ICS 35.240
CCS L67

YD

中华人民共和国通信行业标准

YD/T [×××××]—[××××]
[代替 YD/T]

面向云计算的零信任体系 第1部分：总体架构

Cloud computing oriented zero trust system—
Part 1: Architecture

[点击此处添加与国际标准一致性程度的标识]

（报批稿）

2023.2

[××××]-[××]-[××]发布　　[××××]-[××]-[××]实施

中华人民共和国工业和信息化部　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规则起草。

YD/T ×××××—××××《面向云计算的零信任体系》分为以下六个部分：

——第1部分：总体架构

——第2部分：关键能力要求

——第3部分：安全访问服务边缘能力要求

——第4部分：数据保护工具要求

——第5部分：业务安全能力要求

——第6部分：数字身份安全能力要求

本文件为YD/T ×××××—××××的第1部分。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件由中国通信标准化协会提出并归口。

本文件起草单位：中国信息通信研究院、腾讯云计算（北京）有限责任公司、北京天融信网络安全技术有限公司、北京蔷薇灵动科技有限公司、深信服科技股份有限公司、北京神州绿盟科技有限公司、成都云山雾隐科技有限公司、北京京东尚科信息技术有限公司、华为技术有限公司、中兴通讯股份有限公司、杭州安恒信息技术股份有限公司、中国移动通信集团有限公司、中国电信集团有限公司、中国联合网络通信集团有限公司、网宿科技股份有限公司、新华三技术有限公司、北京金山云网络技术有限公司、西安邮电大学、北京西骏数据科技股份有限公司、北京神州泰岳软件股份有限公司、江苏易安联网络技术有限公司、浪潮电子信息产业股份有限公司、曙光云计算集团有限公司、深圳华大生命科学研究院、北京持安科技有限公司、深圳竹云科技股份有限公司、杭州亿格云科技有限公司、北京芯盾时代科技有限公司

本文件主要起草人：郭雪、吴倩琳、孔松、黄超、蔡东赟、熊瑛、王龑、刘晨、宋园园、田旭达、王浩硕、付怀勇、郭旸、林顺东 王鑫渊、李国、李然、赵亮、林木林、吴奕鹏、秦益飞、王玮、彭园、曾帅、何艺、刘浩、张鹏程、蔡国瑜、张小燕、侯芳、宋桂香、刘娜、邹艳鹏、谌鹏、王拥军、陈吴栋、史晓婧、孙悦、李永波、许金旺、陈晓、沈舒莉

引　言

近年来，云计算、大数据等新一代信息技术与实体经济加速融合，为各产业提质降本增效带来活力，产业数字化转型迎来发展浪潮。同时，数字化转型中 IT 架构的变革为企业带来新的安全需求和挑战，传统安全建设理念和手段遭遇瓶颈，如何更有效地保障数字资产与业务的安全可信，成为企业数字化转型中的难点。零信任、安全即服务、原生安全等新一代安全技术与业态兴起，为企业数字化转型安全建设提供思路和手段。

《面向云计算的零信任体系》标准对满足数字化转型需求的新一代零信任安全架构进行规范，拟由六个部分构成。

——第1部分：总体架构。目的在于规范系列标准所涵盖的内容。

——第2部分：关键能力要求。目的在于规范云环境下零信任产品的核心能力。

——第3部分：安全访问服务边缘能力要求。目的在于规范SASE场景下网络与安全的能力。

——第4部分：数据保护工具要求。目的在于规范云环境下数据保护工具的能力要求，为基于零信任理念进行数据最小化授权和保护提供支撑。

——第5部分：业务安全能力要求。目的在于规范云环境下基于零信任理念的业务安全能力。

——第 6 部分：数字身份安全能力要求。目的在于规范云上资源全面身份化后，其数字身份的安全管控能力。

面向云计算的零信任体系 第1部分：总体架构

1 范围

本文件规定了面向云计算的零信任体系总体架构，包括建设责任、设计原则、总体架构概述及其组成。

本文件适用于云服务客户基于零信任理念建设云化安全防护架构的规划与设计。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 29242-2012 信息安全技术 鉴别与授权安全断言标记语言

T/CESA 1165-2021 零信任系统技术规范

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

访问主体 access subject

能访问客体的主动实体。

[来源：GB/T 29242-2012，3.7]

3.1.2

访问客体 access object

系统中可供访问的资源。

注：资源如应用、系统、接口、服务、数据等。

3.1.3

零信任 zero trust

一组围绕资源访问控制的安全策略、技术与过程的统称。从对访问主体的不信任开始，通过持续的身份鉴别和监测评估、最小权限原则等，动态调整访问策略和权限，实施精细化的访问控制和安全防护。

[来源：T/CESA 1165-2021，3.3]

3.1.4

零信任供应方 zero trust provider

零信任安全能力的供应方。

注：本标准中零信任供应方简称供应方。

3.1.5

零信任应用方 zero trust customer

为使用零信任安全能力同零信任供应方建立业务关系的参与方。

注：本标准中零信任应用方简称应用方。

3.1.6

云工作负载 cloud workload

云环境中从应用程序层到管理程序或处理的自包含组件的整个应用程序堆栈。

注：自包含组件指堆栈中的虚拟机和容器

3.2 缩略语

下列缩略语适用于本文件：

API：应用程序接口(Application Programming Interface)

SASE：安全访问服务边缘（Security Access Service Edge）

SD-WAN：软件定义广域网（Software Defined Wide Area Network）

4 零信任安全建设责任

面向云计算环境下的零信任安全能力建设通常由零信任供应方与应用方共同完成：

a) 应用方作为牵头组织，建设前，充分考虑组织资金、人员、技术能力等情况，规划零信任部署战略；建设中，根据总目标以及阶段性目标推动计划实施；建设后，在保证零信任安全防护能力不中断的情况下，纳管更多组织资源；

b) 供应方作为零信任安全能力提供组织，建设前，配合应用方根据实际情况规划部署方案；建设中，实现零信任安全关键系统与应用方组织内已有系统的对接工作；建设后，按需提供售后服务。

5 零信任安全设计原则

零信任安全应满足如下基本原则：

a）身份安全是基石，单次访问的所有参与单元将基于身份进行认证，建立信任关系，以尽可能使访问客体处于安全状态；

b）访问主体在对访问客体进行资源访问前默认不可信，不为访问主体自动授予任何权限，应经过身份认证、授权和访问控制才可获取权限；

c）身份认证、授权和访问控制在单次访问的全生命周期过程中持续进行，确认本次访问中访问主体的信任状态符合安全策略才予以执行，在必要时重新进行身份认证和授权；

d)通过实时对多源信息进行分析、评估后获得授权策略，仅授予访问主体单次访问请求所需的最小权限。

6 总体架构概述

总体架构描述了基于零信任理念构建云化安全防护架构的能力要素，如图1所示，应用方与供应方基于零信任战略开展落地规划，部署零信任安全关键系统，并与应用方组织内的其他系统进行信息对接，接收身份、日志、合规、安全运营、威胁情报等信息，使得应用方可在身份安全、终端安全、网络安全、数据安全、应用云工作负载安全、安全管理六大领域获得细粒度的安全防护能力。配合业务资源纳管计划，渐进式部署并保障零信任安全架构落地后的正常运转，为应用方提供在远程办公、第三方接入、安全研发与运维、面向公众的服务访问、多分支互连、多云战略等场景下的安全防护能力。

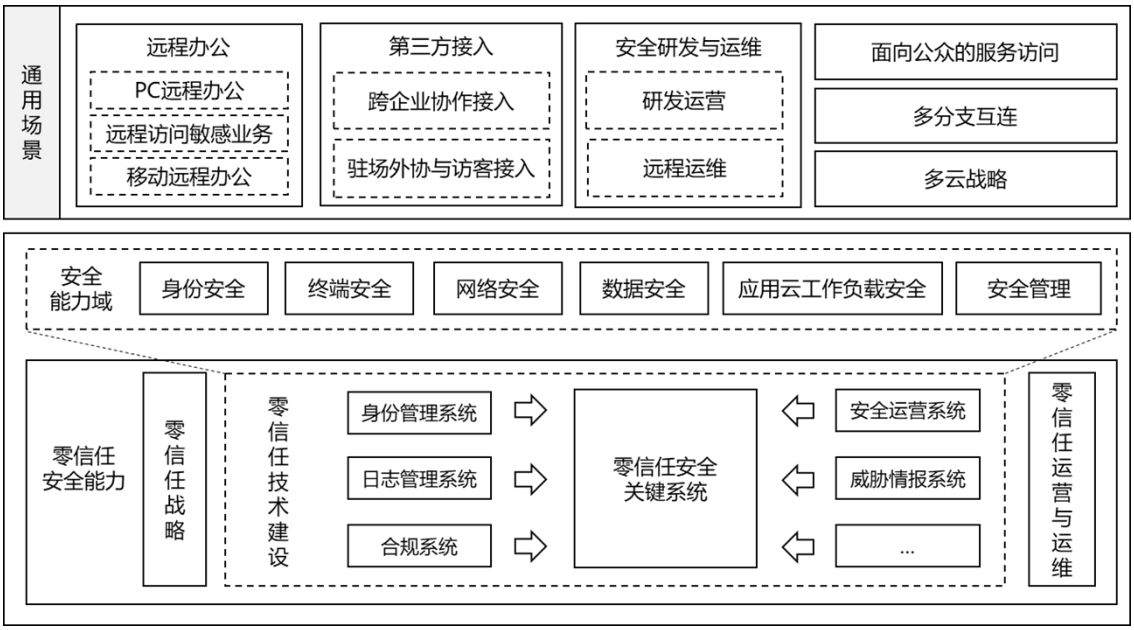

图1 总体架构

面向云计算的零信任总体架构应满足以下特性：

a) 零信任理念贯彻性：指零信任理念应融会贯通于组织内的各个安全域。通过对用户、终端设备、云工作负载、应用、数据等资源实现全面身份化，结合安全管理的持续、动态的安全监测能力，构建以身份为中心，持续认证和最小化实时授权的动态安全防护架构；

b) 原生安全性：指安全能力与组织云架构进行深度融合。

1) 可充分利用组织云平台原生的资源和数据，通过整合、关联分析各类数据，深入挖掘潜在风险；

2) 各安全域能力有效联动，对云资源进行更有力的控制；

3) 可解决云计算面临的特有安全问题。

7 总体架构组成

7.1 零信任安全能力

基于零信任理念的安全防护能力建设过程有三个阶段：

a) 零信任战略：从全局视角规划零信任的建设，根据目标制定阶段性计划，在资金和人员资质得到保障的前提下，推动计划落地实施；
b) 零信任技术建设：零信任安全关键系统是实现访问控制的核心，应支持接收来自身份、终端、网络、数据、应用云工作负载、安全管理系统的安全信息，用以持续地信任评估，提升授权策略判定的准确性，为资源的访问控制开展细粒度的防护，同时赋能上述六大安全能力域；
c) 零信任运营与运维：持续地将新增云上业务资源纳入零信任安全防护体系之下，并对发现的威胁进行及时响应和处理，提供可靠的零信任安全防护能力。

7.2 安全能力域

零信任理念的贯彻将体现在六大安全能力域：
a) 身份安全：提供云计算环境下身份安全能力建设，对资源身份全面数字化后的管控问题提供支撑能力，基于零信任理念赋予人员、设备乃至所有资源唯一身份标识，将以数据中心为中心，一种静态的，从固定场所接入的结构，转变为以身份为中心，一种动态的，从任意位置接入的结构，实现基于身份的动态访问控制；
b) 终端安全：提供云计算环境下终端安全防护以及企业移动化管理能力，基于零信任理念持续监测企业终端资产以确保其处于安全状态，提供端到端的安全性；
c) 网络安全：为组织云计算网络进行分段，提供细粒度的资源防护，并对云工作负载间的链路进行加密，无论网络位置如何，对所有资源与通信链路都进行安全防护；
d) 数据安全：提供云计算环境下数据保护能力的建设，以保障数据全生命周期的安全性和隐私性。基于零信任理念对数据开展分类分级，划分不同等级的访问权限，按最小权限授予访问请求相应数据，并持续监测数据传输过程；
e) 应用云工作负载安全：基于零信任理念对云计算资源进行细粒度的安全隔离，对用户与应用系统间、API间的访问进行监测，对单个资源的访问流量基于会话单独授权，阻断异常流量；
f) 安全管理：对组织内云上安全事件、安全信息等多源数据进行收集、处理、汇总和分析，基于零信任理念对多源数据进行动态地、持续地、综合地评估，为授权决策提供依据。

7.3 通用场景概述

基于零信任理念构建安全防护架构可解决多种场景下不同的安全需求：
a) 远程办公需求，通常涉及PC远程办公、远程访问敏感业务、移动远程办公等场景。组织通常面临访问接入地点分散，资源安全边界打破；接入设备多样化，设备安全状况参差不齐等问题。零信任安全防护架构不再依据网络位置来验证身份和提供权限，默认一切设备均不可信，基于多源评估结果授予权限，降低资源可见性与潜在攻击面；
b) 第三方接入需求，通常涉及跨企业协作接入、驻场外协与访客接入等场景。组织通常面临第三方组织接入，安全能力不对等引入的外部风险；非组织内人员连接内网，默认权限分配不合理等问题。零信任安全防护架构通过建立统一终端安全基线，仅在第三方设备满足基线要求下允许接入，基于最小权限原则授予权限，降低非组织内人员连接组织内网引入的安全风险；
c) 安全研发与运维需求，通常涉及研发运营、远程运维等场景。组织通常面临资源粒度细化，资源变化频繁，安全策略无法随资源变化而变化；安全建设滞后易面临软件代码本身具有安全风险；较多高权限账号的操作行为，存在身份冒用、审计薄弱等安全风险。零信任安全可为云工作负载赋予唯一身份标识，通过微隔离等级技术实现不同层级的安全隔离；同时安全左移，在应用开发、构建、测试、发布、运维的每个流程中引入安全；此外对拥有特权的运维人员在特权访问的过程中展开安全防护；

d) 面向公众的访问需求，通常指用户无需凭证即可访问业务前端资源的场景。组织通常面临服务平台对外暴露，业务系统无零信任网关前置而引入安全访问威胁等问题。零信任安全架构通过零信任控制中心直接向服务后台业务系统下发决策，以实现动态访问控制；

e) 多分支互连需求，通常指组织远程分支不与总部组网仍能安全访问内部资源的场景。组织通常面临分支机构资源连接稳定性不好，访问体验差；专线搭建成本高，资源浪费等问题。零信任安全能力可与SD-WAN结合，将安全能力下沉至网络边缘，通过全球接入点部署加速，满足弱网络、跨境接入网络延迟等问题；

f) 多云战略需求，通常涉及多云、混合云场景。组织通常面临多云权限控制不统一、跨云工作负载通信频繁、云异构接入方式复杂多样带来的安全风险。零信任安全防护以身份为核心，通过统一接入体系与统一权限控制，为用户实现一致的访问体验；同时，流量无需绕行数据中心，降低资源暴露风险。