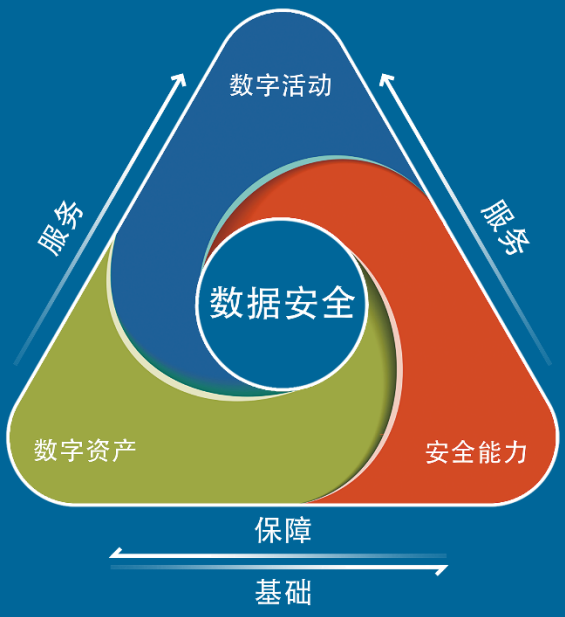
数世咨询
Digital World Consulting

# 云网安一体化能力指南

数世咨询
Digital World Consulting

# 云网安一体化能力指南




数字安全的三个元素分别为，安全能力、数字资产和数字活动。数字资产是安全能力的保护对象，数字活动是安全能力以及数字资产的服务对象，而数据安全则是三元论的核心目标。对于这四者关系的深度理解和相关技能掌握是做好数字安全工作的关键。

数字安全能力模型研究的基础，来自于数世咨询 2020 年首次提出的“网络安全三元论”。三元分别为，网络攻防、信息技术和业务场景。

随着数据成为第五大生产要素为典型标志的数字时代来临，“网络安全三元论”在 2022 年进行了更新迭代升级为“以安全能力、数字资产和数字活动为三元素，以数据安全为核心目标，即三元一核”的“数字安全三元论”，以适应我国数字中国建设的进程。

数世咨询作为国内独立的第三方调研咨询机构，为监管机构、地方政府、投资机构．网安企业等合伙伙伴提供网络安全产业现状调研，细分技术领域调研、投融资对接、技术尽职调查、市场品牌活动等调研咨询服务。

**报告编委**

主笔分析师 **陈发明**

首席分析师 **李少鹏**

分析团队：**数世智库** 数字安全能力研究院

# 目 录

# 前言

随着企业业务纷纷上云，以及远程办公成为新常态，信息安全建设面临巨大挑战。一方面，业务上云带来了数据集中存储和管理的便利，但同时也增加了数据泄露和遭受网络攻击的风险。另一方面，远程办公的普及使得企业网络边界变得模糊，员工可能从任何地点、使用各种设备访问企业资源，这给安全访问控制带来了新的难题。企业迫切需要这么一种解决方案，既能方便地实现跨地域远程访问，又能满足安全合规和业务安全需求，还要能够实现便捷的运营管理。近几年来，逐渐兴起“云网安”一体化解决方案，以满足企业对分散业务和远程访问的集中管理和安全监管需求。

然而“云网安”也带来了技术融合的复杂性，同时甲方用户对解决方案相关产品的可靠性、稳定性以及真实表现也持审慎态度，包括 2019 年 Gartner 提出的 SASE 架构近几来在国内也一直没有很好的落地应用。其中的原因很复杂，除了技术因素之外，国内企业的 IT 建设情况、用云用网的情况跟国外也有明显差异。

为了客观真实地反映云网安一体化解决方案的市场及应用情况，数世咨询通过资料收集、甲方调研、企业访谈、市场数据分析等方法撰写《“云网安”一体化能力指南》，从第三方视角来对该解决方案进行总结，分析用户场景需求，提炼满足需求所需要的关键能力，同时对优秀解决方案及能力企业进行推荐。以供业内人士参考。

本报告**技术部分**主要内容：云网安一体化发展演变、定义、架构、关键能力等。

本报告**市场部分**主要内容：云网安一体化市场规模、应用场景、能力企业点阵图、能力企业主要业务特点及产品、趋势分析以及代表厂商优秀案例。

尽管本报告尽笔者所能尽量充分的进行了技术以及市场方面的调研，但受能力所限或有错误和偏颇之处，欢迎同行与我联系交流。

为了描述上的简洁性，本报告下文中所提到的“云网安”方案均指“云网安一体化”。

勘误或进一步沟通，请联系主笔分析师：陈发明 chenfaming@dwcon.cn

# 关键发现

- ✓ 尽管 SASE 技术目前趋于成熟，但在国内的落地应用情况不佳，主要原因是国内 SaaS 应用大部分是消费者级别的应用，真正的企业级 SaaS 应用目前仍未大量普及。
- ✓ 国内云网一体化解决方案自 2015 以来历经了三个阶段：高效低成本的网络互联、与零信任结合的一体化远程访问、与数据安全结合的云网安一体化。
- ✓ 当前在云网安一体化解决方案中，端点侧的数据安全治理越来越重要和迫切。端点安全保护主要涉及终端安全和敏感数据保护两大方向。
- ✓ 据本次调研统计，2023 年云网安一体化市场规模约 18 亿元，到 2027 年市场预估 35 亿元左右。
- ✓ 云网安一体化各细分领域的市场占比统计：安全及相关服务（占比 20.9%），网络产品及相关服务（占比 46.4%），云计算产品及相关服务（占比 32.7%）。
- ✓ 尽管不少安全厂商都能提供各自的“云网安”解决方案，但是基于不同的企业发展路线，在云、网和安全方面各有侧重，仅有个别厂商能提供云网安整体解决方案。

# 1.云网安一体化

## 1.1. 背景

传统的网络与安全架构以数据中心为核心，但随着大数据、物联网和云计算的快速发展，企业业务上云已成为大势所趋，所带来的变化是，大量的数据和相关业务从数据中心转移到云端。而多数企业为了提高业务灵活性、保证业务连续性和提高数据安全性等原因，选择与多个云服务商进行合作。与此同时，用户、设备和数据分布在企业网络之外的情况也越来越多。多云策略和广泛的跨域数据访问，给网络安全带来了前所未有的挑战。

Gartner 提出的 SASE（Security Access Service Edge）架构，整合了 SD-WAN、SWG（安全 WEB 网关）、CASB（云安全防护代理）、ZTNA（零信任）等一系列技术栈，旨在满足以上所述的网络及安全需求。国外 SASE 技术目前趋于成熟，但近几来 SASE 在国内一直没有很好的落地应用，也少有安全厂商能够完全实现 SASE 所包含的全部能力。相较于国外，国内企业的 IT 建设情况、用云用网的情况以及安全需求跟国外也有明显差异。

比如在应用安全的防护方面，国外用户更多的开始应用 SWG、CASB 来实现安全 WEB 访问和业务防护。相比之下，国内就很少见到 SWG、CASB 等安全产品。据数世咨询的了解，实际上国内目前用户对 SWG/CASB 的需求很少，主要原因是国内 SaaS 应用大部分是消费者级

别的应用，真正的企业级 SaaS 应用目前仍未大量普及。

在云计算应用及实施安全策略方面，根据有关调研数据显示，国外超过 70%的企业已经广泛使用 SaaS 化的公有云服务，如微软 Azure、亚马逊 AWS 等，大部分业务数据和应用程序集中在云端，数据的集中性使得云端数据防护成为其首要关注的重点。

与国外情况不同，国内企业用户更倾向于自建私有云，同时据行业统计超过 50%的企业采用混合云环境，预计未来几年 80%以上的企业会采用混和云部署。因此，大量业务数据广泛分布于自建数据中心、多个公有云平台以及边缘和端侧。

这种数据分布的多样性使得用户在如何规划网络和安全架构，实施网络安全、数据保护变得棘手复杂。一方面，自建私有云需要保障内部数据的安全性和合规性，对传统的网络安全防护措施有一定依赖。另一方面，在混合云环境中，确保数据在不同云平台之间安全传输和访问，需要考虑优化和补充新的安全防护策略。此外，端侧设备的安全性也要兼顾，如防止数据泄露、恶意软件感染等。针对“云、网、边、端”建设多位一体的综合防御体系，实现“云网安一体化”无疑是一个简化安全运营、降本增效的良好思路和建设方向。

在“数字中国”战略的推动下，国内企业正迫切需要提高数字化转型的效率，并对企业网络及其安全资源进行全面的规划和综合考量。随着企业业务向全球化扩展，业务连续性和数据安全性的要

求也变得日益严格。“云网安一体化”不仅在技术层面解决了网络和安全防护的问题，也大大加速企业业务的数字化和云化进程。

## 1.2. 发展阶段

“云网安一体化”的提法出现已有几年，其诞生源于云计算技术的不断进步、产业互联网的蓬勃发展以及企业数字化转型的加速。大概在 2015 年前后，信息通信技术（ICT）服务的全面云化带动企业上云成为主流趋势。在这种形势下，远程接入及数据访问呈现大规模爆发态势，进而推动了“云、网络与安全”的融合以及一体化运营和管理模式的发展。

数世咨询一直在关注着该概念的内涵变化和发展，云网安一体化演变大致分为以下三个阶段：


云网安一体化演变

### 阶段一：高效低成本的网络互联

自从有了互联网，远程访问和远程连接的需求就纷至沓来，但多年以来主要依赖于各类 VPN（如 IPSsec/L2tp）和专线（如 MPLS）技术。在十多年前的“低速”互联网时代，由于远程访问流量相对较小，尽管 VPN 速度慢且成本高昂，但普遍尚能接受。然而近几年

来，随着短视频、实时语音、各种智能终端的激增，对数字数据的访问量呈现爆炸式增长，传统的 VPN 已难以为用户提供畅快的远程访问体验了。

自 2015 年以来，软件定义网络（SDN）与广域网（WAN）结合而成的 SD-WAN（软件定义广域网）逐渐受到市场关注。SD-WAN 的优势在于其能够显著降低网络运营成本，同时提高网络的灵活性和可扩展性。通过利用现有的多种互联网链路和智能选路技术，SD-WAN 能够实现更高效的带宽利用和更优化的网络性能。在此阶段，“云、网络和安全防护”三者协同发展、互相保障。

不过就 SD-WAN 市场来说，国内与国外不同，国内网络资源主要集中于几大运营商，第三方网络服务商基本也只能与运营商合作，SD-WAN 市场相对窄缩。相比之下，国外市场则呈现出更为多元化的格局，网络资源分散到众多电信运营商和网络服务商，大家共同参与竞争，也能提供各种特色化的 SD-WAN 网络服务。

本阶段国内代表性方案和产品有：华为的星河 AI 融合 SASE 解决方案及产品，Panabit SD-WAN 解决方案及其多功能网关产品。

## 阶段二：与零信任结合的一体化远程访问

在疫情时期，移动办公和远程工作模式广泛推行。然而，传统的 VPN 应对复杂的用户身份和多样化的访问需求时，灵活性和适应性不足。VPN 过多的暴露面，让管理员难以精确控制对资源的访问。

零信任模型基于“永不信任，持续验证”的核心原则，对每个访问请求都实施严格的身份验证和权限检查，而无论用户身处何地、使用何种设备。零信任与远程访问的结合大大降低了资源风险暴露面，适应了不断变化的远程办公和业务安全的需求。

诚然，零信任技术的真正落地确实面临诸多挑战。比如有历史包袱问题，企业需要摒弃过去的身份安全架构和策略，重构身份管理体系。有技术复杂性问题，零信任要求实现精细的访问控制，需要对用户的身份、设备状态、应用需求等进行实时评估和动态授权。还有研发投入和成本控制的问题，构建零信任安全系统不仅需要配置相当规模的访问控制软硬件基础设施，还涉及到与众多业务系统的深度集成等。

本阶段国内代表性方案和产品有：网宿安全的 SASE 办公安全一体化系统，亿格云的亿格云枢产品方案，缔盟云的太极界（安全桌面）等。

## 阶段三：与数据安全结合的云网安一体化

随着业务的云化转型，数据存储不再局限于单一的物理位置，而是分散于多云和数据中心。这种分散性增加了数据泄露的风险，需要实施更为严格的资源访问策略、防敏感数据泄露以及数据流转监控，这使得数据管理和保护变得更加复杂。

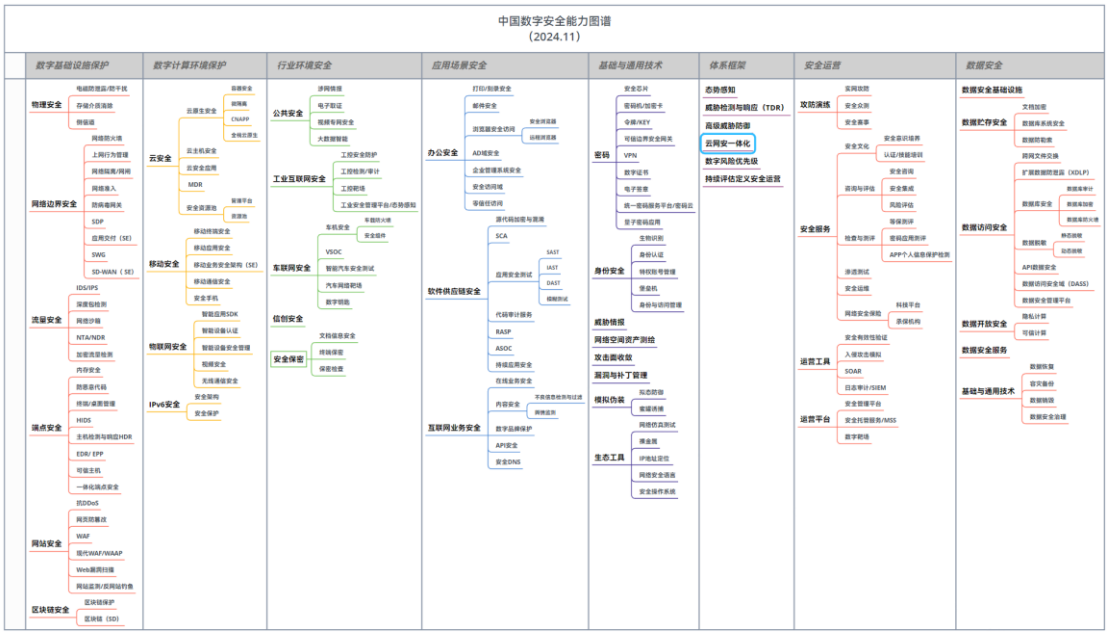
与数据安全结合的云网安一体化进一步融合数据保护理念，为企

业在合规运营、统一管理、降本增效、数据保护等方面提供更全面的防护方案。

本阶段国内代表性方案和产品有：电信安全的云脉 SASE、奇安信的 Q-SASE 安全访问服务一体化平台，数篷科技的 DACS 凌域企业安全工作空间等。

## 1.3. 定义

在 2024 年度数世咨询最新更新的《中国数字安全能力图谱》中，本报告所述能力框架归于“体系框架”-“云网安一体化”细分子项：




2024 年度《中国数字安全能力图谱》

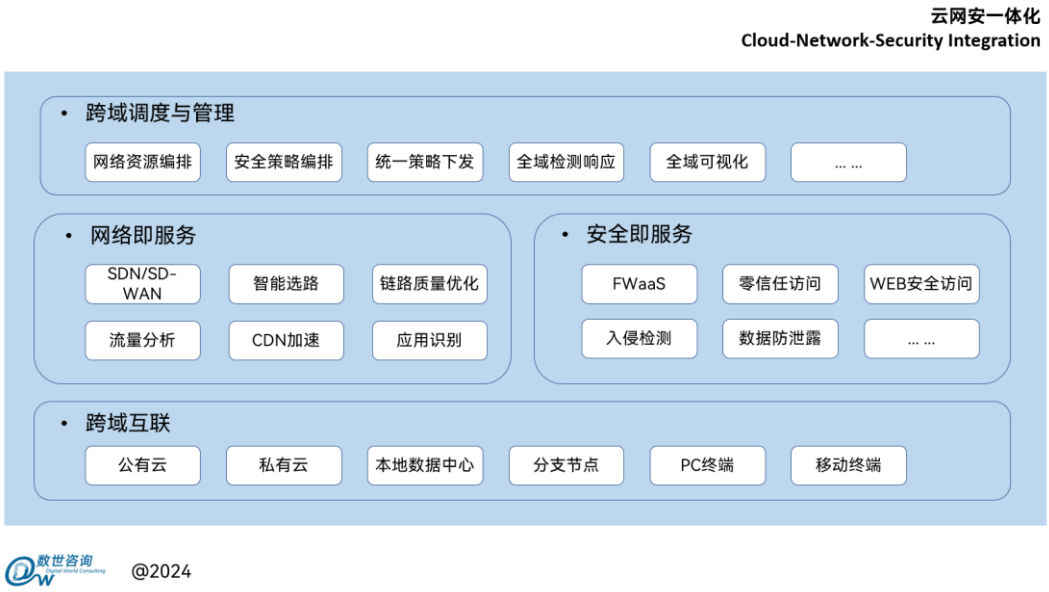
数世咨询对“云网安一体化”的定义如下：

**云网安一体化是一种将云计算、网络通信和信息安全深度融合的技术框架。它通过集成 SaaS 化安全服务、零信任网络访问、广域**

网优化、端点安全和数据安全等技术理念，旨在优化网络性能、提升访问速度，并确保用户能够安全、可靠地实现网络接入访问，并通过一体化的管理模式，实现云、安全、网络资源的统一管理和服务。

## 1.4. 架构

云网安一体化架构通过一个集中的管理平台实现网络与安全的统筹管理和服务，简化了网络和安全的日常管理。这种架构将网络与安全服务化，赋予了系统更大的灵活性和可扩展性，使其能够迅速响应并适应企业业务的动态变化和安全需求，如下图所示：




数世咨询：云网安一体化架构

- **跨域调度与管理**

跨域调度与管理是云网安一体化的核心，它将分散在不同地理位置的节点和终端纳入统一的管理视野，通过统一的管理平台、在

组织的全域范围内实现网络和安全资源的调度与管理，具体包括：网络资源编排、安全策略编排、统一策略下发、全域检测与响应以及全域可视化等。一体化管理确保资源调度与策略管理在整个组织范围内保持高度一致性，从而优化资源配置并提升运营效率。

技术演进：

1）在初期阶段

实现对分支站点设备和业务流量的集中管理，自动化开局等。平台主要聚焦于网络资源的调度和编排，安全策略的统一配置及下发。

2）在进阶阶段

安全管理功能被进一步整合，管理平台开始集成零信任模型、安全策略编排、安全策略优化、全域事件检测和可视化等融合能力。

3）集成数据安全能力

融合纳管数据安全功能（主要是数据分类分级和敏感数据防泄露），数据安全策略配置和泛远程终端的策略管理，实现云、网络、端点及数据安全的一体化。

**说明：**

本报告在此不过分强调所有功能模块的紧密耦合集成。原因之一是所有功能模块的紧密耦合大大增加功能实现和管理的复杂度，有可能还会拖慢管理平台的执行效率。原因之二是，企业根据自身

的规划和安全策略，可能逐步构建了不同的功能平台，比如统一日志收集平台、大数据分析平台和安全运营中心（SOC）平台等。网安管理平台与这些平台的一体化集成，最佳实践是通过 API 实现关联和数据共享。比如，安全管理平台可以与云端 SOC 平台联动，获取 SOC 对流量数据、实体行为分析和日志分析的结果，或者实现日志数据的跨平台关联查询等。

- **网络即服务**

网络即服务（NaaS）要求将网络功能以服务化的形式提供给用户。广域网连接的方式也可以通过各类链路如 MPLS、以太网、宽带、无线以及 5G 链路等实现灵活接入。由 SDN（软件定义网络）发展而来的 SD-WAN 是实现 NaaS 的基础，SD-WAN 使公有云、私有云、数据中心、分支节点、移动终端等节点互联变的轻松便捷，同时实现了低成本、低延迟和高带宽的网络连接服务。

技术演进：

1）智能路由与负载均衡

根据实时网络条件和应用需求选择最优的数据传输路径；实现多链路冗余，当链路发生故障时可以自动切换到备用链路；实现负载均衡，提高带宽利用率和减少网络拥塞与延迟；通过对数据包进行优先级和 QoS 分类，对特定业务进行分流等。

2）基于应用的流量管理

识别业务并能根据业务特点优化链路传输，比如对视频会议、实时语音等业务流实现优化以提升用户体验;实现基于应用的链路负载和智能选路；实现上网行为分析，识别用户上网行为并能分析分类，以辅助管理员实施相应安全合规策略。

3）集中管理与自动化

通过管理平台对分支站点、分支设备及网络进行集中管理，而无需直接访问节点物理设备；实现网络、路由、访问策略的集中编排与管理。

## ● 安全即服务

安全即服务（SecaaS）是指将安全能力 SaaS 化，实现安全能力的订阅和弹性扩展，以适应不同规模的业务的安全需求。安全即服务包括但不限于 FwaaS（防火墙即服务）、SWG（安全 Web 网关）、CASB（云访问安全代理）、ZTNA（零信任网络访问）、DLP（数据防泄露）等。

技术演进：

1）虚拟化安全资源池[1]

SecaaS 早期通过虚拟化安全资源池的服务模式来实现。一般为安全硬件设备的一虚多，或者基于虚机镜像的方式构建，具备一定的弹性扩展能力，但是受限于硬件设备的性能，安全服务扩展能力有限。

[1] 数世咨询《云安全资源池能力指南》(2024)

2）云原生安全资源池

通过安全容器，以云原生化模式构建。云原生模式基于容器化封装、自动化管理和面向微服务的架构，可以实现安全能力的更灵活部署和扩展。

**说明：**

尽管目前云原生安全资源池尚处于技术探索阶段，功能实现上还不够丰富完备，但是云原生化是业务上云以及云安全未来发展的重要趋势之一[2]，本报告编写期间，已有多家厂商开始推出，并实际部署云原生安全资源池。

## ● 跨域互联

跨域互联是指公有云、私有云、本地数据中心、各分支节点以及不同终端之间通过 SD-WAN 或者专线技术实现互联，实现跨地域、跨云的资源调度和远程访问。节点之间通过加密通信、严格的访问控制和身份验证、数据加密解密以及安全审计和监控等技术，确保数据传输的安全性。

技术演进：

1）通过 VPN 以及传统专线技术实现跨域互联

VPN 通过加密技术在公共网络上建立安全的隧道，保护数据传输的安全，而专线则提供物理或逻辑上的专用连接，确保

[2] 数世咨询《云原生安全能力指南》(2024)

数据传输的稳定性和低延迟。这些技术虽然在安全性和稳定性上有所保障，但往往成本较高，且缺乏灵活性和可扩展性。

2）SD-WAN 结合零信任实现跨域互联

SD-WAN 通过集中管理控制平面，实现对广域网资源的动态管理和优化。结合零信任模型，实现进一步强化的网络安全访问。

3）融合端点安全以及端点数据安全的跨域互联

基于数世咨询的调研，当前在云网安一体化解决方案中，端点侧的数据安全治理越来越重要和迫切。端点安全保护主要涉及终端安全和数据保护两大方面。终端安全通过漏洞扫描、病毒查杀、配置检查等技术实时监测终端设备状态，识别潜在威胁。数据保护则侧重于敏感数据的安全管理，比如通过安全沙箱技术对重要数据进行隔离管控，利用 DLP 技术防止敏感数据泄露等。

相较于传统终端安全防护，云网安一体化方案中的终端安全通过整合零信任访问技术、SD-WAN 支持的多路径传输和智能路由选择，以及跨域的统一终端管理，实现组织全域范围内的终端安全运营。

## 1.5. 关键技术

云网安一体化架构是系列技术的融合，涉及到端点、网络、云计算、安全等各个层面。列举部分关键技术如下（为避免文章内容

冗长，尽量减少读者阅读的枯燥感，以表格的形式简单呈现，如需更详细资料请查阅数世咨询相关技术报告）：

| | | |
|---|---|---|
| 跨域调度与管理 | 一体化策略管理 | 简释：全域链路资源分配、网络安全策略、数据安全策略的一致性 |
| | | 实现：通过对全域网络、安全、数据资源的集中管理调度，策略配置下发实现集中管理和监控 |
| | 网络资源编排 | 简释：通过预定义策略自动管理和配置网络资源，实现节点设备的快速部署和优化 |
| | | 实现：网络策略规划、资源调度规划 |
| | 安全策略编排 | 简释：基于总体安全策略对各节点实施安全策略的动态的配置与管控 |
| | | 实现：安全策略规划、策略自动化下发与配置 |
| | 检测与响应 | 简释：基于全域的安全数据，实现安全事件研判和快速响应 |
| | | 实现：大数据分析、基于 AI 的威胁分析，自动化响应 |
| 安全即服务 | 安全能力云化 | 简释：安全能力实现可订阅，服务能够动态扩展 |
| | | 实现：将安全能力以虚拟化安全资源池或者云原生安全资源池的模式部署，实现安全能力的弹性扩展 |
| | WEB 访问保 | 简释：识别应用层的恶意代码和安全风险 |

| | | |
|---|---|---|
| | 护 | 实现：恶意软件扫描、恶意网站和不良内容的检测（通常通过 SWG 类产品实现） |
| | 云安全访问代理 | 简释：确保云计算环境中数据、应用程序和基础设施的安全 |
| | | 实现：数据保护、身份和访问管理合规性审计等（通常通过 CASB 类产品实现） |
| | 安全托管服务 | 简释：识别和预防安全威胁、对处置措施提供指导和协助 |
| | | 实现：通常为一种基于云的远程全天候安全监测和管理的托管式安全服务 |
| 网络即服务 | 链路质量优化 | 简释：流量优化、自动化配置、应用感知、实时监控和分析 |
| | | 实现：利用 QOS 或相关传输优化技术，提高网络灵活性和性能，同时降低成本和复杂性。 |
| | 软件定义网络 | 简释：基于订阅模式的网络服务，允许企业通过云平台按需配置和使用网络资源，而无需自行购买和维护物理网络基础设施 |
| | | 实现：利用软件定义网络（SDN）和网络功能虚拟化（NFV）技术实现，广域网范围一般通过 SD-WAN 实现。 |
| 跨域互联 | 零信任访问 | 简释：基于“永不信任，持续验证”的原则，要求对所有用户、设备和资源访问行为进行持续的身份验证和授权 |

| | | |
|---|---|---|
| | | 实现：基于用户和设备以及访问行为，并综合上下文信息（如位置、时间等）动态调整访问权限。 |
| | 终端安全检测与响应 | 简释：对终端设备自身环境的实时感知和分析，以便更好地保护设备和其上运行的应用程序免受攻击 |
| | | 实现：通过漏洞扫描、病毒查杀、黑白名单、配置检查、进程监控、网络监控、行为分析等技术识别潜在威胁。 |
| | 终端数据安全保护 | 简释：敏感数据安全管控、行为管控、资源访问限制 |
| | | 实现：通过安全沙箱技术实现对数据安全保护，或者限制其对系统资源的访问；通过 DLP 技术保护敏感数据不被泄露 |

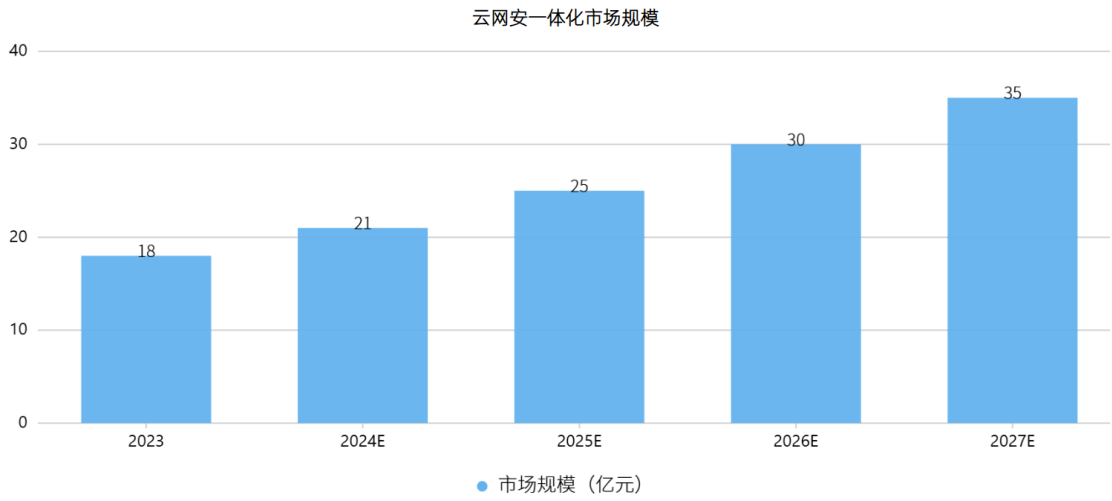
云网安一体化关键技术

# 2.市场情况

本报告的调研选择了 11 家具备云网安一体化方案能力的典型企业进行技术以及市场调研。

## 2.1. 市场规模

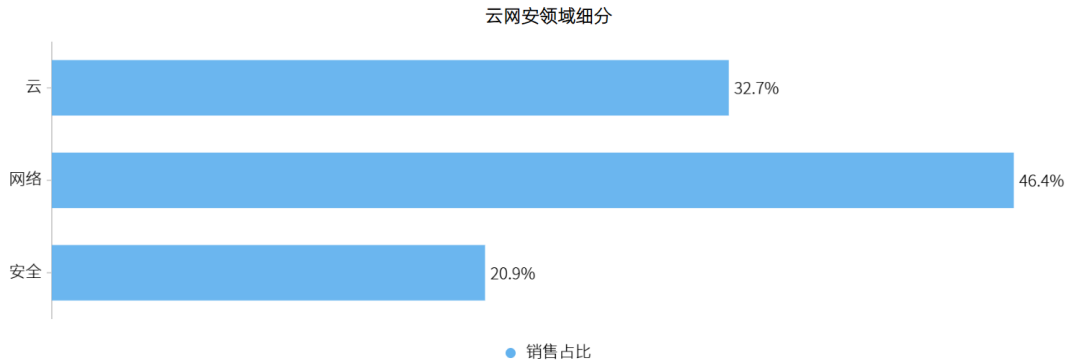
据本次调研统计，2023 年云网安一体化市场规模约 18 亿元。综合行业专家及数世咨询分析师综合分析，到 2027 年市场预估 35 亿元左右。




市场规模

但同时我们也发现，云网安有更大的泛在化市场，即除了方案所需的平台软件、网络组件、客户端软件之外，还包括更多的基础设施以及衍生服务市场，比如网络基础设施、云计算基础设施以及相关的服务，据测算云网安泛在市场 2023 年约有 102 亿规模。其中

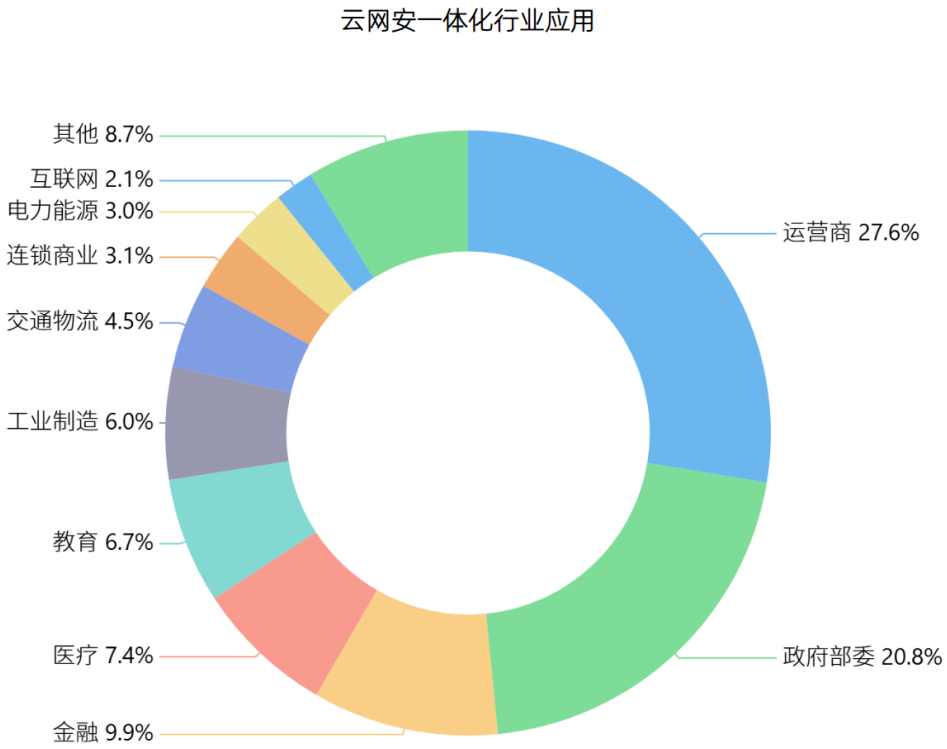
各细分领域的市场占比[3]粗略统计如下：安全及相关服务（占比20.9%），网络产品及相关服务（占比 46.4%），云计算产品及相关服务（占比32.7%）。




云网安各细分领域市场占比

[3] 数据来自参与报告调研的企业 2023 年的市场营收份额统计，数据误差来自样本数量以及部分数据分拆统计的准确性等。

## 2.2. 行业应用




行业应用

重点行业应用：

基于我国国情特点，运营商在推广云网安解决方案时具有显著优势，主要得益于其广泛的网络资源、集成能力、品牌影响力、技术架构和服务能力。运营商拥有遍布全国的网络和专线资源，同时还与国外运营商广泛合作，在边缘云、数据中心云、PoP 站点建设方面有丰富的建设经验。运营商的集成经验使其能够整合不同厂商的网络和安全资源，能够提供全栈、优质的网络和安全服务。运营商既是云网安解决方案的提供者，同时其实也是使用者，占行业应用份额的 27.6%。

政府部委在推动数字中国战略方面积极响应国家政策，着力深化数字中国全面赋能。对于央国企、部委等大型用户，这些用户已经大量应用云基础设施，拥有多种网络线路，并部署了各种安全设备和产品。然而，由于网络安全建设的复杂性，这些用户迫切需要一种一体化管理模式，以简化运营并有效主动地发现安全风险。同时，一体化解决方案，也大大助推政府企业网络安全架构的演进。

对于大型企业集团来说，存在着大量需要整合集团内部信息系统、构建全面安全能力、提升数据治理能力的需求。他们希望能够通过“云、网、端、数”全场景一体化的解决方案，实现为各子系统和子单位安全赋能。而对于中小型的企业，也迫切需要在安全建设和安全管理水平上提升水位，云网安一体化通过网络和安全的订阅服务帮助这些单位提高安全防护水平和降低运营成本。

## 2.3. 场景分析

从场景应用方向来分析,云网安一体化解决方案主要应用于远程办公、数据资源集中访问、多分支管理以及数据跨境传输等场景。

1）远程办公和终端泛在接入

三年的疫情极大地推动了国内远程办公的普及，企业员工的分散化、企业数据资源异地分布，同时还有外包员工、多供应商接入等诸多因素需要考虑。在这种背景下，基于零信任原则的高级安全管控变得至关重要，以确保远程访问和数据安全。国内几年的疫情

尽管给不少企业带来了生存压力，但是也加速了云网安融合的成熟与发展。

2）多云数据访问和数据共享

业务上云已成为各行业的重要发展趋势，企业数据的存储不再局限于单一云平台，而是越来越多地分布在多个云环境中。虽然目前国内云安全需求主要集中在合规监管层面，但数据访问、流通和共享所驱动的安全市场展现出巨大的发展潜力。

3）电子政务互联网管控

电子政务系统对安全性的要求历来严于其他行业，其数据的敏感度也更高。随着监管力度的加大，电子政务领域开始采用基于软件定义边界（SDP）技术，以实现严格的访问控制，确保数据安全。在政务办公领域，近两年的政策强调了统一互联网出口管控的重要性，这对网络与安全的集成管理提出了更高的要求。

4）分支机构或中小企业的安全赋能

大型企业分支机构和国内众多中小企业常常面临专业安全人才短缺以及网络和安全基础设施不足的问题，迫切需要以较低成本提高安全防护水位。云网安一体化服务模式不仅弥补了分支机构和中小企业在技术和人才上的短板，还满足了它们对网络与安全建设的需求。

5）数据跨境传输

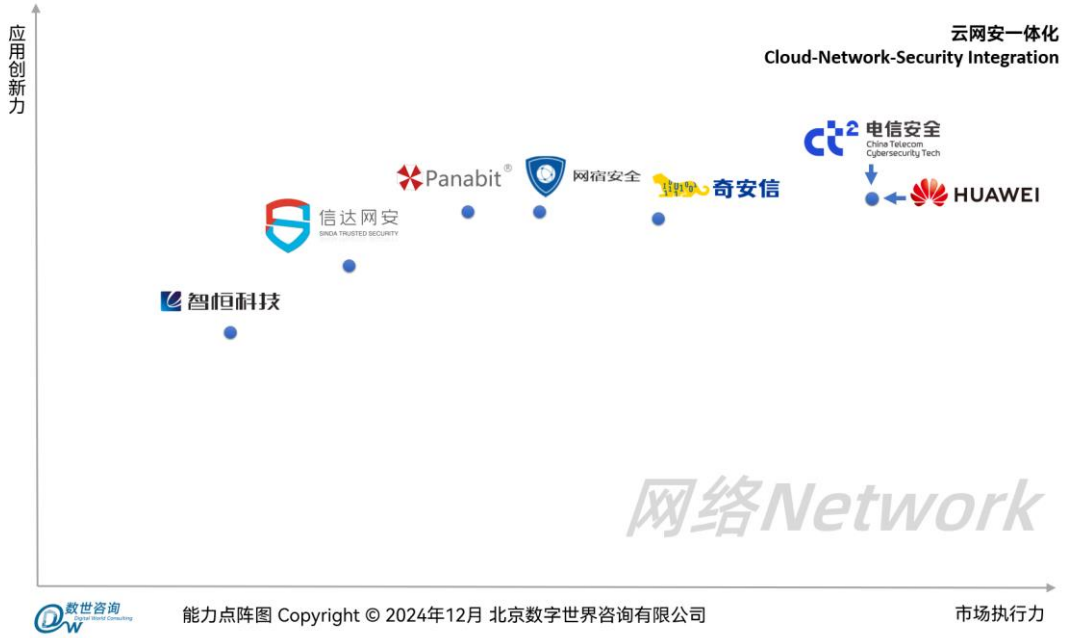
数据出海，作为企业在全球一体化背景下的普遍业务需求，涉及到跨国分支机构间的数据交换以及国际业务合作。这一过程对网络链路的质量和大量数据传输的稳定性提出了高标准，同时必须确保敏感信息的安全，防止数据泄露，并遵守各国的数据合规法规。

# 3.能力企业

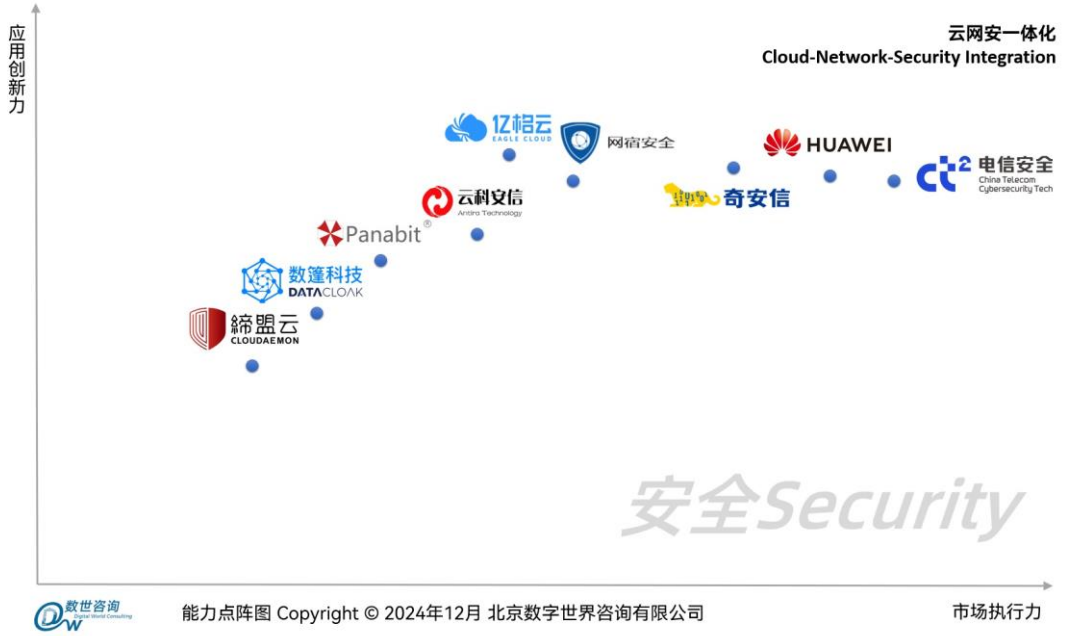
## 3.1. 能力点阵

国内 11 家具备云网安相关解决方案和产品的厂商参与了本次调研，分别是（按公司简称首字母排序）：缔盟云、电信安全、华为、Panabit、奇安信、数篷科技、网宿安全、信达网安、亿格云、云科安信、智恒科技。

尽管大部分被调研都能提供各自的云网安一体化解决方案，但是基于不同的企业技术背景，在网络和安全方面的能力各有侧重。因此本报告基于网络、安全两个方向，按照横轴市场执行力、竖轴应用创新力，通过能力点阵图的方式展现如下：




云网安一体化点阵图<侧重网络能力>




云网安一体化点阵图<侧重安全能力>

## 3.2. 能力侧写

- 能够提供整体解决方案的供应商

国内网络资源主要集中在几家大型电信运营商手中，安全厂商在构建云网安一体化解决方案时，往往需要与这些运营商合作（包括第三方 SD-WAN 供应商）。由于这种合作模式的要求，国内能够提供全面解决方案的厂商相对较少。其中，电信安全是国内为数不多的能够提供整体云网安解决方案的供应商之一。

**电信安全** 依托中国电信强大的云网、安全及数据资源和能力，为各类客户提供全面的安全产品和服务。公司推出的云脉 SASE，面向办公场景提供一体化解决方案，整合了零信任网络访问、终端安全防护、上网行为管理、数据外发管控、网络加速、安全组网以及身份识别与访问管理等多项安全功能，为企业办公提供一站式的全场景安全保障，帮助企业提升安全管理效率和用户体验。

- 侧重网络能力的供应商

侧重提供网络能力的供应商，以华为、Panabit、网宿科技为代表。

**华为** 是运营商基础设施供应商，提供 SASE 管控分析平台、硬件连接设备，同时也有专用的零信任客户端、EDR 和云安全 SaaS 产品。除此以外，还提供私有化 SDN 解决方案，通过 SDN 控制器和因特网链路或本地低成本专线，在企业分支站点 CPE 和 POP 点网关间部署 SD-WAN 隧道，实现跨地域站点之间的低成本高品质互联。

**Panabit** 提供高效、成本适中且安全稳定的类专线业务服务产

品，其产品具备快速灵活的多分支组网能力和精细化的业务 QoS 保障能力。主力产品为七层智能应用网关，集成了负载均衡、流量控制、行为管理、IPv6、威胁情报、SD-WAN 和代播认证等功能。得益于自研的底层协议栈 PanaOS，产品在性能上表现优异。

**网宿安全** 是网宿科技独立子品牌，专注于边缘计算、云分发、云安全等多个领域，借助海量边缘节点资源和边缘防护能力早期布局了 Web 安全、主机安全、DNS 安全。随着零信任技术落地，继而基于零信任、SD-WAN、XDR、XDLP 等技术打造基于零信任的 SASE 办公安全体系。

**信达网安** 提供低成本的 SD-WAN 连接终端，支持多种链路类型的 SD-WAN 组网，支持基于应用的智能路径选择和流量调度等功能。

- 侧重安全能力的供应商

侧重安全能力的供应商除了在安全领域有多年深厚的技术积累的安全大厂（比如奇安信）以外，还有部分专注于单项安全能力的新生代力量，以亿格云、数篷科技为代表。

**奇安信** 无论是研发投入、安全技术积累及市场占有率方面，都体现出网安领域领军者地位，依托 SDN、SDS、SDP 等创新技术，打造了云网安一体化的安全协同防护和安全运营平台，集成云安全资源池的各类安全组件 FWaaS、SWG、DLP、NDR 以及 ZTNA 等，并且与奇安信自有的 SD-WAN 和第三方 SD-WAN 兼容，实现云网安协同的安

全防护。

**亿格云** 通过以零信任为核心的一体化管理平台，提供云原生化的安全服务，其自主研发的 SASE 服务平台--亿格云枢，集成了零信任、数据防泄漏、威胁检测响应、防病毒、上网行为管理和统一端点管理等能力。

**云科安信** 基于风险视角打造全域数字风险管理的整体解决方案，通过云网安一体化方式将全面的服务打造为轻量化的云服务和可私有化部署的标准化云产品。云科安信与多家运营商、CDN 厂商等展开合作。

**数篷科技** 专注于零信任框架下的数据安全领域，其核心解决方案涉及在终端和云环境中部署隔离沙箱（安全空间），以实现数据的精细隔离与严格访问控制。通过一体化管理平台，能够灵活设置不同隔离沙箱的优先级，并通过软件兼容性设计适配多种应用场景。

**缔盟云** 的“太极界”产品提供安全沙箱与零信任网络解决方案。其零信任网络通过强身份验证和动态报文验证确保接入安全，支持 SaaS 及私有化部署，具备弹性与可扩展性。

所调研厂商方案、产品及分析师标签（按厂商名字拼音序）：

| 厂商 | 方案及产品 | 分析师标签 |
| --- | --- | --- |
| 缔盟云 | 太极界（安全桌面） | 零信任安全网关 |

| | | |
|---|---|---|
| | | 基于安全沙箱技术的安全桌面 |
| **电信安全** | **云脉 SASE** | 运营商网络资源<br>一体化的终端安全和数据管控<br>运营商级服务能力 |
| **华为** | **星河 AI 融合 SASE 解决方案** | 领先的广域网优化技术<br>云网边端统一化 SASE 架构<br>云原生安全能力<br>基于图分析的安全客户端 |
| **Panabit** | **Panabit SD-WAN 集中管理控制平台** | 基于应用的智能流量控制<br>多年流量管理技术积累<br>高性能的应用识别和分流技术 |
| **奇安信** | **Q-SASE 安全访问服务一体化管理平台** | 丰富的安全服务化产品能力<br>广域网链路优化技术<br>多业务终端安全能力 |
| **数篷科技** | **DACS 凌域企业安全工作空间** | 基于零信任的数据安全<br>安全沙箱 |
| **网宿安全** | **网宿安全-SASE 办公安全一体化体系** | CDN 网络加速<br>高防 DDOS<br>融合数据安全的终端安全管理<br>零信任远程访问 |
| **信达网安** | **SD-WAN 管理平台** | 低成本的 SD-WAN 连接器<br>基于应用的广域网优化<br>广域网流量优化 |

| | | |
|---|---|---|
| 亿格云 | 亿格云枢 | 零信任访问客户端<br>远程办公、多分支链路安全组网<br>基于公有云 POP 点的多链路接入 |
| 云科安信 | SaaS 化安全产品 | 云 WAF/waap 解决方案 |
| 智恒科技 | SASE 解决方案 | 低成本 SD-WAN 连接器<br>SD-WAN 服务 |

# 4.发展趋势

云网安解决方案有别于传统的通过购买和部署软硬件产品的实现模式，网络、安全能力在云端部署，并通过服务化模式交付。未来的发展趋势更多集中在云、网络及安全防护的一体化、云原生、零信任、兼容性、融合人工智能等方面。

## 向云、网、安一体化方向加速演进

云网安一体化架构越来越依赖于云服务，利用云的全球分布和弹性来提供服务。这意味着云网安一体化越来越依赖云架构，同时与网络、安全紧密融合，以实现资源的最优分配和真正降低安全运营压力。

## 云原生化部署

根据数世咨询 2024 年的报告，2023 年国内云原生安全相关的项目与往年同比增长 50%到 300%不等，显示出云原生安全市场的快速

发展的趋势。云原生安全技术的成熟，将显著提升安全 SaaS 化服务的水平和能力，加速云原生化部署的节奏。

## 更倾向于基于业务的安全防护

随着数字化转型的深入，企业对于安全的需求不再局限于传统的边界防护，而是需要一个能够适应业务变化、动态调整的一体化安全体系。用户将更侧重于从业务系统的视角出发，解决安全问题。

## 人工智能赋能一体化安全管理

毋庸置疑，云网一体化同样需要人工智能技术的深度集成，以实现自动化威胁检测、异常行为识别和安全事件研判等能力。AI 和 ML 将在网络安全防护中扮演更加重要的角色，目前已是普遍共识，不过分强调。

## 标准化和互操作性

数咨询在调研中也了解到，不同厂商的云网安解决方案，产品互相之间多不兼容，对于需要多供应商保障的项目来说，经常需要进行二次开发，这严重产品方案的落地应用。相信将来随着云网安一体化的普及，行业组织和标准机构可能会推动产品方案的标准化，以确保不同厂商的产品和服务能够无缝集成和实现互操作。

# 5.代表厂商优秀案例

## 案例一 某企业零信任网络改造项目--云网安解决方案

（本案例由 电信安全 提供）

### 项目背景

该单位为方便全国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，企业 OA 系统互联网暴露，且存在登录绕过高危漏洞，要求一周内完成安全整改。

在被监管单位通报后，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、便捷接入应用系统；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、全面提升办公应用系统安全管理水平。

### 解决方案

为用户提供解决方案前，我们调研了用户的网络现状，了解到用户办公网内除了传统防火墙外没有其他安全设备；企业在全国有多个分支机构，分支机构所有员工日常均需要访问企业 OA，目前通过互联网访问；员工办公终端系统、类型多样，受限于 IT 人员数量，企业未对全员办公终端开展常态化的基线核查与终端合规准入等管理。

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、监管合规等业务需求，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 小时内高效完成互联网暴露面收敛与应用迁移。

云脉 SASE 上线后，整体基于零信任原则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合规基线、网络位置、用户权限、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。

## 用户价值

### 1）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。

2）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。

3）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。

## 案例总结

1）建立标准的终端合规基线

云脉 SASE 提供终端安全合规基线配置能力，可针对接入终端进行周期性补丁、病毒查杀策略配置；针对接入终端外设、移动存储介质进行合规管理设置；提供软件管控能力，可对用户的终端设备设置合规基线策略，保障终端仅能安装安全可控来源的软件，并提供终端违规软件、盗版软件安装的全局管理可视化界面，为用户提供终端、网络一体化的办公安全管理平台。

### 2）依托运营商资源禀赋提供最便捷的零信任网络接入

相较于传统的硬件 VPN 或 SDP 网关方案，云脉 SASE 依托于运营商优势的云网能力，严格遵照零信任管理理念提供随处可用的零信任安全访问能力（ZTNA）。不限制有用户当前网络，无论用户侧是互联网、专线亦或是 SD-WAN，均能便捷接入云脉 MESH 网络，并通过云脉 SASE 云网基础设施提供的智能选路能力快速连接受控应用资源，保障每一次连接的安全、高效。

### 3）办公内网自适应安全防护能力提升

云脉 SASE 内置持续验证的动态防御策略，提供检查、诊断、分析和阻断能力，可覆盖 ATT&CK 四大攻击过程，九大威胁领域，能够为用户办公终端、网络与核心业务系统建立数字化、智能化的零信任安全防线，最大限度地降低危险用户和主动攻击者的风险。

产品在用户侧运行过程中严格执行零信任原则，为用户提供基于身份的应用访问控制，确保授权用户对指定应用程序的一对一鉴权和授权访问，而不是对网络的完全访问，杜绝应用程序之间或非法/未授权用户在整个网络之间的横向移动，进一步提升用户办公内网在攻防实战视角下的安全自适应防护能力。

# 案例二 某省交通投资集团云网安解决方案

（本案例由 华为 提供）

## 案例背景

某省交通投资集团紧抓数字经济发展先机，全面推进实施《科技赋能三年行动方案（2022—2024 年）》，其中，网络安全就是一个重要业务方向。交通行业关键信息基础设施的自主创新和安全可信，始终关乎着国计民生和公共利益。需要做好重要网络设施、信息系统等基础设施安全防护，保障交通行业迈向安全、稳定、可靠的高质量发展新征程。在建设过程中会面临很多挑战，如：高速公路管理单位多，运维难；路侧、门架海量物联终端接入，风险高；业务统一上云部署，管控难。亟需引入成熟可靠的安全方案帮助集团实现数字化转型。

## 解决方案

根据国家及交通行业标准规范要求，基于省级公路交通业务系统组成架构，华为提出星河 AI 融合 SASE 解决方案，实现从终端、网络、云平台、业务应用到数据的安全防护，提供一体化、可视化、全局化的统一安全运营和全网协同防护。

## 用户价值

### 1）分级分域运营，安全事件秒级处置

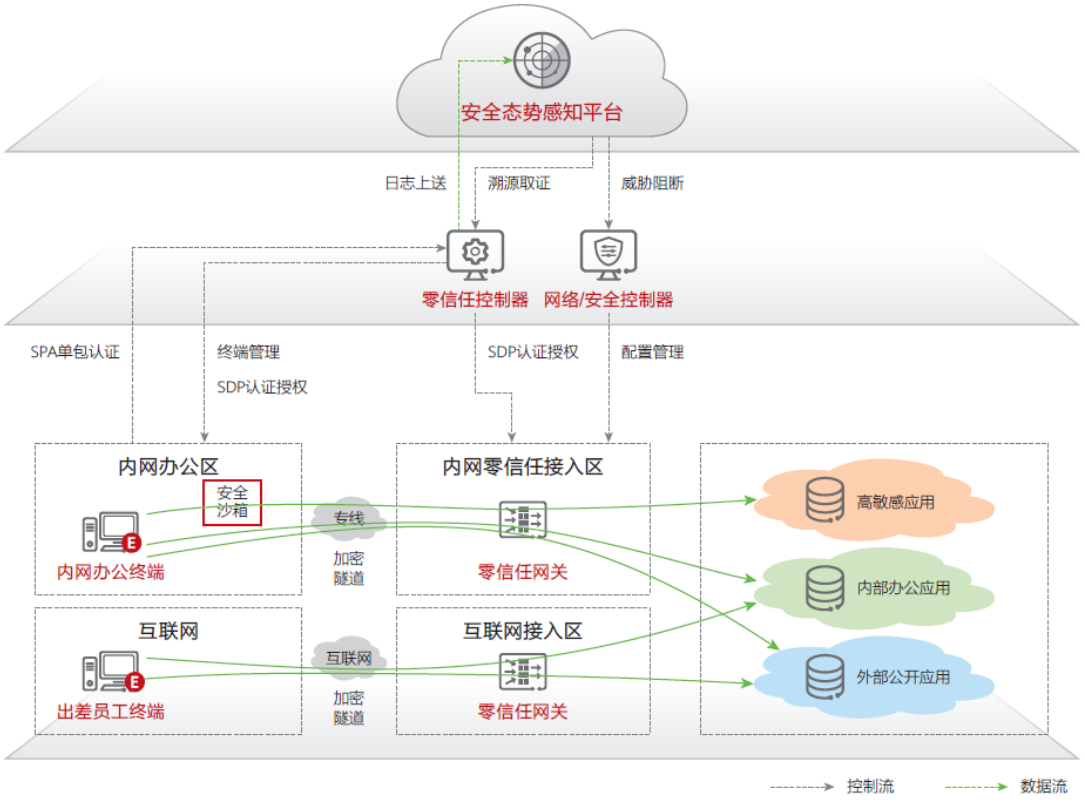
省中心部署 HiSec Insight 态势感知平台，全面收集云、网、

端等安全日志和流量，进行综合分析研判，威胁检出准确率达99%；各区域中心仅需部署流量探针，整体建设成本减少70%。通过在省中心态势感知平台开通二级租户，可实现区域中心分权分域独立运营，满足不同组织架构运营需求。态势感知平台检测到威胁后，可一键联动防火墙、交换机、终端 EDR 近源处置，避免威胁扩散，处置效率从数周提升到分钟级。

**2）资产台账清晰，阻断非法接入**

在路侧、门架、收费站接入侧，通过华为 CloudEngine 交换机内置资产扫描模块实现摄像头、智慧屏等物 联网终端和 PC 终端精准识别，并结合流量探针深度包检测技术，实现终端资产可视、可控、可管，阻断仿冒、私接、劫持等非法终端接入。

**3）零信任体系动态精细化鉴权，避免敏感数据泄露**




根据业务数据敏感度，划分出黄绿蓝不同安全等级区域，财务及干部管理等应用属于安全密级高的黄区，普通办公应用属于安全密级中等的绿区，门户网站等对外公开应用属于安全等级较低的蓝区。交通投资集团通过零信任安全架构建设，实现对用户及终端持续威胁评估、动态授权及细粒度的访问控制，有效缩减业务的“受攻击面”，最大限度减小静态授权、越权访问等带来的数据泄露风险。

## 案例总结

面向未来，交通投资集团将持续携手华为联合创新，基于华为星河 AI 公路云网安一体化安全防护架构，实现资产可视可管，业务访问精细鉴权，安全运营分权分域，建立终端、网络、应用、数据、云的一体化协同防护体系，为交通投资集团智能化转型保驾护航，

也为全国公路安全体系建设提供借鉴与参考。


北京数字世界咨询有限公司（以下简称“数世咨询”）是国内数字化领域独立第三方调研咨询机构，主营业务为网络安全产业领域的调查研究、资源对接与行业咨询。在国内网络安全产业的调查研究领域，无论是专业性还是资源丰富性，均处于业界领先地位。

调查研究方面，撰写发布《中国数字安全大事记》、《中国数字安全能力图谱》、《中国数字安全100强》、《中国数字安全产业年度报告》等业内影响力巨大的公开报告。同时，还为监督机构、国家部委、大型国企等单位提供各种定制化的内部调研报告。

资源对接方面，数世咨询目前已对接国内网络安全企业700余家，以及150余家网络安全投资业务的资本方，建立了频繁且良好的沟通合作关系，包括共同举办会议活动、投资对接，安全产品与企业推荐，企业资源整合等

行业咨询方面，经常性的为监管部门、国家部委、安全企业、安全用户、一二级市场投资机构提供建议、企业培训及专家评审等咨询服务。

公司地址：北京市东城区天鼎218文化金融园东外110号 网安小酒馆
官方网站：www.dwcon.cn
联系邮箱：dw@dwcon.cn

数世咨询
Digital World Consulting
数字安全领域独立第三方调研机构