奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

第1期

零信任架构及解决方案

Gartner

零信任架构及解决方案

云计算和大数据时代，网络安全边界逐渐瓦解，内外部威胁愈演愈烈，传统的边界安全架构难以应对，零信任安全架构应运而生。零信任安全架构基于“以身份为基石、业务安全访问、持续信任评估、动态访问控制”四大关键能力，构筑以身份为基石的动态虚拟边界产品与解决方案，助力企业实现全面身份化、授权动态化、风险度量化、管理自动化的新一代网络安全架构。

本文首先对零信任安全的背景、定义及发展历史进行介绍，然后提出一种通用的零信任参考架构，并以奇安信零信任安全解决方案为例，对零信任参考架构的应用方案进行解读，最后，探讨了零信任迁移方法论，提出确定愿景、规划先行和分步建设的迁移思路。

1. 介绍

企业的网络基础设施日益复杂，安全边界逐渐模糊。数字化转型的时代浪潮推动着信息技术的快速演进，云计算、大数据、物联网、移动互联等新兴 IT 技术为各行各业带来了新的生产力，但同时也给企业网络基础设施带来了极大的复杂性。一方面，云计算、移动互联等技术的采用让企业的人和业务、数据“走”出了企业的边界；另一方面，大数据、物联网等新技术的开放协同需求导致了外部人员、平台和服务“跨”过了企业的数字护城河。复杂的现代企业网络基础设施已经不存在单一的、易识别的、明确的安全边界，或者说，企业的安全边界正在逐渐瓦解，传统的基于边界的网络安全架构和解决方案难以适应现代企业网络基础设施。

另外，网络安全形势不容乐观。外部攻击和内部威胁愈演愈烈，有组织的、攻击武器化、以数据及服务为攻击目标的高级持续攻击仍然能轻易找到各种漏洞突破企业的边界，同时，内部业务的非授权访问、雇员犯错、有意的数据窃取等内部威胁层出不穷。面对如此严峻的安全挑战，业界的安全意识不可谓不到位，安全投入不可谓不高，然而，安全效果却不尽如人意，安全事件层出不穷，传统安全架构失效背后的根源是什么呢？安全的根本在应对风险，而风险与“漏洞”息息相关，是什么“漏洞”导致传统安全架构失效呢？答案是信任。传统的基于边界的网络安全架构某种程度上假设、或默认了内网的人和设备是值得信任的，认为安全就是构筑企业的数字护城河，通过防火墙、WAF、IPS 等边界安全产品/方案对企业网络边界进行重重防护就足够了。事实证明，正确的思维应该是假设网络系统一定有未被发现的漏洞、假设系统一定有已发现但仍未修补的漏洞、假设系统已经被渗透、假设内部人员不可靠，这“四个假设”就彻底推翻了传统网络安全通过隔离、修边界的技术方法，彻底推翻了边界安全架构下对“信任”的假设和滥用，基于边界的网络安全架构和解决方案已经难以应对如今的网络威胁。

需要全新的网络安全架构应对现代复杂的企业网络基础设施，应对日益严峻的网络威胁形势，零信任架构正是在这种背景下应运而生，是安全思维和安全架构进化的必然。

1.1. 零信任定义

零信任架构一直在快速发展和成熟，不同版本的定义基于不同的维度进行描述。在*《零信任网络：在不可信网络中构建安全系统》一书中*，埃文·吉尔曼 (Evan Gilman) 和道格·巴斯 (Doug Barth) 将零信任的定义建立在如下五个基本假定之上：[1]

- 网络无时无刻不处于危险的环境中。
- 网络中自始至终存在外部或内部威胁。
- 网络的位置不足以决定网络的可信程度。
- 所有的设备、用户和网络流量都应当经过认证和授权。
- 安全策略必须是动态的，并基于尽可能多的数据源计算而来。

简而言之：默认情况下不应该信任企业网络内部和外部的任何人/设备/应用，需要基于认证和授权重构访问控制的信任基础。零信任对传统访问控制机制进行了范式上的颠覆，其本质是以身份为基石的动态可信访问控制。

NIST 在最近发表的《零信任架构》(NIST. SP.800-207 - 草案) 中指出，零信任架构是一种网络/数据安全的端到端方法，关注身份、凭证、访问管理、运营、终端、主机环境和互联的基础设施，认为零信任是一种关注数据保护的架构方法，认为传统安全方案只关注边界防护，对授权用户开放了过多的访问权限。零信任的首要目标就是基于身份进行细粒度的访问控制，以便应对越来越严峻的越权横向移动风险。

基于如上观点，NIST 对零信任架构定义如下：

零信任架构 (ZTA) 提供一系列概念、理念、组件及其交互关系，以便消除针对信息系统和服务进行精准访问判定所存在的不确定性。[2]此定义指出了零信任需要解决的关键问题：消除对数据和服务的未授权访问，强调了需要进行细粒度访问控制的重要性。

1.2. 零信任历史

从零信任的发展历史进行分析，也不难发现零信任的各种不同维度的观点也在持续发展、融合，并最终表现出较强的一致性。

零信任的最早雏形源于 2004 年成立的耶利哥论坛 (Jericho Forum)，其成立的使命正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，零信任这个术语正式出现，并指出默认情况下所有的网络流量都是不可信的，需要对访问任何资源的任何请求进行安全控制，零信任提出之初，其解决方案专注于通过微隔离对网络进行细粒度的访问控制以便限制攻击者的横向移动。

随着零信任的持续演进，以身份为基石的架构体系逐渐得到业界主流的认可，这种架构体系的转变与移动计算、云计算的大幅采用密不可分。2014 年开始，Google 基于其内部项目 BeyondCorp 的研究成果，陆续发表了多篇论文，阐述了在 Google 内部如何为其员工构建零信任架构。BeyondCorp 的出发点在于仅仅针对企业边界构建安全控制已经不够了，需要把访问控制从边界迁移到每个用户和设备。通过构建零信任，Google 成功地摒弃了对传统 VPN 的采用，通过全新架构体系确保所有来自不安全网络的用户能安全地访问企业业务。[3]

[1]埃文·吉尔曼，道格·巴斯，零信任网络：在不可信网络中构建安全系统 (O'Reilly Media，2017)

[2] NIST, Zero Trust Architecture, 2019.09, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft.pdf

[3] Google, https://cloud.google.com/beyondcorp/

通过业界对零信任理论和实践的不断完善，零信任已经超越了最初的网络层微分段的范畴，演变为以身份为基石的，能覆盖云环境、大数据中心、微服务等众多场景的新一代安全解决方案。各研究咨询机构也快速对其安全架构和体系进行优化。

综合分析各种零信任的定义和框架，不难看出零信任架构的本质是以身份为基石的动态可信访问控制，聚焦身份、信任、业务访问和动态访问控制等维度的安全能力，基于业务场景的人、流程、环境、访问上下文等多维的因素，对零信任进行持续评估，并通过信任等级对权限进行动态调整，形成具备较强风险应对能力的动态自适应的安全闭环体系。

2. 零信任参考架构

零信任安全的关键能力可以概括为：以身份为基石、业务安全访问、持续信任评估和动态访问控制，这些关键能力映射到一组相互交互的核心架构组件，对各业务场景具备较高的适应性。

2.1. 关键能力模型

零信任的本质是在访问主体和客体之间构建以身份为基石的动态可信访问控制体系，通过以身份为基石、业务安全访问、持续信任评估和动态访问控制的关键能力，基于对网络所有参与实体的数字身份，对默认不可信的所有访问请求进行加密、认证和强制授权，汇聚关联各种数据源进行持续信任评估，并根据信任的程度动态对权限进行调整，最终在访问主体和访问客体之间建立一种动态的信任关系。

零信任架构下，访问客体是核心保护的资源，针对被保护资源构建保护面，资源包括但不限于企业的业务应用、服务 API、操作功能和资产数据。访问主体包括人员、设备、应用和系统等身份化之后的数字实体，在一定的访问上下文中，这些实体还可以进行组合绑定，进一步对主体进行明确和限定。

零信任架构的关键能力包括：以身份为基石、业务安全访问、持续信任评估和动态访问控制。（有关概念模型，请参见图 1。）

1) 以身份为基石

基于身份而非网络位置来构建访问控制体系，首先需要为网络中的人和设备赋予数字身份，将身份化的人和设备进行运行时组合构建访问主体，并为访问主体设定其所需的最小权限。

数字身份是零信任架构的基石，需要实现“全面身份化”。仅仅为人员和/或设备创建身份是远远不够的，需要对人、设备等参与网络交互的所有实体建立数字身份。事实上，在万物互联的时代，物已经成为了重要的参与实体，其基数已经远远超出了人。

在零信任安全架构中，根据一定的访问上下文，访问主体可以是人、设备和应用等实体数字身份的动态组合，在《*零信任网络*》一书中，将这种组合称为“网络代理”。网络代理指在网络请求中用于描述请求发起者的信息集合，一般包括用户、应用程序和设备共三类实体信息，用户、应用程序和设备信息是访问请求密不可分的上下文。网络代理具有短时性特征，在进行授权决策时按需临时生成。访问代理的构成要素（用户或设备）信息一般存放在数据库中，在授权时实时查询并进行组合，因此，网络代理代表的是用户和设备各个维度的属性在授权时刻的实时状态。[4]

图 1 零信任架构的关键能力模型

（来源：奇安信集团，2019）

[4]埃文·吉尔曼，道格·巴斯，零信任网络：在不可信网络中构建安全系统，2019.08

最小权限原则是任何安全架构必须遵循的关键实践之一，然而零信任架构将最小权限原则又推进了一大步，遵循了*动态的*最小权限原则。如果用户确实需要更高的访问权限，那么用户可以并且只能在需要的时候获得这些特权。一方面，强调授权的主体不是单个实体身份，而是网络代理这一复合主体，不仅仅是对用户遵循最小权限原则，对设备也同样遵循；另一方面，权限可以根据主体属性、环境属性、信任等级和客体的安全等级进行进一步的限定。而反观传统的身份与访问控制相关实现方案，一般对人、设备进行单独授权，零信任这种以网络代理作为授权主体的范式，在授权决策时刻按需临时生成主体，具有较强的动态性和风险感知能力，可以极大地缓解凭证窃取、越权访问等安全威胁。

2) 业务安全访问

零信任架构关注业务保护面的构建，通过业务保护面实现对资源的保护，在零信任架构中，应用、服务、接口、数据都可以视作业务资源。通过构建保护面实现对暴露面的收缩，要求所有业务默认隐藏，根据授权结果进行最小限度的开放，所有的业务访问请求都应该进行全流量加密和强制授权，业务安全访问相关机制需要尽可能工作在应用协议层。

构建零信任安全架构，需要关注待保护的核心资产，梳理核心资产的各种暴露面，并通过技术手段将暴露面进行隐藏。这样，核心资产的各种访问路径就隐藏在零信任架构组件之后，默认情况对访问主体不可见，只有经过认证、具有权限、信任等级符合安全策略要求的访问请求才予以放行。通过业务隐藏，除了满足最小权限原则，还能很好的缓解针对核心资产的扫描探测、拒绝服务、漏洞利用、非法爬取等安全威胁。

数据窃取的最常用手段就是网络窃听和中间人攻击。在零信任实践中，需要对所有应用、API 接口调用的流量进行高强度的 TLS 加密，并且需要考虑对国密算法的支持。零信任强调全流量加密代理，而不仅仅是针对认证请求的局部流量进行接管，这也是零信任架构中的可信代理和传统身份认证网关的核心差异之一。

为了防止访问控制机制被旁路，需要有策略强制执行点，在零信任架构中，需要确保所有的访问请求，其主体都经过了认证、进行了授权、具备相当的信任等级。零信任架构需要针对不同的业务场景进行适配，从不同的访问协议和方法中对主体进行识别，对多级多层访问的主体进行关联，只有这样，才能有效确保访问控制严丝合缝不留漏洞。

3) 持续信任评估

持续信任评估是零信任架构从零开始构建信任的关键手段，通过信任评估模型和算法，实现基于身份的信任评估能力，同时需要对访问的上下文环境进行风险判定，对访问请求进行异常行为识别并对信任评估结果进行调整。

人和设备等物理世界的实体，经过身份化后成为数字世界的数字身份，因此，对实体的信任评估首先需要对数字身份进行信任评估，信任评估至少需要涵盖人和设备两类数字身份。需要建立基于身份的信任评估体系并且涵盖数字身份全生命周期的各个环节，包括：数字身份本身的配置、状态和属性的信任评估；物理实体到数字身份的映射过程（身份创建和验证）的信任评估等。前文提到，在零信任架构中，访问主体是人、设备和应用程序三位一体构成的网络代理，因此在基于身份信任的基础上，还需要评估主体信任，主体信任是对身份信任在当前访问上下文中的动态调整，和认证强度、风险状态和环境因素等相关，身份信任相对稳定，而主体信任和网络代理一样，具有短时性特征，是一种动态信任，基于主体的信任等级进行动态访问控制也是零信任的本质所在。

信任和风险如影随形，在某些特定场景下，甚至是一体两面。在零信任架构中，除了信任评估，还需要考虑环境风险的影响因素，需要对各类环境风险进行判定和响应。但需要特别注意，并非所有的风险都会影响身份或主体的信任度。比如，在访问业务的过程中，通过摄像头感知到多人围观这一行为，这种行为对敏感资源来说是一种风险，需要撤销当前访问会话以缓解风险，但大多数情况下并不需要对当前终端和人员的信任等级进行下调，当然，如果这种行为构成了一种固有模式，就有足够的理由对操作者的意图进行怀疑了，或者说，这种情况，操作者的信任应该降级。

基于行为的异常发现和信任评估能力必不可少，包括主体（所对应的数字身份）个体行为的基线偏差、主体与群体的基线偏差、主体环境的攻击行为、主体环境的风险行为等都需要建立模型进行量化评估，是影响信任的关键要素。当然，行为分析需要结合身份态势进行综合度量，以减少误判，降低对使用者操作体验的负面影响。

4) 动态访问控制

动态访问控制是零信任架构的安全闭环能力的重要体现。建议通过 RBAC 和 ABAC 的组合授权实现灵活的访问控制基线，基于信任等级实现分级的业务访问，同时，当访问上下文和环境存在风险时，需要对访问权限进行实时干预并评估是否对访问主体的信任进行降级。

任何访问控制体系的建立离不开访问控制模型，需要基于一定的访问控制模型制定权限基线。访问模型繁多，包括 RBAC、ABAC、MAC、DAC 等各种经典模型及其变种。零信任强调灰度哲学，从实践经验来看，也大可不必去纠结 RBAC 好还是 ABAC 好，而是考虑如何兼顾融合，建议基于 RBAC 模型实现粗粒度授权，建立权限基线满足企业基本的最小权限原则，并基于主体、客体和环境属性实现角色的动态映射和过滤机制，充分发挥 ABAC 的动态性和灵活性。权限基线决定了一个访问主体允许访问的权限的全集，而在不同的访问时刻，主体被赋予的访问权限和访问上下文、信任等级、风险状态息息相关。

另外，在访问控制基线之上，需要根据主体的信任等级和客体的安全等级实现分级访问控制策略。当主体的信任等级高于客体的安全等级时，访问权限被真正授予，否则访问请求被拒绝，从而缓解风险。根据持续信任评估，主体的信任等级会实时进行调整，因此，访问权限是在访问控制基线范围内动态调整的。

需要注意，并非所有的风险都对信任有影响，特别是环境风险，但风险一旦发生，就需要对应的处置策略，常见手段是撤销访问会话。因此，零信任架构的控制平面需要能接收外部风险平台的风险通报，并对当前访问会话进行按需处理，从而实现风险处置的联动，真正将零信任架构体系和企业现存的其他安全体系融合贯穿。

2.2. 基本架构原则

在“关键能力模型”一节中，对“以身份为基石、业务安全访问、持续信任评估、动态访问控制”四项零信任关键能力进行了详细描述，这些安全能力需要在零信任架构中通过架构组件、交互逻辑等进行支撑，在将安全能力进行架构映射的过程中，需要遵循一些基本架构原则，才能确保最终实现的零信任架构能切实满足新型 IT 环境下的安全需求。这些基本架构原则包括：

- **全面身份化原则**

对所有的访问主体需要进行身份化，包括人员、设备等，仅仅对人员进行身份管理是远远不够的；另外，访问控制的主体是网络代理，而不是孤立的人员或设备。

- **应用级控制原则**

业务访问需要尽可能工作在应用层而不是网络层，通常采用应用代理实现；应用代理需要做到全流量代理和加密，切忌不可只对应用的认证请求进行代理。

- **安全可闭环原则**

信任等级基于访问主体的属性、行为和访问上下文进行评估，并且基于信任等级对访问权限进行动态的、近实时的、自动的调整，形成自动安全闭环。

- **业务强聚合原则**

零信任架构具有内生安全属性，需要结合实际的业务场景和安全现状进行零信任架构的设计，建议将零信任安全和业务同步进行规划。零信任架构需要具备较强的适应性，能根据实际场景需求进行裁剪或扩展。

- **多场景覆盖原则**

现代 IT 环境具有多样的业务访问场景，包括用户访问业务、服务 API 调用、数据中心服务互访等场景，接入终端包括移动终端、PC 终端、物联终端等，业务部署位置也多种多样。零信任架构需要考虑对各类场景的覆盖并确保具备较强的可扩展性，以便为各业务场景实现统一的安全能力。

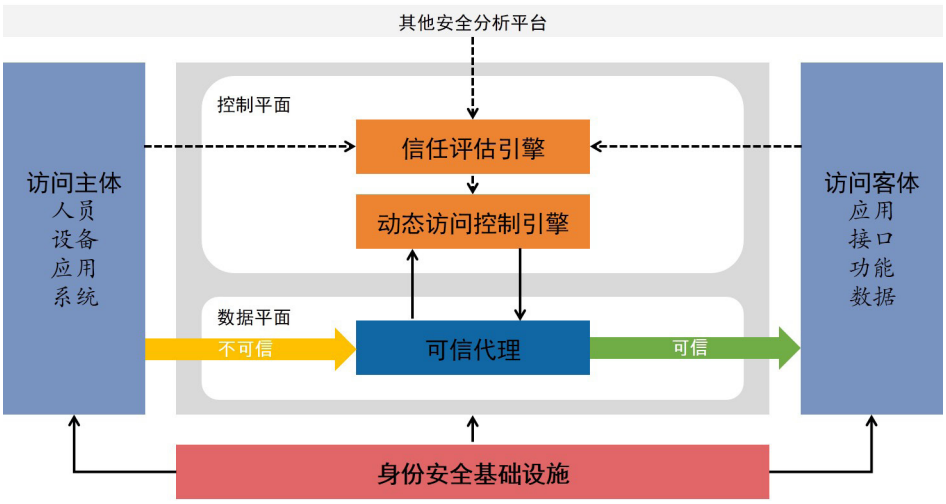
- **组件高联动原则**

零信任各架构组件应该具备较高的联动性，各组件相互调用形成一个整体，缓解各类威胁并形成安全闭环。在零信任架构实践中，切忌不可堆砌拼凑产品组件，各产品的可联动性是零信任能力实现效果的重要基础。

2.3. 核心架构组件

基于前述关键能力模型和基本架构原则，零信任架构的核心逻辑架构组件如图 2 所示：

图 2 零信任架构的核心逻辑架构组件



（来源：奇安信集团，2019）

1) 可信代理

可信代理是零信任架构的数据平面组件，是确保业务安全访问的第一道关口，是动态访问控制能力的策略执行点。

可信代理拦截访问请求后，通过动态访问控制引擎对访问主体进行认证，对访问主体的权限进行动态判定。只有认证通过、并且具有访问权限的访问请求才予以放行。同时，可信代理需要对所有的访问流量进行加密。全流量加密对可信代理也提出了高性能和高伸缩性的需求，支持水平扩展是零信任可信代理必须具备的核心能力。

根据不同的场景，可信代理的具体产品形态具有较大差异，比如，针对用户访问业务的场景，可信代理的形态可能是基于反向代理技术的应用网关形态；针对服务接口调用的场景，可信代理的形态可以是 API 网关形态；针对服务网格场景，可信代理可以简化为运行在服务环境的代理 Agent 模块。同样，不同的场景的能力要求也有差异，同样是用户访问业务的场景，根据业务应用的不同，要求可信代理除了支持应用级反向代理技术以外，还需要支持 TCP 代理技术对一些遗留应用进行代理。在实际方案实现上，各种形态的可信代理必须在控制平面组件的统一管理和控制下工作，确保安全策略在各种场景下的无差异实现。

2) 动态访问控制引擎

动态访问控制引擎和可信代理联动，对所有访问请求进行认证和动态授权，是零信任架构控制平面的策略判定点。

动态访问控制引擎对所有的访问请求进行权限判定，权限判定不再基于简单的静态规则，而是基于上下文属性、信任等级和安全策略进行动态判定。动态访问控制进行权限判定的依据是身份库、权限库和信任库。其中身份库提供访问主体的身份属性，权限库提供基础的权限基线，信任库则由身份分析引擎通过实时的风险多维关联和信任评估进行持续维护。

为了实现基于身份的访问控制策略及动态权限调整，动态访问控制引擎组件需要同时实现对访问主体的身份认证和会话管理，确保所有的访问请求都是身份感知的、可见可控的。

3) 信任评估引擎

信任评估引擎是零信任架构中实现持续信任评估能力的核心组件，和动态访问控制引擎联动，为其提供信任等级评估作为授权判定依据。

信任评估引擎持续接收可信代理、动态访问控制引擎的日志信息，结合身份库、权限库数据，基于大数据和人工智能技术，对身份进行持续画像，对访问行为进行持续分析，对信任进行持续评估，最终生成和维护信任库，为动态访问控制引擎提供决策依据。另外，信任评估引擎也可以接收外部安全分析平台的分析结果，包括：终端可信环境感知、持续威胁检测、态势感知等安全分析平台，这些外部风险源可以很好的补充身份分析所需的场景数据，丰富上下文，从而进行更精准的风险识别和信任评估。

4) 身份安全基础设施

身份基础设施是实现零信任架构以身份为基石能力的关键支撑组件。

身份基础设施至少包含身份管理和权限管理功能组件，通过身份管理实现各种实体的身份化及身份生命周期管理，通过权限管理，对授权策略进行细粒度的管理和跟踪分析。

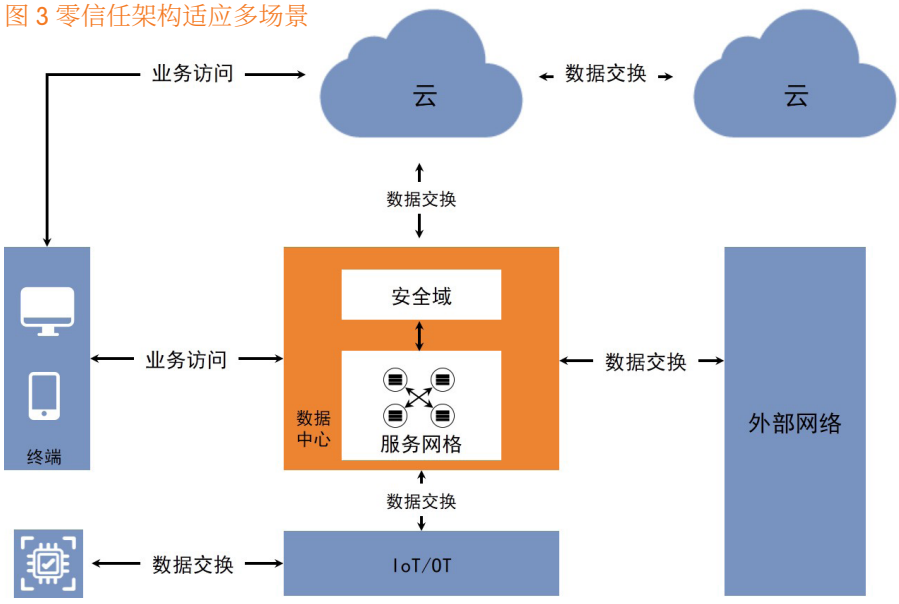
零信任架构的身份安全基础设施需要能满足现代 IT 环境下复杂、高效的管理要求，传统的静态、封闭的身份与权限管理机制已经不能满足新技术环境的要求，无法支撑企业构建零信任安全架构的战略愿景，需要足够敏捷和灵活，需要为更多新的场景和应用进行身份和权限管理。另外，为了提高管理效率，自助服务和工作流引擎等现代身份管理的关键能力也必不可少。

针对企业现有基础设施的现状，在具体方案实现上对身份安全基础设施可以灵活处理。如果企业已有较成熟的满足要求的身份基础设施，零信任架构可和现有系统进行对接，如果企业尚无身份基础设施，或其成熟度难以满足零信任架构的需求，则需要全新构建或改造优化。

2.4. 多场景适应性

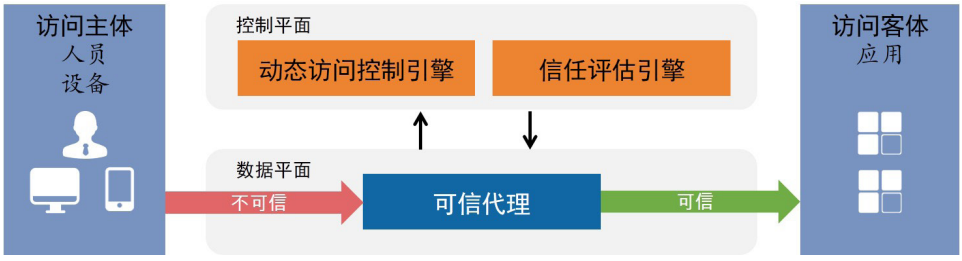
在现代 IT 环境下，业务场景是多样化的，根据典型的业务架构、访问的主客体和流量模型，可以将这些场景概括为：业务访问场景、数据交换场景和服务网格场景，零信任参考架构需要适用于每种场景，并能根据需要对多个场景进行组合，形成统一的零信任安全架构。（有关概念模型，请参见图 3。）

图 3 零信任架构适应多场景



（来源：奇安信集团，2019）

图 4 业务访问场景



（来源：奇安信集团，2019）

下文分别描述各业务场景的零信任参考架构示意图，示意图做了简化，省略了身份安全基础设施和其他安全分析平台等组件，这些组件在个场景下的差异性本文不做描述。

1) 业务访问场景

业务访问场景指用户访问业务应用的场景，也是零信任架构的主要场景，本场景存在较多子场景，比如 PC 办公场景、移动办公场景、哑终端访问场景等。不同子场景的用户、设备、应用类型均有不同，对零信任逻辑组件的实现提出了更多的能力要求。（有关概念模型，请参见图 4。）

作为访问主体的人员/用户可能是企业和组织的内部人员或员工，也可能是外部合作伙伴的人员，甚至可能是企业的客户。其次，访问主体的设备可能是 PC，也可能是移动终端，可能是企业签发的终端设备，也可能是 BYOD 设备。另外，应用类型特别是应用的访问方式也可能有差异，包括基于 HTTP 协议的 WEB 应用，也包括熟知的一些非 HTTP 协议，如 RDP、SSH 等，甚至包括一些非熟知的私有协议。

成熟的零信任解决方案需要能满足不同人员、各种设备对各种应用协议的业务访问需求，在保持相同架构的情况下，具有较高的适应性。

上述业务访问场景架构示意图并未涵盖应用内部的功能级、甚至数据级细粒度访问控制，在具体实现方案上，建议零信任架构和业务架构紧密耦合，零信任架构组件可以传递身份、信任、权限信息给业务应用，业务应用内部基于这些信息进行更细粒度的访问控制，这样，既能将零信任作为业务安全的内生能力，也能一定程度保证安全和业务各自相对独立的进行开发部署和持续演进。

2) 数据交换场景

数据交换场景是指外部应用/平台通过服务接口和企业服务进行数据交换的业务场景，大数据时代，开放协同成为信息技术发展的趋势，数据交换场景变得越来越主流。（有关概念模型，请参见图 5。）

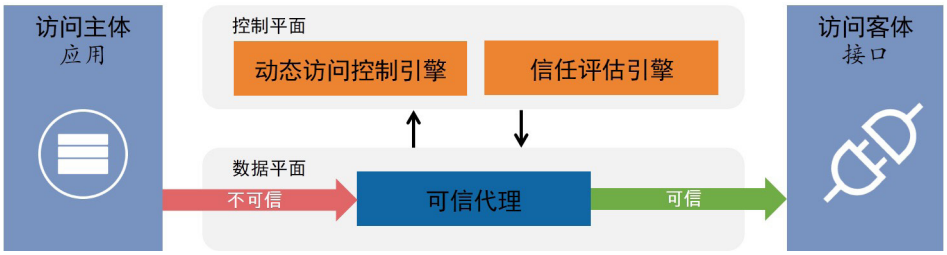
数据交换场景的零信任解决方案面临接口多样化、访问主体所运行的计算环境多样化的挑战。对可信代理而言，需要兼容各种数据交换协议或 API 接口的代理，信任评估引擎则要通过对访问主体所运行的计算环境进行数据采集和评估，同时，需要对数据交换协议进行解析以便更好的识别出异常访问行为，动态访问控制引擎也需要能做到内容级的细粒度访问控制。

另外，在数据交换场景下，和可信代理直接进行数据交换的访问主体是外部应用，而不是用户及用户终端，这种情况下，需要通过一定的技术手段实现对访问外部应用的用户及用户终端进行识别和信任评估，确保端到端的信任建立和身份感知的细粒度访问控制。

3) 服务网格场景

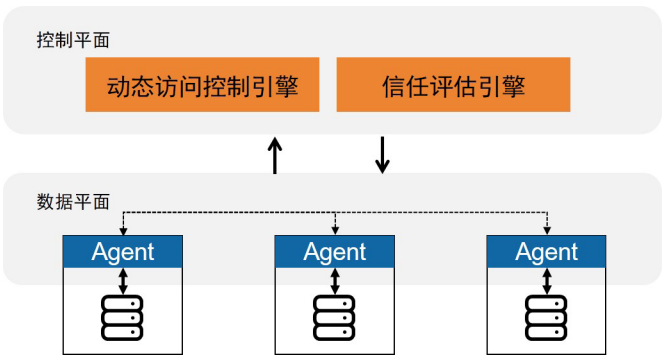
服务网格场景是指数据中心内部服务器和服务器之间的多方交互场景，随着容器编排和微服务技术的大量采用，服务网格的场景越来越演化为数据中心工作负载之间的网状访问控制。（有关概念模型，请参见图 6。）

图 5 数据交换场景



（来源：奇安信集团，2019）

图 6 服务网格场景



（来源：奇安信集团，2019）

服务网格场景的零信任方案一般不采用独立形式的可信代理作为数据平面组件，而是将其分散，通过在各个服务器、工作负载运行载体上部署可信代理 Agent，对相互之间的访问请求进行接管并和控制平面进行联动。服务网格场景零信任解决方案因为面临节点数量多，访问控制规则复杂等现实困难，对动态访问控制引擎和信任评估引擎都提出了较高要求。

服务网格场景也是对业务架构嵌入最深的场景，需要结合服务网格或容器编排技术进行构建，最好是在业务平台构建的同时将零信任架构进行统一规划，实现真正的内生安全。

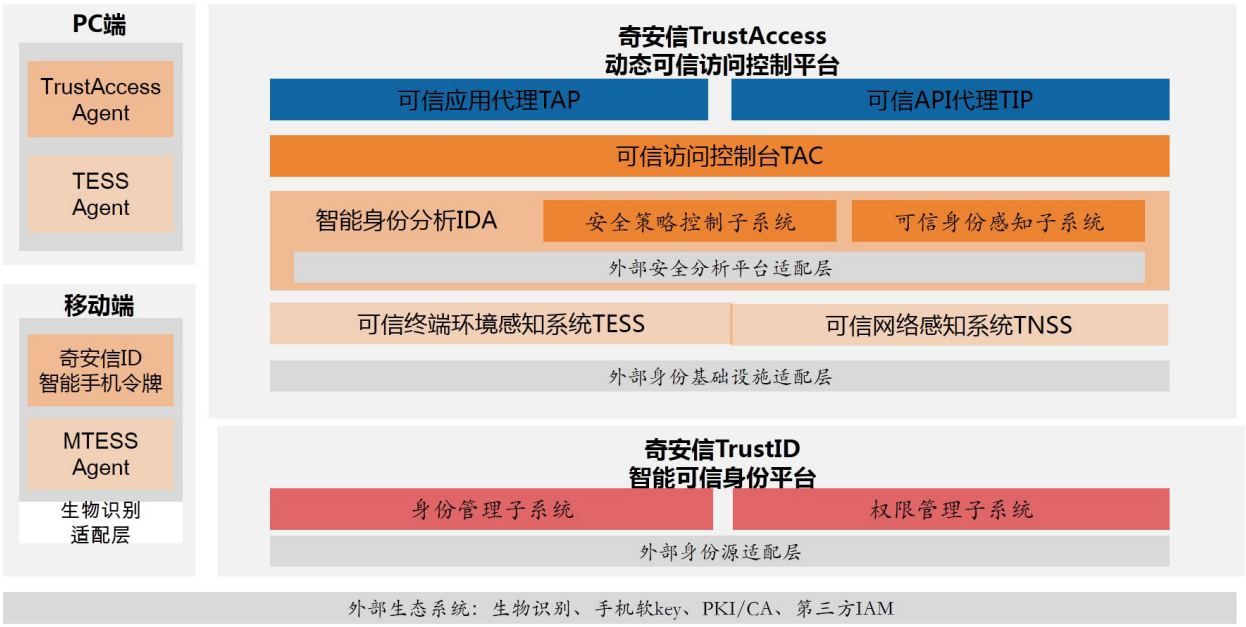
3. 零信任安全解决方案

本节以奇安信零信任安全解决方案为例，对零信任参考架构的具体实践要点进行解读，奇安信一直保持对零信任的高度关注，奇安信零信任安全解决方案基于零信任参考模型进行设计，充分利用国内外先进技术成果，结合国内典型的业务及安全现状进行完善优化，目前已经过国内大型部委和央企进行大量实践验证并得到广泛认可，具有极强的先进性和可行性。

3.1. 核心产品体系

奇安信零信任安全解决方案主要包括：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，如图 7 所示。奇安信零信任安全解决方案中，动态可信访问控制平台和智能可信身份平台逻辑上进行解耦，当客户现有身份安全基础设施满足零信任架构要求的情况下，可以不用部署智能可信身份平台，通过利用现有系统可降低建设成本。

图 7 奇安信零信任安全解决方案



（来源：奇安信集团，2019）

1）奇安信 TrustAccess 动态可信访问控制平台

奇安信 TrustAccess 提供零信任架构中动态可信访问控制的核心能力，可以为企业快速构建零信任安全架构，实现企业数据的零信任架构迁移。

TrustAccess 的核心组件包括：可信应用代理 TAP、可信 API 代理 TIP、可信访问控制台 TAC、智能身份分析系统 IDA、可信终端环境感知系统 TESS 和可信网络感知系统 TNSS。

- **可信应用代理系统 TAP**

可信应用代理系统 TAP 是零信任参考架构中的可信代理在业务访问场景的产品实现。

针对企业应用级访问控制需求，实现了应用的分层安全接入、一站式应用访问、应用单点登录、应用审计等能力。

- **可信API代理系统 TIP**

可信 API 代理系统 TIP 是零信任参考架构中的可信代理在数据交换场景的产品实现。

针对 API 服务的安全保护需求，实现了 API 接口的统一代理、访问认证、数据加密、安全防护、应用审计等能力。

- **可信访问控制台 TAC**

可信访问控制台 TAC 是零信任参考架构中动态访问控制引擎的产品实现。

TAC 为 TAP/TIP 提供自适应认证服务、动态访问控制和集中管理能力，针对企业的各个业务访问场景，实现了自适应认证服务、访问控制策略统一配置管理、WEB 应用和 API 服务集中管理、动态授权、风险汇聚关联、应用审计等功能。

- **智能身份分析系统 IDA**

智能身份分析系统 IDA 是零信任参考架构中信任评估引擎的产品实现。

IDA 基于身份及权限信息、TAP/TIP/TAC 访问日志、可信环境感知上报的属性和风险评估、其他外部分析平台上报的日志及事件进行综合风险关联判定，利用大数据分析和人工智能技术，构建信任评估模型进行持续信任评估，为 TAC 提供信任等级作为决策依据。

- **可信终端环境感知系统 TESS**

可信终端环境感知系统 TESS 提供各种场景的终端环境的安全状态和环境感知，为 IDA 提供实时的终端可信度的判断依据，是 IDA 的重要数据源。

- **可信网络环境感知系统 TNSS**

可信网络环境感知系统 TNSS 提供网络环境的安全状态和环境感知，为 IDA 提供实时的网络可信度的判断依据，是 IDA 的重要数据源。

2) 奇安信 TrustID 智能可信身份平台

奇安信 TrustID 智能可信身份平台是零信任参考架构身份安全基础设施的产品实现，是一种现代身份与权限管理系统。

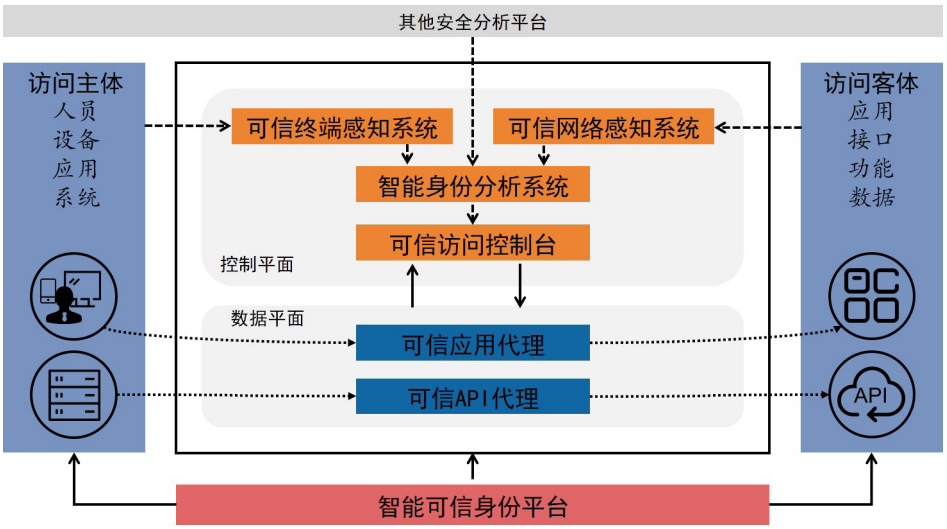
TrustID 可为企业提供更高级、更灵活的现代身份与权限管理能力，当 TrustAccess 自带的基础身份和权限管理能力，或企业现有的身份基础设施无法满足企业的管理需求时，可借助 TrustID 对身份与权限管理方面的能力进行提升，达到零信任架构对身份安全基础设施的能力要求。除了为 TrustAccess 服务，TrustID 也可为企业的业务系统和其他需要身份、认证、授权的场景提供身份及权限基础服务。

奇安信 TrustID 也支持对接企业现有的外部身份源系统，包括 PKI、4A、AD 等，通过将企业现有的身份源进行汇聚和同步，形成完善的身份生命周期管理能力，为 TrustID 提供身份基础设施服务。

3) 奇安信零信任安全解决方案与参考架构的关系

奇安信零信任安全解决方案在零信任参考架构的基础上对产品组件进行了拆分和扩展，但在总体架构上保持了高度一致，将其产品组件映射到零信任参考架构，如图 8 所示：

图 8 奇安信零信任安全解决方案与参考架构的关系



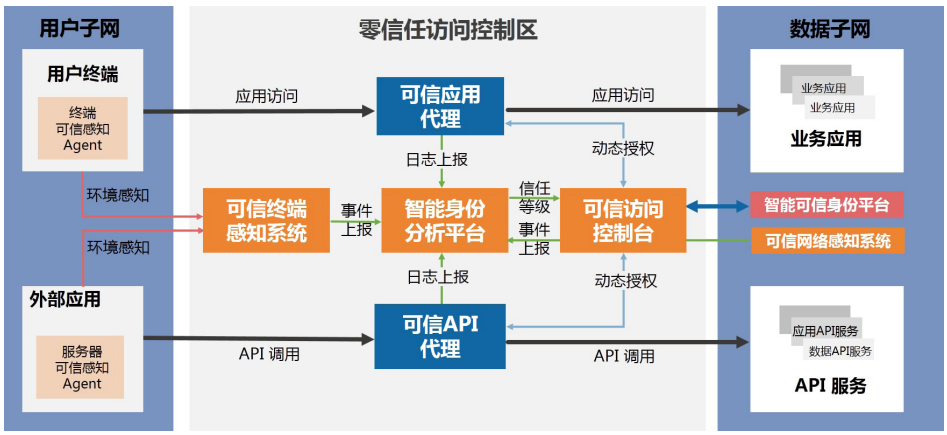
（来源：奇安信集团，2019）

另外，奇安信零信任安全解决方案和奇安信丰富的安全产品和平台之间可以实现联动，比如，和奇安信的移动安全解决方案联动，可以实现强大的移动零信任解决方案；和奇安信的数据安全解决方案联动，可以实现数据访问场景的零信任解决方案；和奇安信云安全管理平台联动，可以实现云及虚拟化场景的零信任解决方案。

3.2. 典型场景方案

下面以一个典型应用场景为例，描述奇安信零信任安全解决方案的逻辑原理。此应用场景数据子网需要保护的资源包括业务应用和 API 服务，用户/外部平台子网的用户终端需要访问业务应用，外部应用需要通过接口调用 API 服务，方案逻辑图如图 9 所示。

图 9 典型场景方案



（来源：奇安信集团，2019）

在此方案中，通过在用户子网和数据子网之间部署逻辑的零信任访问控制区构建端到端的零信任解决方案。通过可信应用代理接管所有的用户终端业务访问请求，通过可信 API 代理接管所有的外部应用 API 调用请求，所有的访问请求通过可信访问控制台进行身份验证及动态授权。可信终端感知系统持续对终端进行感知和评估，可信网络感知系统持续对网络流量进行感知和评估，并生成安全事件上报至智能身份分析平台，智能身份分析平台综合访问日志信息、安全事件信息、身份与权限信息进行关键信息和信任评估，为可信访问控制台输出信任等级作为权限判定或撤销的依据。

4. 零信任迁移方法论

零信任架构作为一种全新的安全架构，和企业现有的业务情况、安全能力、组织架构都有一定的关系，零信任迁移不可能一蹴而就，需要遵循一定的方法论，结合企业现状，统一目标和愿景后进行妥善规划并分步建设。

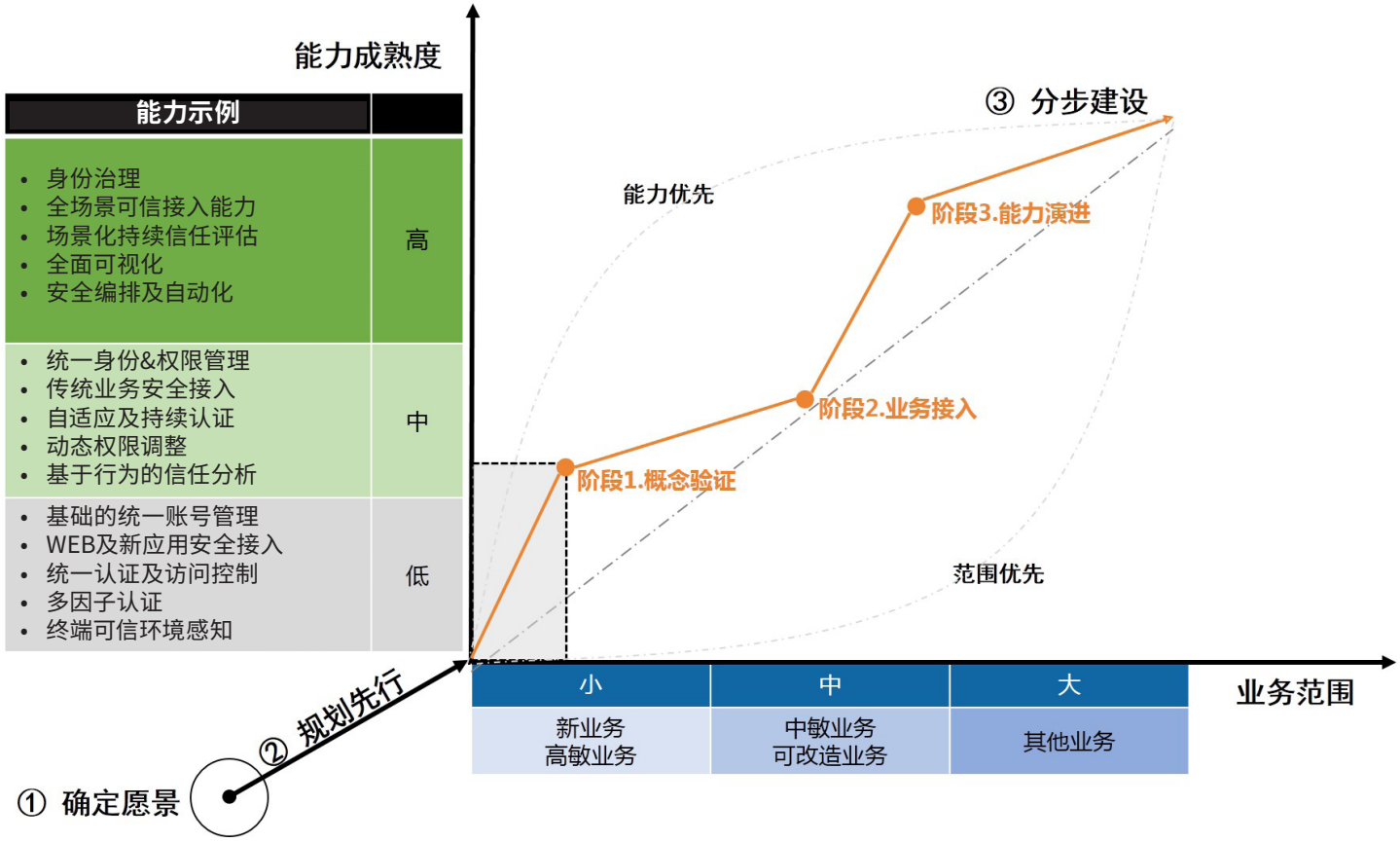
零信任迁移方法如图 10 所示：

4.1. 确定愿景

零信任的建设和运营需要企业各干系方积极参与，可能涉及到安全部门、业务开发部门、IT 技术服务部门和 IT 运营部门等。企业数字化转型的关键决策者应该将基于零信任的新一代安全架构上升到战略层面，确定统一的愿景，建议成立专门的组织（或虚拟组织）并指派具有足够权限的人作为负责人进行零信任迁移工作的整体推进，建议至少由 CIO/CSO 或 CISO 级别的人员在公司高层决策者的支持下推动零信任项目。

需要特别注意的是，在很多企业安全部门话语权并不高，安全项目往往受到业务部门的阻碍甚至反对，零信任项目的发起者一定需要从零信任的业务价值出发，说服业务部门和公司的高层决策者。

图 10 零信任迁移方法



（来源：奇安信集团，2019）

另外，在零信任的迁移过程中，需要更多部门和人员的配合和支持，特别是大量的普通员工，他们作为零信任项目的最终使用者，他们的支持至关重要，建议通过公司级的持续的安全文化活动加强全体人员对零信任安全的认可，这一点也至关重要。

4.2. 规划先行

零信任架构是安全思维和安全架构进化的必然，聚焦身份、业务、信任和动态访问控制等维度的安全能力，而这些能力业务密不可分，所以零信任天生就应该是一种内生安全。零信任的建设路径需要结合现状和需求，将零信任的核心能力和组件内嵌入业务体系，构建自适应内生安全机制，建议在业务建设之初进行同步规划，进行安全和业务的深入聚合。

规划的目的在于厘清形状，确定路径。对于零信任架构而言，需要从两个维度进行梳理和评估，一是能力成熟度维度，一是业务范围维度。

零信任架构的关键能力包括：以身份为基石、业务安全访问、持续信任评估和动态访问控制，每一项关键能力又可以划分为若干子能力，企业需要评估当前具备的安全能力，并基于风险、安全预算、合规要求等信息，确定安全能力建设的优先级。

零信任架构最终需要覆盖企业的所有资源，为其构建保护面。企业资源包括但不限于：应用、接口、功能和数据等。在规划阶段，需要确定迁移至零信任的业务优先级。一般来说，新建业务和核心业务作为第一优先级考虑。

对安全能力现状、需求，业务现状、优先级进行梳理后，需要进一步对核心业务的暴露面进行梳理，对各暴露面的访问主体、访问主体的权限进行梳理，确定初步的总体建设路径及第一阶段建设方案。

4.3. 分步建设

规划完成后进入建设阶段，根据规划的思路导向，建设阶段的划分依各企业而各有不同。如果是能力优先型建设思路，需要针对少量的业务构建从低到高的能力，通过局部业务场景验证零信任的完整能力，然后逐步迁移更多的业务。范围优先型则先在一个适中的能力维度上，迁移尽量多的业务，然后再逐步对能力进行提升。两种建设思路各有侧重，依据企业的具体情况，在规划阶段选定思路和建设阶段的划分。

一种建议的分步思路主要包含三个阶段：概念验证、业务接入和能力演进。首先在一个较小业务范围内，构建中等的零信任安全能力，对整体方案进行验证；方案验证完成后，对验证过程的一些局部优化点进行能力优化，并同时迁入更多的业务进一步验证方案并发现新的安全需求；最后，基于验证结果规划后续能力演进阶段，逐步有序的提升各方面的零信任能力。

零信任架构作为一种全新的安全思路，是持续演进的过程，需要基于业务需求、安全运营现状、技术发展趋势等对零信任能力进行持续完善和演进。

5. 结束语

零信任架构对传统的边界安全架构思想重新进行了评估和审视，并对安全架构思路给出了新的建议：默认情况下不应该信任网络内部和外部的任何人、设备、系统和应用，而是应该基于认证、授权和加密技术重构访问控制的信任基础，并且这种授权和信任不是静态的，它需要基于对访问主体的信任评估进行动态调整。零信任架构是一种全新的安全理念和架构，认为不应该仅仅在企业网络边界上进行粗粒度的访问控制，而是应该对企业的人员、设备、业务应用、数据资产之间的所有访问请求进行细粒度的访问控制，并且访问控制策略需要基于对请求上下文的信任评估进行动态调整，是一种应对新型 IT 环境下已知和未知威胁的“内生安全”机制。

来源：奇安信集团

Gartner 的调研报告

零信任网络访问指南

零信任网络接入 (ZTNA) 取代传统技术，需要企业给予员工和合作伙伴过度信任才能实现连接和合作。安全和风险管理负责人应该为面向员工/合作伙伴的应用程序规划 ZTNA 试点项目。

重要发现

- 数字业务转型要求可以随时随地使用任何设备通过互联网从多个生态系统访问系统、服务、API、数据和流程。这就扩大了攻击者的可攻击范围。
- 安全访问功能必须进化以适应云端，这是用户、应用程序和服务的转移方向。许多软件定义的边界产品都是基于云的。
- 基于 IP 地址和位置建立网络访问信任将不再现实。
- 零信任网络访问可提供自适应、识别身份的精确访问。不再将网络位置当作一种优势，以消除过度的隐式信任。
- ZTNA 提高了灵活性、敏捷性和可扩展性，使数字生态系统能够在不将服务直接暴露于互联网的情况下工作，从而降低分布式拒绝服务攻击风险。
- 尽管更换虚拟专用网络是采用 ZTNA 的常见驱动因素，但 ZTNA 还可以提供允许非托管设备安全访问应用程序的解决方案。

建议

负责安全网络访问的安全和风险管理负责人应：

- 不仅仅使用 IP 地址和网络位置作为访问信任的替代品。只有在经过足够的用户和设备身份验证后，才可将 ZTNA 用于应用程序级的访问。
- 更换面向员工和合作伙伴的应用程序（其服务直接暴露给互联网连接）的设计。使用一项需要作为用例供合作伙伴访问的数字业务服务试行 ZTNA 部署。
- 针对高风险用例，逐步淘汰传统的基于 VPN 的访问，并开始逐步引入 ZTNA。这样可以减少支持广泛部署的 VPN 客户端的持续需求，并引入了无客户端身份识别和设备感知访问。支持员工的非托管设备。
- 选择将身份保证扩展到单个因素之外的 ZTNA 产品/服务，这是对基于上下文/自适应访问控制的 ZTNA 原则的重要补充。

战略规划设想

到 2022 年，在向生态系统合作伙伴开放的新数字业务应用程序中，80% 将通过零信任网络访问 (ZTNA) 进行访问。

到 2023 年，60% 的企业将逐步淘汰大部分远程访问虚拟专用网络 (VPN)，转而使用 ZTNA。

到 2023 年，40% 的企业将采用 ZTNA 用于本调研报告中描述的其他用例。

市场定义

ZTNA 也被称为软件定义边界 (SDP)，它围绕一个或一组应用程序创建基于身份和上下文的逻辑访问边界。应用程序不会被发现，并且通过信任代理将访问权限限制为一组命名实体。代理验证指定参与者的身份、上下文和策略遵守情况，然后才会允许访问。这样，将应用资产从公众的视线中移除，大大减少了可攻击范围。

市场描述

在数字业务领域，“内部意味着受信任”和“外部意味着不受信任”的旧安全观念被打破，这就要求随时随地能从任何设备访问可能不在本地数据中心“内部”的服务。同样，旧模型期望所有程序员都是安全工程师，能构建本质安全的网络应用程序，并结合复杂的身份验证和访问控制。这些在今天已经不适用了。

新模型提出了一种方法，在这种方法中，信任代理调节应用程序和用户之间的连接。ZTNA 对安全机制进行了抽象和集中，以便安全工程师和人员都能对其负责。ZTNA 以默认的零信任拒绝状态开始。它可根据身份以及其他属性和情况（例如时间/日期、地理位置和设备状态）授予访问权限，并自适应地提供当时所需的适当信任。结果是提供一个具有更高灵活性和更好监控效果的、恢复能力更强的环境。ZTNA 将吸引希望以适应性强且安全的方式与其数字业务生态系统、远程员工和合作伙伴进行连接和协作的组织。

ZTNA 提供对资源的受控访问，从而减少可攻击范围。ZTNA 提供的隔离改善了连接性，无需将应用程序直接暴露给互联网。互联网成为一种不受信任的传输方式，对应用程序的访问需要通过中介进行。中介可以是由第三方供应商控制的云服务，也可以是自托管服务。在这两种情况下，用户成功通过身份验证后，进入应用程序的流量始终会通过中介程序传输。

如 Gartner 的持续适应性风险和信任评估（CARTA）框架所述，在许多情况下，实体行为是否存在异常活动会持续受到监控。从某种意义上说，ZTNA 创建了仅包含用户、设备和应用程序的个性化“虚拟边界”。ZTNA 使用户体验规范化，消除了连接或不连接公司网络时存在的访问差异。

市场方向

自从在 2014 年云安全联盟峰会上引入了软件定义边界 (SDP) 的初始规范以来，ZTNA 的概念一直在发展。最初的 SDP 规范仅针对基于 Web 的应用程序，并且对该规范的更新已滞后，但预计将于 2019 年晚些时候发布。基于这个初始规范的商业产品以及基于谷歌 BeyondCorp 零信任网络愿景的产品大致是可用的，但也仅限于支持 Web 的应用程序。此外，大量使用其他方法且不限于 Web 应用程序的替代商业产品已经进入市场。

ZTNA 市场仍处于初期阶段，但正在快速发展。它激起一些寻求更灵活的其他 VPN 替代方案的组织的兴趣，也激起了那些寻求对本地和云中的应用程序进行更精确的访问和会话控制的组织的兴趣。ZTNA 供应商在不断吸引风险投资资金。反过来，这也鼓励新的初创公司进入市场并寻求差异化方法。这一市场上的并购 (M&A) 活动已经开始，已有三家初创供应商被大型的网络、电信和安全供应商收购。

尽管 ZTNA 产品的技术方法有所不同，但是它们提供的基本价值主张大致相同：

- 消除应用程序和服务在公共互联网上的直接可见性。
- 只有在对身份、设备运行状况（强烈鼓励）和上下文进行评估之后，才允许指定用户对特定应用程序进行精确（“及时”和“刚好够”）访问。
- 使访问独立于用户的物理位置或设备的 IP 地址（除非政策禁止，例如世界的某些特定区域）。访问策略基于用户、设备和应用程序身份。
- 仅授予对特定应用程序的访问权限，而不授予底层网络的访问权限。这样可以限制对所有端口和协议或所有应用程序（其中一些可能是用户无权访问的）的过度访问需求。
- 提供网络通信的端到端加密服务。
- 提供可选的对流量流的检查，以检查敏感数据处理和恶意软件形式的过度风险。
- 支持可选的对会话的监控，以指示异常活动、持续时间或带宽需求。
- 为访问应用程序提供一致的用户体验 —— 无需客户端或使用 ZTNA 客户端，而不管网络位置如何。

Gartner 确定了多种供应商在为市场开发产品和服务时所采用的不同方法。

客户端启动的 ZTNA

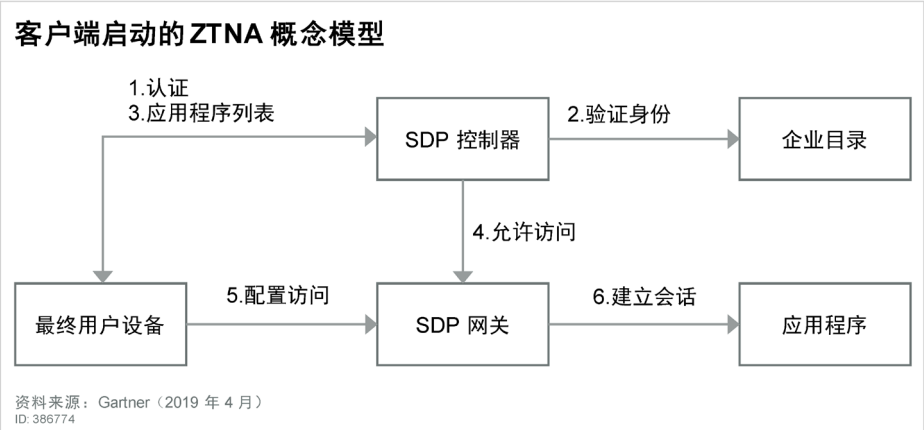
这些产品更加严格遵从最初的云安全联盟 (CSA) SDP 规范。安装在授权设备上的代理程序将有关其安全情况的信息发送到控制器。控制器提示设备上的用户进行身份验证，并返回允许访问的应用程序列表。在对用户和设备进行身份验证之后，控制器将通过网关调配来自设备的连接，从而屏蔽服务使其无法直接通过互联网进行访问。这种屏蔽可保护应用程序免受分布式拒绝服务 (DDoS) 攻击。

在控制器建立连接后，有些产品仍保留在数据路径中，另一些产品则自行删除。由于需要安装代理程序，因此要在非托管设备上实现这种方法是很困难的，甚至是不可能的。在某些情况下，第三方移动威胁防御 (MTD) 产品（与全面的设备管理相比，用户可能更愿意接受）可以为信任代理提供状态评估。（有关概念模型，请参见图 1。）

服务启动的 ZTNA

这些模型更接近谷歌的 BeyondCorp 愿景。连接器与应用程序安装在同一网络，用于建立并维护与供应商云的出站连接。用户向供应商进行身份验证以访问受保护的应用程序。然后，供应商通常对企业身份管理产品进行身份验证。应用程序流

图 1
客户端启动的 ZTNA 概念模型



量通过供应商的云传输，该云对通过代理的直接访问进行隔离。企业防火墙不需要为入站流量开放。但是，供应商的网络成为必须评估的网络安全的另一要素。

这种模型的优势在于，最终用户的设备上不需要安装代理程序，因此，对于非托管设备来说这是一种有吸引力的方法。缺点是应用程序的协议必须基于 HTTP/HTTPS，因而限制了访问 Web 应用程序和协议的方法，例如通过 http 进行安全壳 (SSH) 或远程桌面协议 (RDP) 访问。（有关概念模型，请参见图 2。）

有些供应商提供两种选择。这使企业能够根据需要进行混合和匹配，以解决特定的用例。

市场分析

互联网的设计初衷是为了方便地连接事物，而不是阻止连接。互联网使用固有的弱标识符（特别是 IP 地址）进行连接。如果您拥有一个 IP 地址和一个路由，那么您就可以连接其他 IP 地址并与之通信，而这些 IP 地址从未被设计成需要身份验证机制。复杂的身份验证问题由更高层级的堆栈（通常是操作系统和应用程序层）处理。对于网络连接，这种默认允许状态会产生过多的隐式信任。

攻击者则会滥用这种信任。最早连接到公共互联网的公司很快发现，他们需要一个内部网络连接到互联网的分界点。这最终创造了一个价值数十亿美元的周边防火墙市场。内部的网络系统是“受信任的”，并且可以相互自由通信。外部系统是“不受信任的”，在默认情况下，与外部的入站或出站通信是被阻止的。如果需要与外部进行通信，则需要在防火墙上设置一系列例外（即漏洞），维护和监控起来既困难又麻烦。

这种受信任/不受信任的网络安全模型是一种相对粗略和简单的控制，不过最初它是有效的。但是，它会（在内部）造成过度信任，被外部攻击者滥用（一旦他们穿透防御并到达内部）。当需要从外部访问我们的系统和服务时，我们通常会执行以下两项操作之一。对于某些用户，我们创建一个 VPN 以允许用户通过防火墙并连接到内部网络。一旦进入“内部”，VPN 连接将被视为可信任。

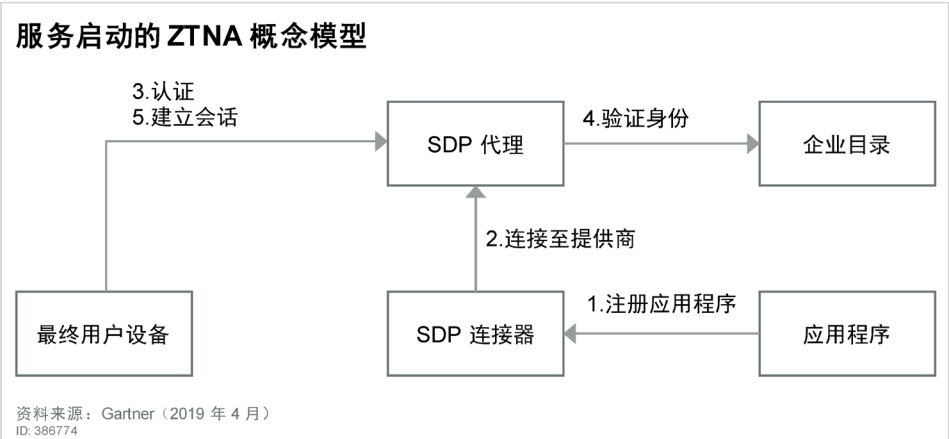
或者，我们将服务的前端置于可直接连接互联网的网段（称为隔离区 [DMZ]），以便用户可以访问该服务。两种操作都造成了过度信任，并且几乎没有横向运动限制，因而导致了潜在风险。在使用 VPN 的情况下，拥有凭据访问权限的攻击者现在就可以访问我们的网络。（Target HVAC 泄漏就是一个例子。）同样，如果该服务在 DMZ 中公开，即使它受到 web 应用程序防火墙 (WAF) 的保护，互联网上的任何人（包括所有攻击者）也可以看到它。

过度的网络信任会导致过多的潜在风险。这将不可避免地被利用，从而导致违规行为，并带来法律、财务和监管方面的风险。网络连接（即使是使用“ping”或查看服务器的权利）也不应该是一项权利；它应该基于信任来获得。Gartner 认为，现在是时候将服务和应用程序与公共互联网的危险隔离开来，并且仅在任何给定情况下才提供对所需应用程序的隔离访问。互联网连接服务的数量急剧增加，并且服务和用户可以位于几乎任何 IP 地址的可能性也越来越大，这加剧了旧模型的弱点。

优点和用途

ZTNA 的优势是显而易见的。与传统的 VPN 类似，ZTNA 环境中提供的服务在公共互联网上不再可见，因此可以免受攻击者的攻击。此外，ZTNA 在用户体验、敏捷性、适应性和易于策略管理方面也具有明显的优势。而基于云的 ZTNA 产品，还具有可扩展性和易用性的优势。ZTNA 支持不适合传统访问方法的数字业务转换场景。由于数字化转型的努力，大多数企业在企业外部将拥有比在内部更多的应用程序、服务和数据。基于云的 ZTNA 服务将安全控件放在用户和应用程序所在的云端。一些大型 ZTNA 供应商已在全球范围内投资了数十个接入点，用以提供低延迟的用户/设备访问。

图 2
服务启动的 ZTNA 概念模型



资料来源：Gartner（2019 年 4 月）
ID: 386774

有几种用例适用于 ZTNA：

- 向协作的生态系统成员（例如分销渠道、供应商、承包商或零售店）开放应用程序和服务，不需要 VPN 或 DMZ。访问更紧密地耦合到应用程序和服务。
- 规范用户访问应用程序的体验——ZTNA 消除了在公司网络内外的区别。
- 在不信任运营商或云供应商的情况下，一直对端点进行加密。
- 为 IT 承包商和远程或移动员工提供特定于应用程序的访问，以替代基于 VPN 的访问。
- 在并购活动期间扩展对被收购组织的访问，而无需配置站点到站点 VPN 和防火墙规则。
- 允许世界上潜在危险地区的用户以减少或消除源自此类地区风险的方式与应用程序和数据进行交互——注意对强身份和端点保护的要求。
- 在网络或云端隔离高价值的企业应用程序，以减少内部威胁并影响管理访问权限的分配。
- 在个人设备上对用户进行身份验证——ZTNA 可以通过减少全面管理要求并启用更安全的直接应用程序访问来提高安全性并简化自带设备 (BYOD) 程序。
- 创建物联网 (IoT) 设备的安全飞地或在 IoT 网段上创建用于连接的虚拟设备连接器。
- 恶意网络上的隐蔽系统（例如本来是面向公共互联网的系统）用于协作。
- 使 SaaS 应用程序能够连接回企业系统，和需要 SaaS 应用程序与企业本地或基于基础设施即服务 (IaaS) 的服务进行交互的流程的数据。

风险

尽管 ZTNA 大大降低了总体风险，但并没有完全消除所有风险，如以下示例所示：

- 可信任代理有可能会成为任何类型故障的单点。当 ZTNA 服务关闭时，使用 ZTNA 的完全隔离的应用程序将停止工作。精心设计的 ZTNA 服务包括具有多个入口和出口点的物理和地理冗余，以最大程度地减少中断可能对整体可用性的影响。此外，可以将供应商的 SLA（或缺乏 SLA）作为一个指标，用以评估其产品的稳健性。支持具有 SLA的供应商，尽量减少业务中断。
- 攻击者可能会试图破坏信任代理系统。尽管可能性很小，但风险并不为零。基于公共云或主要互联网运营商的 ZTNA 服务受益于供应商强大的租户隔离机制。不过，租户隔离的崩溃将使攻击者能够渗透到供应商客户的系统中，并在它们内部和之间横向移动。受破坏的信任代理应立即故障切换到冗余代理。如果它无法进行故障切换，那么它应该进行故障关闭——也就是说，如果它不能转移滥用，则应该断开互联网连接。应选择可以采取这种立场的供应商。
- 受损的用户凭据可能使本地设备上的攻击者可以观察和窃取该设备中的信息。将设备身份验证与用户身份验证相结合的 ZTNA 架构在一定程度上遏制了这种威胁，阻止了攻击传播到设备本身之外。我们建议尽可能使用更强的访问身份验证。
- 一些 ZTNA 供应商选择将开发重点放在仅支持 Web 应用程序协议（HTTP / HTTPS）上。通过 ZTNA 服务承载旧版应用程序和协议可能会变得更加困难。
- 市场在不断变化，较小的供应商可能会消失或被收购。

评估因素

在评估 ZTNA 技术时，需要提出以下关键问题：

- 供应商是否要求安装端点代理程序？支持哪些操作系统？支持哪些移动设备？在存在其他代理程序的情况下，代理程序的表现如何？
- 产品是否支持单包身份验证 (SPA) 作为对信任代理的初始身份验证形式？如果第一次通信尝试未包含专用的加密数据包，SPA 允许代理忽略任何尝试。
- 该产品是否能够在不需要统一端点管理 (UEM) 工具的情况下对设备执行安全状态评估（操作系统版本、补丁程序级别、密码和加密策略等）？是否提供了在非托管设备上实现此功能的选项？
- 该产品是否与 UEM 供应商集成，或者本地代理程序能否将设备的运行状态和安全状况确定为访问决策的一个因素？ZTNA 供应商与哪些 UEM 供应商合作？

- 信任代理支持哪些身份验证标准？是否可以与本地目录或基于云的身份服务集成？信托代理是否与组织的现有身份提供商集成？信任代理是否支持多因素身份验证 (MFA) 的通用选项？提供者是否可以为管理员强制实施严格的用户身份验证？

- 是否有用户和实体行为分析 (UEBA) 功能可以识别在受 ZTNA 保护的环境中发生异常的时间？

- 某些 ZTNA 产品部分或全部以云服务的形式交付。这是否满足组织的安全和驻留要求？供应商是否通过了一项或多项第三方认证，例如 SOC 2 或 ISO 27001？

- 供应商在全球的入口和出口点（称为边缘位置和/或接入点）的地域差异如何？供应商使用哪些边缘/物理基础设施提供商或主机托管设施？

- 当 ZTNA 服务受到持续攻击时，供应商会采取什么技术行为？服务是失效关闭（从而阻止数字业务合作伙伴访问企业服务）还是失效打开？是否可以为特定的企业应用程序有选择地选择失效关闭或失效打开？如果需要失效打开，不要忘记添加其他防御层以保护不再受 ZTNA 服务保护的应用程序。

- 该产品是否仅支持 Web 应用程序，或者旧版应用程序是否也能获得相同的安全优势？

- 供应商选择了哪些算法和密钥长度？供应商获得了哪些第三方认证？供应商的产品描述是否显示出他们对当代加密技术的理解，还是将其描述成好到不真实的加密“万能药”？

- 用户和设备通过身份验证后，信任代理是否仍驻留在数据路径中？这种方法值得考虑。保留在数据路径中的信任代理提供了更大的可见性，并且可以监视异常和可疑的活动。但是，它们可能会成为瓶颈或单点故障。包含故障切换支持的设计可以缓解这种担忧，但可能容易受到试图绕过检查的 DDoS 攻击。

- 供应商是否可以针对不适当的敏感数据处理、恶意软件检测和异常行为对会话流和内容进行检查？

- 部分或全部隐藏，或者允许或禁止入站连接，在隔离应用程序安全要求中所占比例如何？也许给予内容分发网络 (CDN) 的最低保护就足够了。不同的企业应用程序可能有不同的要求。

- 供应商是否有一个漏洞奖励计划，并有一个可靠的、负责任的公共或私人信息披露政策？对于软件供应商而言，不断测试和消除产品漏洞至关重要。应选择积极这样做的供应商。

ZTNA 替代方案

有几种替代 ZTNA 的方法：

- 传统的 VPN 仍然很流行，它们可能无法为公开的服务提供足够的风险管理，而且由于数字业务的动态性，它们可能也难以管理。需要设备和用户身份验证的始终在线式 VPN 与 ZTNA 模型一致；但基本网络访问 VPN 则不是。将安全需求纳入 VPN 模型和用户满意度期望。对于第三方对企业系统的特权访问，特权访问管理 (PAM) 工具可能是 VPN 的有用替代方法。

- 通过基于反向代理的 WAF 公开 Web 应用程序则是另一种选择。使用 WAF 即服务（即云 WAF）后，流量会通过供应商的 WAF 服务进行检查，然后才交付到目的地。为了避免误报或潜在的应用程序故障，与其他 WAF 一样，云 WAF 通常需要一些时间来测试和调整规则。由于受保护的服务对公共互联网上的攻击者仍然可见，因此隔离仅限于 WAF 的强度。但是，面向合作伙伴和员工的应用程序通常不适合使用 WAF。

- 选择保留现有设计模式并在传统 DMZ 中公开数字业务应用程序仍然是备选方案。但是，DMZ 对现代攻击（通常是反向代理 WAF）只提供了有限的隔离。此外，DMZ 仍会使所有攻击者能发现该应用程序。

- 远程浏览器隔离产品提供了另一种选择，专门用于隔离支持 Web 的应用程序访问。在这里，浏览器会话本身是由终端用户的设备（通常是在服务中）从企业网络（例如，基于云的远程浏览器服务）呈现的，在两端提供隔离。

- CDN 可以吸收 DDoS 攻击，降低机器人攻击的噪声和威胁，并防止网站遭到破坏。但是，它们不提供应用程序级别的保护，也不提供匿名性——攻击站点的攻击者可以发现站点受到 CDN 保护，并可能试图利用 CDN 中存在的漏洞。许多 CDN 都包含基本的云 WAF。

- 尽管 ZTNA 在这里也可以发挥作用，不需要完全交互式互联网连接但只向公共互联网公开 API 的应用程序可以受到 API 网关的保护。API 网关强制执行身份验证，验证授权并协调应用程序 API 的正确使用。如果应用程序缺乏确

保 API 安全性的机制，则这项功能会特别有用。大多数 API 网关还通过本地监控工具或与流行的安全信息和事件管理 (SIEM) 工具集成来公开所有活动的日志。支持与企业目录和单点登录 (SSO) 协议集成的 API 网关，或改用 ZTNA 服务。

- 可以采用完整的 IaaS。当 ZTNA 或其他隔离措施不够好时，将应用程序完全移出企业则是最好的选择。许多建议的隔离机制可用于放置在云中的工作负载，并且更多地被设计用于提供初步保护，而不是企业隔离。目标转移至保护应用程序和数据，减少对隔离的关注。但是，这仍然使系统容易受到攻击，特别是如果在云中复制了旧版的 DMZ 架构。

代表性供应商

本市场指南中列出的供应商是非详尽的。此部分旨在加深对该市场及其产品的认识。

市场简介

供应商以以下两种方式之一提供 ZTNA 产品和服务：

- 作为云服务提供
- 作为独立产品提供，由客户负责支持

与独立产品相比，即服务产品（请参见表 1）所需的设置和维护更少。即服务产品通常需要在终端用户或服务端进行预配，并通过供应商的云路由流量以执行策略。独立产品（请见表 2）要求客户部署和管理产品的所有要素。此外，一些主要的 IaaS 云提供商还为其客户提供 ZTNA 功能。

表 1. ZTNA 即服务的代表性供应商

供应商	产品或服务名称
Akamai	Enterprise Application Access（企业应用程序访问）
Cato Networks	Cato Cloud（Cato 云）
思科	Duo Beyond（由思科收购）
CloudDeep Technology（仅限中国）	DeepCloud SDP
Cloudflare	Cloudflare Access（Cloudflare 访问）
InstaSafe	Secure Access（安全访问）
Meta Networks	Network as a Service Platform（网络即服务平台）
New Edge	Secure Application Network（安全应用网络）
Okta	Okta 身份云（收购 ScaleFT）
Perimeter 81	Software Defined Perimeter（软件定义边界）
SAIFE	Continuum
赛门铁克	Luminate 安全访问云（由赛门铁克收购）
Verizon	Vidder Precision Access （收购）
Zscaler	Private Access（专用访问）
资料来源：Gartner（2019 年 4 月）	

表 2. 独立 ZTNA 产品代表性供应商

供应商	产品或服务名称
BlackRidge Technology	Transport Access Control（传输访问控制）
Certes Networks	Zero Trust WAN（零信任 WAN）
Cyxtera	AppGate SDP
Google Cloud Platform (GCP)	云身份感知代理（云 IAP）
Microsoft （仅 Windows 系统）	Azure AD Application Proxy（Azure AD 应用程序代理）
Pulse Secure	Pulse SDP
Safe-T	Software-Defined Access Suite（软件定义访问套件）
Unisys	Stealth
Waverley Labs	Open Source Software Defined Perimeter（开源软件定义周边）
Zentera Systems	Cloud-Over-IP (COiP) Access（基于 IP 的云访问）
资料来源：Gartner（2019 年 4 月）	

市场建议

鉴于公共互联网存在重大风险，以及对互联网公开系统采取折衷方式以图在企业系统中获得立脚点的吸引力，企业需要考虑隔离数字业务服务，使之无法从公共互联网可见。不要把 Gartner 的建议误认为是经过实践检验的、真正的“默默无闻的安全根本就不是安全”的公理。尽管 ZTNA 将服务掩藏起来避免被发现和探测，但它建立了真正的屏障，事实证明，与过去简单的混淆概念相比，攻击者要绕过这些屏障更具挑战性。

传统的 VPN 访问可以寻找这样的场景，通过 ZTNA 服务执行其工作的目标用户组可以在改善组织的整体安全状况方面提供即时的价值。在大多数情况下，这可能是一个面向合作伙伴或员工的应用程序。ZTNA 项目是迈向更广泛的零信任网络（默认拒绝）安全立场的一步。具体来说，考虑到扩展网络连接的风险和当前情境，在建立足够的信任之前，任何人都无法与应用程序资源通信（甚至看不到）。

对于基于 DMZ 的应用程序，评估哪些用户集需要访问。对于那些具有一组已确定用户的应用程序，计划在未来几年内将它们迁移至 ZTNA 服务。可以将这些应用程序迁移到公共云 IaaS 作为这种架构转变的催化剂。

具体建议

- 对 ZTNA 项目进行预算和试点，以向组织展示 ZTNA 的优势。
- 规划用户到应用程序的映射。基于角色的访问控制 (RBAC) 可以帮助解决这个问题。避免允许所有用户可以访问所有应用程序。
- 确定哪些应用程序和工作流程不适合 ZTNA，并将它们排除在范围之外。这包括访问和下载不受面向应用程序和消费者的应用程序保护的非结构化数据。
- ZTNA 市场正在兴起，因此，随着市场的发展和成熟，只签订不超过 12 至 24 个月的短期合同，才能保留更大的供应商选择灵活性。
- 对于大多数数字业务场景，最好选择提供 ZTNA 服务的供应商，以便更易部署，提高可用性并抵御 DDoS 攻击。支持不需要在防火墙中开放侦听服务（入站连接）的供应商，这是 ZTNA 的大多数即服务形式的典型特征。
- 当安全需求要求在本地安装 ZTNA 产品时，支持选择尽可能减少防火墙开口数量的供应商。
- 如果命名用户将使用不受管的设备，则计划部署基于反向代理的 ZTNA 产品或服务，以避免需要安装代理程序。
- 确保供应商支持组织和合作伙伴现在使用的身份验证协议，包括企业的标准身份存储以及将来希望使用的任何身份验证协议。可用范围越广越好，包括云 SSO 供应商和 SaaS 交付的访问管理供应商。
- 不要指望合作伙伴使用您的身份存储。需要支持 SAML、OAuth、OIDC 和类似的联合身份验证功能。
- 评估供应商查询其他类型的设备代理（例如 UEM、端点检测和响应 (EDR) 以及 MTD）能力的有效性，以获取更多背景信息以改进自适应访问决策。
- 攻击者将瞄准 ZTNA 信任代理。对于本地 ZTNA 产品，使用支持本地部署的云工作负载保护平台 (CWPP) 工具加固主机操作系统，该工具主要依靠默认的拒绝允许列表来显式定义允许在系统上执行的代码。不要仅仅依靠补丁来保持系统的坚固。
- 如果您选择了一家小型供应商，计划通过在合同中放置适当的条款来进行潜在的收购，并在需要的时候列出备选供应商。

注 1. 代表性供应商选择

选择本指南中指定的供应商意味着可以选择两种 ZTNA 产品：即服务型产品和独立型产品。针对这两种产品类型，我们列出了截至 2019 年 4 月 Gartner 已知的供应商。

注 2. Gartner 的初步市场范围

本市场指南提供了 Gartner 对市场初步范围的介绍，重点介绍了市场定义、市场原理和市场动态。

资料来源：Gartner 研究纪要 G00386774, Steve Riley, Neil MacDonald, Lawrence Orans, 2019 年 4 月 29 日

奇安信集团介绍

奇安信集团（以下简称“奇安信”）是一家致力于为政府、金融、能源、电信等广泛领域的关键和有价值网络资产提供保护的领先安全提供商，是国内网络安全领域中成长最快的企业，自 2015 年来连续年复合增长率超过 90%。在 6500 余名员工不懈努力下，已有 90% 的政府部门、国有企业和大型银行采用了奇安信的技术。奇安信在 2019 年开始发展国际业务，并在印度尼西亚、新加坡、加拿大、中国香港、中国澳门等国家和地区扩展全球业务。

奇安信以“保护大数据时代的安全”为使命，以“数据驱动安全”为技术思想，以大数据收集和分析为支撑，为企业客户保驾护航。

奇安信的公司愿景是全面提升中国组织和企业的安全保护能力和水平，为经济发展构建可靠的网络环境。奇安信利用大数据分析等“互联网 +”的创新手段，帮助中国组织和企业更好地应对安全威胁。

奇安信

BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

奇安信身份安全实验室，是奇安信集团下属专注“零信任安全架构”研究的专业实验室。该团队以“零信任安全，新身份边界”为其核心理念，探索“企业物理边界正在瓦解、传统边界防护措施正在失效”这一时代背景下的新型安全体系架构，推出“以身份为基石、业务安全访问、持续信任评估、动态访问控制”为四大关键能力的奇安信零信任安全解决方案。该团队结合行业现状，大力投入对零信任安全架构的研究和产品标准化，积极推动“零信任安全架构”在业界的落地实践，其方案已经在部委、央企等进行广泛落地实施，得到市场、业界的高度认可。