易安联 Enlink Cloud

云计算开源产业联盟 OpenSource Cloud Alliance for industRy,OSCAR

零信任关键技术白皮书

2023

江苏易安联网络技术有限公司

云计算开源产业联盟

2023年8月9日

COPYRIGHT STATEMENT

版权声明

编制单位

江苏易安联网络技术有限公司

云计算开源产业联盟

编制人员

杨正权、秦益飞、于振伟、张英涛、张晓东

目录 CONTENTS

前　言

第一章　零信任发展概况

零信任起源与发展 02

零信任的基本原则 03

第二章　全面建设零信任关键技术全景

全面建设零信任概述 07

全面建设零信任关键技术 09

1.可信身份与认证 09

2.数据隔离保护 11

3.动态访问控制 13

4.自动化响应与可视化 15

第三章　全面建设零信任实施指南

全面建设零信任参考架构 17

1.NIST零信任架构 17

2.CSA软件定义边界架构 20

全面建设零信任典型实践 22

1.谷歌BeyondCorp项目 22

2.微软MCRA项目 24

全面建设零信任落地场景 26

1.远程办公场景 26

2.数据防护场景 27

第四章　结束语

附　录　编制单位介绍

前言

“云时代”信息技术变革引发了企业网络基础架构的变化，网络安全架构也随之发展，围绕访问安全的“零信任”成为网络安全架构趋势之一。

从 2004 年耶利哥论坛上零信任理念萌芽，到当前零信任项目不断实施落地，经过政府机构、标准化组织、学术团体、企业和安全专家十余年的共同努力，零信任体系日臻成熟，“永不信任，持续验证”逐渐成为企业网络安全架构建设的核心理念。为了指导企业的零信任网络安全建设，本白皮书从理念发展、技术体系和实施指南等方面对零信任进行了研究、分析，以助力企业零信任理念的实施落地。

白皮书首先回顾了零信任理念的起源、发展和内涵，从体系化安全防护的视角，综合访问实体、会话管理和控制位置等不同维度，提出了全面建设零信任的技术全景，包括可信身份与认证、数据隔离保护、动态访问控制和自动响应与可视化。最后，针对复杂多样的企业网络环境，以零信任关键能力的实施为出发点，对典型零信任架构的关键技术能力进行分析，讨论了每种架构的技术特点和应用场景，为全面建设零信任的实施方案提供参考。

零信任作为一种新兴的网络安全架构理念，在未来的发展过程中必然遇到各种挑战，企业需要不断的创新思维，以积极的心态推进理论发展和技术实践。全面建设零信任通过体系化的安全规划，能够从宏观上明确企业网络安全实施方法，对业务资源形成全方位的保护能力，为企业组织的数字化转型保驾护航。

PART 01

零信任发展概况

（一）零信任起源与发展

在传统边界安全模型中，企业 IT 部门采用以防火墙、VPN 为代表的网络安全产品和技术，通过对流经企业网络边界的流量进行检查、验证和加密，保护网络中的应用、服务和数据等资产。

在全球数字化转型浪潮下，企业网络安全面临诸多挑战。一是基础设施多样化、云化，业务访问需求复杂化，使得企业原有的网络边界逐渐模糊；二是远程办公、自有设备（BYOD）增加了数据泄露的风险；三是内部横向移动、APT 攻击、勒索软件等网络攻击手段不断提升，网络内部安全态势严峻。传统基于边界的网络安全防护手段已无力应对各种潜在的安全威胁，企业组织迫切需要优化网络安全架构，以为遍布世界各地的分支机构、合作伙伴、客户和员工提供多样化的网络接入和服务访问。

秉承“永不信任，持续验证”理念的零信任理念是解决上述问题的有效手段之一。零信任起源于耶利哥论坛（Jericho Forum，成立于 2004 年）对企业“去边界化”网络安全解决方案的探索。2010 年，Forrester 的首席分析师 John Kindervag 正式提出零信任概念（Zero Trust），认为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鉴别，通过微隔离架构实现对网络的细粒度访问控制，以限制攻击者的横向移动。

伴随着云计算、移动互联网的发展，零信任逐渐开始向以身份为基础的动态访问控制体系演变。2014 年，谷歌通过一系列论文介绍了 BeyondCorp 的设计思路和落地方案，

使用零信任架构替代了传统 VPN 的使用，将安全边界细化至用户和应用，确保来自不同位置的所有用户均能安全地访问企业业务。

2013 年，云安全联盟（CSA）提出 SDP（Software Defined Perimeter）软件定义边界，成为零信任的代表解决方案，并于 2014 年发布《SDP 标准规范》（1.0 版），介绍了 SDP 的架构组成、工作流程、交互协议和应用场景等内容。2020 年 8 月，美国国家标准技术研究所（NIST）发布《零信任架构》（SP 800-207），全面阐述零信任理念的核心原则、逻辑架构、典型场景的部署方式，以及与已有系统的交互支撑等内容。2021 年 2 月，DISA 和 NSA 联合发布了《DOD 零信任参考架构》，该报告采用美国军队体系结构描述方法（DoDAF），对零信任架构的预期目标、能力组成、组件关系、数据流转，以及应用场景等内容进行了说明。2021 年 10 月，ITU-T 发布标准《服务访问过程的持续保护指南》（X.1011），提出从主体发起访问请求到收到服务响应的访问过程中，基于零信任理念执行动态策略保护，通过不断分析相关实体的安全状况，验证访问活动的合理性，以保护访问过程的安全，推动零信任内涵从“持续验证”向“持续保护”升级。2022 年 4 月，CSA《SDP 标准规范》（2.0 版）正式发布，与 1.0 相比，该版本对 SDP 架构、部署模型和单包认证协议进行了细化说明，并解释了 SDP 与 NIST 零信任架构的映射关系。

综合来看，近几年零信任标准化研制工作已经进入高产阶段，零信任相关技术和产品逐步走向成熟。2019 年，中国信通院发布的《中国网络安全产业白皮书》指出：“零信任已经从概念走向落地”。2021 年以来，由奇安信牵头制定的国家标准《信息安全技术零信任参考体系架构》、中国信通院牵头制定的系列行业标准《面向云计算的零信任体系》等工作也取得了持续进展，为我国零信任产业的规模化发展打下良好基础。

（二）零信任的基本原则

零信任代表了新一代的企业网络安全架构，将由防火墙、IPS/IDS 等安全设备所构建的网络安全边界，转换成围绕受保护资产的软件定义边界，放弃了基于网络位置的信任假设，重新审视网络中信任关系的建立、维系方式，通过基于上下文的精细化访问控制，减少暴露面和攻击面，使网络安全管理能够更灵活地应对复杂的安全事件和网络变化。

零信任在萌芽阶段，主要关注企业网络的微隔离保护问题，John Kindervag 围绕零信任网络架构，给出了 3 个基本原则：

（1）不再以网络位置区分网络、设备接口和用户的可信度；

（2）访问控制应该遵从最小权限原则；

（3）所有的访问都应当被记录和跟踪。

在零信任蓬勃发展阶段，应用场景不断变化，安全技术更新迭代，零信任理念的关注方向已经从企业网络基础架构发展为企业业务访问安全架构，提供了旨在消除访问决策不确定性的一系列概念和组件，进一步细化明确了零信任架构设计的前提假设和基本原则，以便指导零信任架构的落地实施，为企业数字资源建设打造体系化的安全控制能力。

零信任的安全假设是其基本原则的设计前提，在以 NIST 零信任架构为代表的安全框架中，零信任重点关注企业应用与资源的访问安全问题，对上下文的安全状况做出了一些基本的前提假设，主要包括：

（1）从访问所处的空间维度来看，在网络的不同位置（内网、外网、云端等）、区域、节点，均存在无法避免的各种安全威胁；

（2）从访问过程的组成维度来看，参与访问过程的所有对象默认都不可信任，包括用户、设备、网络、应用、数据等；

（3）从访问发生的时间维度来看，在整个访问过程中，每个实体对象的安全性（机密性、完整性、可用性、真实性等）是动态变化的。

基于这些前提假设，零信任架构设计需要遵循的基本原则包括：

（1）受保护资源应覆盖企业的所有数字资产，包括用户、设备、数据、服务等；

（2）业务、资源访问所依赖的通信机制必须满足相应的安全要求（身份鉴别、机密性、完整性保护等），而且与资源的网络位置无关；

（3）对资源的访问授权均应以会话为粒度，当且仅当请求方通过身份认证后，方可授予其最小访问权限（遵循最小权限原则）；

（4）对资源的访问授权是通过动态策略决定的，影响策略判决结果的因素包括用户身份、应用 / 服务、目标资源的状态，以及与安全态势相关的行为或环境因素等；

（5）企业持续监控和测量所有 IT 资产的安全状态，以便对处于不同安全态势下的资源采用不同的安全策略；

（6）所有资源的认证、授权是动态完成的，并且必须在允许访问前完成；

（7）企业尽可能收集 IT 资产的实时状态数据（如网络流量、访问请求的元数据），以便评估网络的安全态势。

上述原则体现了“永不信任、持续验证”的零信任理念，其核心要义是通过持续收集实时上下文，基于动态策略对所有资源的所有访问进行持续验证，通过实施最小权限原则，最大限度地收敛暴露面和失陷范围。

“实时上下文”是零信任的实现基础，由业务访问过程中，所有可能影响业务安全的内、外部因素组成，包括与访问相关的实体的状态、环境、事件、时序等，例如主体的历史行为、客体的安全状态、业务数据流转记录、当前网络（系统）的漏洞 / 补丁、恶意代码、升级更新、威胁情报、安全政策等。

零信任架构的基础设施需要实时收集，并使用组织业务中的安全上下文，快速、准确地确定访问的授权结果，确保用户体验不受影响。在零信任架构中，上下文的定义需要综

合考虑业务安全的要求和现有安全工具的能力，并在策略执行过程中进行验证，根据安全态势的变化加以调整，以确保动态策略的实施执行，收紧受保护资源的安全边界。

“持续验证”意味着无论什么时间，访问环境中不存在可信区域、凭据或设备，企业范围内的所有数字资产均面临威胁，需要对它们实施最大范围、基于风险的全过程访问控制，这种控制能力需要通过动态可扩展策略的部署来加以保证，以确保兼顾来自风险管理、安全合规、快速部署和用户体验等多部门多层面的综合要求。

通过实时上下文和持续验证的统一协同，零信任限制了用户身份凭据的使用范围和访问路径，实现了企业范围内的“收敛暴露面和失陷范围”，有助于将攻击威胁的可能性和影响（风险）降至可接受的范围内，使安全系统和人员能够获得足够的响应时间，以减少攻击带来的损失。

PART 02

全面建设零信任关键技术全景

（一）全面建设零信任概述

企业全面建设零信任的目的是为了提升业务资源访问的速度与安全性，企业需要建设能贯通整个业务访问过程的安全架构和基础设施，形成对企业资源的全方位保护。零信任架构通过提供自适应的持续保护和主动威胁管理，为用户、设备和应用建立多层级的“永不信任、持续验证”安全访问环境，并支持为安全团队提供业务访问的完整视图，安全策略全局一致，能够快速并精准地对威胁进行检测与响应。

零信任架构聚焦资源和业务的访问环境安全性，结合不同维度的上下文，从参与访问的实体对象（用户、设备、网络、应用、数据等）、访问会话所处的时间阶段（身份认证，会话建立、业务通信、会话关闭）、访问发生的空间位置（终端、数据中心、云端）等层面，通过融合现有的网络安全工具和技术能力，实施全流程、全区域的零信任安全访问，形成动态、立体的体系化安全防御能力，全面建设零信任的概念组成如图 1 所示。

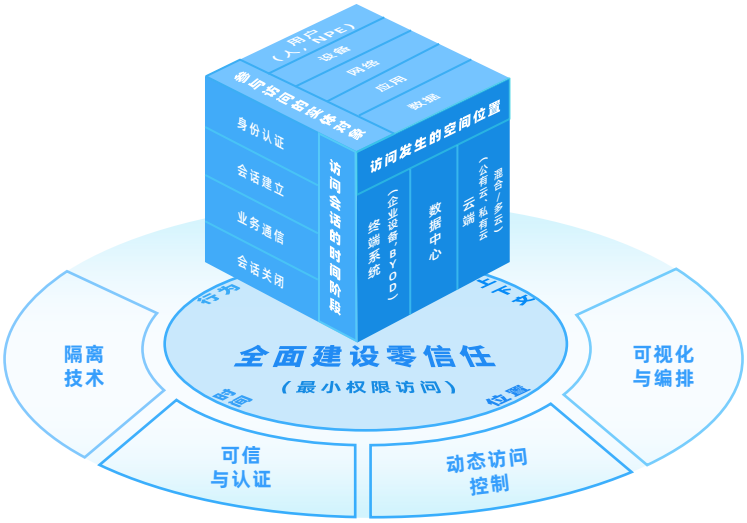

图1 全面建设零信任概念

在现阶段主流的零信任架构中，访问安全的核心关联元素包括：

(1)访问主体：

a) 用户：访问发起者，即真实自然人、NPE 在网络中的身份映射；

b) 设备：访问发起者所用设备，包括系统软硬件、执行环境等；

c) 工作负载：访问发起的工作负载，包括容器、虚拟机等；

(2)资源：访问或获取的目标客体，如应用、业务数据或服务；

(3)网络：访问主体与资源间各中间节点构成的物理或逻辑通道。

在业务访问过程中，根据各关联要素的安全状态变化情况，可大致将单次会话的访问过程划分为 4 个阶段：

(1)身份认证：访问关联实体进行身份认证；

(2)会话建立：访问主体发起资源访问请求，鉴权中心经过动态策略判定，授予访问主体相应权限；

(3)业务通信：用户通过安全链路访问业务资源；

(4)会话终止：主客体之间关闭访问会话。

围绕业务资源可能所处的位置，受保护对象的分布位置可分为 3 种情况：

(1)终端：受保护资源处于用户办公终端内，包括企业设备，BYOD 等；

(2)数据中心：受保护资源处于数据中心内部，企业围绕数据中心提供安全防护边界；

(3)云端：受保护资源处于云环境中，包括公有云、混合云、多云等。

在零信任理念下，所有访问主体在被允许访问资源之前都需要经过身份认证和授权，再通过全流程的访问监测、管控，多方位、全层面落实零信任理念，形成动态、立体的安全防御体系。身份认证的覆盖范围涉及与访问相关的所有实体，包括用户、终端、网络设备、应用服务等。授权决策不仅仅基于网络位置、用户角色或属性等传统静态访问控制模型，

而是通过持续的安全监测和信任评估，进行动态、细粒度地授权。“全面建设零信任”的安全技术图谱如图 2 所示，覆盖了为全面建设零信任而需考虑采用的技术，第二章将围绕其中的关键能力域，讨论支撑全面建设零信任的关键技术。

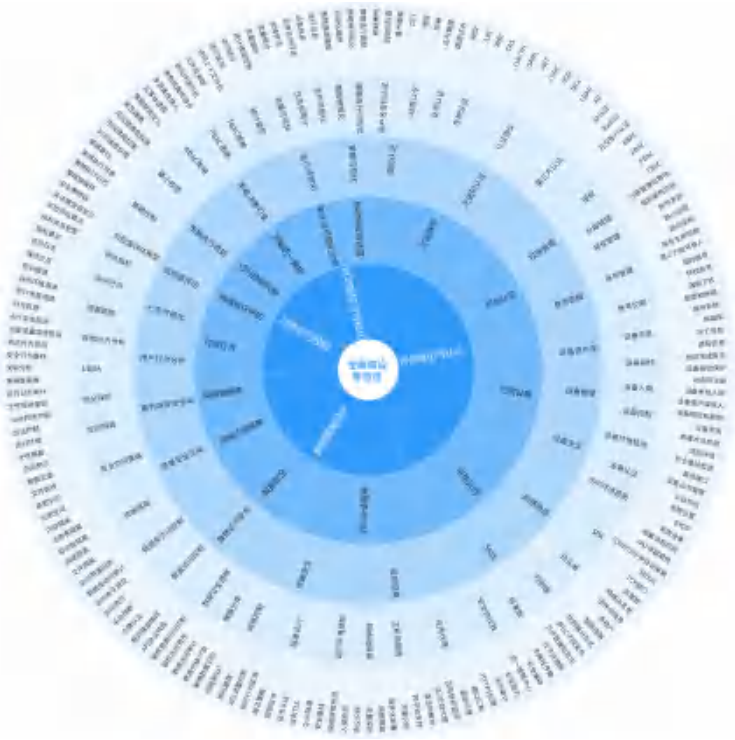

图2 全面建设零信任技术图谱

（二）全面建设零信任关键技术

本章从体系化安全防护的视角，统揽用户访问的上下文全局，对全面建设零信任所需的关键技术进行梳理，主要包含 4 类技术：可信身份与认证、数据隔离保护、动态访问控制和自动响应与可视化。

1.可信身份与认证

零信任理念下，基于数字身份实现用户和受控设备的可信识别，包括用户身份认证和单点登录，以及受控设备的设备指纹、设备认证和安全基线管理，并基于身份属性和行为特征对用户进行信任评估，以动态应对风险并调整访问权限，零信任架构中实现可信身份

的关键技术如图3所示。

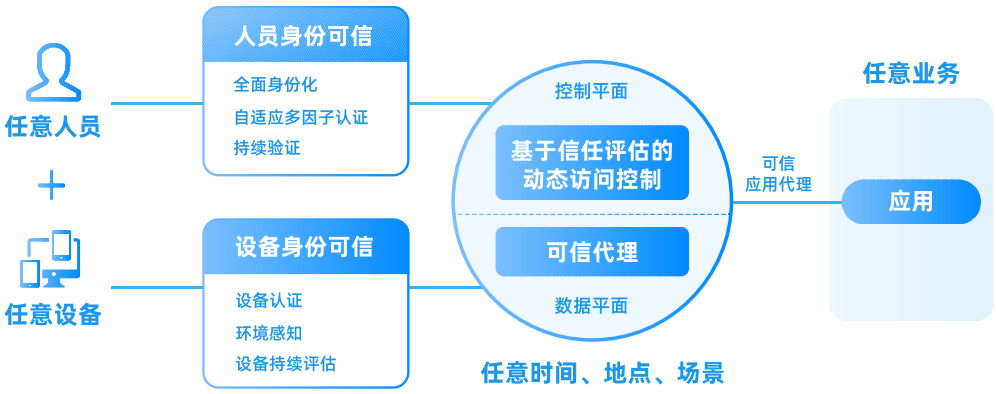

图3 零信任架构中可信身份关键技术

(1) 可信用户身份

用户数字身份由用户属性、行为、生物特征等标签共同组成，用户的可信正建立在对数字身份认证的基础之上，用户通过动态口令、人脸识别、指纹识别以及认证令牌等方式完成身份认证。零信任架构中的身份认证是一个持续验证的过程，首先在建立连接之前先执行身份认证，只有经过验证的最终用户才能访问资源；其次，在访问的整个生命周期中持续进行身份验证，以确定每个访问请求的身份和安全状况；同时，访问控制引擎结合用户行为、地址位置、访问时间等进行风险分析与判断，并实时做出访问权限调整；最后，授予对资源的最小访问权限。零信任通过自适应的、基于风险的评估来识别潜在威胁，做到精细化的权限控制，减少因身份凭证被盗或泄露所带来的潜在威胁，该评估机制会贯穿整个用户生命周期。

(2) 可信设备身份

数字设备身份由客户端设备信息、访问时间、入网位置等标签共同组成。零信任架构中，设备的可信主要通过对设备的安全性进行持续检查和发现来实现。一方面，根据预先收集的设备信息对设备的访问行为赋予初始权限策略；另一方面持续监控设备行为，对于

偏离既定策略的设备进行告警。首先，信任评估引擎将对所有登录的设备进行注册，收集、记录设备详细信息，并生成设备指纹，初始化客户端证书。再次登录时，信任评估引擎根据存储的信息校验登录设备信息以及证书有效性，判断是否为可信设备；其次，可信设备管理将持续、自动化地识别、记录和跟踪组织内不同类型设备资产及对应属性，为设备动态访问控制提供前置条件；然后，信任评估引擎基于ABAC、RBAC等模型持续评估设备主体属性及上下文环境，完成对设备的动态认证与授权；最后，零信任架构将持续对所有接入设备进行威胁检测与响应，同时，信任评估引擎将持续验证设备相关配置策略，并针对不符合配置基线的设备执行修复操作。可信设备的重点在于持续对每个访问企业资源的设备进行监控，并采取相对应的安全防护和控制性措施。

(3) 可信认证方式

零信任架构默认不信任访问主体的身份，在单次会话全生命周期中持续验证访问主体的身份，并根据风险等级提供额外的认证因子，自适应SSO和MFA可在不影响用户体验的同时增加访问安全性。SSO单点登录允许用户通过一组登录凭证访问多个相关的应用程序和服务。为了降低多个应用程序依赖于同一组登录凭证的风险，通常需要对SSO使用自适应认证。如果用户在尝试通过SSO登录时或在其SSO认证会话期间表现出异常行为，如通过无法识别的VPN进行连接、访问用户会话认证令牌未涵盖的应用程序或数据等，SSO会要求他们提供额外的认证因子。MFA认证通过用户提供的多种非密码认证因子，降低密码泄露带来的潜在安全隐患。

2.数据隔离保护

(1) 终端沙箱隔离

数据沙箱可以为员工提供可信的终端工作环境，如图4所示，支持多域多安全级别的安全工作空间，提升企业数据安全性。一是将BYOD私人环境与企业办公环境分隔，安全工

作空间与宿主机之间保持数据、网络、应用、进程和通信全隔离，工作空间内数据强加密并且数据流转受控，企业员工只能在安全工作域内访问业务资源；二是工作空间全生命周期管理，访问控制引擎负责维护并下发各工作空间的安全策略，并对工作空间内所有操作持续检测、分析上报日志，如发现异常行为，可自动强制清空工作空间，降低数据泄露和攻击风险；三是对端侧环境风险、业务系统异常访问、用户异常行为及时检测识别，身份、流量、环境的实时检测与安全工作空间基于策略控制的有机结合，可以最大程度保障端的安全。

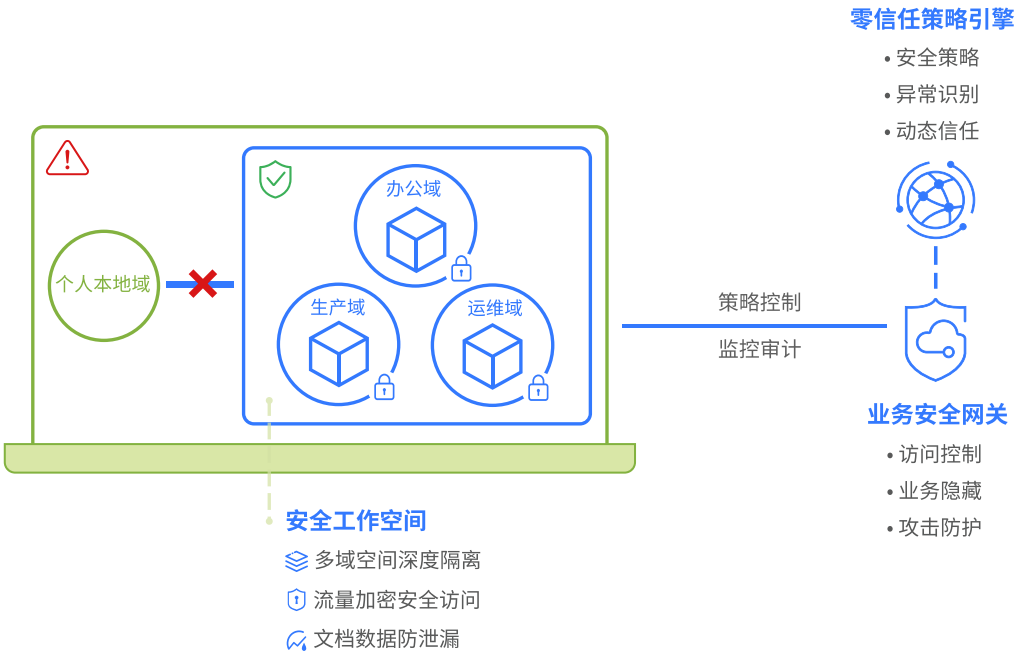

图4 终端沙箱的安全能力

数据沙箱使用内存映射技术，为每个进程创造一个单独的地址空间，用以隔离多个进程的代码和数据，通过内核空间和用户空间不同的特权级来隔离操作系统和用户进程的代码和数据。关键隔离技术包括：文件隔离——隔离宿主机与空间文件系统；剪切板隔离——隔离剪切板的数据通道；网络隔离——隔离应用访问通道；注册表隔离——隔离应用系统配置；进程通信隔离——隔离进程避免数据逃逸。

(2) 网络微隔离

微隔离技术主要实现工作负载间的安全隔离，按逻辑将数据中心网络划分为不同安全段，阻断各分段间异常东西向流量，提升企业网络安全性。一是细化策略管控力度，微隔离可以将细粒度的安全策略应用于工作负载，单个机器、用户或应用程序，这些策略可以根据真实世界的构造定义，例如用户组、访问组和网络组，并且可以跨多个应用程序或设备应用；二是微隔离访问主体拥有唯一身份标识，无论是服务器、应用程序或用户，基于其身份权限提供访问控制；三是网络流量高可见性，微隔离通过安插网络流量探针，可以为安全团队提供全网流量视图和上下文，便于快速定位问题。

(3) 访问会话隔离

远程浏览器隔离（RBI）是一种访问会话隔离技术，将浏览器执行从用户设备转移到云中安全环境。用户使用本地浏览器连接到一个远程服务器上，用服务器上的“远程浏览器”上网，全程数据只落在远程服务器上，不落在本地。当用户访问网页时，RBI 服务器首先需要对连接到它的用户进行身份验证，然后 RBI 服务器上会创建一个远程浏览器会话，本地的交互操作同步到远程浏览器。打开的网页代码在远程浏览器中加载，传给用户本地的只有“影像”，网页内容不实际下载到本地，防止任何基于 Web 的攻击进行恶意软件感染的尝试。

3.动态访问控制

(1) 访问控制

访问控制是通过某种途径显式地准许或限制主体对客体访问能力及范围的一种方法，其目的在于限制访问主体的行为和操作。当前应用比较广泛的访问控制技术包括基于角色的访问控制（RBAC）和基于属性的访问控制（ABAC），同时也存在两者结合的授权方式，既基于策略的访问控制（PBAC）和基于任务的策略访问控制（TBAC），PBAC 方式兼顾

RBAC 的简单、明确的特性，也具备 ABAC 的灵活性，实现了基于主体属性、客体属性、环境风险等因素的动态授权，TBAC 重在基于完成一项任务所需要访问的资源，对任务参与者进行权限分配。

动态访问控制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，信任库提供访问主体历史信任评估等级。信任评估引擎基于大数据和人工智能技术，对访问行为进行持续分析，对信任等级进行持续评估，对访问主体身份进行持续画像，最终为访问控制引擎提供决策依据。

(2)持续信任评估

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，持续信任评估是访问控制的重要输入，如图 5 所示，以身份为中心，对访问主体进行持续地信任评估，以业务安全为目标，授予最小化权限，并根据访问主体行为进行持续评估，以实现访问权限的动态调整。

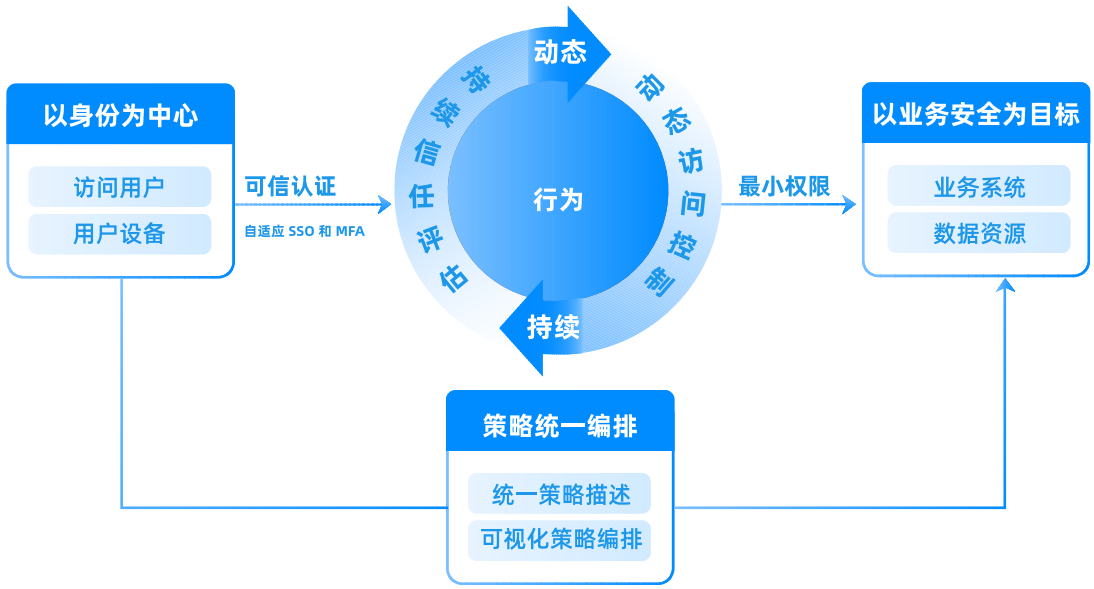

图5 零信任动态访问控制的核心功能

通过信任评估模型和算法，实现基于身份的持续信任评估，信任评估包含：一是对

受控设备进行基于环境因素的风险评估，利用环境感知技术，获取终端环境的信任评分，为动态访问控制提供有效输入；二是对访问主体访问上下文行为分析的评估，结合访问主体身份属性信息，对访问的上下文进行风险判定，识别异常访问行为。持续地对信任评估结果进行调整，覆盖“运行态”访问安全。

(3)策略统一编排

策略统一编排实现网络安全设备内部安全策略可视化编排和可视化监控运行，借助可视化的安全策略链编排框架，定义统一的安全策略描述模板，解决传统网络安全产品中安全策略管理分散、策略执行过程不可见等运维难题，极大提高安全运维的效率。

统一的安全策略描述，可以实现所有安全策略规范化描述，安全策略描述模板包含如下属性字段：策略类型、策略编号、策略规则、策略优先级、策略动作和策略关联关系等。其中，策略规则用于描述策略匹配的具体条件；策略优先级用于定义策略执行的先后顺序；策略动作标识满足策略规则之后所采取的动作。

安全策略按优先级从高至低链接形成策略链，可实现安全策略的自动化控制。通常，根据业务流程可以将安全策略分成认证策略和访问策略两类。认证策略包括：首登改密，强密码策略，密码超期策略，管理员白名单策略，登录并发数限制策略，长时间未登录策略，防暴力破解策略等。访问策略包括：入向报文过滤策略，应用访问策略，出向报文过滤策略等。通过策略链，安全运维人员可更便捷地查看安全策略配置以及安全策略的执行情况。

4.自动化响应与可视化

(1)自动化响应与处置

零信任架构下，基于风险驱动和上下文感知的自动化安全响应能够识别行为的不一致性，如登录时间、登录位置等，并基于风险分析结果自动做出处置动作，包括二次认证、

拒绝访问请求、强制退出、禁用账户等操作。同时，通过与其他安全产品对接，实现联动安全响应与处置。安全编排是将企业不同安全技术按照一定的逻辑关系组合到一起，以实现安全响应与处置流程的自动化，在此过程中，企业需要简化安全堆栈，消除不必要与重复技术，以及使系统维护与管理复杂化的技术，令编排过程变得更简单、更模块化，消除管理难题，显著减少运营开销。

(2)审计与可视化分析

零信任架构需要支持最新的外部合规审计要求，结合自身行业、业务特点制定信息安全管理体系，对用户操作行为进行审计，并将审计信息上传至零信任控制中心，零信任控制中心通过对信息进行统计分析，得出用户安全访问基线、设备安全访问基线和服务间流量安全基线。

零信任控制中心将监视、记录、关联分析网络中的每个活动，对可疑行为展开时空线索分析，展现特定用户、特定设备时空访问行为，通过可视化技术将访问路径、访问流量、用户异常访问行为直观展示，帮助安全运营人员更直观、全面地了解访问主体的安全状态和行为，从而更快速、更精准的找到风险点。

PART 03

全面建设零信任实施指南

在复杂多样的企业网络环境中，部署和实施零信任是一项庞大且长期的工程，需要紧密契合企业网络安全的需求，将已有的网络安全工具和能力纳入零信任架构，并进行不同程度的能力融合和完善，形成体系化的安全防御能力。

本章以零信任关键能力的实施为出发点，围绕两大零信任典型架构，并选取了两个零信任典型实践案例，明确其技术特点和应用场景，并对每种架构的关键技术能力进行分析，为全面建设零信任的实施方案建设提供参考。近年来较多零信任优秀实践案例涌现，因篇幅所限，本章仅以谷歌 BeyondCorp 和微软 MCRA 为分析代表，其它案例不再赘述。

（一）全面建设零信任参考架构

1.NIST零信任架构

（1）核心组件与功能

在《零信任架构》（SP 800-207）中，NIST指出“零信任架构（ZTA）提供了一个概念、思想以及组件关系（架构），旨在消除在信息系统和服务中执行准确访问决策的不确定性”。零信任架构是一种企业网络/数据安全框架，包括身份、凭据、访问管理、操作、终端、托管环境和网络基础设施等组件。传统的企业网络安全解决方案只关注外围防御，导致对内部用户开放了过多的访问权限，而零信任的主要目标是提供基于身份的细粒度访问控制，以应对日益严峻的横向移动风险。

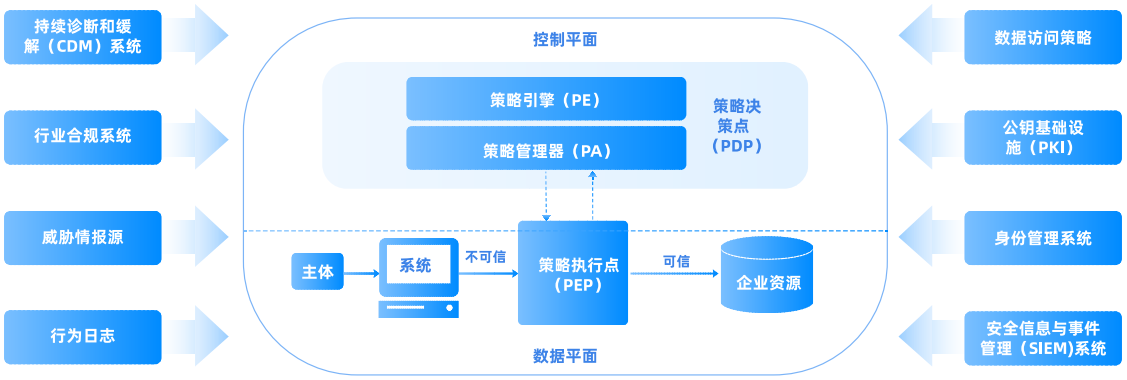

图6 NIST零信任架构

图 6 给出了 NIST 的零信任架构示意图，各逻辑组件使用独立的控制层面进行通信，应用数据则在数据层面进行通信。

a）策略决策点（PDP）

PDP 是访问授权的决策中心，包括两个组件：策略引擎（PE）和策略管理器（PA）。

PE 负责决定是否授予主体对资源（访问客体）的访问权限，使用来自外部信息源（例如 IP 黑名单、威胁情报服务）的输入，通过信任算法评估访问主体的可信度，以决定授予或拒绝对该资源的访问。

PA 根据 PE 的决策结果向 PEP 下达控制指令，建立和 / 或切断主体与资源之间的访问路径。

b）策略执行点（PEP）

该组件负责启用、监视或终止主体和资源之间的连接。PEP 可以是 ZTA 中的单个逻辑组件，也可以分解为多个组件，分别部署于客户端（例如，用户便携式电脑上的 Agent 代理程序）、资源端（例如，在资源之前控制访问的网关组件）或充当通信路径防护的门户组件。

除了企业中实现 ZTA 策略的核心组件之外，其它多个数据源也可以提供输入和策略规则，以供策略引擎在做出访问决策时使用。这些数据源包括本地数据源和外部（即非企业控制或创建的）数据源。其中包括：

a) 持续诊断和缓解系统

该系统收集关于企业资产当前状态的信息，并对配置和软件组件应用进行更新。企业CDM系统向策略引擎提供发出访问请求的系统的状态信息，例如，当前操作系统和应用程序是否打过补丁、企业准入软件/组件的完整性状态、是否存在已知漏洞或未经批准的组件。CDM系统还负责对活跃在企业基础设施上的非企业设备进行识别，并执行相应的安全策略。

b) 行业合规系统

该系统确保企业遵守相关监管制度（如医疗或金融行业信息安全要求HIPAA、PCI-DSS等），包括企业为确保合规而制定的所有策略规则。

c) 威胁情报源

该系统提供外部来源的信息，帮助策略引擎做出访问决策。

d) 数据访问策略

一组与企业数据资源访问相关的属性、规则和策略集合。这些策略是授予对资源访问权限的规则条件，为企业中的参与者和应用/服务提供了基本的访问特权。

e) 企业公钥基础设施

此系统负责生成和签发由资源、主体、服务和应用程序使用的数字证书，并将其记录在案。

f) 身份管理系统

该系统负责创建、存储和管理企业用户账户和身份记录，包含必要的用户信息（如姓名、电子邮件地址、证书等）和其他企业特征，如角色、访问属性或分配的IT资产。

g) 安全信息和事件管理系统（SIEM）

该系统聚合系统日志、网络流量、资源授权等事件信息，以供策略优化和潜在威胁的

发掘。

(2) 关键技术能力

在可信身份与认证方面，NIST架构中的身份管理系统负责统一管理用户的账号、角色等信息，保证用户的身份可信；持续诊断和缓解系统、数据访问策略负责收集关于企业资产当前状态的信息，并对配置和软件组件应用进行更新，威胁情报源、安全信息和事件管理系统负责收集各类威胁数据和安全事件数据，保证设备和环境可信。

在动态访问控制技术方面，NIST架构中的PEP将访问主体和访问客体分隔。作为访问主体侧的用户想获取作为访问客体的数据资源，必须通过PEP进入。零信任要求对用户的身份、设备、行为路径等内容进行检测和分析，PEP收到用户访问请求后，PDP综合评估是否允许当前访问通行，当上述输入的数据产生变化时，评估结果随之变化，PE将新的评估结果告知PA，PA向PEP发出信号允许或拒绝会话。

在自动化响应与可视化方面，NIST架构通过日志系统、SIEM系统以及各个安全系统，收集架构本身和其他安全系统的信息，联动处置安全事件。

2.CSA软件定义边界架构

(1) 核心组件与功能

CSA 2022年5月发布了SDP 2.0规范，其基本架构如图7所示，包括SDP控制器、发起主机和接受主机。

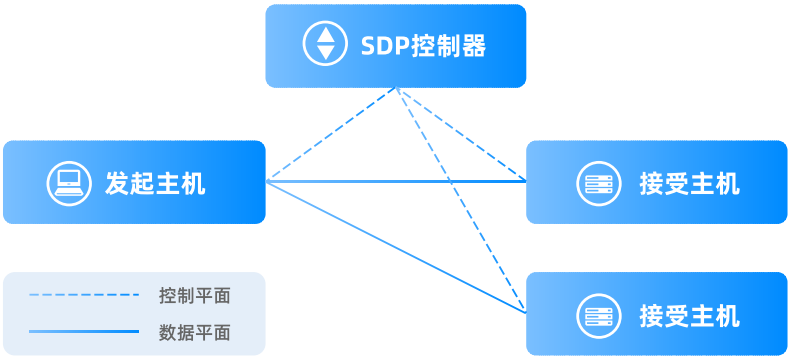

图7 CSA SDP架构

a）SDP 控制器

SDP 控制器是软件定义边界中的策略决策点（PDP），用于定义访问控制策略。SDP 控制器可与内部实体进行通信，如身份和访问管理（IAM）服务，如果组织正在使用基于云的身份即服务（IDaaS），则可与外部实体进行通信。

b）SDP 主机

SDP 主机是零信任策略的实施点（PEP），用于执行 SDP 控制器定义的访问策略。SDP 主机可以细分为两类：发起主机或接受主机。发起主机（IH）与控制器通信以请求它们可以连接的 SDP 接收主机（AH）列表。在提供任何信息之前，控制器可以从 SDP IH 请求获取硬件或软件清单等信息。默认情况下，SDP AH 拒绝来自控制器以外的所有通信，只有在收到控制器指示后，SDP AH 才接受来自 IH 的连接。

（2）关键技术能力

在可信身份与认证方面，SDP 架构以身份为核心，通过建设本地帐号管理能力，持续完善用户身份的合法性管理和统一维护，也可集成对接第三方统一身份管理，完成身份验证与绑定。对发起访问的终端设备进行终端环境状态采集，检测终端环境安全性，生成设备资产台账，对终端设备的全生命周期进行管理，完善设备资产身份的合法性管理和统一化维护。

在数据隔离保护方面，SDP 能够实现基于用户自定义控制的网络微隔离。通过 SDP 可以自动控制对特定服务的网络访问，从而消除了手动配置。

在动态访问控制方面，SDP 组件通过敲门和认证机制，形成了动态的安全隔离区，能够抵御基于网络的攻击，并通过动态创建和删除访问规则（出站和入站）来启用对受保护资源的访问。

在自动化响应与可视化方面，SDP 基于 AH 记录所有 IH 对应用的访问请求以及每次

访问的执行情况，并把这些日志上报给 SDP 控制器。一方面 SDP 控制器将对日志分析结果进行展示，另一方面 SDP 控制器将针对异常日志进行问题定位，并快速地对访问中的异常做出响应。

(二) 全面建设零信任典型实践

1.谷歌BeyondCorp项目

(1) 核心组件与功能

谷歌 BeyondCorp 项目的目标是“让所有 Google 员工从非可信网络中，不接入 VPN 就能顺利工作”，如图 8 所示，处于外部公共网络和本地网络的设备在默认情况下都不会授予任何特权。在全新的无特权内网访问模式下，访问仅依赖于设备和用户身份凭证，而与用户所处的网络位置无关，无论用户是在公司内网、家庭网络或公共网络，所有对企业资源的访问都要基于设备状态和用户身份凭证进行认证、授权和加密。

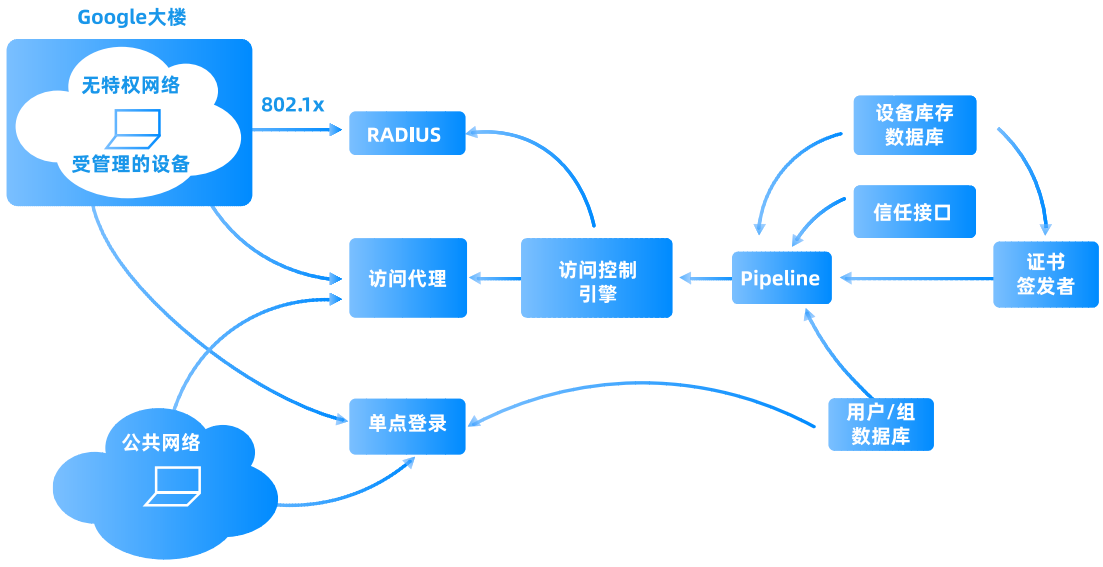

图8 BeyondCorp架构与业务访问流

BeyondCorp的基本组件包括：用户/组数据库、信任评估引擎，设备资产库存数据库、访问控制引擎、访问代理和资源。其中：

用户 / 群组数据库系统与谷歌的 HR 流程紧密集成，管理着所有用户的岗位分类、用户名和群组成员关系，BeyondCorp 跟踪和管理用户 / 群组数据库中的所有用户。当员工入职、转岗、或离职时，数据库就会相应更新。HR 系统将需要访问企业的用户的所有相关信息都提供给 BeyondCorp。

设备资产库围绕“受控设备”进行建设，只有受控设备才能访问企业应用。在设备的生命周期管理中，谷歌追踪每个设备上发生的变化，这些信息会被监控、分析，并提供给 BeyondCorp 的其他组件使用。通过元清单数据库，掌握了所有需要访问企业应用的设备信息。

访问控制引擎是集中化策略编排和下发的核心组件，用来确保网关正确地实施安全策略，它基于访问策略、信任评估引擎、资源需求、实时凭证提供二值型的授权决策。信任评估引擎是一个持续分析、评估设备安全状态的系统。系统设置设备可访问的最大信任层级，并在公司网络上分配设备要使用的 VLAN。这些数据记录在设备资产服务中，状态变化或更新失败会触发重新评估。

BeyondCorp 的访问代理起到了安全网关的作用，只支持 web 网站的接入，不支持 C/S 架构的应用。

另外，资源是受访问控制保护的应用、服务和网络基础设施，例如可通过网关访问资源（如 SSH 服务、Web 代理、802.1x 网络），网关提供授权（如分配最低信任层、分配 VLAN）的访问对象。资源可能包括在线知识库、财务数据库、链路层连接、实验网络。每个资源都与访问所需的最低信任级别相关联。

（2）关键技术能力

在可信身份评估方面，BeyondCorp 在实施前确定了唯一的身份数据源，即 HR 系统中的员工数据，并通过用户 / 群组数据库系统与谷歌 HR 系统的紧密集成，拉通所有用户

的岗位分类、用户名和群组成员关系，当员工入职、转岗、或离职时，数据库就会相应更新。HR系统将需要访问企业网络和应用的用户的所有相关信息都提供给BeyondCorp。

在动态访问控制方面，访问代理中的访问控制引擎，基于每个访问请求，为企业应用提供服务级的细粒度授权。授权判定基于用户、用户所属的群组、设备证书以及设备清单数据库中的设备属性进行综合计算，动态决策每个访问的权限。

在终端的网络隔离方面，BeyondCorp项目将所有办公设备默认分配到一个无特权网络中，避免直接接入内部业务网络，并在内网中构建了一个与外网环境类似、且只能访问互联网的网络环境，以及部分网络基础设施服务如DNS、DHCP、NTP或Puppet系统，这个无特权网络和谷歌网络的其他部分之间由严格管理的ACL（访问控制列表）进行控制。

2.微软MCRA项目

（1）核心组成与功能

微软网络安全参考架构（MCRA）基于零信任原则设计，分别在身份与访问、安全运营、设备合规管控、多云和跨云平台管理、软件即服务（SaaS）的云原生安全控制、物联网与运营管理，信息保护等功能上进行细化和落地。该架构在假定出现了信息泄露的情况下，对所有访问请求进行验证，无论该请求出自何处、要访问什么资源，以保护位于任何位置的用户、设备、应用程序和数据等资产，简化架构如图9所示：

微软零信任安全架构的核心是安全策略的统一部署执行，安全策略引擎提供实时的策略评估与决策。该引擎通过对身份、设备、组织策略和威胁情报的分析综合决策访问的权限，在授予对数据、应用程序、基础设施和网络的访问权限之前，确保身份得到验证以及设备的安全性。

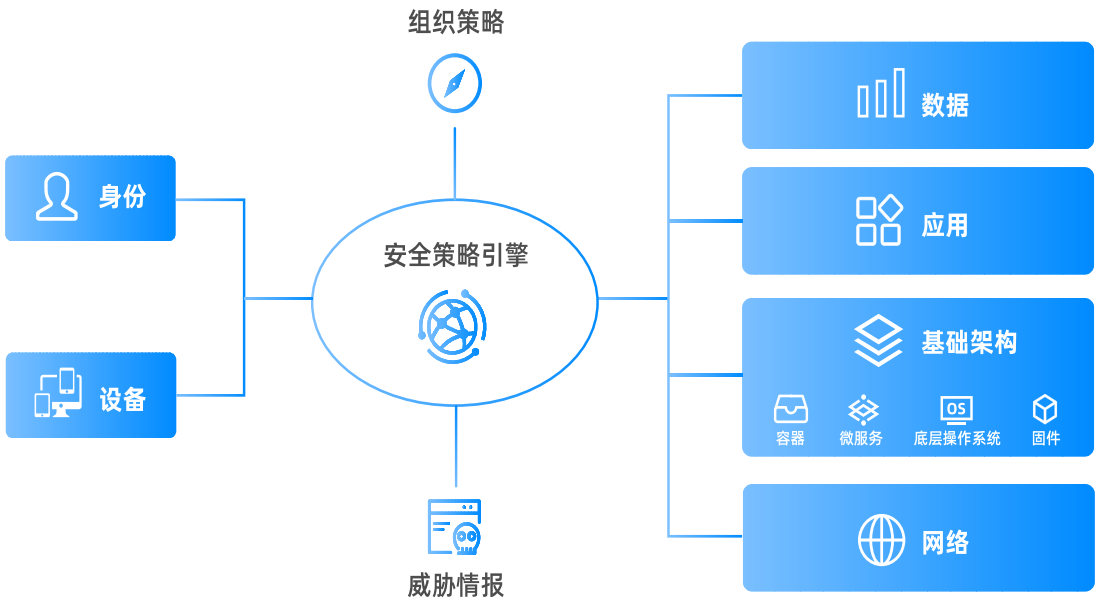

图9 微软零信任架构示意图

(2)关键技术能力

从可信身份与认证技术方面来看，在微软零信任架构下，用户若想要访问到目标资源，首先要收集身份、设备的安全态势信息（风险判定）。身份信息方面，通过 Azure AD Identity Protection，Azure ATP 和 Cloud App Security 并结合微软自建的威胁情报库来监控和分析网络中的用户活动和信息。使用基于非对称密钥的用户身份验证（无密码方式）Hello for Business 和 Azure MFA 完成多因子的用户鉴别。设备信息方面，通过 Microsoft Defender ATP 进行基于风险的漏洞管理和评估，判断是否是受控设备，是否满足设备合规性要求，同时通过 Intune 完成设备管理。

在动态访问控制方面，内置于 Azure Active Directory 的 Conditional Access 在收到初次访问请求后，基于用户和设备的风险状况进行策略评估，调整已有的访问策略。当用户暂不满足信任要求时，通知用户再次进行多因子认证。上述过程持续地进行信息监测，且对用户无感知。

在自动化响应和可视化方面，微软在网络安全架构中，基于自身实践提出了安全运营架构，认为安全运营的需要通过工具和数据进行集成，而目前的安全运营主要依靠采集数据到进行 SIEM 的分析是不够的，因为采集的数据缺少检测、缺少一致性的语言定义。为此，微软统一了基本覆盖企业所有各类资产的 XDR 控制台，实现了数据的共享和集成，在通过安全自动化平台，以减轻安全运营的人工工作量，提高安全运营的效率和效果。

（三）全面建设零信任落地场景

1.远程办公场景

随着云计算、大数据、物联网、5G等技术的迅猛发展，数字化进程进一步推进，企业呈现出服务形式“网络化”、内部流程“数字化”、核心应用“云端化”、业务节点“边缘化”、办公场地和设备“多样化”等多种“新态势”。在新态势之下，企业远程办公已经成为一种常态，但以VPN接入、应用映射至外网、反向代理接入等为代表的传统远程办公手段存在资源暴露面大、权限管理粒度较粗等问题，企业资产易遭受网络攻击。

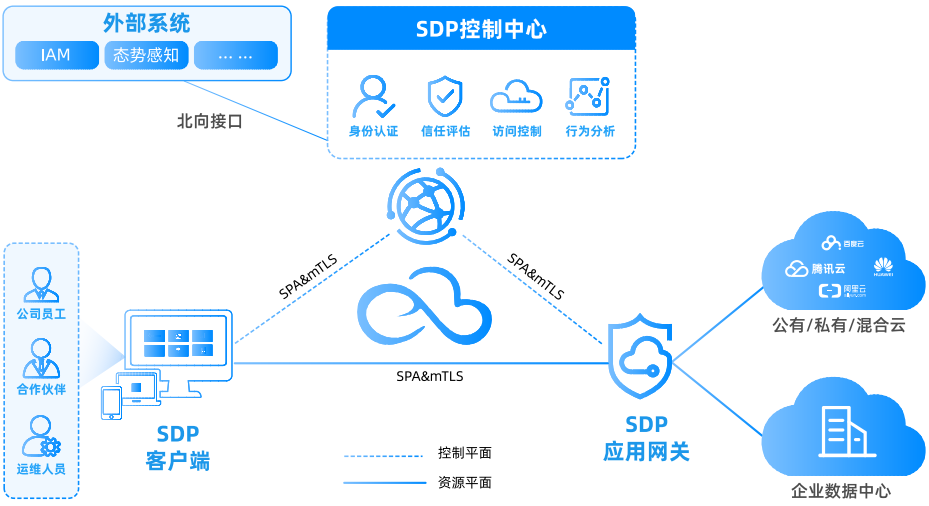

图10 零信任远程办公场景

基于 SDP 的零信任解决方案可以更好解决远程办公场景下的安全问题，一是基于 SDP 独有的三角形架构，实现控制平面和数据平面的分离，未经授权的访问无法建立数据平面的连接，大幅提升企业远程办公的安全性；二是 SDP 仅使用软件即可部署并管理，消除安全栈对硬件的依赖，扩展性强；三是 SDP 基于身份而非 IP 控制对资源的访问，仅授权用户才能访问相应的数据和应用程序，降低网络攻击风险。与传统 VPN 相比，零信任远程办公具有应用访问安全、数据使用安全、用户体验便捷三方面的优势：

- 应用访问安全。一方面，通过隐藏应用网关，确保只有合法用户才能够接入；另一方面，通过多因子认证、社交化账号接入和设备清单关联，确保只有身份可信的用户使用清单内的设备才能访问。
- 数据使用安全。通过精细化访问控制，实现人员对数据“可用可见、可用不可见、不可用不可见”等状态的统一授权管理。
- 用户体验便捷。一方面，可为用户提供一致的便捷体验，可基于 Web、客户端、移动 APP等多种访问方式；另一方面，可为管理员提供多维度的用户行为分析和应用访问状态分析，快速发现异常，即时告警、溯源、处置。

2.数据防护场景

内部员工恶意或无意的行为，是导致企业发生安全事件重要原因之一，如员工私下售卖设计图纸，离职员工将源代码传播至竞争企业、员工设备遭受木马导致数据泄露等。由于企业的数据可能存于云上、数据中心、员工设备、甚至合作伙伴和第三方人员设备中，因此数据防泄露工作难以开展。基于零信任的安全工作空间，可对物理上分散的数据进行逻辑上的封闭管理，为企业数据安全提供保障。

图11 数据安全场景

如图 11 所示，零信任控制中心统一管控工作空间的应用准入策略，一方面补足零信任在终端数据安全方面的能力，另一方面和零信任的自适应动态策略和细粒度权限管控相结合，形成完整的数据安全保护方案。与传统数据安全产品比较，零信任安全工作空间具有体验便捷、管理方便、数据安全几方面的优势：

- 体验更便捷。公私分离，个人数据不受影响，在终端开辟出的安全工作空间内，企业控制和记录员工的操作行为，并对数据进行管控，在安全工作空间之外，不涉及个人隐私，不改变用户的使用习惯。
- 管理更方便。零信任策略中心可以集成多安全产品，提供完整的用户行为审计和终端安全分析，通过零信任自适应动态策略管控和安全工作空间终端数据安全的融合，一次部署就可以实现多种安全防护，以最优的性价比完成统一安全管控。
- 数据更安全。安全工作空间与应用服务器之间建立安全加密隧道，数据在加密隧道内传输，防止网络监听，中间人篡改等黑客行为。同时每个安全工作空间可配置独立的安全策略，数据一旦进入安全工作空间，便不能私自将数据发送出去，实现自适应最小权限数据管控。

PART
04

结束语

零信任理念从提出至今，历时十八载（2004 年开始）——从早期耶利哥论坛对企业“去边界化”网络安全解决方案的探索，到 2010 年零信任概念（Zero Trust）正式提出，到 Google 开始正式推行 BeyondCorp 项目，再到如今，传统安全企业纷纷拥抱零信任，围绕零信任的创业型企业如雨后春笋般涌现，零信任重筑传统安全架构的时代已来。

基于零信任理念的企业安全架构关注整个业务访问过程中各个实体的可信，全面建设零信任的过程中，各个参与实体需要在零信任要求的框架下进行信任度的判断。本报告梳理出了可信身份与认证、数据安全隔离、动态访问控制、自动化响应和可视化四类关键技术：

- 传统边界安全以内外网划分作为信任边界，随着云和移动办公时代到来，传统的信任边界逐渐模糊，基于身份的访问控制更能够适应安全访问需求；
- 传统边界安全通过访问权限控制数据的安全，随着移动办公以及远程办公逐渐兴起，企业网络很难抵御来自内部的攻击，数据隔离保护实现了服务侧更细粒度的隔离以及数据不落地，降低了数据泄露地风险；
- 传统边界安全使用静态的访问控制策略来保证内网安全，随着业务资源逐渐上云，资源环境不断变化，静态策略不足以防护不断变化的资源，动态访问控制可以实时调整策略，使得策略控制更加灵活；
- 传统边界安全通过人工排查、半自动化处置等方式对告警进行处理，随着企业规模的增长，以人工方式解决问题的效率无法满足企业需求，自动化响应与可

视化可帮助企业快速定位问题节点并及时处理故障。

随着网络安全技术地不断发展，这些技术也不断地赋予着零信任新的内涵，推动了基于零信任理念的新安全模式被市场接受。

附录 编制单位介绍

江苏易安联网络技术有限公司

国家高新技术企业、专精特新小巨人企业——江苏易安联网络技术有限公司，专业从事网络安全产品研发与销售，是网络安全行业内领先的“零信任”解决方案提供商。公司总部位于南京，同时在北京、深圳、安徽、山东、杭州、西安等地铺设分支机构，致力于成为零信任安全领导者！

易安联专注零信任领域多年，围绕应用访问安全，先后发布 EnSDP（零信任安界防护平台）、EnBox（零信任安全工作空间）、EnCASB（零信任云应用安全接入平台）、EnAppGate（统一资源发布系统）、EnIAM（零信任身份管理平台）、EnDTA（天织·DTA 威胁分析平台）6 款产品，推出 ZTNA 零信任网络架构解决方案和 EnSASE 安全访问服务边缘解决方案并提供包括安全运营、实战攻防、应急演练等安全服务，目前合作客户已超 700 家，涵盖教育、运营商、电力、金融、互联网等行业。

云计算开源产业联盟

云计算开源产业联盟成立于 2013 年，挂靠在中国信息通信研究院。致力于联合国内云计算产业界相关方，共同推动云计算开源生态系统搭建、标准研制、测试评估、政府支撑、行业交流、国际合作等工作，是国内主流活跃的联盟组织之一。

易安联 Enlink Cloud

云计算开源产业联盟 OpenSource Cloud Alliance for industRy,OSCAR

编制单位

江苏易安联网络技术有限公司

云计算开源产业联盟