计算机

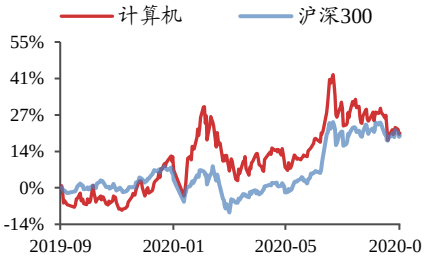
2020 年 09 月 23 日

零信任：网络安全理念的重塑

——行业深度报告

投资评级：看好（维持）

行业走势图



数据来源：贝格数据

相关研究报告

《行业点评报告-阿里“犀牛工厂”正式亮相，工业互联网大风已起》-2020.9.18

《行业点评报告-网络安全行业正在迎来积极变化》-2020.9.3

陈宝健（分析师）
chenbaojian@kysec.cn
证书编号：S0790520080001

刘逍遥（分析师）
liuxiaoyao@kysec.cn
证书编号：S0790520090001

● **零信任大风已起，有望开启百亿市场空间**

零信任作为 IT 无边界化趋势下一种新安全理念，已经成为全球网络安全的关键技术和大趋势。当前海外零信任市场已走向规模化落地，商业模式较为成熟，而国内零信任市场刚刚兴起，腾讯、阿里等互联网巨头及深信服、奇安信、绿盟科技等安全厂商均结合自身业务推出零信任产品和解决方案。长期来看，国内零信任市场规模有望达百亿。推荐在零信任领域有前瞻布局的深信服、奇安信、安恒信息、启明星辰，建议关注绿盟科技、南洋股份、美亚柏科、山石网科。

● **零信任：IT 无边界化趋势下的安全理念变革**

IT 无边界化大势所趋，高级网络攻击肆虐，内外部威胁愈演愈烈，在此背景下传统的边界安全体系需要迭代升级，零信任理念应运而生。与传统边界模型的“信任但验证”不同，零信任的核心原则是“从不信任、始终验证”。目前零信任架构建设已形成三大主要技术路径：软件定义边界（SDP）、身份识别与访问管理（IAM）、微隔离（MSG），在业内被广泛认知与应用。

● **海外市场：零信任已走向规模化落地，商业模式较为成熟**

1）市场认知度较高，已步入快速向零信任架构转型阶段。根据 Gartner 预测，2022 年将有 80%面向生态合作伙伴的新数字业务应用采用零信任网络访问。2023 年将有 60%的企业从远程访问 VPN 向零信任网络架构转型。2）市场参与者众多，实现路径各有差异。既有谷歌、微软等率先在企业内部实践零信任并推出完整解决方案的业界巨头，有“以身份为中心的零信任方案”的 Duo、OKTA、Centrify、Ping Identity，也有偏重于网络实施方式的零信任方案的 Cisco、Akamai、Symantec、VMware、F5 等。3）商业模式较为成熟，SECaaS 为主流交付模式。

● **国内市场：产品与解决方案快速涌现，重在探究与原有业务的结合**

1）随着“攻防演练”的常态化推进及更多企业的参与，减少暴露面及核心资产隐藏的急迫需求，已经使零信任架构成为“攻防演练”取得高分的利器之一。同时，零信任安全也引起了国家相关部门和业界的高度重视。2）以腾讯、阿里云为代表的互联网巨头及深信服、奇安信、绿盟科技等安全厂商均结合自身业务推出零信任产品和解决方案，并已逐步在中央部委、国家机关、中大型企业实践落地。3）从交付模式来看，考虑国内信息化发展水平及对安全的重视程度，短期内仍以解决方案为主，长期有望向 SECaaS 模式转变；4）零信任市场已经踏上高速发展的起点，根据我们粗略测算，到 2024 年国内零信任市场规模有望达百亿人民币。

● **风险提示：**疫情影响全年业绩风险；市场竞争加剧风险；人才流失风险。

目 录

1、 零信任是安全建设思路的转变 4
1.1、 零信任诞生的背景：IT 无边界化 4
1.2、 零信任的核心原则：从不信任、始终验证 4
1.3、 实现零信任的三大技术路径：SDP、IAM、MSG 5
1.4、 零信任体系架构典型场景：远程办公、大数据中心、云安全平台 8
2、 海外零信任已走向规模化落地，商业模式较为成熟 10
2.1、 海外零信任市场参与者众多，实现路径各有差异 11
2.1.1、 谷歌 BeyongCorp：企业零信任体系建设的标杆 11
2.1.2、 Illumio：利用微隔离技术实现零信任防护 12
2.1.3、 Okta：领先的第三方企业身份管理平台 13
2.2、 SECaaS 成为海外零信任市场主流交付模式 15
3、 国内零信任市场仍处于探索阶段，有望实现高速增长 16
3.1、 国内零信任产品开始涌现，重在探究与原有业务的结合 17
3.1.1、 腾讯：国内最早落地零信任安全架构的探索者之一 17
3.1.2、 阿里云：全资收购九州云腾，构建云上零信任体系 18
3.1.3、 深信服：推出精益信任 aTrust 安全架构，获得用户认可 19
3.1.4、 奇安信：零信任解决方案已经在部委、央企、金融等行业进行广泛落地实施 20
3.1.5、 绿盟科技：拥抱零信任理念，重构安全体系架构 21
3.1.6、 启明星辰：已推出启明星辰零信任管控平台 21
3.1.7、 芯盾时代：引领零信任安全风向的创新型企业 22
3.2、 国内零信任交付模式仍以解决方案为主，长期有望向 SECaaS 转变 23
3.3、 长期来看，国内零信任市场规模有望达百亿 23
4、 投资建议 24
5、 风险提示 25

图表目录

图 1： 传统边界安全架构无法适应当前业务体系 4
图 2： 零信任安全理念在国外逐渐被广泛认知 4
图 3： 零信任逻辑组件基本关系及其相互作用 5
图 4： 软件定义边界（SDP）模型包括三大组件 6
图 5： IAM 涉及四个领域的内容：IGA、AM、PAM 及认证权鉴 7
图 6： 零信任建设对 IAM 的需求 7
图 7： 微隔离技术重点用于阻止攻击者进入企业数据中心网络内部后的横向平移 8
图 8： MFA 和 SSO 技术是目前零信任实施过程中最常用到的技术手段 8
图 9： 微隔离和 SDP 或将成为未来几年最受欢迎的技术 8
图 10： 基于零信任架构的远程办公安全参考架构 9
图 11： 基于零信任架构的大数据中心安全参考架构 9
图 12： 基于零信任架构的云计算平台安全参考架构 10
图 13： 零信任的采用才刚刚起步，但是其重要性已被多数企业认知 10
图 14： 2023 年预计将有 60%的企业从远程访问 VPN 向零信任网络架构转型 11
图 15： 海外零信任市场参与者众多 11
图 16： Google 的 BeyondCorp 取代 VPN 提供安全远程访问 12

图 17: BeyondCorp 组件和访问流程 12
图 18: Illumio 的核心产品就是其自适应安全平台 13
图 19: Illumio Edge 主要通过三个步骤来阻隔不必要的网络通信 13
图 20: Okta 在 Gartner 定义的 AM 魔力象限中地位领先 14
图 21: Okta 在 Forrester 定义的 IDaaS 象限中居领导者地位 14
图 22: Okta 拥有完整的身份认证管理平台 14
图 23: Okta Identity Cloud 用户覆盖广泛 15
图 24: CSA 将 SECaaS 细分为十个子集类别 15
图 25: 腾讯 iOA 打造零信任最佳实践 17
图 26: T-Sec SDP “三唯”访问控制，护航移动办公全场景安全 18
图 27: 九州云腾产品分为生成令牌 IPG 和解析令牌 SPG 两大系列 19
图 28: 深信服精益信任 aTrust 安全架构在零信任的基础上做了增强 19
图 29: 奇安信零信任解决方案整体架构 20
图 30: 奇安信零信任安全解决方案已在某头部客户的大数据中心部署 20
图 31: 绿盟发布零信任安全解决方案 21
图 32: 绿盟零信任解决方案通过增加零信任安全组件以实现零信任网络访问控制 21
图 33: 启明星辰零信任安全体系以“四横三纵”为主要逻辑框架 22
图 34: 芯盾时代拥有四大产品系列 22
图 35: 芯盾时代已五次入选 Gartner 报告 23
图 36: 缔盟云已开始尝试 SECaaS 的交付模式 23
图 37: 全球零信任安全市场规模预计到 2024 年将达 386 亿美元 24

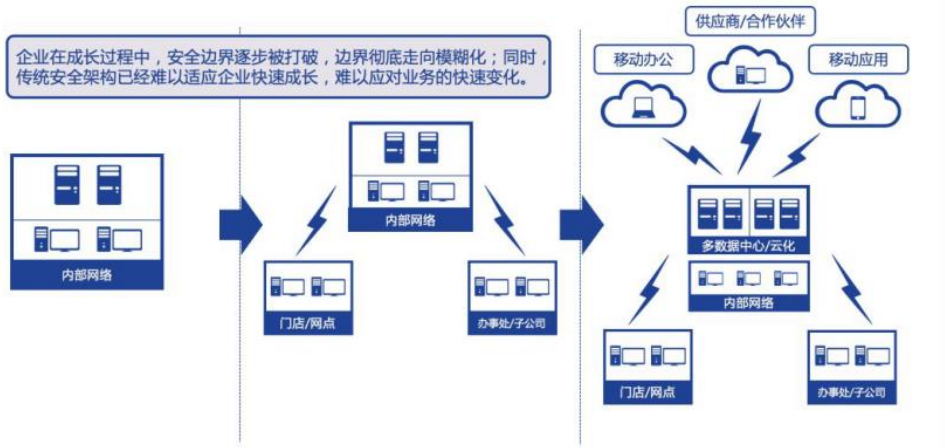
表 1: 区别于传统安全架构，零信任的核心原则是“从不信任、始终验证” 5
表 2: SECaaS 成为零信任主流的交付模式 16
表 3: 中性假设下，到 2024 年国内零信任市场规模有望达百亿人民币 24
表 4: 推荐深信服、奇安信、安恒信息、启明星辰，建议关注绿盟科技、南洋股份、美亚柏科、山石网科（截止 2020.9.23 收盘） 24

1、 零信任是安全建设思路的转变

1.1、 零信任诞生的背景：IT 无边界化

在传统的安全体系下，内网用户默认享有较高的网络权限，而外网用户如异地办公员工、分支机构接入企业内网都需要通过 VPN。不可否认传统的网络安全架构在过去发挥了积极的作用，但是在 IT 无边界化已经成为大趋势，高级网络攻击肆虐，内外部威胁愈演愈烈的环境下，传统的边界安全体系需要迭代升级，零信任理念应运而生。

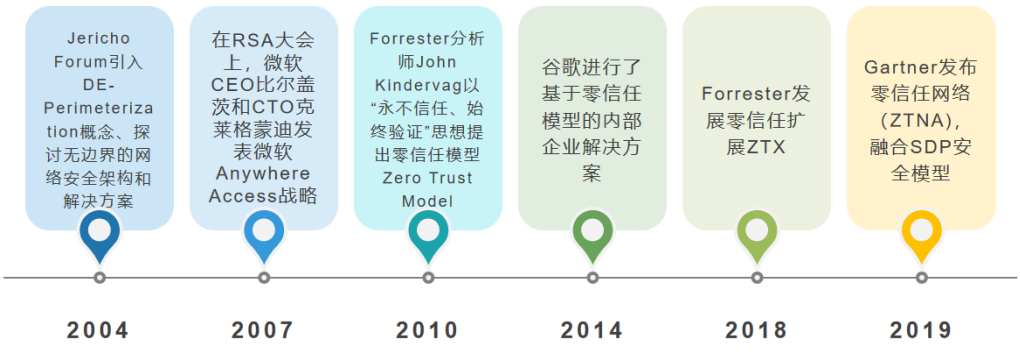
图1：传统边界安全架构无法适应当前业务体系



资料来源：深信服

零信任的最早源自 2004 年成立的耶利哥论坛（Jericho Forum），其成立的使命是为了定义无边界趋势下的网络安全问题并寻求解决方案。2010 年约翰·金德维格（John Kindervag）首次提出了零信任安全的概念，其核心思想是企业不应自动信任内部或外部的任何人/事/物，应在授权前对任何试图接入企业系统的人/事/物进行验证。历经十年发展，零信任安全理念在国外逐渐被广泛认知。

图2：零信任安全理念在国外逐渐被广泛认知



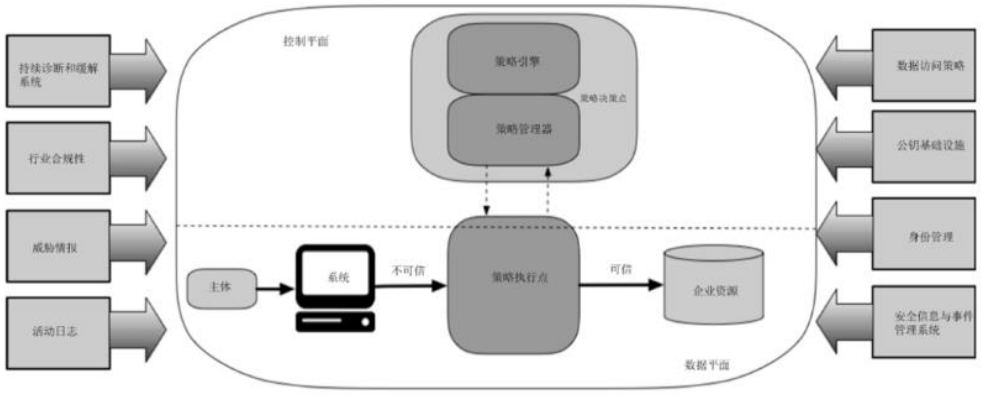
资料来源：云安全联盟 CSA、开源证券研究所

1.2、 零信任的核心原则：从不信任、始终验证

根据 NIST 的定义，零信任（Zero trust）提供了一系列概念和思想，旨在面对被

视为受损的网络时，减少在信息系统和服务中执行准确的、权限最小的按请求访问决策时的不确定性。零信任架构（ZTA）是一种企业网络安全规划，它利用零信任概念，并囊括其组件关系、工作流规划与访问策略。因此，零信任企业作为零信任架构规划的产物，是指为企业准备的（物理和虚拟的）网络基础设施及操作策略。

图3：零信任逻辑组件基本关系及其相互作用



资料来源：NIST

与边界模型的“信任但验证”不同，零信任的核心原则是“从不信任、始终验证”。传统上机构（及一般企业网络）都专注于边界防御，授权主体可广泛访问内网资源。而根据 Evan Gilman《Zero Trust Networks》书中所述，零信任网络建立在五个假设前提之下：1）应该始终假设网络充满威胁；2）外部和内部威胁每时每刻都充斥着网络；3）不能仅仅依靠网络位置来确认信任关系；4）所有设备、用户、网络流量都应该被认证和授权；5）访问控制策略应该动态地基于尽量多的数据源进行计算和评估。

表1：区别于传统安全架构，零信任的核心原则是“从不信任、始终验证”

	传统安全架构	零信任安全架构
防护对象	以“网络”为中心的防护	以“数据”为中心的防护
	“攻防对抗”为主	关注“应用/资源”
防护基础	基于“边界”的防护	“无边界”防护
	以“信任”为基础	默认“不信任”，最小权限
防护理念	一次认证、静态策略	持续评估、动态访问控制
	被动、静态地防御	主动、自动化防御

资料来源：绿盟科技、开源证券研究所

1.3、 实现零信任的三大技术路径：SDP、IAM、MSG

零信任是一种理念，而不是一种技术。因此，没有单一的产品或解决方案能够使企业独自实现零信任。但是，业内普遍认为软件定义边界（SDP）、身份识别与访问管理（IAM）、微隔离（MSG）是实现零信任的三大技术路径。

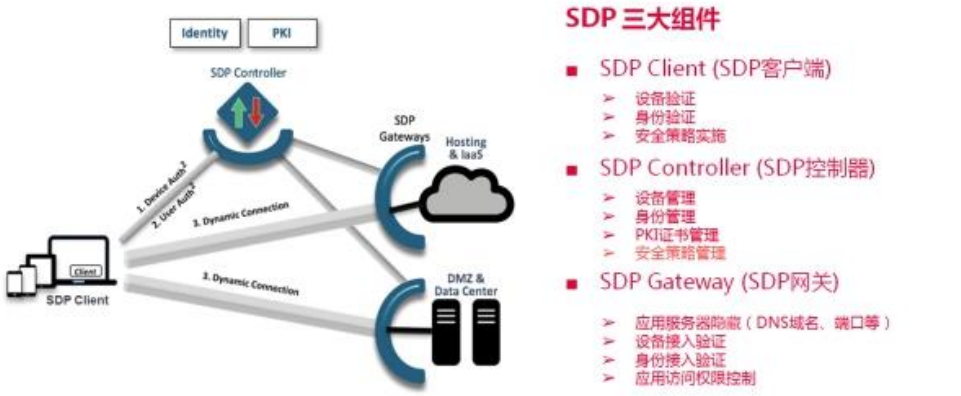
- **软件定义边界（SDP）**

软件定义边界（SDP）由云安全联盟（CSA）于 2013 年提出，用应用管理者可控的逻辑组件取代了物理设备，只有在设备证实和身份认证之后，SDP 才提供对认

证基础设施的访问，SDP 使得应用所有者部署的边界可以保持传统模型中对于外部用户的不可见性和不可访问性，该边界可以部署在可以访问的任意位置，如网络上，云中，托管中心中，私有企业网络上，或者同时部署在这些位置。

SDP 改变了传统的网站连接方式。在传统的连接中，首先，客户端需要建立与服务器端的连接，这一步骤使服务端暴露在公网中，若服务端有漏洞，则有可能被利用；其次，用户通过登录页面输入用户名和密码，这一步骤有可能使得用户名和密码被窃取；最后，除用户名和密码外还可使用多因素认证，通过多因素认证，可以抵抗用户名和密码的丢失，但是多因素认证对于用户而言不是很友好。而在 SDP 中，首先，客户端进行多因素认证，认证设备的可靠性等，这一步对用户而言是透明的。认证通过之后，才进入用户登录阶段。这两步均是客户端与 Controller 进行交互，不涉及对于具体服务的访问。当认证通过后，客户端才能够与可访问的服务建立连接。

图4：软件定义边界（SDP）模型包括三大组件



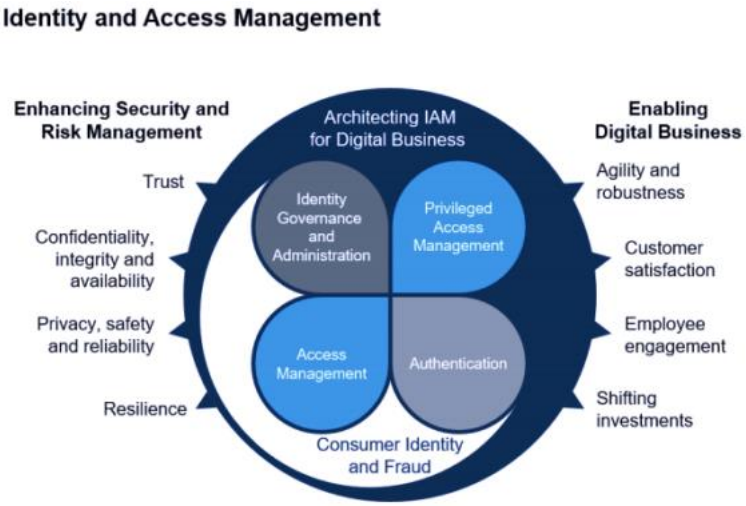
资料来源：CSA、关注网

- **身份识别与访问管理（IAM）**

身份识别与访问管理（IAM）具有单点登录、认证管理、基于策略的集中式授权以及审计、动态授权等功能。它决定了谁可以访问，如何进行访问，访问后可以执行哪些操作等。

IAM 涉及四个领域的内容：包括身份治理与管理 IGA、访问管理 AM、特权访问管理 PAM 及认证权鉴。1）身份治理与管理 IGA 用于跨企业不同应用和系统上提供统一的用户的数字身份认证及访问控制权限的管理，涉及到的关键能力包括数字身份的生命周期管理、权限管理、角色和组织架构管理、访问控制请求、交互流程的处理、日志审计和分析报告。2）访问管理 AM，由访问控制引擎来实现业务的访问控制，包括统一集中认证、单点登录、会话管理和授权的策略的执行。3）特权访问管理 PAM 保障特权人员对关键资产设备的安全管理，国内一般叫堡垒机、4A。4）认证权鉴包含支持的认证凭证及支持的认证方式，如静态口令、Token、生物特征的验证方式。

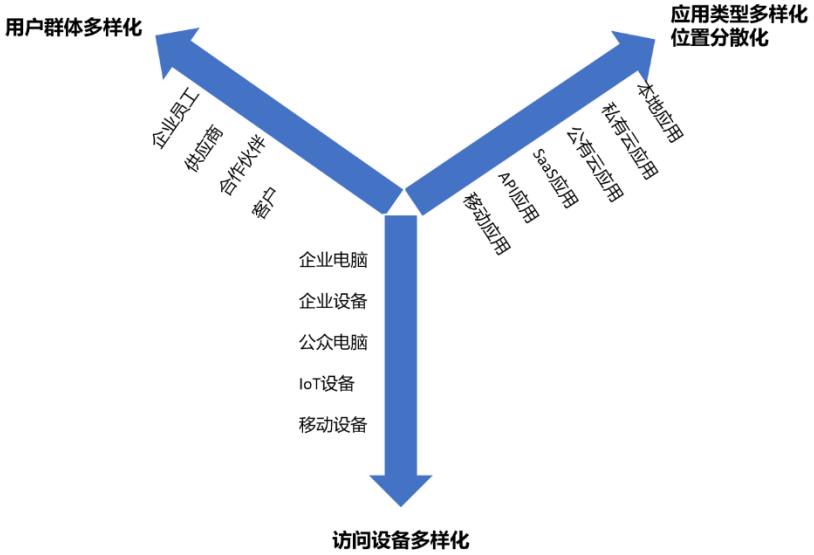
图5：IAM 涉及四个领域的内容：IGA、AM、PAM 及认证权鉴



资料来源：Gartner

作为零信任体系的基础组件 IAM，需要同步考量业务需求和 IT 环境变化带来的新挑战，如满足更多用户群体在访问企业资源过程中的安全性和便捷性，以及满足访问方式的多样化，接入资源多样化和分散化。

图6：零信任建设对 IAM 的需求

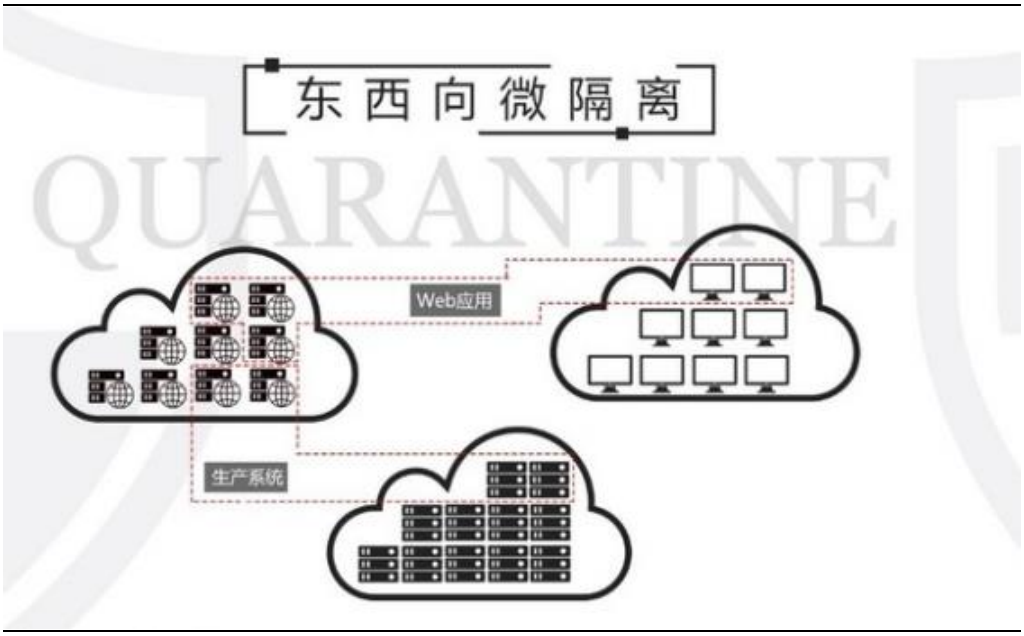


资料来源：绿盟科技、开源证券研究所

- **微隔离技术**

微隔离是细粒度更小的网络隔离技术，能够应对传统环境、虚拟化环境、混合云环境、容器环境下对于东西向流量隔离的需求，重点用于阻止攻击者进入企业数据中心网络内部后的横向平移。

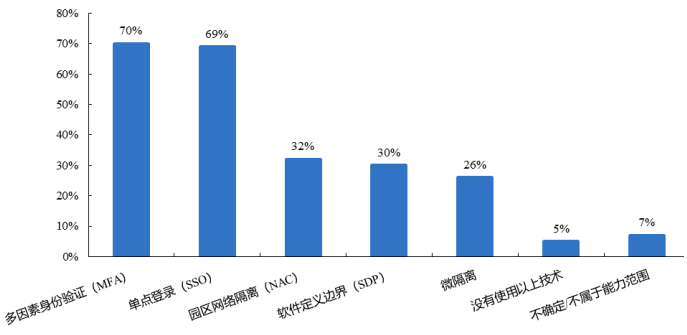
图7：微隔离技术重点用于阻止攻击者进入企业数据中心网络内部后的横向平移



资料来源：FreeBuf

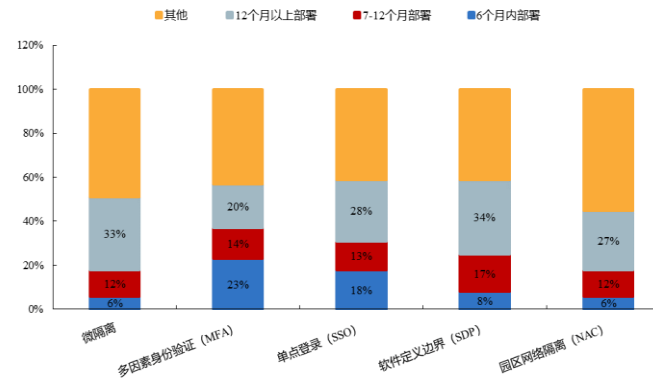
MFA 和 SSO 技术是目前零信任实施过程中最常用到的技术手段，而微隔离和 SDP 或将成为未来几年最受欢迎的技术。根据 Illumio 数据统计，目前多因素身份验证（MFA）在使用它的受访者中占 70%，位居榜首。紧随其后的是单点登录（SSO），达到 69%。超过一半的受访者计划从下一年开始总体部署微隔离，通过阻止横向移动来防止重大破坏。在大型组织中，拥有 2,500-5,000 名员工的组织中有 70%和超过 5,000 名员工的组织中 61%都有微隔离部署计划。

图8：MFA 和 SSO 技术是目前零信任实施过程中最常用到的技术手段



数据来源：Illumio、开源证券研究所

图9：微隔离和 SDP 或将成为未来几年最受欢迎的技术



数据来源：Illumio、开源证券研究所

1.4、零信任体系架构典型场景：远程办公、大数据中心、云安全平台

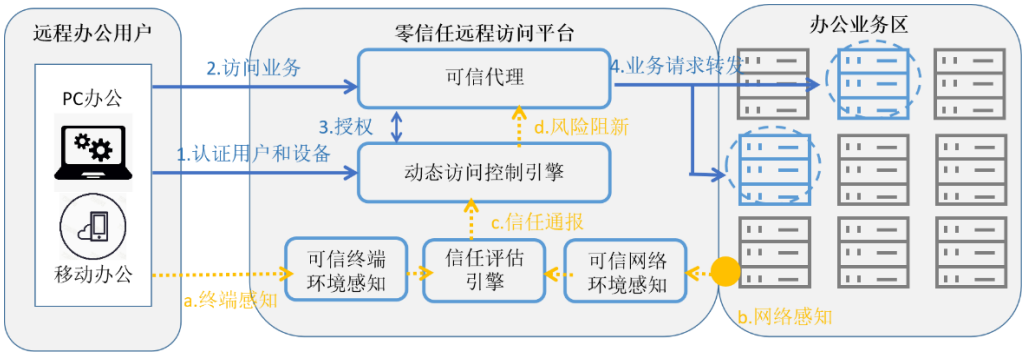
任何企业网络都可基于零信任原则进行设计。大多数组织的企业基础架构已经具备了零信任的某些要素，或者正在通过实施信息安全、弹性策略和最佳实践来实现零信任。目前比较典型的应用场景包括：远程办公、大数据中心、云安全平台等。

- **远程办公**

在疫情的催化下，远程办公逐渐成为一种常态化的办公模式。常见的远程接入

方式主要有两种：一种是通过端口映射将业务系统直接在公网上开放；二是使用 VPN 打通远程网络通道。然而这些手段基本上可以视为边界安全方案的单点增强，难以系统性环节远程办公带来的安全威胁。零信任安全架构针对远程办公场景，不再采用持续强化边界思维，不区分内外网，针对核心业务和数据资产，梳理访问这些资产的各种访问路径和场景，在人员、设备和业务之间构建一张虚拟的基于身份的边界，针对各种场景构建一体化的零信任动态访问控制体系。

图10：基于零信任架构的远程办公安全参考架构

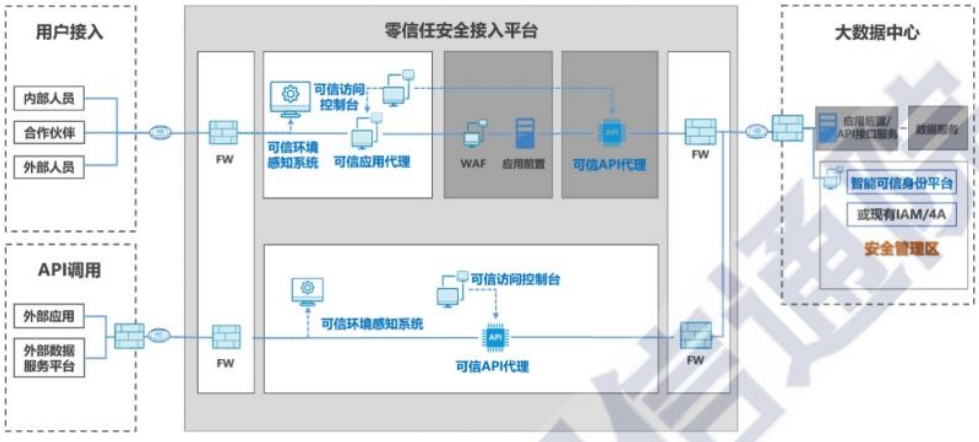


资料来源：中国信通院、开源证券研究所

- **大数据中心**

目前大数据中心访问中东西向流量大幅度增加，而传统的安全产品基本都是南北向业务模型基础上进行研发设计的，在大数据中心内部部署使用时，出现诸如部署困难、运算开销太大，策略管理不灵活的问题。零信任架构通过微隔离等技术，实现环境隔离、域间隔离、端到端隔离，根据环境变化自动调整策略。

图11：基于零信任架构的大数据中心安全参考架构



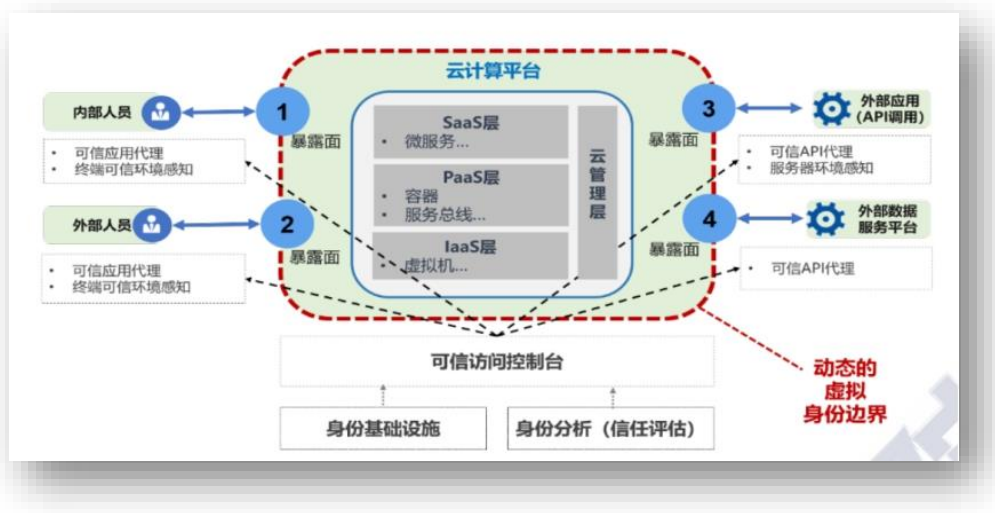
资料来源：中国信通院

- **云安全平台**

网络安全形势日益严峻，企业内部使用微服务、容器编排和云计算资源池等技术架构导致云计算环境越来越复杂。企业可通过梳理云平台内部资源，建立微隔离机制，实现零信任安全架构。在通过分析内部人员的访问路径、外部人员访问通道、外部应用调用、外部数据服务平台对接通道等确定其暴露面以后，可部署相应访问代理，在可信访问控制台的控制下，基于微服务管理平台等建立动态的虚拟身份边

界，并通过计算身份感知等安全信息分析平台数据，建立最小访问权限动态访问控制体系。

图12：基于零信任架构的云计算平台安全参考架构

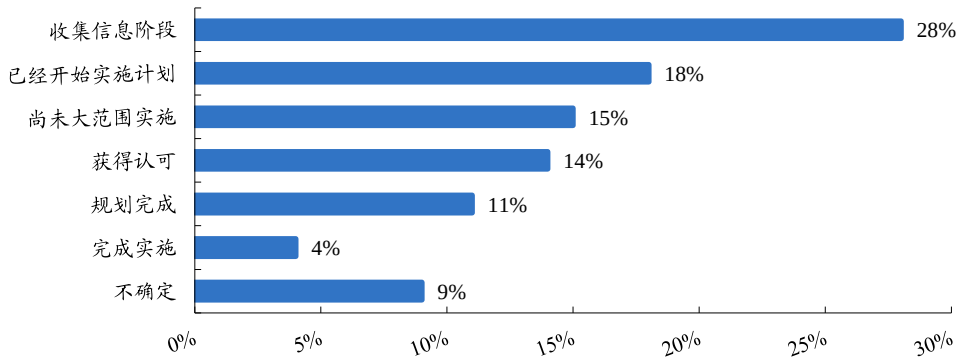


资料来源：中国信通院

2、 海外零信任已走向规模化落地，商业模式较为成熟

零信任的重要性已被多数企业认知。根据咨询公司 Illumio 的最新企业调查，仅 4％的人声称完全实施了零信任，但接近半数的企业已处于调研或试点阶段。

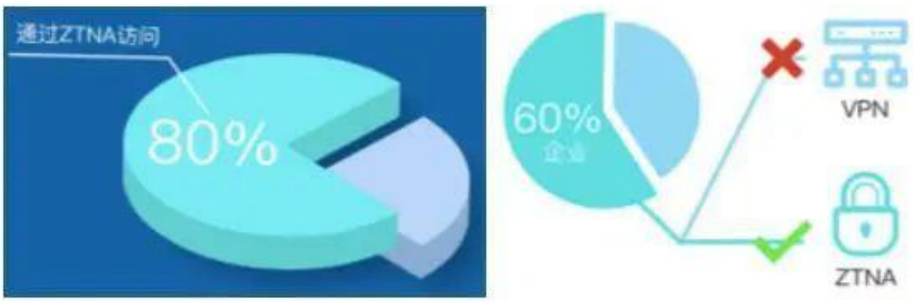
图13：零信任的采用才刚刚起步，但是其重要性已被多数企业认知



数据来源：Illumio、开源证券研究所

根据 Gartner 预测，2022 年将有 80%面向生态合作伙伴的新数字业务应用采用零信任网络访问。2023 年将有 60%的企业从远程访问 VPN 向零信任网络架构转型。

图14：2023 年预计将有 60%的企业从远程访问 VPN 向零信任网络架构转型

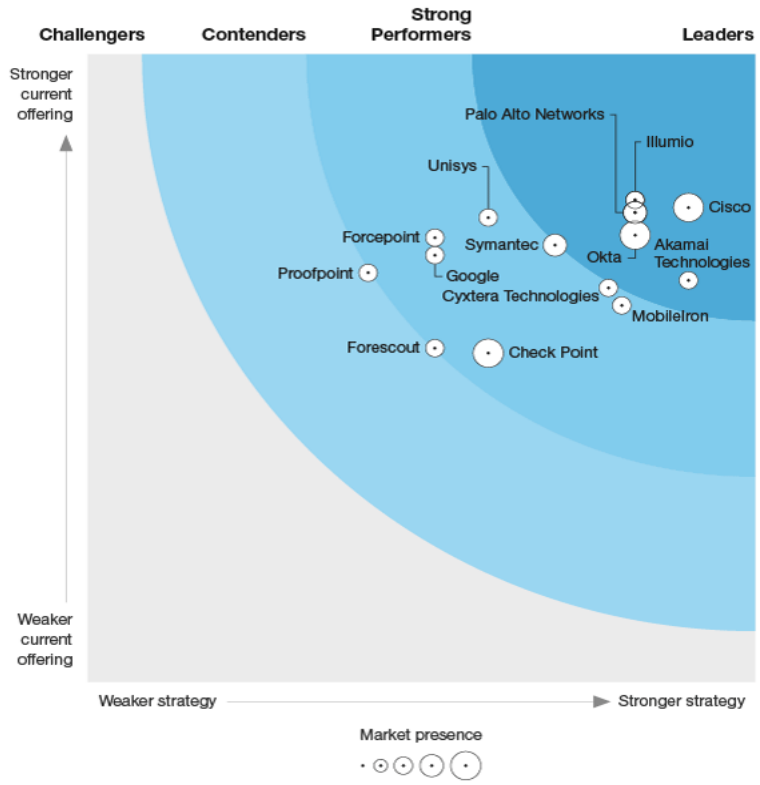


资料来源：Gartner

2.1、 海外零信任市场参与者众多，实现路径各有差异

海外零信任市场参与者较多。其中：1）谷歌、微软等业界巨头率先在企业内部实践零信任并推出完整解决方案；2）Duo、OKTA、Centrify、Ping Identity 推出“以身份为中心的零信任方案”；3）Cisco、Akamai、Symantec、VMware、F5 推出了偏重于网络实施方式的零信任方案；4）此外，还包括 Vidder、Cryptzone、Zsclar、Illumio 等初创公司。

图15：海外零信任市场参与者众多



资料来源：Forrester

2.1.1、 谷歌 BeyongCorp：企业零信任体系建设的标杆

谷歌的 BeyongCorp 是较早落地的零信任项目。从 2014 年 12 月起，谷歌共在

《login:》杂志上发表了 6 篇 BeyondCorp 相关的论文，全面介绍 BeyondCorp 的架构和谷歌从 2011 年至今的实施情况。2017 年，Google 对外宣布其基于零信任架构实践的新一代企业网络安全架构——BeyondCorp 项目成功完成，为零信任在大型、新型企业网络的实践提供了参考架构。2020 年谷歌宣布完成其内部使用的远程安全访问零信任方案 BeyondCorp 的产品化，并在谷歌云服务上发布销售，每个用户的月订阅费用是 6 美元。并且，无需成为谷歌现有云服务或企业协同工具的用户也可使用该服务。

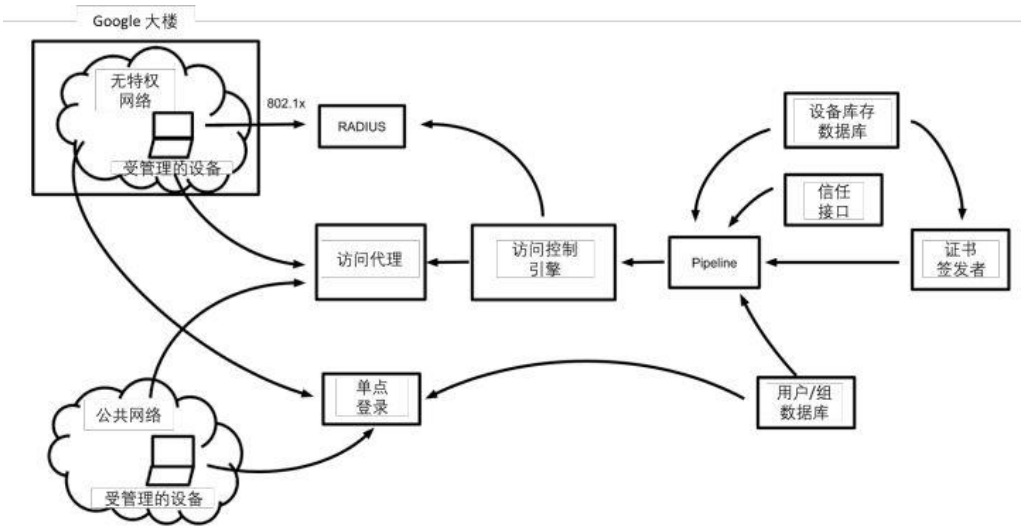
图16：Google 的 BeyondCorp 取代 VPN 提供安全远程访问



资料来源：BeyondCorp

BeyondCorp 实现的核心是引入或扩展网络组件，例如单点登录，访问代理，访问控制引擎，用户清单，设备清单，安全策略和信任库。这些组件协同工作，以维护三个指导原则：1）特定的网络连接不得确定用户可以访问哪些服务；2）根据对用户和设备的了解来授予对服务的访问权限；3）所有对服务的访问都必须经过认证，授权和加密。

图17：BeyondCorp 组件和访问流程



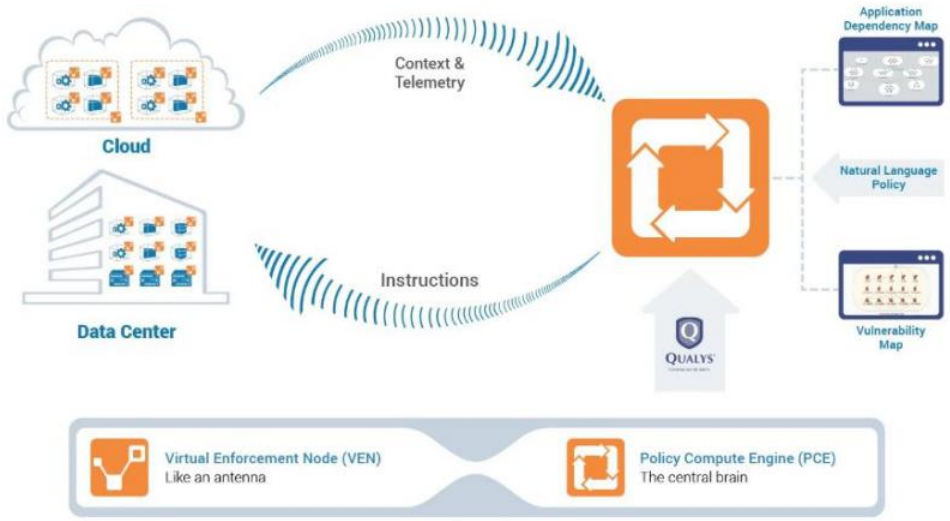
资料来源：BeyondCorp

2.1.2、Illumio：利用微隔离技术实现零信任防护

Illumio 是领先的微隔离厂商，通过构建独特的自适应安全架构，可自内而外地安全监控和防护每个工作单元或应用。公司主要利用自适应微隔离技术（adaptive

micro-segmentation）防止泄露在数据中心和云中扩散。Illumio 的核心产品就是其自适应安全平台，可帮助企业分隔网络和用户。该平台含有一个策略计算引擎，作为设置网络和用户最佳实践及安全策略的主控节点。此外，还有嵌入工作负载里的虚拟执行节点，确保工作负载遵从 PCE 定义和管理的策略。Illumio 拥有 100 多名订阅客户，包括摩根士丹利、Salesforce 和 Workday 等。

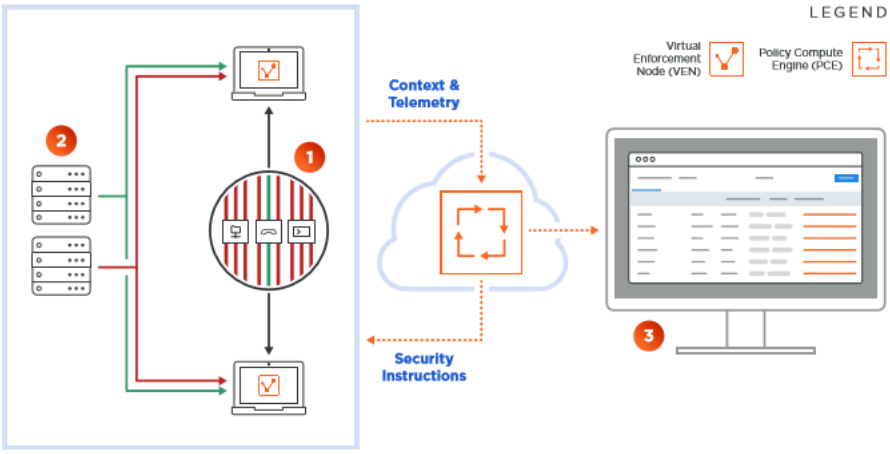
图18：Illumio 的核心产品就是其自适应安全平台



资料来源：Illumio

Illumio Edge 主要通过三个步骤来阻隔不必要的网络通信：1）定义授权的服务；2）对自定义应用程序进行微调；3）在测试模式下运行以确保策略正确，然后执行并监视流量。

图19：Illumio Edge 主要通过三个步骤来阻隔不必要的网络通信

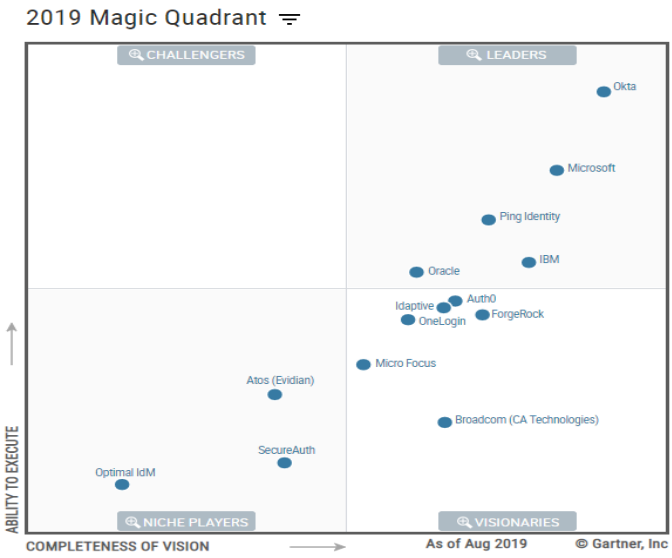


资料来源：Illumio

2.1.3、Okta：领先的第三方企业身份管理平台

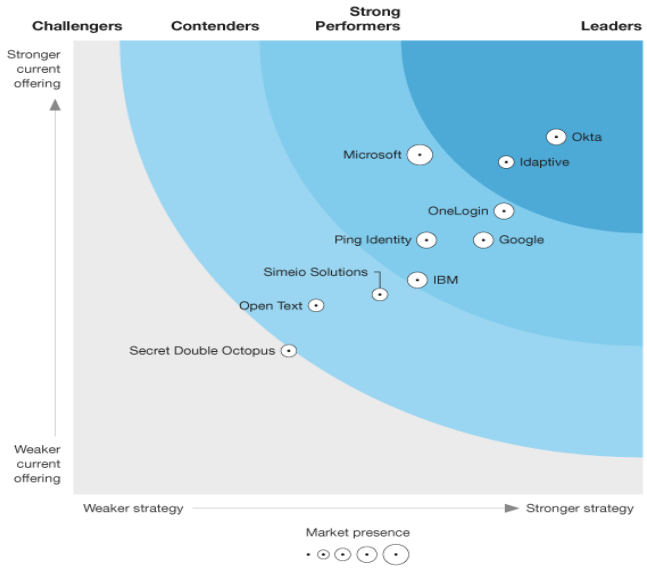
Okta 成立于 2009 年，是全球领先的身份认证与访问管理厂商。无论是在 Gartner 定义的访问管理（AM）魔力象限，还是在 Forrester 定义的身份认证即服务（IDaaS）象限中，Okta 均处于市场领导者地位。

图20：Okta 在 Gartner 定义的 AM 魔力象限中地位领先



资料来源：Gartner

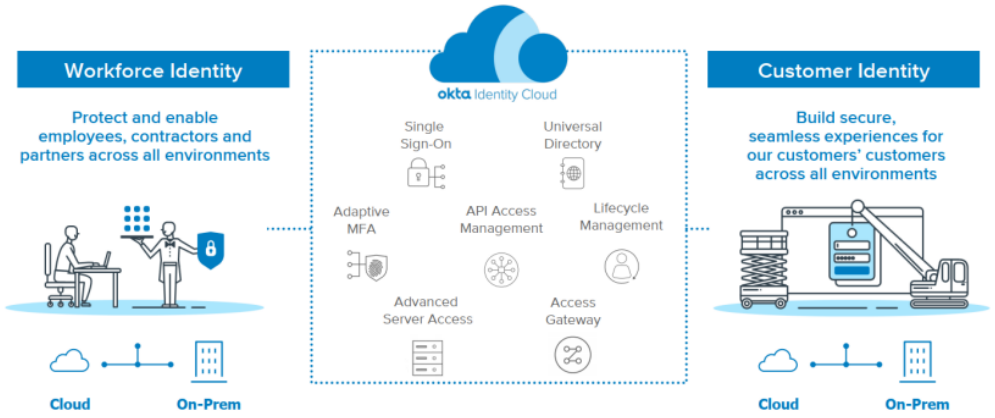
图21：Okta 在 Forrester 定义的 IDaaS 象限中居领导者地位



资料来源：Forrester

按照面向对象不同，Okta Identity Cloud 分为员工身份认证和客户身份认证。而 Okta Identity Cloud 的三项主要服务是 Okta 单点登录（SSO），Okta 自适应单点登录（Adaptive SSO）和自适应多因素身份验证（Adaptive MFA）。

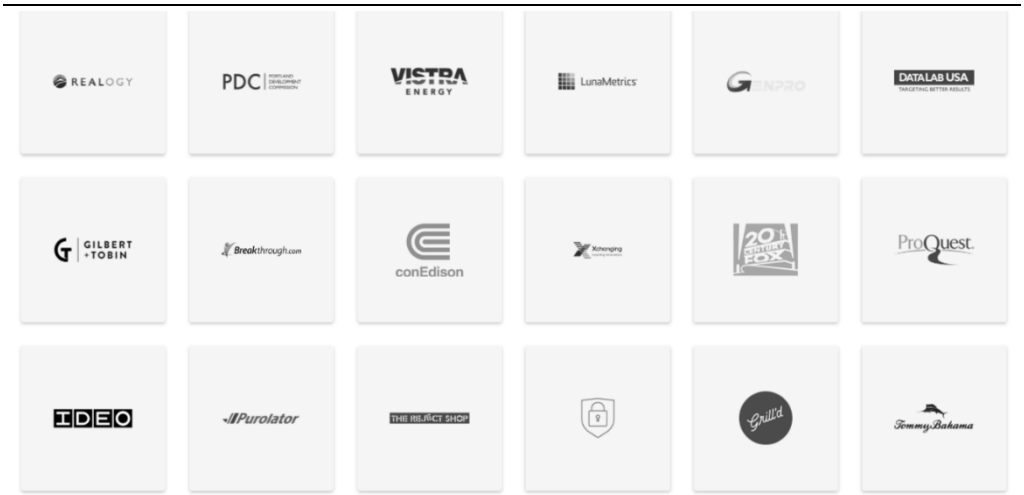
图22：Okta 拥有完整的身份认证管理平台



资料来源：Okta

目前公司已经拥有超过 8,950 个客户，其中合同价值超过 10 亿美元的客户超过 1,450 个。公司客户几乎涵盖了所有行业领域，既覆盖了 100 名员工的规模较小的小型组织，也包括多达数十万员工的《财富》50 强公司，甚至有些企业使用 Okta Identity Cloud 管理数百万个客户的身份。

图23：Okta Identity Cloud 用户覆盖广泛

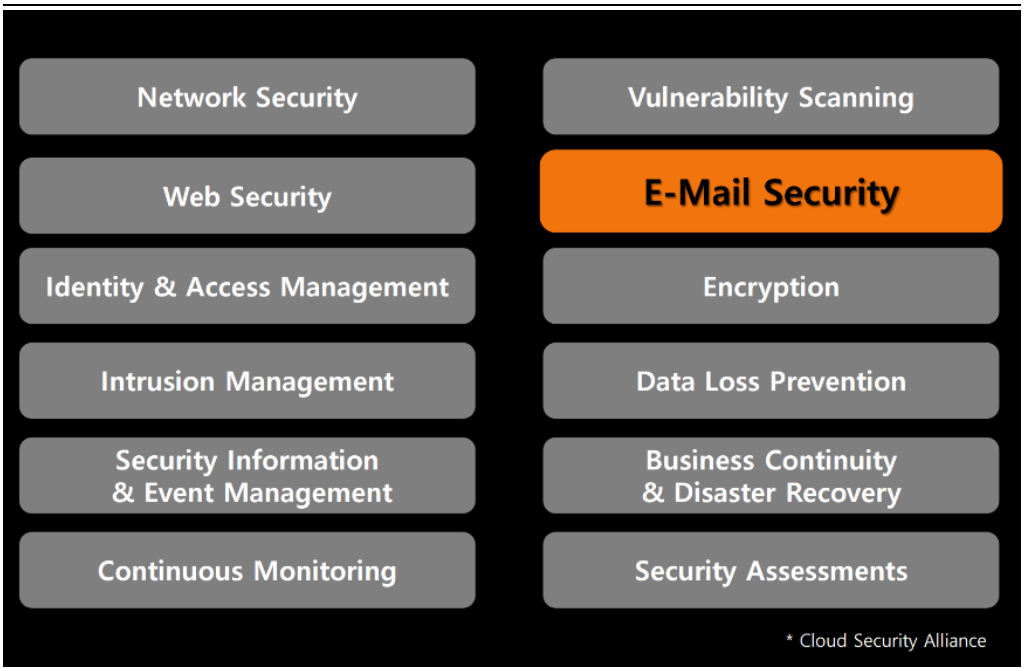


资料来源：Okta

2.2、 SECaaS 成为海外零信任市场主流交付模式

安全即服务（SECaaS）一般指网络安全服务的云交付模型。与软件即服务（SaaS）非常相似，SECaaS 在由云提供商托管的订阅基础上提供安全服务。随着 IT 基础架构向云的迁移，安全模型不得不进行调整以保证信息系统的安全。安全即服务是这一趋势下的产物，意味着安全工具也正在向云转移。SECaaS 是使用第三方托管的基于云的软件来保证组织安全。通过减少本地服务器成本，访问许可费用和管理开销，同时优化了 IT 组织安全工具集的总体拥有成本（TCO）。CSA 将 SECaaS 细分为十个子集类别：1）身份和访问管理；2）防止数据丢失；3）网络安全；4）电邮安全；5）安全评估；6）入侵管理；7）安全信息和事件管理；8）加密；9）业务连续性/灾难恢复；10）网络安全。

图24：CSA 将 SECaaS 细分为十个子集类别



资料来源：CSA

SECaaS 成为零信任主流的交付模式。现代企业环境正在不可避免地向云环境迁移，零信任关于网络不可信、不受控的假设，非常适合云环境部署。Gartner 估计，超过 90％的客户更偏好于 SECaaS 模式。此外，第三种选择是采用云和本地访问代理的结合的方式，主要适用于应用程序的远程访问和本地访问需求兼有的企业。

表2：SECaaS 成为零信任主流的交付模式

交付模式	公司名称	典型产品
SECaaS 模式	Akamai	Enterprise Application Access
	Axis Security	App Access Cloud
	Broadcom	Secure Access Cloud
	Cato Networks	Cato Cloud
	Cisco	Duo
	Citrix	Workspace Essentials
	Clouddeep Technology	DeepCloud SDP
	Cloudflare	Cloudflare Access
	Cognitas Technologies	Crosslink
	Google	BeyondCorp Remote Access
	Hangzhou Cloudaemon Technology	Hangzhou Cloudaemon Technology
	InstaSafe	Secure Access
	Secure Access	Zero Trust Networking Platform
	Netskope	Netskope Private Access
	Okta	Okta Identity Cloud
	OPAQ	Secure Access Service Edge
	Palo Alto Networks	Prisma Access
	Perimeter 81	Software-Defined Perimeter
独立解决方案	AppGate (split from Cyxtera)	AppGate SDP
	Banyan	Zero Trust Remote Access Platform
	BlackRidge	Transport Access Control
	Google Cloud Platform (GCP)	Cloud IdentityAware Proxy(Cloud IAP)
	Microsoft	Azure AD Application Proxy Web Application Proxy (Windows server only)
	Odo	Zero trust access platform
	Pulse Secure	Pulse SDP
	Safe-T	Secure Application Access
	Systancia	Systancia Gate

资料来源：Gartner、开源证券研究所

3、 国内零信任市场仍处于探索阶段，有望实现高速增长

国内零信任市场仍处于探索阶段。一方面，随着“攻防演练”的常态化推进及更多企业的参与，减少暴露面及核心资产隐藏的急迫需求，已经使零信任架构成为

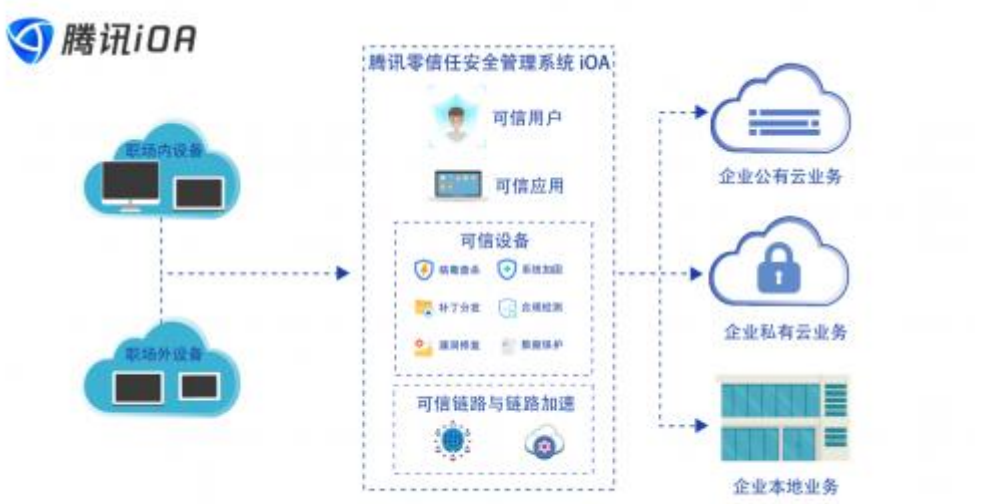
“攻防演练”取得高分的利器之一。2018 年至今，中央部委、国家机关、中大型企业开始探索实践零信任安全架构。另一方面，零信任安全也引起了国家相关部门和业界的高度重视。工信部公开征求对《关于促进网络安全产业发展的指导意见（征求意见稿）》的意见，零信任安全首次被列入网络安全需要突破的关键技术；中国信息通信研究院发布《中国网络安全产业白皮书（2019 年）》，首次将零信任安全技术和 5G、云安全等并列列为我国网络安全重点细分领域技术。

3.1、 国内零信任产品开始涌现，重在探究与原有业务的结合

3.1.1、 腾讯：国内最早落地零信任安全架构的探索者之一

腾讯从 2015 年开始自主设计、研发并在内部实践落地了一套零信任安全管理系统-腾讯 iOA。基于按需、动态的实时访问控制策略，腾讯 iOA 实现了身份安全可信、设备安全可信、应用进程可信、链路保护与加速优化等多种功能，能够满足无边界办公/运维、混合云业务、分支安全接入、应用数据安全调用、统一身份与业务集中管控、全球链路加速访问等六大场景的动态访问控制需求，为企业达到无边界的最小权限安全访问控制，实现安全管理升级提供一站式的零信任安全方案。同时针对远程办公场景痛点，可助力打造员工无论位于何处(Anywhere)、何时(Anytime)使用何设备(Any device)都可安全地访问授权资源以处理任何业务（Any work）的新型“4A 办公”。

图25：腾讯 iOA 打造零信任最佳实践

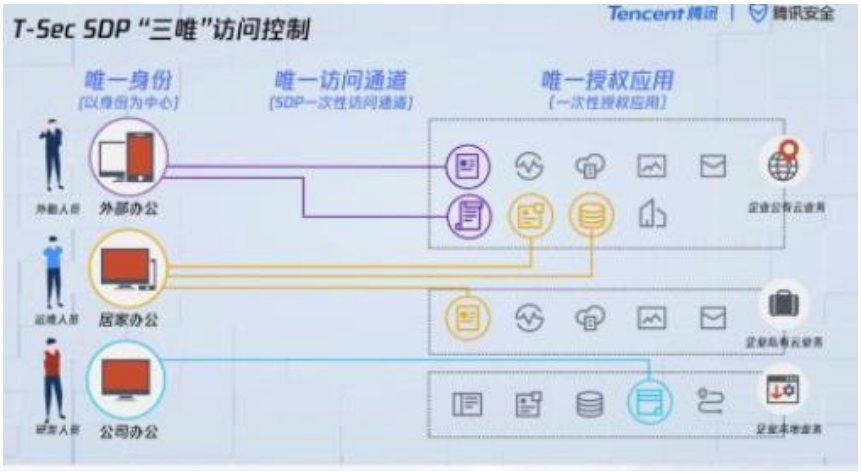


资料来源：腾讯、站长之家

腾讯 iOA 在实现内部安全保障的同时，也实现了能力外溢。在腾讯内部，腾讯 iOA 保障了 7 万员工和 10 万台终端远程办公的安全，在满足基本办公需求基础上，实现了 OA 站点和内部系统、开发运维、登录跳板机等的远程无差别访问，为全网员工打造全尺寸安全工作环境。同时，腾讯 iOA 也是“腾讯级”安全能力对外开放的良好实践，目前已在政府、金融、医疗、交通等多个行业领域应用落地，基于零信任安全实践，推动产业安全管理效率与水准升级。疫情期间在线教育需求高涨，为满足猿辅导在线教育 3.5 万内部员工面向 4 亿用户的办公需求，腾讯 iOA 为猿辅导打造了兼具云端业务与员工终端安全高效连接和快速扩容安全响应的一站式零信任安全体系，实现业务安全和办公效率双重提升。

2020 年 9 月，腾讯安全基于零信任架构打造的新一代全场景安全接入方案——SDP（软件定义边界）正式发布。通过 T-Sec SDP 隐身网关、单包授权协议（SPA）及动态端口使业务应用在互联网上“隐身”，最大程度减少被攻击面；遵循“零信任”安全理念，任何连接均需要先认证后接入，基于身份及设备信息提供持续可信认证，保护企业免受多种网络威胁及黑客技术侵害，防止企业网络被攻破。

图26：T-Sec SDP “三唯”访问控制，护航移动办公全场景安全



资料来源：腾讯安全

3.1.2、 阿里云：全资收购九州云腾，构建云上零信任体系

阿里云全资收购身份认证即服务公司九州云腾。2019 年 10 月，阿里云全资收购九州云腾，九州云腾是国内最早提供商业化（IDaaS）身份认证即服务的公司，拥有丰富的场景化解决方案。阿里云收购九州云腾，既能基于云原生建设整个身份认证管理体系，衍生出混合云多应用场景下的身份治理方案，还能打通“身份认证”与云产品、云安全产品，为企业零信任安全架构奠定更高基础。

九州腾云产品分为生成令牌 IPG 和解析令牌 SPG 两大系列产品：1）IPG 产品线，支持多租户，分级管理，其模块包括 SSO、UD、PS、STS、MFA、SM2 密码控件。2）SPG 产品线，取代 VPN，起到堡垒机作用，其模块包括 API、RP。所有产品模块均可独立工作，模块化部署，实现按需供给。

图27：九州云腾产品分为生成令牌 IPG 和解析令牌 SPG 两大系列

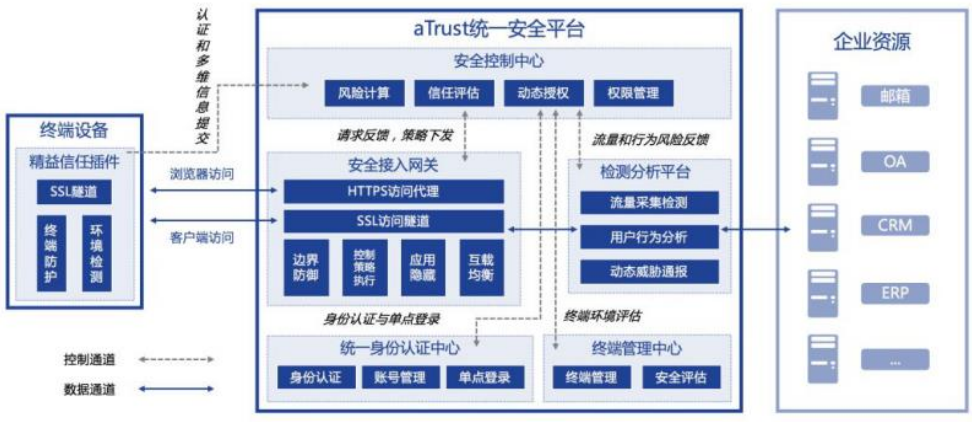


资料来源：九州腾云官网

3.1.3、 深信服：推出精益信任 aTrust 安全架构，获得用户认可

深信服精益信任 aTrust 安全架构在零信任的基础上做了增强，通过信任和风险的反馈控制，实现“精确而足够”的信任。同时，精益信任 aTrust 安全架构下，终端、边界、外网的已有安全设备可以基于信任和风险的闭环进行联动，形成自主调优、快速处置的统一安全架构。深信服精益信任 aTrust 安全架构主要由全面身份化、多源信任评估、动态访问控制、统一安全、可成长等五点组成。

图28：深信服精益信任 aTrust 安全架构在零信任的基础上做了增强



资料来源：深信服官网

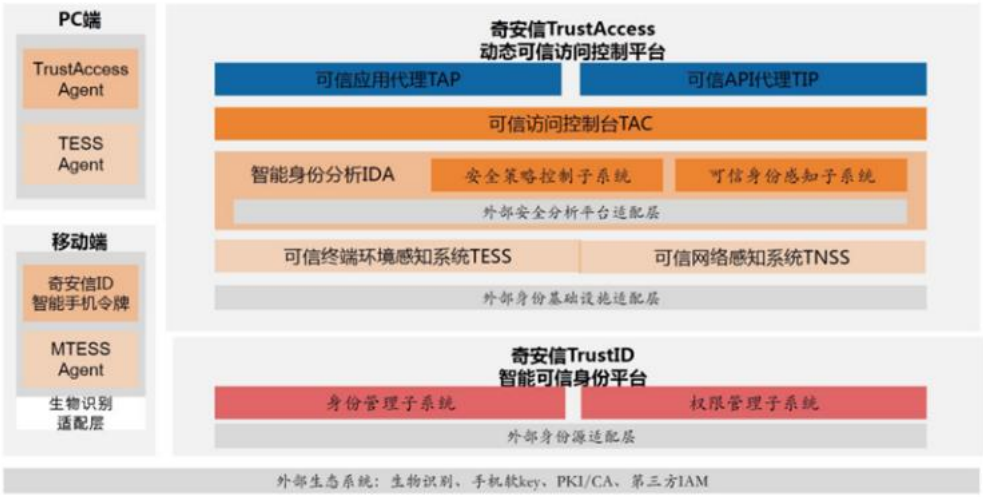
深信服打造的零信任解决方案，已经获得了用户的高度认可。2020 年 8 月，视

源股份与深信服正式宣布签约零信任联合实验室，双方将围绕零信任建设落地和技术创新，进一步紧密合作。

3.1.4、 奇安信：零信任解决方案已经在部委、央企、金融等行业进行广泛落地实施

奇安信集团作为国内领先的零信任架构的践行者，拥有专注“零信任身份安全架构”研究的专业实验室——奇安信身份安全实验室，团队以“零信任安全，新身份边界”为核心理念，推出以“以身份为基石、业务安全访问、持续信任评估和总台访问控制”为四大关键能力的解决方案。奇安信零信任解决方案主要包括：奇安信 TrustAccess 动态可信访问控制平台、奇安信 TrustID 智能可信身份平台、奇安信 ID 智能手机令牌、及各种终端 Agent 组成。

图29：奇安信零信任解决方案整体架构



资料来源：奇安信集团

奇安信零信任身份安全解决方案覆盖了政企行业用户的典型应用场景，如业务访问场景、数据交换场景和服务网格场景等，适用于政府、部委、金融、能源、央企、其他大型组织与企业。以零信任安全架构方案在大数据中心应用为例，奇安信零信任安全解决方案在某头部客户的大数据中心已大规模持续稳定运行超过半年，通过零信任安全接入区，覆盖应用达到 60 多个，用户终端超过 1 万，每天的应用访问次数超过 200 万次，数据流量超过 600G，有效保证了相关大型组织对大数据中心的安全。

图30：奇安信零信任安全解决方案已在某头部客户的大数据中心部署

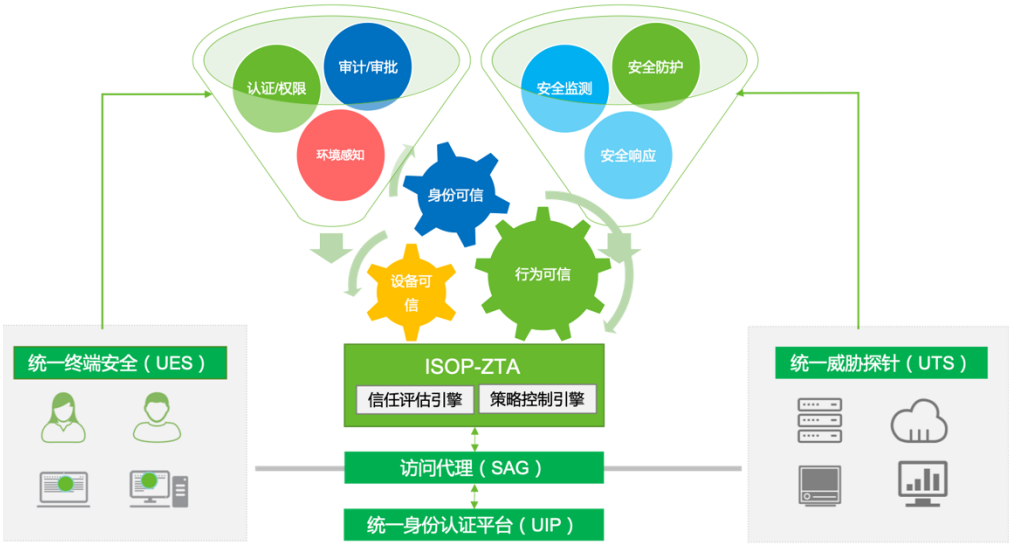


资料来源：奇安信集团

3.1.5、 绿盟科技：拥抱零信任理念，重构安全体系架构

绿盟科技零信任安全解决方案，遵循零信任安全理念，组合终端安全，身份识别与管理，网络安全，应用和数据安全，安全分析协作与响应等模块，构建以用户信任和设备信任为基础，持续评估访问过程的行为可信，自适应访问控制的零信任安全架构。

图31：绿盟发布零信任安全解决方案



资料来源：绿盟科技官网

零信任网络安全解决方案实际部署时，在原有的网络安全基础上，增加零信任安全组件，实现零信任网络访问控制。

图32：绿盟零信任解决方案通过增加零信任安全组件以实现零信任网络访问控制



资料来源：绿盟科技官网

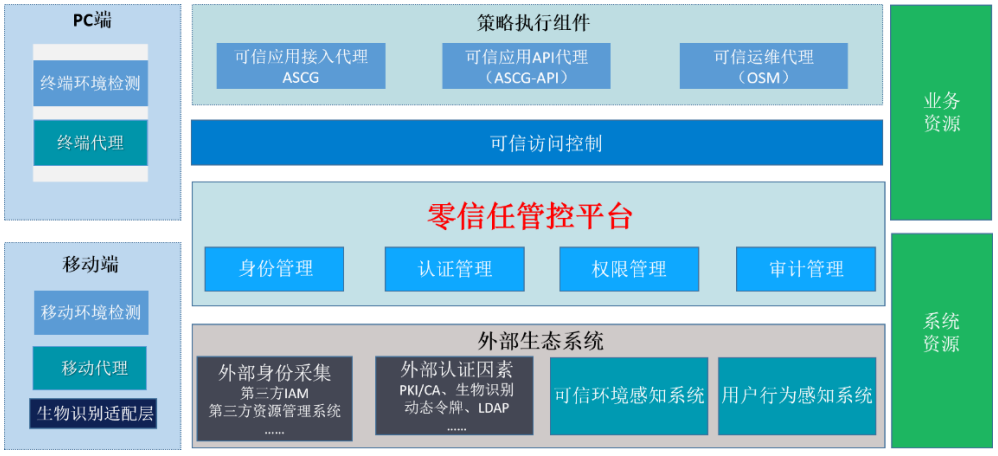
3.1.6、 启明星辰：已推出启明星辰零信任管控平台

启明星辰认为零信任首先关注于数据保护，但可以扩展到包括所有的企业资产，例如设备、基础设施、用户。零信任安全模型假设网络上已经存在攻击者，并且企业内网和其他网络没有任何不同，不再默认内网是可信的。在这种新模式中，企业必须连续分析和评估其内部资产和业务功能所面临的风险，然后采取措施减轻这些

风险。在零信任状态下，这些保护通常涉及对资源的最小化授权访问，仅提供给那些被识别为需要访问的用户和资产，并且每个访问请求持续进行身份和权限验证。

启明星辰零信任安全体系以“四横三纵”为主要逻辑框架。其中四横包含：外部生态系统；零信任管控平台；可信访问控制服务；策略执行组件。三纵包含：用户端；安全访问通道；资源端。其中，零信任管控平台包含身份管理、认证管理、权限管理和审计管理 4 个模块，是整个零信任安全体系的智慧大脑。

图33：启明星辰零信任安全体系以“四横三纵”为主要逻辑框架



资料来源：启明星辰专家视野公众号

3.1.7、 芯盾时代：引领零信任安全风向的创新型企业

芯盾时代从零信任安全出发，“安全+AI”赋能，为客户提供场景化的业务安全解决方案。芯盾时代创立于 2015 年，基于信息安全、人工智能、身份认证等多维技术驱动，依托于坚实的企业服务能力，目前已拥有具有自主知识产权的多因素认证、统一身份管理、人工智能反欺诈、零信任安全等 4 个产品系列。芯盾时代已为政府、金融、互联网、运营商等行业提供了数十种业务安全解决方案，覆盖金融账户及交易安全、企业用户安全管理、智能风控反欺诈、用户和实体行为分析等领域，已有近千家客户选择芯盾时代的产品和服务，并获得商业成功。

图34：芯盾时代拥有四大产品系列



资料来源：芯盾时代官网

目前芯盾时代已五次入选 Gartner 报告，2020 年入选《新兴技术：风险投资增长洞察-信息物理系统安全》报告，成为访问管理领域亚太区唯一入选厂商；凭借客户真实的高度评价入选 2019 《Gartner Peer Insights 客户心声：访问管理》报告，成为亚太区唯一上榜企业，获得了全球总榜单前三的好成绩；2019 年连续入选《市场指南：中国 AI 初创公司》和《竞争格局：中国 AI 初创公司》，并在竞争格局报告中作为五大代表企业被重点解读；2018 年作为唯一业务安全厂商入选《中国区人工智能

实践案例》报告。

图35：芯盾时代已五次入选 Gartner 报告

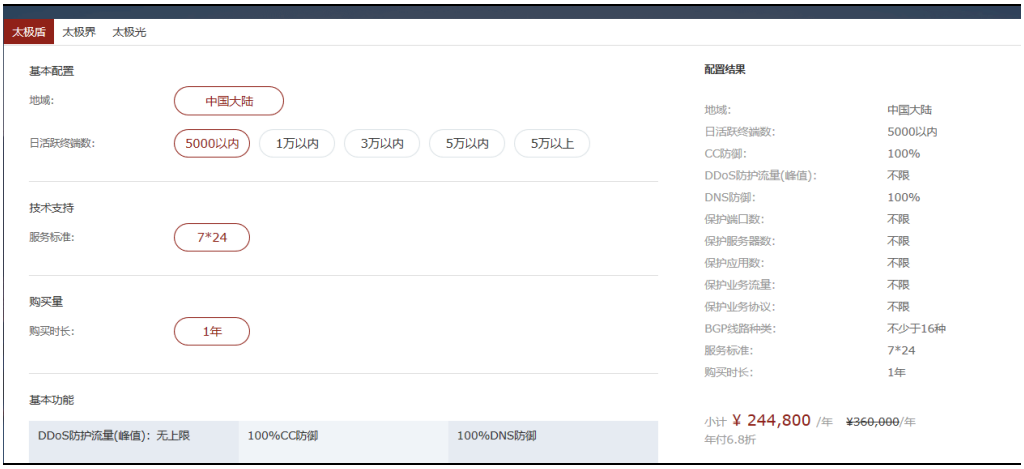


资料来源：芯盾时代官网

3.2、 国内零信任交付模式仍以解决方案为主，长期有望向 SECaaS 转变

国内已经有很多企业将零信任理念付诸实践，大多零信任产品交付模式上仍以解决方案为主，当然也有包括绵盟云在内的少数企业开始尝试 SECaaS 的交付模式。国内外差异的形成主要原因在于：一是国内外信息化发展阶段不同，海外的云计算发展比国内要成熟得多，由云提供商托管的订阅基础上提供安全服务的模式也得到广泛接受。二是国内网络安全发展甚至落后于信息化发展，很多政企主动安全意识弱，更愿意接受解决方案安全建设模式。从更长的时间维度来看，随着我国信息化建设水平提升，安全意识增强，零信任交付模式也有望逐渐向 SECaaS 转变。

图36：绵盟云已开始尝试 SECaaS 的交付模式

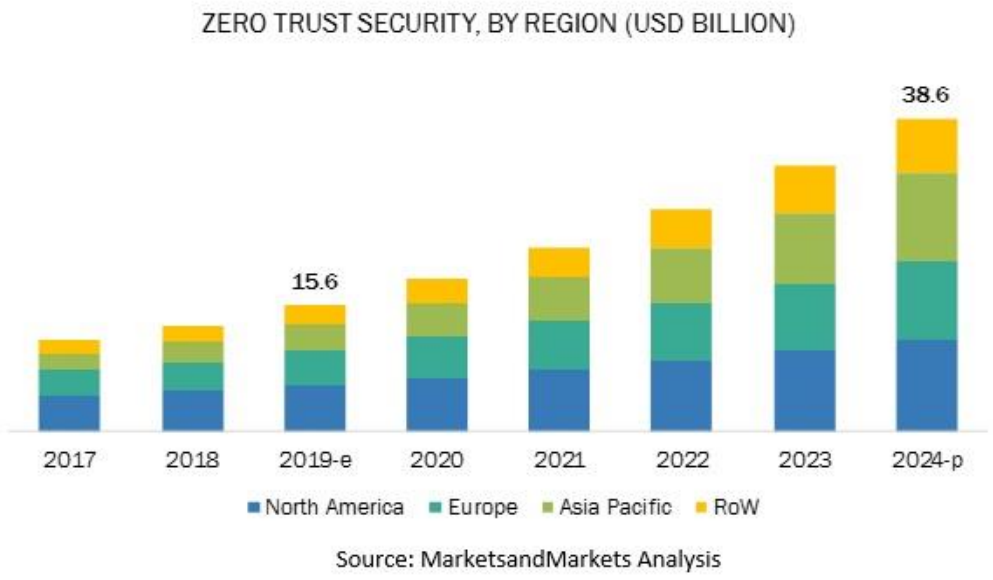


资料来源：绵盟云官网

3.3、 长期来看，国内零信任市场规模有望达百亿

全球零信任占整体安全市场规模比例有望在 2024 年达到 15%。根据 MarketsandMarkets 的报告，全球零信任安全市场规模预计将从 2019 年的 156 亿美元增长到 2024 年的 386 亿美元，从 2019 年到 2024 年的复合年增长率为 19.9%。而在其另一份报告中预测，到 2023 年全球网络安全市场规模将达 2482.6 亿美元。因此，据此可以估算全球零信任占整体安全市场规模比例有望在 2024 年达到 15%。

图37：全球零信任安全市场规模预计到 2024 年将达 386 亿美元



资料来源：MarketsandMarkets

中性假设下，到 2024 年国内零信任市场规模有望达百亿人民币。1）根据 IDC 最新预测，2020 年中国网络安全市场总体支出将达到 78.9 亿美元，预计 2024 年将达到 167.2 亿美元，2020-2024 年均复合增长率为 18.7%。2）到 2024 年，假设乐观、中性、悲观条件下，国内零信任占整体安全市场规模比例分别为 5%、10%、15%，所对应市场规模分别为 8.36 亿、16.7 亿、25.1 亿美元。

表3：中性假设下，到 2024 年国内零信任市场规模有望达百亿人民币

	市场占比	市场规模
乐观	15%	25.1 亿美元
中性	10%	16.7 亿美元
悲观	5%	8.36 亿美元

资料来源：开源证券研究所

4、 投资建议

零信任作为 IT 无边界化趋势下一种新安全理念，已经成为全球网络安全的关键技术和大趋势。当前海外零信任市场已走向规模化落地，商业模式较为成熟，而国内零信任市场刚刚兴起，腾讯、阿里等互联网巨头及深信服、奇安信、绿盟科技等安全厂商均结合自身业务推出零信任产品和解决方案。长期来看，国内零信任市场规模有望达百亿。推荐深信服、奇安信、安恒信息、启明星辰，建议关注绿盟科技、南洋股份、美亚柏科、山石网科。

表4：推荐深信服、奇安信、安恒信息、启明星辰，建议关注绿盟科技、南洋股份、美亚柏科、山石网科（截止 2020.9.23 收盘）

证券代码	公司简称	当前市值（亿元）	归母净利润（亿元）			PE			PS			
			2020E	2021E	2022E	2020E	2021E	2022E	2020E	2021E	2022E	评级
300454.SZ	深信服	838	9.03	11.77	14.83	93	71	57	14	11	8	买入
688561.SH	奇安信	725	-3.28	0.06	4.85	-234	11952	158	16	11	8	买入
688023.SH	安恒信息	197	1.32	1.83	2.44	149	108	81	14	10	8	买入

证券代码	公司简称	当前市值（亿元）	归母净利润（亿元）			PE			PS			
			2020E	2021E	2022E	2020E	2021E	2022E	2020E	2021E	2022E	评级
002439.SZ	启明星辰	325	8.54	11.09	14.02	38	29	23	8	6	5	买入
300369.SZ	绿盟科技	166	3.20	4.28	5.59	52	39	30	8	6	5	-
002212.SZ	南洋股份	278	6.09	8.40	11.12	46	33	25	-	-	-	-
300188.SZ	美亚柏科	150	4.17	5.58	7.38	36	27	20	6	4	3	-
688030.SH	山石网科	70	1.21	1.57	1.95	58	45	36	8	6	5	-

数据来源：Wind、开源证券研究所（绿盟科技、南洋股份、美亚柏科、山石网科盈利预测均来源于 Wind 一致预期）

5、 风险提示

疫情影响全年业绩风险；市场竞争加剧风险；人才流失风险。

特别声明

《证券期货投资者适当性管理办法》、《证券经营机构投资者适当性管理实施指引（试行）》已于2017年7月1日起正式实施。根据上述规定，开源证券评定此研报的风险等级为R4（中高风险），因此通过公共平台推送的研报其适用的投资者类别仅限定为专业投资者及风险承受能力为C4、C5的普通投资者。若您并非专业投资者及风险承受能力为C4、C5的普通投资者，请取消阅读，请勿收藏、接收或使用本研报中的任何信息。
因此受限于访问权限的设置，若给您造成不便，烦请见谅！感谢您给予的理解与配合。

分析师承诺

负责准备本报告以及撰写本报告的所有研究分析师或工作人员在此保证，本研究报告中关于任何发行商或证券所发表的观点均如实反映分析人员的个人观点。负责准备本报告的分析师获取报酬的评判因素包括研究的质量和准确性、客户的反馈、竞争性因素以及开源证券股份有限公司的整体收益。所有研究分析师或工作人员保证他们报酬的任何一部分不曾与，不与，也将不会与本报告中具体的推荐意见或观点有直接或间接的联系。

股票投资评级说明

	评级	说明
证券评级	买入（Buy）	预计相对强于市场表现 20%以上；
	增持（outperform）	预计相对强于市场表现 5%～20%；
	中性（Neutral）	预计相对市场表现在－5%～＋5%之间波动；
	减持（underperform）	预计相对弱于市场表现 5%以下。
行业评级	看好（overweight）	预计行业超越整体市场表现；
	中性（Neutral）	预计行业与整体市场表现基本持平；
	看淡（underperform）	预计行业弱于整体市场表现。
备注：评级标准为以报告日后的 6~12 个月内，证券相对于市场基准指数的涨跌幅表现，其中 A 股基准指数为沪深 300 指数、港股基准指数为恒生指数、新三板基准指数为三板成指（针对协议转让标的）或三板做市指数（针对做市转让标的）、美股基准指数为标普 500 或纳斯达克综合指数。我们在此提醒您，不同证券研究机构采用不同的评级术语及评级标准。我们采用的是相对评级体系，表示投资的相对比重建议；投资者买入或者卖出证券的决定取决于个人的实际情况，比如当前的持仓结构以及其他需要考虑的因素。投资者应阅读整篇报告，以获取比较完整的观点与信息，不应仅仅依靠投资评级来推断结论。		

分析、估值方法的局限性说明

本报告所包含的分析基于各种假设，不同假设可能导致分析结果出现重大不同。本报告采用的各种估值方法及模型均有其局限性，估值结果不保证所涉及证券能够在该价格交易。

法律声明

开源证券股份有限公司是经中国证监会批准设立的证券经营机构，已具备证券投资咨询业务资格。

本报告仅供开源证券股份有限公司（以下简称“本公司”）的机构或个人客户（以下简称“客户”）使用。本公司不会因接收人收到本报告而视其为客户。本报告是发送给开源证券客户的，属于机密材料，只有开源证券客户才能参考或使用，如接收人并非开源证券客户，请及时退回并删除。

本报告是基于本公司认为可靠的已公开信息，但本公司不保证该等信息的准确性或完整性。本报告所载的资料、工具、意见及推测只提供给客户作参考之用，并非作为或被视为出售或购买证券或其他金融工具的邀请或向人做出邀请。本报告所载的资料、意见及推测仅反映本公司于发布本报告当日的判断，本报告所指的证券或投资标的的价格、价值及投资收入可能会波动。在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的报告。客户应当考虑到本公司可能存在可能影响本报告客观性的利益冲突，不应视本报告为做出投资决策的唯一因素。本报告中所指的投资及服务可能不适合个别客户，不构成客户私人咨询建议。本公司未确保本报告充分考虑到个别客户特殊的投资目标、财务状况或需要。本公司建议客户应考虑本报告的任何意见或建议是否符合其特定状况，以及（若有必要）咨询独立投资顾问。在任何情况下，本报告中的信息或所表述的意见并不构成对任何人的投资建议。在任何情况下，本公司不对任何人因使用本报告中的任何内容所引致的任何损失负任何责任。若本报告的接收人非本公司的客户，应在基于本报告做出任何投资决定或就本报告要求任何解释前咨询独立投资顾问。

本报告可能附带其它网站的地址或超级链接，对于可能涉及的开源证券网站以外的地址或超级链接，开源证券不对其内容负责。本报告提供这些地址或超级链接的目的纯粹是为了客户使用方便，链接网站的内容不构成本报告的任何部分，客户需自行承担浏览这些网站的费用或风险。

开源证券在法律允许的情况下可参与、投资或持有本报告涉及的证券或进行证券交易，或向本报告涉及的公司提供或争取提供包括投资银行业务在内的服务或业务支持。开源证券可能与本报告涉及的公司之间存在业务关系，并无需事先或在获得业务关系后通知客户。

本报告的版权归本公司所有。本公司对本报告保留一切权利。除非另有书面显示，否则本报告中的所有材料的版权均属本公司。未经本公司事先书面授权，本报告的任何部分均不得以任何方式制作任何形式的拷贝、复印件或复制品，或再次分发给任何其他人，或以任何侵犯本公司版权的其他方式使用。所有本报告中使用的商标、服务标记及标记均为本公司的商标、服务标记及标记。

开源证券研究所

上海
地址：上海市浦东新区世纪大道1788号陆家嘴金控广场1号楼10层
邮编：200120
邮箱：research@kysec.cn

深圳
地址：深圳市福田区金田路2030号卓越世纪中心1号楼45层
邮编：518000
邮箱：research@kysec.cn

北京
地址：北京市西城区西直门外大街18号金贸大厦C2座16层
邮编：100044
邮箱：research@kysec.cn

西安
地址：西安市高新区锦业路1号都市之门B座5层
邮编：710065
邮箱：research@kysec.cn