场景、三方伙伴接入场景、外包员工接入场景、物联网安全接入场景、内网安全准入场景、员工上网场景、分支组网场景、流量加速访问场景，企业根据自身业务场景的量级和迫切升级防护方向选择合适场景试点，制定配套的安全流程、制定策略和明确需求，并充分考虑用户活动范围变化支持和优化的体验，逐步推进全场景覆盖。

4、重要功能选择

SASE并没有提供一套强制性标准的工具集，而是提供了一个帮助企业构筑边缘防御措施的框架。企业当前的迁移解决方案应该建立在各个基础组件功能之上，虽然现在很多企业都具备如防火墙、SWG功能，但它们很可能分散在多个平台上，这增加了复杂性。寻找一个能够支持这些基本功能以及ZTNA和SWG的平台，这有助于降低复杂性和成本。此外，当传统设备合同更新时，借机聚合供应商、消减复杂性和成本，评估可以综合这些安全边缘服务的整体交付机会。

5、执行差距分析

一旦确认了要保护的对象、场景和需要集成的工具之后，应当开始执行差距分析以确定组织IT目前在哪些方面足够成熟，以及在哪些方面还需要投资以完成转型战略。在差距分析中，了解哪些功能对目前的业务模式更为重要。这取决于组织运营形态和模式需要，例如如何为员工队伍、分公司提供网络支持以及如何为客户提供服务、如何与合作伙伴协作。除此之外，还应审查合规性和审计结果，明确哪些方面有必须遵守的合规和质量要求。

6、规划SASE过渡阶段

对于大多数公司来说，向SASE过渡将是一个包含多个阶段的过程。企业需要明确验证围绕访问业态的各方身份、地理位置、差异化设备类型、应用服务及工作负载，制定在出现违规行为时的处置动作，尽量减小影响、划分访问范围，逐步建设完善。这还可能包括随着原有各个单点解决方案的陈旧过时，相应需要逐渐淘汰掉这些解决方案，制定时间计划，拟定妥当的更新切换清单。同时，根据审查差距分析结果评估决策需要优先应对哪些风险，并制定方案优先处理。

7、充分进行测试

在将SASE方案投入生产环境之前，需要对其进行充分的测试和安全评估。这不仅可以为用户使用这些类型的系统提供经验，还可以帮助管理员以及安全团队掌握响应事件和处理安全问题的经验，以改进未来的全面实施上线和进阶扩展。

8、选择合适的实施起点

ZTNA零信任网络访问应是SASE实施的合适起点，它适合分布式、多方访问的现状需要，同时也是新一代的框架，细粒度控制应用程序级访问，减少横向移动、抑制安全风险和已知漏洞。零信任面向适用范围内的用户、设备及应用程序配置并实施网络身份认证和授权。防止任何未经身份认证的实体连接到网络，零信任解决方案可以在任意需要的位置提供安全性，以满足现代企业的需求。在起始阶段，可选择部署ZTNA代替传统VPN，为远程用户提供安全访问，特别是高风险的用户场景，如移动办公、高敏数据访问、运维访问等。零信任的云化交付模型将保护范围进一步扩展到全部服务、业务，包括云端和边缘。

采取这八个步骤来评估、规划并开发集成的SASE安全战略，然后与选择的供应商讨论并开始测试、实施。充分复用云资源能力，将保护范围扩展到企业的核心、分支、云端和边缘及全部用户，以尽可能降低风险、提升业务效率，支持业务战略的未来发展。

在具体实施SASE的技术路径上，采取逐步替换、升级原有基于固化边界的安全防御方法的单点方案，以打造以零信任方法为核心的全新安全管理平台和可信计算环境。大多数企业都在通过实施零信任方案改进安全技术堆栈，以尽可能减少IT网络中存在的隐式信任，进而推动实现SASE系统的更多集成组件。企业的应用程序服务通常分布在云服务商、数据中心和其他异构虚拟化环境中，为了将现有环境向SASE模型引导，必须要在网络通信点完成信任评估和访问控制决策。

3.3. SASE建设阶段策略

SASE充分应用人员、设备和物联网多样化和量级增长的威胁，伴随员工BYOD自有设备的剧增，企业网络中的设备数量也相应地增多。从物联网到打印机，从OT到医疗设备，支撑企业正常运营的设备比以往任何时候都要更多。正因为如此，由设备所创造的攻击面也比以往任何时候更大。根据用户和设备的行为判断设备的受信任程度，并在出现风险因素时再进一步限制对设备的访问。此外，能通过持续的通信监控以及持续的安全策略改进，不断降低网络中的假设信任，对网络通信实施更严格的限制，并根据信任度执行相应的自适应策略，强化网络内部的安全。从而有效降低这些设备遭恶意活动利用的风险，并针对任何可疑流量做出更及时的响应。SASE全面的目标达成，需要做到端到端安全检测、多信息源评估利用和高级策略实施及编排分析、自动化，在SASE的根据企业实际的组织实践中，可划分成4个阶附段，来针对性规范SASE在企业的IT建设中启用进阶的目标。

图 8 企业SASE转型路线图

1、为复杂的网络风险做好准备，跨内部孤岛和更广阔的生态系统整合网络安全体系。考虑与生态伙伴开展合作，共同承担安全转型计划的治理责任，共创价值并建立整体业务弹性。

2、零信任访问，建立零信任访问基线。定义身份/设备/资源ID，构造用户和应用间的权限映射图，自动化移除过期和不使用的授权，引导访问流经策略控制以消除直接访问风险，无论用户位置在哪里，实施ZTNA安全访问，用适当的访问控制策略来执行最小特权原则，并使用MFA强化身份验证。

3、情报综合研判应用，跨各种执行点共享与用户、设备和应用程序相关联的身份、漏洞和威胁的动态情报信息，协调安全策略的情报利用，需要与整个体系的不同部分协同，使用不同类型的策略创建和执行方法。

4、应用安全控制策略到跨不同环境的多台设备的能力。一个统一的高级访问控制策略引擎，同时管理在多云、多数据中心、本地环境中的访问控制设备，由此简化对应用程序的可见性控制和访问管控管理。

5、适应性访问，丰富信任基线以在访问活动中鉴权校验，增加访问策略中的上下文信息综合评估，支持环境条件自动触发要求强认证或阻止访问的动作处置，将上下文环境评估纳入到用户整体可信度判断中，持续调整访问策略。

6、按需隔离，对访问目标实施显式可信控制。包括使用RBI隔离访问有风险的低信誉网站，充分利用威胁情报，监测C&C连接尝试和其他恶意行为。

7、保障客户数据业务合规问题，持续进行数据保护，持续评估和移除过度信任，适应性地执行最小权限模型。受控设备和非受控设备的差异化访问策略，基于上下文适应性的访问策略，云资源错误配置检测校正，对数据进行分类分级，对敏感数据提高可见性和控制，使用用沙箱来保护敏感数据访问和使用，云上和本地均需要基于效率与合规角度来控制数据和敏感信息的扩散。

8、AI和自动化增强网络安全，在安全运营中利用AI技术来优化策略制定和执行。结合利用AI和自动化来改善行为分析、安全控制、威胁检测和响应性能，从而增强事件发现能力并加快响应速度。

9、选择能够控制配置检查控制点、流量路由、审计日志和日志存放位置的厂商，以满足隐私要求和合规诉求

10、实时分析监控，闭环策略调优和执行，强化评估分析访问中的用户、设备的安全和可信状态，维护应用和风险的可视化，提供定制化的可视分析，检测云和Web活动，及时根据设备、功能及企业需求的变化，不断调整边缘访问策略适用的范围、设备和人员，更好地评估、调整安全策略。
11、访问控制的自动更新，确保正确的授权人员可以快速连接、访问特定信息，以自动化手段保持权限的准确性，并以最新状态进行持续性评估与调整。
12、建立一个由安全和网络专家组成的专门团队，其责任为从流程、职责上支持保障企业内部、远程员工、分支、边缘位置的安全访问。

SASE以其集成的组件化能力，借助AI和自动化技术的支持，到高级阶段即通过无人监管的机器学习技术和行为分析技术来监控恶意活动的迹象。一旦发现恶意行为，网络就会立即隔离威胁来源并撤销信任。在访问场景多样化、来源角色众多的情况下，访问场景的变化的速度超出了人工管理的能力范围，必须通过自动化技术来解决问题。凭借更优质的自动化分析洞察、更快速的关联追踪以及对应用通信更深入的钻取挖掘，从最初的威胁入侵到横向移动再到数据窃取和泄露，恶意活动在整个网络连接过程中都清晰可见，SASE利用各类安全组件执行探测和防控。

第四章 网宿SASE实践

4.1. 网宿SASE平台的关键特性

网宿SASE平台是国内首个基于云原生，以全球分布网络架构提供高度融合的一体化云服务，将网络连接能力与数据业务安全防护能力深度整合，安全访问服务边缘从用户者侧开始构建，在资源访问的网络通道上以ZTNA、WAAP、NGFW来保护业务访问并识别、抵御攻击流量，通过多安全级别沙箱、RBI来有效隔离网络攻击风险，智能识别用户异常行为，保护企业关键业务设施和敏感数据，灵活的管理策略支撑组织内控安全基线要求，保障访问者从任意位置高效安全地接入企业的资产业务和数据。

值得一提的是，网宿SASE方案中当前对CASB未做重点支撑，这主要是为了因应中国安全市场的发展特点。当前，国内尽管企业上云在持续发展之中，然而公有云SaaS服务在大中型组织，如政策合规与安全基线较高的行业如政务、金融、国企等，目前对采用公有云服务比较谨慎,这主要是基于各类行业政策、安全机制上的全盘限制和考量。CASB作为特定针对云SaaS服务提供保护的一种安全产品，尽管其为Gartner的SASE定义中的标准组件，然而在国内的应用前景，则仍然有待于云SaaS服务业务模式的进一步大规模行业渗透，及相关配套政策和标准的支持。

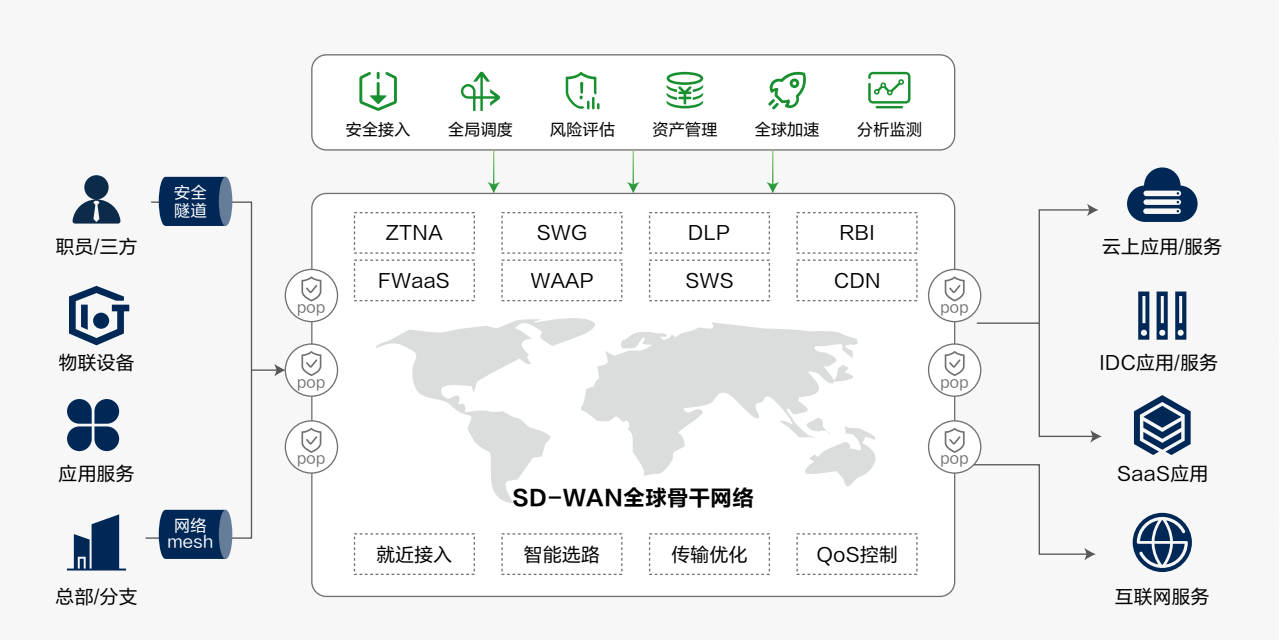

图 9 网宿SASE平台框架

1、全球化高速线路，具备分布世界各地的高吞吐量数据中心，在互联网的日益分割的现实环境下，区域性限制境内外的访问和数据流转处理，而网宿在中国和俄罗斯可以提供高速访问和本地安全控制能力。网宿与全球200多家顶级的网络服务提供商(ISP)合作，在自有服务专网上运行的网络连接服务，以此克服了互联网线路连接过程中的的延迟、丢包问题，并且已与各主流公有云平台打通高速直连，极大简化上云路线开通流程，可实现分钟级接入，提供最快的路由来满足任何网络连接请求。通过流量特征识别技术DPI，准确识别用户应用类型，结合QoS流量控制策略，保障核心业务高效运行。通过路由优化、协议优化、路径优化、数据优化等多种广域网优化技术提高网络速度。实现速度、安全性和用户满意度的同步提升。

2、组件化安全能力，网宿SASE将广域网组网功能与全面的安全功能结合在一起，包括安全Web网关、NTA流量分析、WAAP防护、防火墙即服务和零信任网络访问，共同保障和促进安全云和移动环境中的网络访问，保护企业应用、服务接口及数据的可用性，同时提供调度控制手段，并防护企业关键数据离开企业控制。网宿SASE是国内首个以零信任安全访问控制ZTNA为核心，集RBI、SWG和端点安全工作空间为一体的网络安全、访问安全、数据安全保护平台，并在用户侧提供all In One式的EDR安全防御能力，是以AI机器学习识别异常行为，具备成熟的端到端访问控制、审计和流量分析能力的全功能平台。

3、零信任控制，实施最小权限控制，消除协议与服务对公共互联网的暴露面，从而减少整体攻击面，持续监测环境变化、用户、设备和应用的风险，在不断变动的条件下根据信任模型进行可信度评估，从而完成动态适应性的访问授权，使用适应性策略和安全状态监测进行风险监测，将零信任原则从私有应用扩展至云和SaaS资源，基于风险洞察控制应用访问的特定动作，基于风险等级执行高级数据防泄露保护服务。

4、云原生框架，SASE服务使用没有特定硬件依赖关系的云原生架构，由软件定义和管理，不再依赖单一服务链，其分布化的PoP节点边缘分布，安全能力即开即用，部署便利，统一可扩展的架构，高性能和云化高可用服务，弹性自动缩扩容，支持企业业务发展。

5、边缘计算，随着数据中心不再是网络中心，SASE将检查引擎携带到就近的PoP点，更加符合边缘环境实际情况，网宿SASE安全组件针对性过滤恶意流量，对恶意软件/敏感数据进行单通道或并行扫描，基于软件、硬件中立的架构，控制面与数据面分离，高效实现灵活的安全策略部署和执行。

6、安全与业务可视化，基于用户行为检测、终端检测、入侵检测等各种要素洞悉客户网络安全风险。对流量威胁、用户的异常访问和操作行为进行审计，并将记录下的所有信息传送到企业已部署的SIEM等安全管控平台，同时通过平台安全风险感知对大量信号数据进行统计分析，检测入侵事件/异常事件/风险事件，对网络流量进行分析、识别、检测、告警及追溯审计可能的入侵行为和违规行为，为管理员提供安全运维的决策依据。

4.2. 网络服务与安全服务高集成化

对一个组织来说，并非使用的安全产品越多，就代表安全性越高，事实上，这些工具产生的影响可能恰恰相反，传统的烟囱式安全设施，存在互不协作、扩容困难、缺乏统一管理和一致策略的缺陷。要应对安全工具的叠床架屋的问题，必须进行整合。企业需要能够集成在一起并无缝协作的平台化服务，而不是部署单个解决方案来满足一次性的需求，在降低复杂性、减少管理开销和提高有效性等需求的推动下，安全技术正在加速融合，单一的SASE平台，可提供网络与安全栈之间更紧密的融合，部署与管理都更为快速，最小化复杂度以提升效率。

网宿SASE打破传统网络安全的固化边界概念，引导安全架构从网络中心化转向身份中心化、资源中心化，以集合的组网和安全能力组件，通过对用户、设备、网络、应用、数据的动态连接访问控制，建立应用层可视化、自动化、智能化的安全防护体系。对安全功能的整合将降低总体成本，提高长期运营效率，并进而提高整体安全系数。

图 10 集成化SASE平台

1、服务集成泛化兼容，平台服务所有类型用户，针对性提供无端、有端的接入途径，支持兼容各类目标资源，包括各类CS/BS服务应用，跨端口和协议实现广泛、可靠的安全访问防护覆盖。

2、快速实施，无障碍与企业现有IDP的各类协议标准开放对接，通过单点登录访问各种类型的应用资源，确保统一流畅的用户体验。

3、多种接入的集成，网络级和应用级的支持，同时提供远程用户、分支的统一接入，移动用户级接入通过边缘接入节点访问目标资源，同时提供分支连接接入方式，以SD-WAN组网提供总分连接，提供IPSEC加密访问通道。

4、通过信任评估引擎确保安全性，实时检测用户和设备的状态、网络连接信息、应用业务上下文、访问时空环境等多维数据，收集SASE各安全组件检测结果和告警信息，同时支持外接企业现网各类安全设备日志，综合研判识别风险进行动态访问权限管控。

5、云平台原生安全能力，开箱即用云防护，面向网络内部和外部提供可扩展的快捷安全保护，提供分布式边缘防护，包括DDoS防护能力、WAF安全能力等，保障企业业务安全稳定运行。

6、全球网络加速能力，解决企业远程访问速度和稳定性问题，提供高效用户连接体验。

7、管理便捷，一站式管理平台，使用统一管理平面，易于运营维护管理，通过统一的云交付服务和管理面板，可开启所有安全能力，相对于传统安全产品的部署、配置和整合方式，显著差减少时间、成本和资源支出。对用户操作行为全面追踪审计，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，满足企业运维和安全控制需求，提高管理效率。

8、统一安全控制体系，具有单个数据湖，并支持多安全组件单通道解密，检查恶意软件和敏感数据，防止网络入侵和数据泄露，统一的策略管理企业安全基线，支持威胁监测、告警和安全处置的闭环。

4.3. 数据防泄露与安全合规

4.3.1. 数据防泄露安全保护

网宿SASE通过对网络空间用户、设备、网络、应用、数据的安全连接保障和访问控制，建立应用层可视化、自动化、智能化的安全防护体系。其身份可信、终端可信、行为可信的核心特性能力，以及从传输加密、边缘防护、网络隐身打造的平台安全能力，为企业搭建统一安全访问体系，实现用户使用任意终端在任意位置、网络环境中安全、高效、可靠、便捷地访问企业资源和进行日常办工。

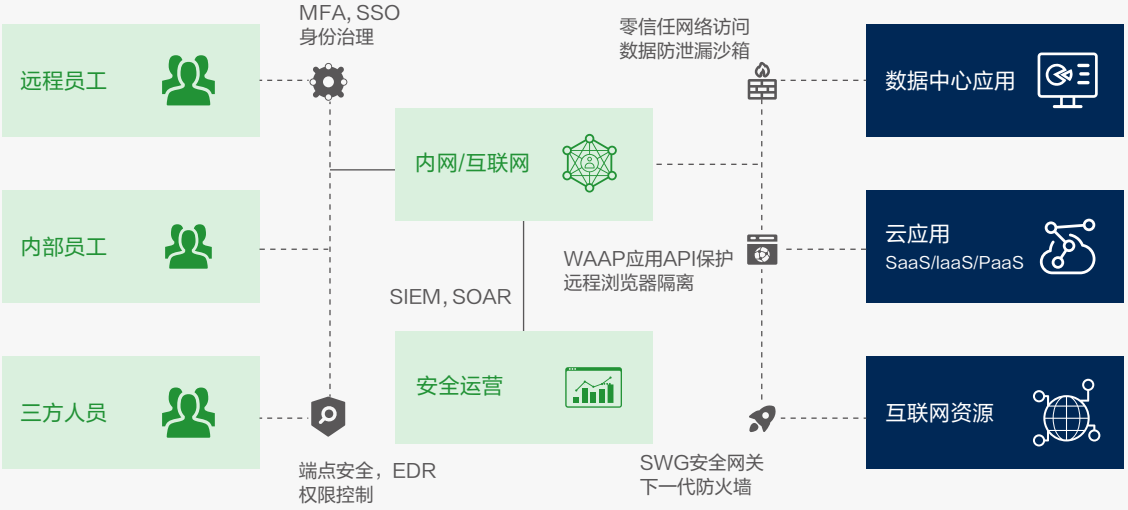

图 11 多方接入的安全控制

1、网络隐身，使用ZTNA保护数据中心的应用和云上服务，减少应用暴露面，限制网络横向移动，抵御入侵和数据窃取。
2、对所有受控、非受控的应用、云服务实施SSO/MFA，高强度身份认证，包括基于用户、设备、应用、数据、用户行为进行可适应策略控制，触发双步认证保护，确保合法访问。
3、安全工作空间，提供安全办公和上网的环境，空间中数据强加密由企业主体控制，使用者无法自行外发，有效防止数据泄露。
4.检测阻断不合规网络连接，提供高速RBI工具，将互联网风险内容与用户设备、办公网络隔离开，对Web应用上敏感信息进行防护，RBI支持管控文件上传、下载、复制、粘贴等行为，确保敏感数据不落地。
5、Web访问数据保护，访问敏感数据业务时提供禁拷贝、水印防护手段。
6、提供智能信任评估引擎，实时检测用户和设备的状态、网络连接信息、应用业务上下文、访问时空环境等多维数据，根据识别的风险动态调整用户的访问权限。同时支持多种威胁模型，对用户行为进行实时的可信建模和全时空分析。
7、对所有云、Web流量进行多层次、内置解析和威胁保护，阻断恶意软件攻击终端，同时也阻断外向恶意软件通信，防止敏感数据外流。
8、在企业的资产、用户、网站、设备和位置间实施细粒度策略控制，保护数据安全流动。
9、实施高级行为分析，数据活动异常、失败的登录、异常动作事件，追踪用户行为并进行信任评估评分，探测内部威胁、数据泄露、失陷设备和被盗凭证，多层次防护访问安全。
10、可视化高级分析，挖掘应用和数据活动的风险、威胁事件、数据保护异常、关键安全基线偏差，并支持追溯取证。

4.3.2. 网络安全防护运营

当前，许多行业都在关注数据安全。IT信息化时代，对企业核心数据的保护是关系企业营运持续的关键，并且合规要求更加明确，所有行业和所有地理地域都处于数据安全风险之中，针对攻击和数据泄露制定响应计划十分重要，有效的预防手段、处置方案会对所花费时间和经济损失产生显著影响。网宿安全服务团队可以为企业开展全面的网络安全情况评估，对企业网络进行漏洞检测、渗透测试，并提出整改加固建议，组织安全培训和演练，制定针对数据窃取、勒索攻击事件准备响应计划，同时考虑所需的业务和技术应对措施，帮助企业组织为网络攻击事件做好充足应对准备。

1、对员工进行网络安全常识如钓鱼攻击的培训和提醒，实施攻击应急演练；
2、制定商业延续性计划，盘点企业重要资产和数据，并规划安全防护框架；
3、执行常规周期的重要数据备份，需要同时进行多种方式备份，备份数据应当加密，确保规避可能的勒索软件攻击；
4、执行系统周期备份计划，如关键数据、配置、日志，以支持紧急状态下的系统恢复；
5、系统和配置管理，对网络内的设备资产进行梳理，移除不必要的软件、硬件，检视修正操作系统、网络设备的安全配置；
6、启用现代化的硬件安全特性，如UEFI安全启动、TPM、硬件虚拟化等，对老旧设备进行刷新或报废，启用系统的安全性、诊断能力和风险隔离能力以保护系统、关键数据和用户凭据；

7、攻击后处理应对机制，提前规划应对攻击者可能可能实施的多种威胁施压手段，包括盗窃并在网上发布机密数据、加密关键数据并中断运行服务、将事件通知股东/合作伙伴/供应商以施压的情况；
8、按照合规和法律要求，向相关机构报告攻击事件；
9、考虑周全的事件响应计划，使企业在面对灾难级局面时，在各个层面、组织上进行有效的协同和处置，减少最终损失；

表 4 安全体系阶段防御

第一层：屏蔽攻击	实施安全隐身网关防护，隐藏企业网络资产
	通过安全网关检测、阻止、隔离威胁站点和文件数据
第二层：用户意识	周期的培训、演练以帮助用户辨认出网络攻击如钓鱼邮件
	提供模拟帮助用户探索和识别欺诈攻击
	构建服务体系，方便用户寻求帮助和报告可疑事件
第三层：安全防护	保护账户安全，启用MFA校验合法身份
	SASE安全边缘，安全网关检测过滤检测网络访问
	启用沙箱空间，保护用户侧关键数据
	安装终端杀毒EDR，反恶意攻击的安全软件
第四层：事件响应	设置和周期修订的攻击事件应急响应计划
	内部通畅的安全事件、可疑事件报告机制

4.4. 基于风险的的安全防御框架

凭借全球分布式的安全传输网络的天然优势，网宿SASE平台建立起一张虚拟安全网络，为企业打造安全、高效的零信任安全办公环境，提升网络业务环境安全性。当前，几乎所有行业和所有地理地域都处于网络攻击的风险之中，网宿SASE平台对既有IT网络安全架构进行范式更新，因应云化、大数据、物联网、移动化的网络架构演化趋势，针对各类网络威胁构建体系化、多层面立体防御体系，在攻击实施各阶段进行识别和阻断。

零信任SASE包含如何阻止现代网络攻击的一套原则。网络攻击者往往遵循一定的轨迹，在初始进入到访问环境之后，他们会在网络上横向移动，控制更多的应用帐户，并提升帐户权限，以便可以采取另外更具破坏性的行动。虽然最终的攻击结果可能是部署勒索软件或窃取数据，但攻击者必须首先摸清企业的IT环境，才能真正触及攻击的首要目标。在这个过程中，组织有很多机会可以发现入侵并切断连接通道，减小入侵安全事件的实际损害。在真正的零信任SASE方案中，有很多技术手段可以实现这一点，比如在访问敏感资源之前多次核验用户权限及其行为，或者将IT环境分成多个不同的子段，并赋予不同的安全策略，实行多层防御机制。

总体而言，网宿SASE通过暴露面收敛隐藏、应用细粒度访问控制、横向移动阻止、身份MFA校验、凭证密码加固、恶意访问威胁检测、流量深度分析和设备环境安全感知、UEBA行为异常识别等能力，能够在攻击的初期阶段就进行安全检测、识别和干预，力图在威胁到达网络或终端、应用资源之前加以阻止。借助SASE实现将风险持续评估能力、动态访问连接控制、实时审查能力集成于复杂的一体化安全架构。

图 12 网络攻击链和防御

SASE解决方案针对网络攻击的各个阶段进行针对性防御，从以下各个场景进行干预处置和防护：

▶ 攻击者嗅探网络寻找目标，非法获得用户凭证进一步访问敏感系统获取重要信息时，通过网络层面隐身和身份强验证、限制权限范围、环境评估来抵御攻击：

1、网络隐身技术，隐藏网络资产，网络只对认证授权的可信任用户可见，解决资产和应用暴露在公网的问题，攻击者无法嗅探、扫描到企业内部的服务，无法利用内部服务的漏洞，有效保护企业内部网络、业务的脆弱性，遏制漏洞利用和攻击流量横向移动。

2、多因子认证（MFA），重要的账户凭据（即用户名和密码）在很多时候都是通过网络钓鱼攻击或被攻击的第三方遭到窃取，然后被远程恶意攻击者(包括僵尸网络)重新使用，增强网络业务对用户身份鉴定能力，实施MFA实际上改变了威胁态势，威胁实施者仅仅利用被盗的登录密码凭证无法攻破企业安全防线。

3、账户安全加固，采取强密码校验、密码周期强制更换策略，支持限时开放临时权限、有效期的账户管理，防止攻击者获得有效账户信息。

4、最小权限限制，仅允许按用户所需为其分配最低访问权限（也称为“最小权限”），实施RBAC、ABAC用户权限控制模型，支持账户权限自动回收，对用户访问权限进行实时管控，防止攻击者获取系统特权。

5、设备安全基线，受信任设备进行标记，拒绝或降低非授信设备的接入权限，监测用户终端设备的健康状态，判断终端是否授信准入。终端安全检测，保护用户设备安全性，确保漏洞检查合格的终端设备才允许接入，防止攻击者利用终端设备作为内网入侵的跳板。

▶ 用户点击邮件、附件中恶意链接访问未知恶意网站时，通过威胁情报阻断恶意链接访问，使用RBI隔离威胁站点，高敏应用使用沙箱安全空间保护规避入侵：

1、支持DNS层安全，可通过禁止连接来阻止对恶意软件、勒索软件、网络钓鱼和僵尸网络的请求。安全Web网关会记录并深入检查所有Web流量，帮助加强透明度、可控性和安全保护。云交付的防火墙有助于使用IP、端口和协议规则来记录和屏蔽流量，从而在整个环境中实现一致的保护。
2、威胁情报利用，系统对接海量威胁情报，保持最新业界对恶意地址的追踪，对用户访问“风险网站”进行阻断，降低遭遇欺诈网站、挂马、钓鱼等安全风险的可能。
3、流量深度解析能力，实时分析、检测访问流量中的威胁攻击从而进行告警和阻断，通过EDR终端异常攻击风险检测、NDR的异常网络攻击检测，并结合威胁情报识别黑客的控制行为及C2服务器。
4、安全工作空间，保障接入和数据使用的安全性，与宿主机的系统、网络、存储进行隔离，数据加密存储，阻断外部恶意软件渗透，网络连接采取白名单机制，用户尝试连接到可疑站点时即进行阻断。
5、RBI网络威胁隔离，对各类Web互联网访问提供RBI隔离安全访问，可进行沙箱查杀、恶意文件扫描，避免基于浏览器漏洞、挂马网站、网络恶意文件的攻击和威胁。

▶ 用户打开恶意文件、恶意网站下载恶意代码后，后台自动下载的恶意软件在本地加载、运行、嗅探时，设备本地AV/EDR进行杀毒和威胁处置：

1、用户端点安全，自动扫描检测邮件附件、网络文件，识别病毒、蠕虫、木马和恶意软件并进行处置隔离、删除，并支持有文件、无文件攻击识别和处置。
2、可信应用控制，避免使用来路不明的软件和启动可疑服务进程，禁用命令行等特权工具，只允许企业安全许可的应用运行，避免恶意软件运行，窃取和发送敏感数据或实施系统参透破坏。
3、所有经过平台的流量全程加密，保障通信安全，避免间谍软件的嗅探和监听窃密。

▶ 恶意软件尝试窃取数据外发、破坏或加密用户数据时，系统触发外发敏感数据阻断，识别异常外发并即时处置：

1、数据外发控制，用户失误或恶意外发数据时，对敏感文件、敏感信息进行识别和外发封禁处置。
2、网络访问检测，监测用户主动、软件自动地进行可疑网络活动和外发连接时，告警和阻断外网访问连接。
3、数据存储安全，通过对安全工作空间的数据磁盘存储区进行伪装、同时加密空间内部数据，从而防止恶意软件识别重要文件，实施窃取或勒索加密，有效保障数据安全。

4.5. 踏上SASE之旅

为了降低数字供应链风险，组织机构需要采取新的应对之策，提高安全控制和实施最佳安全实践。借助SASE，现在我们可以将风险持续评估能力、动态访问控制、实时审查能力集成于复杂的安全架构。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。对于许多企业来说，SASE的建设需要全面改变架构、流程和安全意识，这不是一蹴而就的改变，而是一个循序渐进的过程。

很多企业已经有意或无意地走上了SASE之旅，所采用方法因企业IT架构阶段而不同，其战术、架构或战略的选取也相应不同。任何零信任之旅都将面临各种阻碍，它需要整个企业给予强有力的领导层支持、投资和认同才能确保成功。您需要首先考量与企业相关的业务驱动因素、现有流程功能和关键场景用例，对自身的网络、安全资产体系进行梳理和规划，合理评估定位自身IT建设水准，设定明确规划目标，明确IT资产管理、安全基线规范和数据治理诉求，为业务、数据资产和企业用户量身定制可行的SASE保护场景化方案，并逐步向高成熟度的SASE安全接入服务边缘全能力模型演进。

图 13 企业建设SASE实践路径

如上图所示，对于企业来说，在以SD-WAN方式进行组网后，集团化、全球化的组织得以通过IT网络基础设施高效连接起来，支持日常运营、企业人员互联、业务互通。此后，即需要将原有针对从外部接入内部资源的粗放陈旧的VPN使用模式，切换到零信任访问方式，这是建设SASE必不可少的核心环节，也是达成企业全面零信任转型的初始步骤。在零信任平台逐步承载内外网络连接、业务交互、数据传输的状态下，依据行业政策和企业安全合规基线，利用SASE方案部署于云、管、端、边的安全设施（包括各类安全网关、安全客户端、POP安全算力边缘等），为关键业务、敏感数据提供分级、识别和防泄露保护。最后，在实现内外统一零信任的基础上，提供接入互联网资源的安全防护，深度识别加密流量，过滤阻截网络威胁攻击，并同时在终端上建立防护屏障，针对钓鱼攻击、勒索软件攻击等提供端到端一体化防御。

企业过渡到完整的SASE架构需要时间。实际上有许多企业零信任框架搭建早已起步，企业希望在硬件和软件方面可以继续利用剩价值。领导者需要能够制定转型的战略路线图和迁移计划，以及未来几年采用SASE的实施规划。在走向零信任的网络安全大道上，公司并非需要重新购买所有的新技术才能达到SASE演进目标，而是可以结合应用已部署技术以及各种技术组合，将安全效益在SASE框架中最大化利用。

最后，SASE不仅仅是一项技术解决方案，更是一次企业文化变革，需要组建新的运营团队，支持流程的变更调整、业务保障沟通、员工专业培训，人员认知等软因素是取得转型成功的重要要素，为了顺利实施SASE，企业安全制度和工作文化需要提升适配，公司必须注重培养一种倡导透明、信任和开放沟通的企业文化，辅以持续培训和相应技术升级，有效提升员工的安全意识，从而确保企业的业务融合创新和整体演进战略得以安全、有效地实施，获得数字化转型带来的持续益处。

参考文献

[1] 2022 SONICWALL CYBER THREAT REPORT
[2] X-Force Threat Intelligence Index 2023，IBM Security
[3] Market Guide for Single vendor SASE，Gartner 2022
[4] Strategic Roadmap for SASE Convergence Gartner 2022
[5] IDC MarketScape : 中国零信任网络访问解决方案2022厂商评估
[6] 2021网络安全前瞻调研报告，Deloitte
[7] Cost of a Data Breach Report 2021，IBM Security
[8] The definitive guide to ransomware，IBM Security
[9] 2020年中国互联网网络安全报告，CNCERT|CC
[10] 勒索软件安全防护手册，CAICT中国信息通信研究院
[11] SDNLAB:Gartner公布首个SSE魔力象限排名
[12] Gartner Magic Quadrant for Security Service Edge,2022
[13] Market Guide for Zero Trust Network Access 2020,Gartner
[14] checkpoint research report global cyberattacks
[15] Evolving Zero Trust - Microsoft Position Paper

版权信息

CHINA INTERNET SECURITY REPORT