2021

中国零信任全景图

（第二版）

发布单位：

CSA GCR cloud security GREATER CHINA REGION alliance

联合发布单位：

天融信 TOPSEC　SANGFOR 深信服科技　BJCA 数字认证　白山云科技 BAISHANCLOUD　美创 MEICHUANG

2021年12月30日

前言

随着云计算、移动互联、物联网等新技术的发展，网络空间已经发生了巨大的变化，从传统的网络边界已经发展到了无界化。面对全球数字化和万物互联的加速，传统物理边界被彻底打破，以零信任“永不信任，始终验证“为理念安全战略被国内外政产学研各界广泛认可。

零信任，是在不可信网络中构建安全系统。作为新一代信息技术安全架构，零信任创新性的安全思维契合数字基建技术特点，能更好地提升企业信息化系统和网络的整体安全性。

云安全联盟 CSA 作为零信任技术研究、标准制定的先行者及践行者，于 2020 年提出零信任十周年，成功举办零信任十周年暨第一届零信任峰会。云安全联盟大中华区为了向业界完整呈现中国零信任的行业生态，让读者对零信任有一个全面的认知，同时提高零信任领域相关厂商和优秀实践者（甲方）的曝光度和知名度，为打算实施零信任的甲方提供完整的参考，在 2020 年 12 月发布了《2020 中国零信任全景图》（第一版）。

在这一年里，零信任在落地应用方面取得长足进步与发展，这得益于网络安全厂商、用户、专家的支持与贡献，CSA 大中华区刷新推出《2021 中国零信任全景图》（第二版），供业界一览“零信任”全景概况，作学习及落地参考，共同推动零信任的落地应用，更好保障新网络新业务新场景的安全。

《2021 中国零信任全景图》如有疏漏或不妥之处，敬请各界包容与不吝指正。

目 录

1. 简要

《2021 中国零信任全景图》（第二版）共收录 88 家单位，比第一版零信任全景图参加的单位增加了 35%，为了更好地体现各单位擅长的领域，这次的评审归类结合各单位提供的申报材料与零信任相关项目的实际落地情况进行编制。相较第一版本，我们对第二版零信任全景图进行了优化调整，主要调整包括：

1）新增 1 个模块”公司类型“，对所有被调研的单位进行了分类；

2）“被保护对象”分类下增设“API”二级分类；

3）“业务场景”分类下增设“数据交换”、“企业多云战略”、“物联网”二级分类；

4）“业务类型”分类下增设“评估服务”和“治理服务”，取消“测评服务”二级分类；

5）“部署架构”分类下增设“终端”二级分类。

图 1.1：《2021 中国零信任全景图》

（关注“云安全联盟 CSA”公众号，回复“零信任全景图”，下载高清图片）

以下将从**零信任概述、零信任成熟度模型、零信任驱动因素以及零信任全景图分析**四个方面进行分析介绍，并对相关的代表厂商进行了分类汇总，希望能为甲方实践零信任提供参考和帮助。

2. 零信任概述

零信任思想的起源可以追溯到 1994 年由 JerichoForum 提出的 “去边界化”网络安全概念。而“零信任”这个词汇则是由 Forrester 原首席分析师 John Kindervag 于 2010 年首次提出的。零信任思想摒弃了“信任但验证”的传统方法，将“从不信任、始终验证（Never trust, always verify）”作为其指导方针。零信任发展大事记见图 2.1，零信任的标准演进见图 2.2。

图 2.1：零信任发展大事记

图 2.2：零信任标准的推进

零信任正在快速的发展中，越来越多的组织都在拥抱零信任。其中美国国防部 DoD 全面启动零信任战略并且发布了《DoD 零信任参考架构》。《DoD 零信任参考架构》分别从全景视角（AV）、作战视角（OV）、能力视角（CV）和标准视角（StdV）对零信任架构进行了描述。

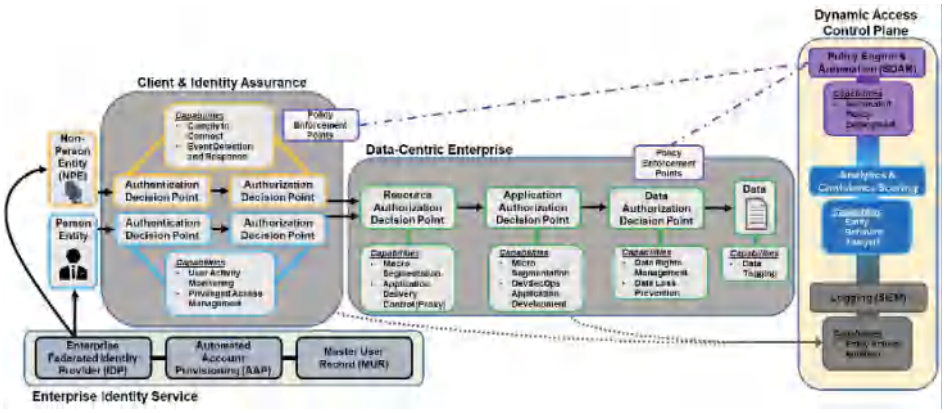


图 2.3：《DoD 零信任参考架构》

在本次收集的样本数据中，从客户行业分布来看，目前国内零信任的目标客户主要集中在政府及事业单位、金融、制造业、运营商、互联网、能源、电力和医疗行业。

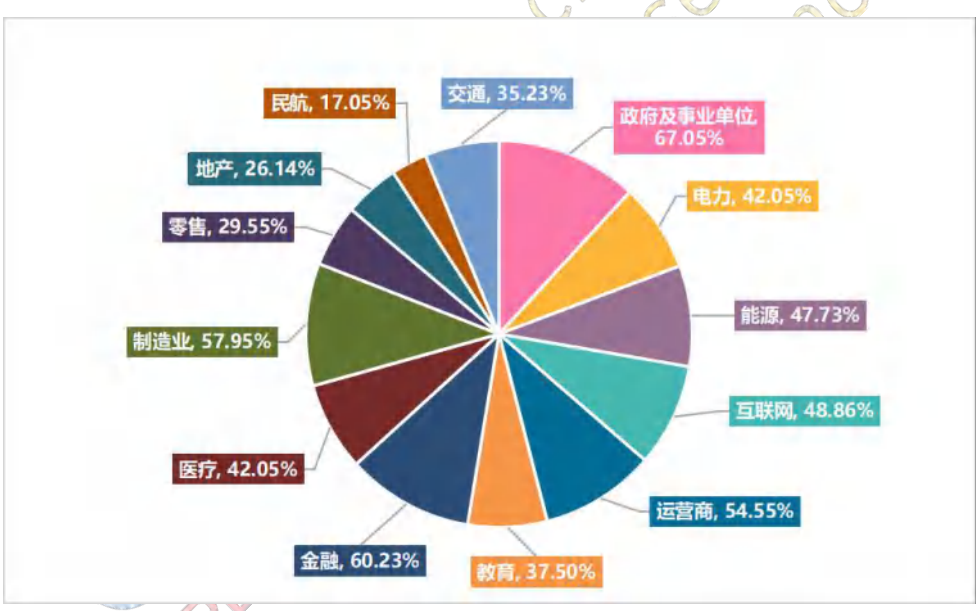


图 2.4：零信任应用行业分布图

3. 零信任成熟度模型

2021 年 9 月 7 日，美国网络安全与基础设施安全局(CISA)发布《零信任成熟度模型》草案。成熟度模型的推出给企业、组织、机构在零信任实践上提供了参考，有助于通过零信任加固设施，通过该模型可以评价当前的零信任能力和水平，同时作为零信任能力提升的参考。

成熟度模型包括五个支柱和三个跨领域能力，以零信任为基础。

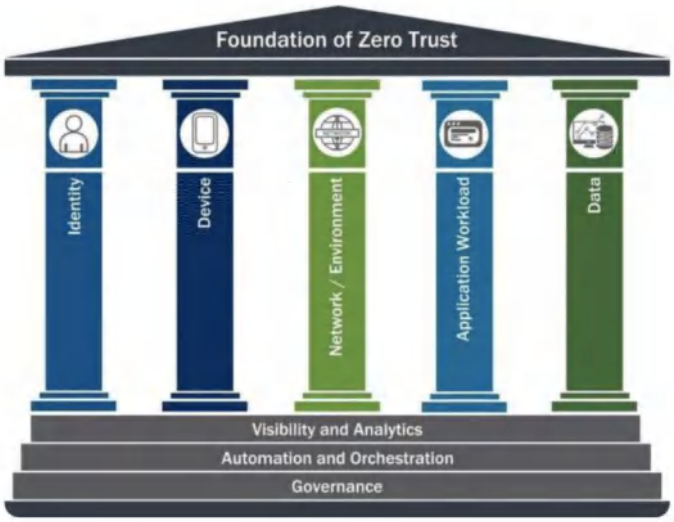


图 3.1：零信任成熟度模型五大支柱和三大能力

在每个支柱中，成熟度模型都为机构提供了传统、先进和最佳零信任架构的具体示例。

图 3.2：零信任成熟度模型的示例

而在国内，云安全联盟大中华区与中国信通院正联合编写“零信任能力成熟度模型”，相信中国特色的零信任模型将会很快诞生。

4. 零信任的驱动因素

4.1 合规驱动

近年来，数据安全形势日益严峻，侵犯个人隐私，攫取、破坏和滥用数据资源的行为时有发生，严重危害社会公共利益乃至国家安全。特别是随着数字经济日益成为国际竞争的制高点，数据安全和个人信息保护的重要性被提升至前所未有的高度。许多国家都认识到数据安全的重要性，逐步开始颁布并实施相关法律。从全球范围看，立法成为大国竞争和争夺数字经济领先地位的重要标志。

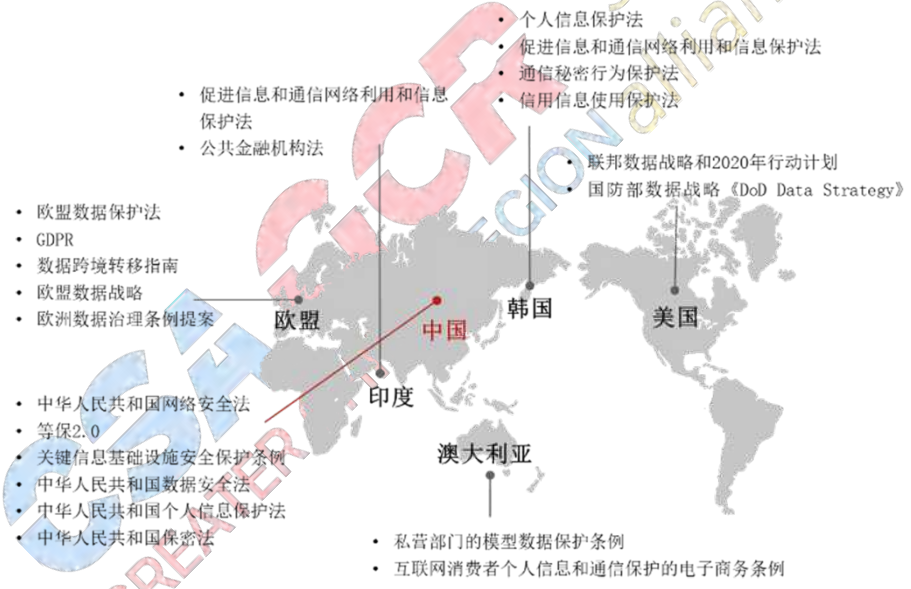


图 4.1：全球相关的法律法规和条例

2021 年 6 月 10 日，《中华人民共和国数据安全法》正式表决通过并于 2021 年 9 月 1 日正式实施，掀起整个行业对数据安全的聚焦，也凸显国家层面对保护数据安全的坚定意志。同年 8 月 20 日，《中华人民共和国个人信息保护法》正式表决通过并于 11 月 1 日正式实施。

因此，各行各业都迫切需要寻求新的数据安全解决之道，以零信任为代表的安全理念及架构等脱颖而出，成为推动并赋能合规建设的重要方法和指南，及赋能数字经济持续健康发展的坚实底座。

4.2 合需驱动

数字经济时代，数据已经成为基础性、战略性生产要素，成为决定各国数字经济发展水平和竞争力的核心资源。因此，数字化伴生的新技术和应用对网络安全技术和管理方式提出了更高要求。

图 4.2：零信任的合需场景

例如在全球 COVID-19 影响下，远程会议、远程运维、移动办公、数字孪生、元宇宙、各类沉浸式体验等新技术、新应用和新场景的层出不穷，加速了传统物理安全边界模糊化，同时也增加数据的暴露面，从而大大增加了在身份安全、链路安全、设备安全、应用安全、接入安全、大数据平台、云计算方面的安全风险。因此，需要一个更符合未来安全趋势的理念和架构来开展整体安全建设，也直接驱动了零信任在终端安全、应用安全、访问安全、设备准入、流动数据安全、勒索病毒防护等能力的应用和落地，满足金融、医疗、交通等领域全方位的零信任安全体系建设的需求。

5.零信任全景图分析

5.1 公司类型

今年我们对所有被调研的厂商进行了如下分类：甲方零信任实践者、增加零信任业务的原有安全厂商以及零信任领域的新兴创业公司。

由于零信任方案的落地需要与业务场景高度结合，作为自身拥有强大研发和安全能力的甲方企业，在这方面具有得天独厚的优势。自 Google 发表 Beyond Corp 系列论文至今，已经有不少甲方公开了他们的零信任实践经验，为业内提供了良好的参考。也有一部分企业在自身成功实践的基础上，将零信任方案或者产品商业化，从甲方优秀实践者转变为零信任厂商。

增加零信任业务的原有安全厂商基于之前已有的通用技术积累和丰富的产品化经验、项目实施经验，通过对已有产品的适当改造和一定程度的技术创新，快速切入零信任市场。对于国内大多数既有通用安全合规需求，又希望通过零信任提升现有安全能力（而不是彻底重建）的甲方来说，更倾向选择已经有过良好合作基础的此类厂商。

另一类就是零信任领域的新兴创业公司，这类厂商更倾向把产品做精做专，也相对更愿意迎合客户需求进行功能创新，因此也获得不少甲方的青睐。按公司类型分类，相关代表厂商如图 5.1 所示：

01 公司类型

甲方零信任实践者

SANGFOR 深信服科技 · 白山云科技 BAISHANCLOUD · HUAWEI · 腾讯云 · inspur 浪潮 · 网宿科技 WANGSU.COM · Midea Cloud 美云智数 · 持安科技 CHIANSEC · 德迅云安全 · 敬捷科技 agile technology

零信任领域的新兴创业公司

云深互联 · 芯盾时代 TRUSFORT.COM · 缔盟云 CLOUDAEMON · 数篷科技 DATACLOAK · WUOUN 物盾安全 万物互联 安全有盾 · 漠坦尼 · 盾御灵动 · 宁盾 · CyberEX · 易安联 · 绎云 · 云山雾隐 · 持安科技 CHIANSEC · 德思科技 Data Think · 数安行 DataSecOps · 虎符网络 · 01智维 · 指掌易 · 安几网安 NGeek C.S. · 星阑科技 · 完信科技 WeTrust · 中云网安 ZYPROTECT · 6cloud 六方云 · 驭安科技 YUANSEC · 从云科技 · 一知安全 · 志翔科技

原有安全厂商增加零信任业务

天融信 TOPSEC · SANGFOR 深信服科技 · 数字认证 · 白山云科技 BAISHANCLOUD · 美创 · 阿里云 · HUAWEI · 腾讯云 · 奇安信 · NSFOCUS 绿盟科技 · 360政企安全 · 亚信安全 · 知道创宇 · 竹云 bamboocloud · UCLOUD 优刻得 · 任子行 SURFILTER · yytek 云盾科技 · 九州云腾 IDsManager.com · 智安网络 ZHIAN NETWORK · DPtech · 观安 · 全知科技 QUAN ZHI TECH · 安恒信息 DAS-SECURITY · 安讯奔 · LUOAN 珞安科技 · 网御星云 · 网宿科技 WANGSU.COM · 世平信息 SPINF · TEPAIDT 万物安全 · 中孚信息 · 申石软件 · 安全狗 · Midea Cloud 美云智数 · 派拉软件 · 美亚网安 · H3C · 德迅云安全 · Hillstone 山石网科 · 敬捷科技 agile technology · 联软科技 · 吉大正元 · 上元信安 · Neusoft 东软 · ultrapower 神州泰岳 · 开安科技 · 创安恒宇 BDSECURITY.COM · 默安科技 · 明朝万达 Wondersoft · sansec 三未信安 · 圣博润 SBR-info · 青藤云安全 · EVERSEC 恒安嘉新 · Ftrans 飞驰云联 · 格尔软件 KOAL

发布单位：CSA GCR cloud security GREATER CHINA REGION alliance

联合发布单位：天融信 TOPSEC · SANGFOR 深信服科技 · 数字认证 · 白山云科技 BAISHANCLOUD · 美创

（排名不分先后）

5.2 被保护对象

零信任聚焦于保护“资源”，即本文所述“被保护对象”，包括组织拥有的全部数据、应用和 IT 资产（设备、设施、工作负载等）。保护数据主要是指防止数据泄露和非授权访问；保护应用主要是应用程序的隐身、应用的细粒度动态权限管控、以及业务安全等；保护设备/设施/工作负载主要是指终端设备、基础设施或工作负载的隔离与保护，比如云主机、容器等工作负载之间的隔离与安全保护。**考虑到 API（应用程序接口）在数字化进程中所起的作用越来越大，而 API 安全问题导致的数据泄露事件也在不断增加，因此我们今年在被保护对象中增加了 API 这一分类。保护 API 主要包括 API 安全代理与业务隐藏、访问者身份鉴别和权限控制等。**

组织在选择零信任策略执行点（PEP）组件时，首先应识别所需要保护的资源类型（如前所述）以及对资源的访问方式，例如用户访问业务应用、运维人员访问 IT 资产、微服务之间进行 API 接口调用、应用系统访问后台数据库，等等。然后选择适当的防护产品，以代理或网关方式部署在被保护对象本地或前端，并配合零信任策略决策点（PDP）实现对资源的动态保护。按被保护对象分类，相关代表厂商如图 5.2 所示：

02 被保护对象

数 据

设备、设施或工作负载

应用

API

发布单位：CSA GCR cloud security GREATER CHINA REGION alliance

联合发布单位：天融信 TOPSEC、SANGFOR 深信服科技、数字认证、白山云科技 BAISHANCLOUD、美创

（排名不分先后）

5.3 业务场景

安全产品往往具有很强的场景化特征，在不同场景下选择合适的厂家是安全实施的第一步。**跟去年相比较，我们今年增加了数据交换、企业多云战略、物联网等场景**，这是因为数字化改革越来越深入，数据交换是数字经济的基础，数据往往掌握在不同部门、不同组织手里，只有把这些数据联合起来才能更好的发挥数据的价值。Gartner 调查表明：到 2022 年底，35%的大型机构将通过正式的在线数据市场成为数据的卖家或买家，而 2020 年这一比例为 25%. 这也说明数据交换市场正在放大，自然安全问题也会越来越明显。而云化和物联网的发展，大家都能切身感受到。

上云还加快了 SASE 的发展，SASE 是一种基于实体的身份、实时上下文、企业安全/合规策略，以及在整个会话中持续评估风险/信任的服务。SASE 整合了软件定义网络和安全，安全即服务。根据 Gartner 的预计，到 2024 年，至少 40%的企业将有明确的策略采用 SASE，高于 2018 年底的不到 1%。

当我们的业务正在快速放大，安全问题往往会成为一个障碍。Gartner 的研究预计到 2022 年底，80%的云漏洞将来自客户配置错误，凭证管理不善或内部盗窃。避免这些缺陷的最佳方法是使用自动化平台运行策略来确保安全合规性。安全厂家有责任为组织提供合适的产品或者解决方案，推进业务的创新和变革。按业务场景分类，相关代表厂商如图 5.3 所示：

5.4 业务类型

与去年相比，我们删除了测评服务，但是增加了评估服务和治理服务。零信任是一个安全新概念，不同的厂商在零信任市场上提供的业务类型也有所不同，主要包括产品、服务和方案，业务类型体现了厂商的业务侧重点。标准产品解决相对比较明确的业务场景，它的特点是投入成本相对比较少，项目实施周期短，可控性高。服务指的是安全相关的一些咨询、评估等，当然厂商可能会有自己的一些工具配合人力服务。而方案一般是产品加服务的形式，形成一个整体解决方案，某些提供方案的厂商，可能也会使用其他厂商的一些产品甚至服务，一般周期会比较长。

随着数字经济的高速发展，对于安全的诉求越来越高。根据 Research Dive 最新发布的报告显示，全球零信任网络安全市场规模从 2019 年的 185.0 亿美元增长到 2027 年的 667.413 亿美元，从 2019 年到 2027 年的复合年增长率为 17.6%，而其中零信任整体解决方案的市场份额将会越来越大。零信任从单一产品往平台、整体解决方案发展的趋势越来越明显。对于甲方而言，选择合适的零信任厂商可以加速零信任改造，为业务赋能，有助于数字化改革，同时从数字化改革中获取增量业务所带来的创收。按业务类型分类，相关代表厂商如图 5.4 所示：

04 业务类型

产品和解决方案

咨询服务

5.5 技术类型

跟去年相比，技术类型并没有调整，虽然技术不断发展，但零信任领域使用的主要技术还是 SDP，IAM 和微隔离。IAM 作为身份治理的核心技术，SDP 解决南北向安全问题，微隔离解决东西向安全问题。其中有一个有趣的事情：微隔离产品入选了 Gartner 发布的 2021 年 CWPP 市场指南，说明数据中心内部东西向流量的安全问题越来越受重视。这跟现在的系统越来越复杂，微服务、中间件、各种中台以及云部署有一定关系。按技术类型分类，相关代表厂商如图 5.5 所示：

IAM

安讯奔 阿里云 宁盾 芯盾时代 TRUSFORT.COM 亚信安全 九州云腾 奇安信
美创 MEICHUANG Ultrapower 神州泰岳 默安科技 inspur 浪潮 HUAWEI 腾讯云
数字认证 派拉软件 数安行 SANGFOR 深信服科技 KOAL 易安联 网宿科技 WANGSU.COM
德迅云安全 持安科技 CHIANSEC Midea Cloud 美云智数 bamboocloud NSFOCUS 绿盟科技
云山雾隐 指掌易 吉大正元 安几网安 NGeek C.S. 安恒信息 绎云
任子行 SURFILTER 星阑科技 CyberEX 德思科技 Data Think H3C 驭安科技 天融信 TOPSEC
sansec 三未信安 绵安科技 网御星云 360政企安全 全知科技 QUAN ZHI TECH 美亚网安

微隔离

Hillstone 山石网科 阿里云 美创 MEICHUANG 芯盾时代 TRUSFORT.COM 数篷科技 DATACLOAK 青藤云安全
6cloud 六方云 Neusoft 东软 inspur 浪潮 亚信安全 Ultrapower 神州泰岳 派拉软件
安全狗 志翔科技 上元信安 sansec 三未信安 星阑科技 SANGFOR 深信服科技 CyberEX
KOAL 漠坦尼 H3C 创安恒宇 G'HANIR 360政企安全 美亚网安

辅助技术

中云网安 ZYPROTECT 芯盾时代 TRUSFORT.COM 敏捷科技 agile technology 美创 MEICHUANG 数篷科技 DATACLOAK 阿里云
数安行 DataSecOps 数字认证 易安联 九州云腾 志翔科技 TEPAIOT 万物安全 绵盟云 CLOUDAEMON
星阑科技 Ftrans 飞驰云联 Midea Cloud 美云智数 inspur 浪潮 世平信息 SPINFO 美亚网安 Ultrapower 神州泰岳
NSFOCUS 绿盟科技 绎云 创安恒宇 亚信安全 一知安全 sansec 三未信安
DP tech 智维 绵安科技 虎符网络 KOAL 明朝万达 Wondersoft
吉大正元 宁盾

发布单位：CSA GCR CREATER CHINA REGION alliance cloud security

联合发布单位：天融信 TOPSEC SANGFOR 深信服科技 数字认证 白山云科技 BAISHANCLOUD 美创 MEICHUANG

（排名不分先后）

5.6 服务模式

零信任服务的部署模式取决于安全要求，和去年相比，没有做调整，主要包括私有化、云化以及混合模式。私有化的部署模式下相关的产品或服务以私有化的形式提供，相关的资源或服务由一个用户独占使用；云化通过公有云的形式为众多用户提供零信任服务，所有的用户共享公共的云资源；还有一种模式是同时支持私有化和云化服务的混合模式。不同的组织因为业务形态、数据的敏感程度、风险承受能力或监管的要求不同，而选择不同的服务模式。很多高监管行业的客户可能更倾向于选择私有化服务模式，将产品部署在自己的私有环境。公有云模式因为可以以云服务的形式服务于多个客户，可以节省相关的 IT 基础设施成本支出，具有较高的性价比。**但从调查来看，目前绝大多数的零信任部署优先采用私有模式，说明大量的客户还是希望对平台有较强的管控力。**按服务模式分类，相关代表厂商如图 5.6 所示：

5.7 部署架构

零信任的经典部署架构主要包括：设备代理/网关部署、飞地部署、资源门户、沙箱、终端和探针等，相比去年，我们增加了“终端”。设备代理/网关部署架构 PEP 位于资源上或资源前，网关作为资源的代理，与资源通信。飞地部署架构下网关位于某一资源飞地边界(如数据中心的边界)。资源门户部署架构 PEP 充当用户请求网关(如公有云的资源管理门户、企业的办公门户站点等)。沙箱部署则是通过沙箱让程序隔离运行。除此以外还有部署与终端、核心交换机旁路部署、微隔离等形式。部署架构的选择很大程度上由业务场景决定，企业选择的部署模式需要结合实际的业务场景。从目前的落地情况看，设备代理和终端这两种架构的部署模式占据了主流。按部署架构分类，相关代表厂商如图 5.7 所示：

资源门户


亚信安全
安讯奔
九州云腾
Ultrapower 神州泰岳
阿里云
Hillstone 山石网科
芯盾时代 TRUSFORT.COM
奇安信
默安科技
数篷科技 DATACLOAK
易安联 Enlink cloud
腾讯云
联软科技
派拉软件
宁盾
网宿科技 WANGSU.COM
格尔软件 KOAL
德迅云安全
安恒信息
天融信 TOPSEC
持安科技 CHIANSEC
Midea Cloud 美云智数
NSFOCUS 绿盟科技
inspur 浪潮
云山雾隐
吉大正元
bamboocloud
绎云
指掌易
H3C
一知安全 yizhisec.com
任子行 SURFILTER
CyberEX
德思科技 Data Think
安几网安 NGeek C.S.
星阑科技
观安
SupreAXES
智维
DPtech
从云科技
网御星云

飞地


Ultrapower 神州泰岳
締盟云 CLOUDAEMON
芯盾时代 TRUSFORT.COM
阿里云
指掌易
inspur 浪潮
奇安信
九州云腾
持安科技 CHIANSEC
德迅云安全
云山雾隐
安全狗
星阑科技
bamboocloud
从云科技
格尔软件 KOAL
智维
安几网安 NGeek C.S.

沙箱


芯盾时代 TRUSFORT.COM
締盟云 CLOUDAEMON
数篷科技 DATACLOAK
美创
SANGFOR 深信服科技
数安行
指掌易
inspur 浪潮
易安联 Enlink cloud
联软科技
阿里云
奇安信
星阑科技
安全狗
一知安全 yizhisec.com
格尔软件 KOAL
HUAWEI
创安恒宇
安几网安 NGeek C.S.
九州云腾
完信科技 WeTrust

终端


G'HANIR
Hillstone 山石网科
宁盾
芯盾时代 TRUSFORT.COM
智维
美创
亚信安全
奇安信
敏捷科技 agile technology
TEPAIOT 万纲安全
数篷科技 DATACLOAK
联软科技
HUAWEI
腾讯云
阿里云
九州云腾
明朝万达 Wondersoft
网宿科技 WANGSU.COM
数安行
易安联 Enlink cloud
Ultrapower 神州泰岳
安恒信息
安全狗
Neusoft 东软
Ftrans 飞驰云联
派拉软件
H3C
云山雾隐
inspur 浪潮
白山云科技 BAISHANCLOUD
持安科技 CHIANSEC
指掌易
志翔科技
bamboocloud
NSFOCUS 绿盟科技
绎云
数字认证
CyberEX
星阑科技
DPtech
WUOUN 物盾安全
德思科技 Data Think
任子行 SURFILTER
创安恒宇
安几网安 NGeek C.S.
从云科技
观安
360政企安全
网御星云
完信科技 WeTrust

6.零信任落地案例

6.1 深信服-葛洲坝集团零信任安全办公项目

6.1.1 方案背景

中国葛洲坝集团股份有限公司是一家集工程建设、工业制造、投资运营、综合服务为一体的跨国经营企业集团，是大型基础设施投资建设领域的“国家队”，是水利水电建设的“全球名片”，创造了 5000 余项精品工程和 100 多项世界之最。葛洲坝集团多次荣获国家科技进步特等奖、国家科技进步一等奖、国家优质工程金质奖、中国建筑工程鲁班奖、中国土木工程詹天佑奖、全国五一劳动奖状、中国对外承包工程企业社会责任金奖等荣誉，入选美国《工程新闻记录》（ENR）全球国际承包商 225 强、《财富》中国 500 强企业、中国建筑业竞争力 200 强企业等排名。

葛洲坝集团坚持科技创新引领发展，是国家创新型企业和国家高新技术企业，在数字化浪潮下，葛洲坝集团也在积极投入数字化建设。随着数字化转型的不断深化，在业务访问上，越来越多的业务系统需要实现随时随地的移动接入，建设面临诸多挑战：

1）过去考虑便利性，一些移动接入的业务系统直接暴露在互联网上，且明文传输，存在极大的安全风险，需要收缩业务系统暴露面，实现数据安全传输；

2）员工可以通过办公 APP、企业微信、浏览器等多种方式访问业务系统，希望提供安全、快捷的认证方式，以及一致的访问权限；

3）组织架构上存在众多分支单位，需实现安全接入策略的分级分权管理；

4）日志审计合规，需要提供详尽的日志审计功能，满足 6 个月以上的日志审计的要求。

葛洲坝集团希望找到一套合适的方案来解决上述问题。

6.1.2 方案概述和应用场景

通过前期的方案调研，葛洲坝选择了以零信任理念构建业务安全访问的防护体系，结合自身需求及实际测试，最终选择了深信服零信任安全办公方案。

1）通过集群部署零信任控制中心和零信任代理网关，实现统一管理和保障办公业务安全访问的高可靠性；

2）通过策略配置，将业务系统收缩进内网，避免直接暴露在互联网，并通过 SSL 加密

技术实现数据传输加密；

3）通过零信任控制中心与企业微信、统一认证平台、办公 APP 进行对接，实现统一身份管理和无密码认证，PC 端采用企业微信扫码登录，手机端可实现指纹快捷认证；

4）通过管理员分级分权功能，将系统管理员、安全管理员、审计管理员角色分开，满足等保合规要求，并通过创建二级管理员，实现下级单位自助运维管理；

5）通过零信任的日志中心平台将所有的用户日志、管理员日志统一存储、查询，并提供用户访问行为、统计报表和风险分析功能；将用户访问应用的行为明文镜像给态势感知，实现安全联动。

6.1.3 优势特点和应用价值

葛洲坝集团通过零信任方案建设实现了安全移动办公，员工可以随时随地安全地访问各内网业务系统，办公效率得到了大幅提升；

通过办公 APP、统一认证平台、企业微信与零信任结合，实现了门户入口集约化和统一身份管理，提高办公效率与安全性；

管理员分级分权、日志留存等，满足合规以及日常管理要求。

6.1.4 经验总结

项目实施过程也经历了不少挑战，最终在厂商的配合下顺利落地：

1）业务系统的快速上线：由于业务系统众多，涉及到零信任设备要与办公 APP、企业微信、统一认证平台对接，除了产品能力外，实施经验也尤为重要。在整个业务上线过程中，深信服积极提供同类场景的经验参考，保障了业务顺利上线；

2）业务的延续性：在零信任上线前，原本 VPN 的访问路径要保持不能中断，涉及到现有应用、权限等策略的迁移和零信任上线前期的并存使用，既要考虑策略的平滑迁移，也要考虑并存场景下的冲突问题。深信服在实施中提供了 VPN 配置转化服务，保障了策略平滑迁移，且零信任采用与 VPN 不同的技术架构，避免了客户端的兼容冲突，在不中断业务的情况下实现了零信任的上线。

6.1.5 其他（反馈/荣誉）

客户评价：深信服零信任解决方案极大地提升了葛洲坝集团的办公业务访问的安全性，满足等保合规、审计合规的要求，产品兼容性好、日志审计详细，能很好地提升运维效率。

6.2 天融信-某省公安大数据智能化安全建设采购项目

6.2.1 方案背景

某省公安厅大数据安全整体解决方案，以“一切资源化、资源目录化、目录全局化、全局标准化”为设计理念，以“分层解耦，异构兼容”为设计思路，以“安全、合规、可信”为实现目标，提升科学实用的体系化安全防护能力，规范化安全管理能力，综合化安全运维能力，实现全网安全态势敏锐感知，安全威胁快速检测与处置确保大数据全程可知可控，可管可查，变静态为动态，变被动为主动，为某省公安厅公安大数据智能化建设保驾护航。

6.2.2 方案概述和应用场景

本案以数据安全为中心，以安全基础设施为支撑，以安全大数据智能分析为抓手，从“云、数据、应用、网、边界、端”六维构建纵深，实现统一安全管理，构建“安全、可信、合规”的大数据智能化安全立体纵深防御体系，形成科学实用的规范化安全管理能力、体系化安全防护能力、综合化安全运维能力，变静态为动态，变被动为主动，为公安大数据智能化建设提供坚实保障。本次重点建设跨域安全访问与数据交换平台。

本案紧密结合新一代公安信息网网络架构设计和大数据、云平台、智能应用设计开展大

数据智能化工程安全体系设计，确保框架先进性；运用国际通用安全架构指导大数据智能化安全体系设计，确保理念先行；深入结合可信技术、大数据技术开展大数据智能化安全系统设计。

总体架构图

本案建设以满足“安全、可信、合规”总体建设目标为前提，提出了“统一规划、统一标准、急用先行、分步实施”的总体原则，采用如下核心组件进行建设。

审计中心

审计中心具有超强的审计洞察和可扩展性，可支持各类信息（日志信息、威胁信息等）的处理与分析，通过采集关键节点服务日志信息，以大数据技术驱动过程行为数据分析，采用机器学习方法进行安全分析，能够检测高级、隐藏和内部威胁的行为分析技术，不需要使用签名或规则。且在杀伤链上能关联数据，进行有针对性的发现。

审批中心

审批中心负责审批工作的信息化、流程化和规范化，实现任务的上传下达、工作督办监督体系、规范数据查询和侦控手段审批流程。审批中心提供业务流程同步，实现接入系统信息管理、权限同步，可通过短信发送申请信息或审批信息，还能实现与安全代理、认证、权限、审计及应用系统的联动。

安全管理中心

安全管理中心基于大数据基础架构平台开发，使用 ETL 组件进行数据预处理，根据行业

数据治理标准规范和行业规范安全数据治理需求，实现数据治理功能，能够提供对各种采集数据进行数据解析、标准化、丰富化、归一化、过滤、补全、清洗等处理，保障数据的完整性、可用性，支持通过编写配置文件实现非编程方式的日志数据解析。

可信接入代理

可信接入代理支持可信接入、访问控制、NAT、应用层检测、流量监控、日志记录、告警等功能，主要用于为不可信任的外网用户提供可信接入，为内网资源提供可信任安全屏障。可信接入代理在为用户提供可信接入时，可轻松适应某些资源具有大量的 IP 地址信息，且 IP 地址不固定的应用场景。

可信 API 代理

可信 API 代理通过流量控制、攻击防御、传输加密等多种 API 相关安全防护技术，为业务提供 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，对 API 进行全生命周期的权限管理，全面解决企业 API 接口服务面临的安全问题。

可信代理控制服务

可信代理控制服务可针对业务应用及 API 服务的访问控制需求，采用了用户认证授权、身份权限管理、风险感知、UEBA 等多项技术，集中解决应用访问场景的安全问题等。同时，可信代理控制服务也是零信任体系安全解决方案中的重要组成部分，联动各个平台的控制中心。

数据安全交换系统

数据安全交换系统具体包括前后置、单向光闸三部分。前置代理系统是双网信息交换中面向低安全级别网络的信息采集及推送系统，前置代理系统的作用主要是以各种形式采集外网中需要传输到内网的数据，通过安全处理及分流，传输到内部网络。

6.2.3 优势特点和应用价值：

根据公安大数据“一切资源化、资源目录化、目录全局化、全局标准化”的原则，通过本案的建设，做到全网安全态势敏锐感知，安全威胁快速检测与处置，确保大数据全程

可知、可控、可管、可查，为公安大数据智能化建设提供严密安全保障。

6.2.4 方案价值

符合新一代公安信息网标准规范要求

通过“新一代公安信息网项目”成功落地，项目实践证明产品完全满足公安部相关标准规范要求。

以安全管理中心为中枢构建全局化安全防护服务体系

通过为公安客户构建事前主动防御、事中持续检测与响应、事后迅速恢复的全局化安全防护体系。

建立起行业建设标准

通过本案的实施，树立起新一代公网网的建设标准，打造一个中心（即安全管理中心）、两大体系（即零信任体系和安全防护体系）的安全支撑能力。

6.2.5 方案优势

高性能无瓶颈

- 本案重点对核心产品(可信 API 代理)和数据交换通道的性能重点做了优化设计。
- 由于可信 API 代理负责对业务应用 API 接口的访问控制，承载较多的业务并发访问压力，极容易成为整个安全访问平台的瓶颈。通过在可信 API 代理设备前部署负载均衡，通过轮询、随机等多负载均衡算法将业务访问压力均衡分摊到两台可信 API 代理设备上，并可在不影响正常业务情况下灵活扩展多台可信 API 代理设备。
- 数据交换通道性能设计最大通道带宽可达 20GBPS，单个文件可支持 30G 大小进行无丢包交换。

国产化适配

- 本案涉及的国产硬件适配能力，充分保护用户已有建设投资，最大化保护 IT 投资成本。
- 各产品互兼容性高
- 本案的产品和方案均以构建强大的扩容能力、广泛的产品技术兼容性为设计原则，不仅新产品建设完美兼容，还与原有业务系统、身份认证充分融合，发挥利旧原则，建设好新一代公安网。

6.2.6 经验总结：

本项目基于公安大数据相关规范对公安应用业务的流程再造与优化，改造过程中势必会对当前业务造成一定的影响，为了尽量减少规避影响范围，建议从业务稳定性、安全性等角度综合考虑：

项目实施期间，如何保证原业务的稳定运行。为了解决这个问题，需要提前做好前期准备，包括原业务系统的备份、安排在非业务办理时间进行业务部署割接；在业务割接过程前设计好应急保证措施，当遇到无法排除的故障时应该及时回退到部署前状态。

新部署的安全访问平台增加了可信接入代理、可信 API 代理等多个验证功能执行点，如何保障部署后业务访问体验不受影响。通过对新安全访问平台的访问流程进行梳理后发现新通道的瓶颈在可信 API 代理网关系统上本案选用了业界最高性能的专用硬件平台，将可信 API 代理的性能提高至 40G 左右，同时在两台可信 API 代理网关之前部署了负载均衡系统来保证该平台的稳定性及连续性。

本项目中设计了多类安全产品的部署联调，如何能够保证在规定时间内完成本工作内容。本项目中设计的核心产品包括可信接入代理、可信 API 代理和可信代理控制服务，为了保证系统的快速联调部署，通过三大核心部件的快速部署，确保实施周期。

6.2.7 其他

通过建设本案，实现了统一的身份认证管理的精细化、动态化的授权能力。这部分需求的目的是解决人或者接入设备的身份安全，确保所有接入人员和设备的身份是安全可信的。由于大数据中心的数据涉及大量的国家安全、社会安全、个人隐私等敏感信息，所以对权限的要求非常严格。必须采用能够根据数据的敏感程度和重要程度进行细粒度的授权，并结合人员的行为分析和访问的环境状态动态授权，在不影响业务效率的前提下，确保数据访问权限最小化原则，避免因为权限不当导致的数据泄露。该省公安厅通过建设省级大数据智能化平台建设，树立起新一代公网网的建设标准。

6.3 数字认证—零信任安全架构在医疗领域的应用

6.3.1 方案背景

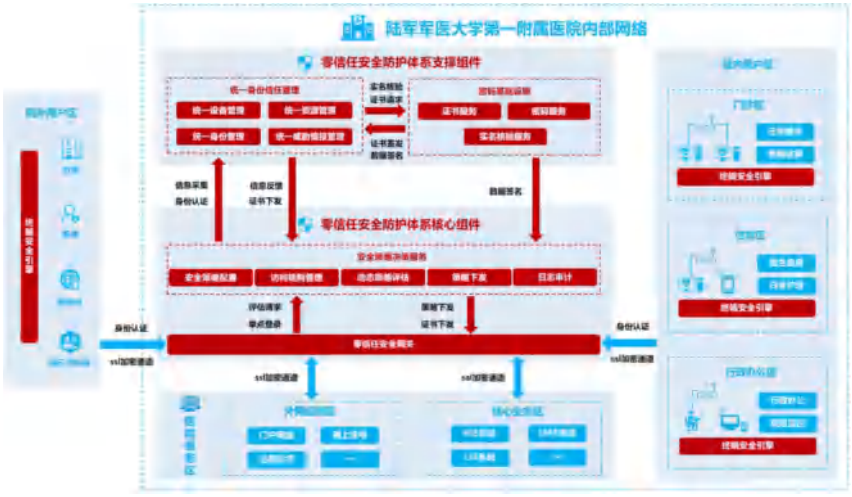
陆军军医大学第一附属医院又名西南医院，是一所现代化综合性“三级甲等”医院。近年来随着远程问诊、互联网医疗等新型服务模式的不断丰富，医院业务相关人员、设备和数据的流动性增强。网络边界逐渐模糊化，导致攻击平面不断扩大。医院信息化系统已经呈现出越来越明显的“零信任”化趋势。零信任时代下的医院信息化系统，需要为这些不同类型的人员、设备提供统一的可信身份服务，作为业务应用安全、设备接入安全、数据传输安全的信任基础。

6.3.2 方案概述和应用场景：

1、方案概述

本方案主要建设目标是为陆军军医大学第一附属医院内外网建立一套基于“可信身份接入、可信身份评估、以软件定义边界”的零信任安全体系，实现医院可信内部/外部人员、可信终端设备、可信接入环境、资源权限安全。全面打破原有的内外网边界使得业务交互更加便利，医疗网络更加开放、安全、便捷，为医院全内外网业务协作提供安全网络环境保障。

根据对陆军军医大学第一附属医院安全现状和需求分析，采用基于零信任安全架构的身份安全解决方案，为医院构建零信任体系化的安全访问控制，满足医院内外部资源安全可信诉求。总体架构设计如下：



陆军军医大学第一附属医院总体架构设计图

面向互联网医疗的应用场景，通过与可信终端安全引擎、零信任安全防护体系核心组件、零信任安全防护体系支撑组件结合，为医院设备、医护人员和应用提供动态访问控制、持续认证、全流程传输加密。

陆军军医大学第一附属医院零信任安全架构主要构成产品：

1、终端安全引擎

在院内外公共主机、笔记本电脑、医疗移动设备等终端设备中，安装可信终端安全引擎，由统一设备管理系统与院内资产管理系统对接，签发设备身份证书。医院用户访问院内资源时，首先进行设备认证，确定设备信息和运行环境的可信，通过认证后接入院内网络环境，自动跳转到用户身份认证服务。

院内资源访问过程中，引擎自动进行设备环境的信息收集、安全状态上报、阻止异常访问等功能，通过收集终端信息，上报访问环境的安全状态，建立“医护人员+医疗设备+设备环境”可信访问模型。

2、零信任安全网关

为避免攻击者直接发现和攻击端口，在医院 DMZ 区部署零信任安全认证网关，提供对外访问的唯一入口，采用先认证后访问的方式，把 HIS、LIS、PACS 等临床应用系统隐藏在零信任网关后面，减少应用暴露面，从而减少安全漏洞、入侵攻击、勒索病毒等传统安全威胁攻击面。

零信任安全网关与可信终端建立 SSL 网络传输数据加密通道，提供零信任全流程可信安

全支撑（代码签名、国密 SSL 安全通信、密码应用服务等），确保通信双方数据的机密性、完整性，防止数据被监听获取，保证数据隐私安全。

3、安全策略决策服务

安全策略决策服务对医院用户账号、终端、资源接入进行访问策略评估和管理，并对接入医院用户和医疗设备进行角色授权与验证，实现基于院内用户及设备的基础属性信息以及登录时间、登录位置、网络等环境属性做细粒度授权，基于风险评估和分析，提供场景和风险感知的动态授权，并持续进行身份和被访问资源的权限认证。

4、统一身份信任管理

统一身份信任管理分为统一身份管理模块、统一设备管理模块、统一资源管理模块、统一威胁情报管理模块四个部分。统一身份管理模块实现用户面向各业务系统的统一身份访问，解决信息化系统集中管理难、用户使用不便、认证授权不安全等问题。统一设备管理模块提供面向各类终端设备的统一管理、身份核验以及终端环境检测、终端接入应用安全管理等功能。统一资源管理模块提供对资源的可信签名和资源的统一管理等功能。统一威胁情报管理模块可实现对网络流量实时监控，用户行为收集分析，终端设备漏洞扫描及服务端设备运行环境和运行状态安全监控，并针对重大事件进行主动告警等功能。

5、密码基础设施

密码基础设施分为证书服务模块、密码服务模块和实名核验服务模块三个部分。证书服务模块主要是针对医院用户、医疗终端设备进行证书签发，保证用户和设备的合法性。密码服务模块主要针对统一身份信任管理和零信任安全网关在传输、存储过程中的数据进行签名操作，保证数据的完整性、可追溯以及抗抵赖性。实名核验服务模块用于证书签发时对用户身份的核验工作，保障用户身份的真实性。

6.3.3 优势特点和应用价值：

1、应用价值

1）用户管理方面价值

解决医院当前面对医疗访问群体多样化的问题，建立统一的身份管理，减轻了运维成本。

2）设备管理方面价值

将医疗设备进了统一管理，保障了设备接入的安全管控，对接入设备进行了有效的身份鉴别。

3）权限管控价值

（1）隐藏医疗应用系统，无权限用户不可视也无法连接；对有权限的业务系统可连接但无法知悉真实应用地址，减少黑客攻击暴露面。

（2）以访问者身份为基础进行最小化按需授权，避免权限滥用。

4）访问安全价值

（1）采用了“用户+设备+环境”多重认证方式，即保证了认证的安全，还不影响用户使用体验。

（2）通过感知环境状态，进行持续认证，随时自动处理各种突发安全风险，时刻防护医院业务系统。

5）数据安全价值

（1）进行了全链路信道安全，消除了医疗数据传输安全风险。

（2）对患者数据进行了隐私保护，解决了数据内部泄露问题。

2、优势特点

1）围绕设备证书建立设备信任体系

在传统数字证书框架中，增加针对设备信任的评估环节，以设备证书作为零信任安全体系的基石。

2）自动化授权体系

零信任访问控制区建立的一整套自动化授权体系，可根据用户属性、用户行为、终端环境、访问流量等多维度数据，自动对用户权限进行实时变更，从而保障内部系统安全性。

3）基于设备信任最小化攻击平面

在任何网络连接建立时，首先进行设备认证，能够有效阻止非法设备的连接、嗅探、漏洞扫描等恶意行为，既能最小化系统的暴露平面，又可以灵活适应一人多设备、多人共用设备、物联网设备等不同场景。

4）以信任的持续评估驱动用户认证

通过信任的持续评估驱动认证机制的动态调整，根据动态的信任评估结果反馈调整用户认证机制。

5）海量的应用加密通道支撑

逻辑虚拟化技术的深入推进，支持海量的应用加密通道。

（1）通过 SSL 多实例技术，实现同一台设备上支持多个 SSL 服务，实例之间通过密码卡实现密钥物理隔离。

（2）基于高性能网络协议栈，实现海量的 TCP/SSL 连接支持，通过算法和代码流程的优化，不断提高每秒新建连接数。

（3）吞吐率、并发连接数和每秒新建连接数等网关指标做到业界领先

6.3.4 经验总结：

在项目的实施阶段,首先要明确医疗内部和外部的访问者身份，实现医院人员的统一身份管理。在此阶段，需要对内外部用户身份目录进行梳理，由于医院系统用户涉及医生、患者、临聘人员、其他医疗机构人员等多方用户，所以需要整合多部门的用户信息，保证用户信息的实时性、同步性和一致性。另外，由于医院业务系统数据存储方式多样，项目组根据不同业务系统数据结构编写了大量针对性的数据清洗脚本，进行身份数据统一收集、清洗、整理、加密。

其次，对医院信息科进行调研，将需要接入医院网络进行应用数据传输的医疗终端及手持设备，如：PC、智能手机、平板以及患者随身佩戴的小型监测设备等物联网设备信息收集汇总和统一管理。由于医院没有资产管理系统，未对设备进行统一管理，为此数字认证临时开发了一套在线设备信任凭证在线签发系统，自助采集设备基本信息、自助签发下载设备信任凭证。另外，在集成可信终端安全引擎模块前，针对医院各类终端存在时间跨度久且种类繁多的特点，在各类、各版本操作系统进行多次软件兼容性测试等工作，解决与医院各类终端适配问题。

然后，集成医院现有的各类业务系统，接入零信任安全网关，通过 API 代理统一对外提供服务。医院物理场所开放、网络多样，各类网络基础设施的物理安全无法统一保障，在院内各医疗服务网络出口前端部署应用安全网关后，为传输的业务数据进行加密保护，有效防止攻击者窃取、篡改、插入或删除敏感数据。

最后，通过分析医院的访问需求，制定可信的安全策略，管控访问内容和访问权限。在

可信身份服务的基础上综合评估设备安全风险、访问行为频率、以及发生访问请求的时间地点等因素，进行持续风险评估和动态授权，保障各项医疗服务被医院各类用户同时访问的安全性。在制定安全策略时，遵循“动态最小权限”原则，结合医院实际业务需求，通细粒度的动态访问控制，应对医院诊疗业务中的精细化安全管理风险。

6.3.5 其他（反馈/荣誉）

1、用户体验方面:

引入零信任体系后，在进行远程医疗访问、内部业务访问、互联网访问时，原有访问流程不变，将因网络安全架构改变而对用户造成的影响降至最小。

2、网络安全方面：

以往医院针对不同用户及需求分配内网和外网访问权限，但内外网部分应用需要进行数据共享，无法对内外网进行严格意义的完全隔离，因此在数据共享过程中即存在严重安全隐患。在引入零信任体系后，所有用户、设备、应用和服务等身份都被抽象成主体身份，不再通过内外网区分安全域，都需要通过主体身份的属性进行动态认证和鉴权，上述安全问题迎刃而解。

6.4 白山云-零信任远程访问实践案例

6.4.1 案例背景：

白山云作为一家致力于为政府及企业客户提供综合解决方案的领先边缘云平台服务商，借助数字化转型的力量，优化服务流程，提升用户体验，加速业务发展，为客户提供更多创新的产品和优质的服务。白山云因其分支机构较多、业务系统多样、组织职能细分等特性，欲落地零信任远程访问解决下列问题：

1、八个分支分布在全球不同区域，客户遍布全球各地，基于业务发展需求，员工随时随地可能通过 VPN 方式远程开展工作，受限于接入方式和接入环境，在接入工作前需要做一系列的准备工作，工作效率受到很大的影响；

2、员工远程访问企业内部服务，存在一定安全隐患，一是建立远程连接时可能导致业务受到外界非法攻击，二是内部数据存在泄露风险；

3、不同员工职能不同，具有不同的业务环境访问需求，业务系统繁多，既有云上 SaaS 服务，又有企业内部自建服务，以粗粒度方式管理员工应用访问授权，每个应用都有一个独立访问路径和账户体系，给管理员带来极大挑战。

员工不局限于内网环境办公、业务系统不仅位于内网环境，办公设备不止 PC 设备，基于网络边界作为安全边界的传统架构体系已经无法满足白山云业务发展的需求，亟需以一种安全有效、便捷稳定的方式来助力员工开展远程办公。

6.4.2 案例概述：

为应对业务发展过程中出现的安全隐患、用户体验差和资源难管控的三大挑战，助力企业数字化转型，白山云开展实施基于零信任理念的 Access 远程访问解决方案。

首先，建立统一身份管理体系确保合法访问请求身份可信，将企业应用隐藏在后端，不对外进行暴露，屏蔽外界的非法攻击；

其次，构建统一 SSO（单点登录）访问系统和统一应用访问入口门户，将分散于云上云下的服务汇聚于统一访问页面，借助 1000+边缘节点的能力，为员工提供就近访问，提升员工访问体验，将员工更聚焦于业务上；

最后，针对用户、访问链路、应用、数据等各个环节进行全局统一管控，实现可管控、可审计。

此次业务开展涉及到白山云内部近百个自建系统及 SaaS 服务，同时还有 Linux、Windows 服务的 SSH、RDP、VPN 等协议应用。针对全员近千人，几十种职能角色，统一由旧的办公方式，改善为新的访问方式，大大提升远程办公体验和效率。

6.4.3 安全技术应用情况：

Access 是基于零信任架构和理念，构建“访问端、身份、应用端“ 三元合一的可信访问实体，实现在非特权网络中对业务资源和数据的安全、稳定、高效的访问。具体如下：

1、Access 的边缘网关充当了业务应用的访问入口，最大化的降低了业务应用被暴露在互联网中各类攻击风险，无法被外部扫描渗透，不再被动的修复漏洞，实现了对源站应用的隐身保护；

2、访问可信检测：通过对企业网络流量的接管，持续检查网络应用现状和用户行为，更好地透视与管控企业网络环境，限制任何不符合安全要求的访问；

3、访问控制引擎：根据特定用户/用户组的身份、职能、需求授予访问权限，实行最小权限原则，更好地保护敏感生产环境的访问安全；

4、身份信任管理：提供身份生命周期管理，包括 OTP 动态口令、企业微信、OIDC、SAML 等多种身份验证方式；

5、应用可信接入：提供上千种 SaaS 应用接入模板；提供 SSH、RDP、VNC 等协议应用远程安全接入；提供内网仅出站连接的单向隧道，实现内网应用 SaaS 化。

6.4.4 案例实践成果：

Access 帮助白山云建立身份认证体系、高效便捷的接入方式、标准化资源控制、降低

IT 复杂度，全面强化安全。

案例实践具体效果如下：

1、整体工作接入效率提升 3-5 倍，具有更强的安全体系和更便捷的管理工作；

2、建立集中身份信任服务，形成统一的身份认证中心、SSO 和多因子认证，辅助建立多层次防御，加强身份验证的安全性；

3、可通过统一门户接入，提升用户体验，内网应用快速 SaaS 化，保障所有终端同时在线的情况下稳定、高效、安全的办公，提供员工生产力；

4、标准化资源控制、隐藏资产攻击面，无法被外部扫描渗透，不再被动的修复漏洞，摆脱对防火墙、设备的依赖，降低 IT 维护成本；

5、细粒度访问控制手段，可视化的策略管理能力，云原生安全平台防护能力，多维度的强化网络安全。

零信任安全与企业数字化转型是相互促进与协同发展，Access 作为白山云数字化转型的最佳安全访问接入方案，因为它不仅仅是一个简单的远程访问工具，而是一个全新的网络安全架构模式。

Access 是白山云零信任安全架构实践的开始，白山云会持续探索零信任安全架构，逐步实现真正的“永不信任，持续验证”的网络安全架构。

6.5 美创科技-浙江省肿瘤医院基于零信任理念的数据安全建设最佳实践

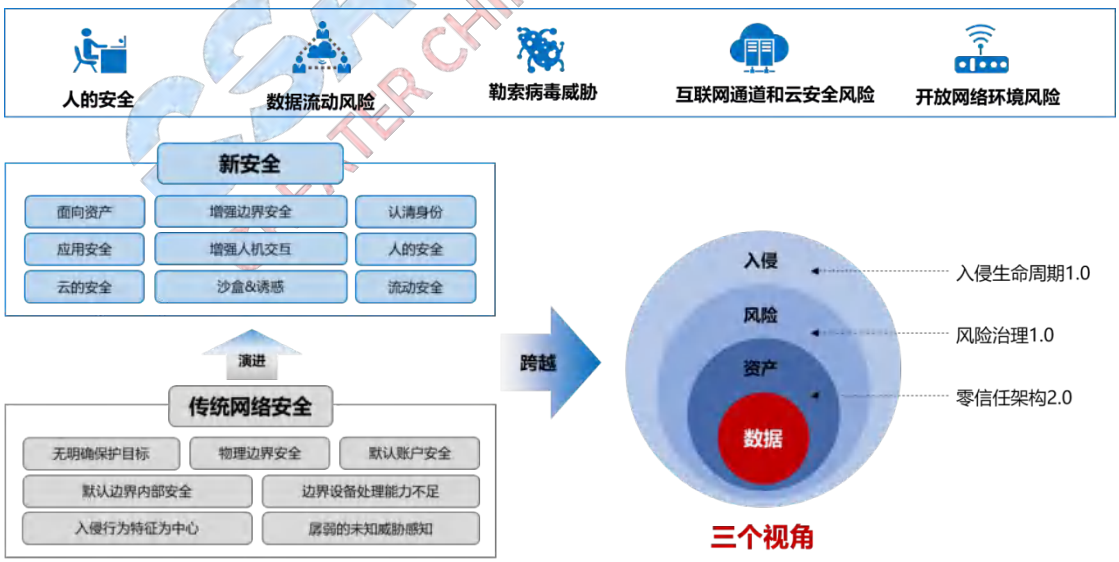
6.5.1 方案背景：

中国科学院大学附属肿瘤医院（浙江省肿瘤医院）是国内成立最早的四家肿瘤专科医院之一，是浙江省规模最大的三级甲等肿瘤专科医院，也是中国首批三级甲等医院。

近年来，医院不断重视和加强信息化建设，深化“最多跑一次改革”，大力开展“医防融合”、智慧医疗、自动化办公等等信息化工作，伴随着医疗应用系统不断增多，医院实现了数据互联互通、资源共享，但医院缺乏足够、专业的运维人员，不得不依靠第三方运维团队，因此运维环节的数据泄露成为重要的安全隐患之一。

零信任是美创安全产品非常重要的一个理论框架，SDP（Software Defined Perimeter）作为数据访问安全的新边界，是一个很好的实践方式，美创科技也已将 SDP 融入零信任 2.0 架构中。零信任并不是没有边界，是把原来静态的物理边界转变成了动态的虚拟边界，通过软件定义边界，把数据控制在一个最小授权的安全边界内，最大程度保障数据的安全。

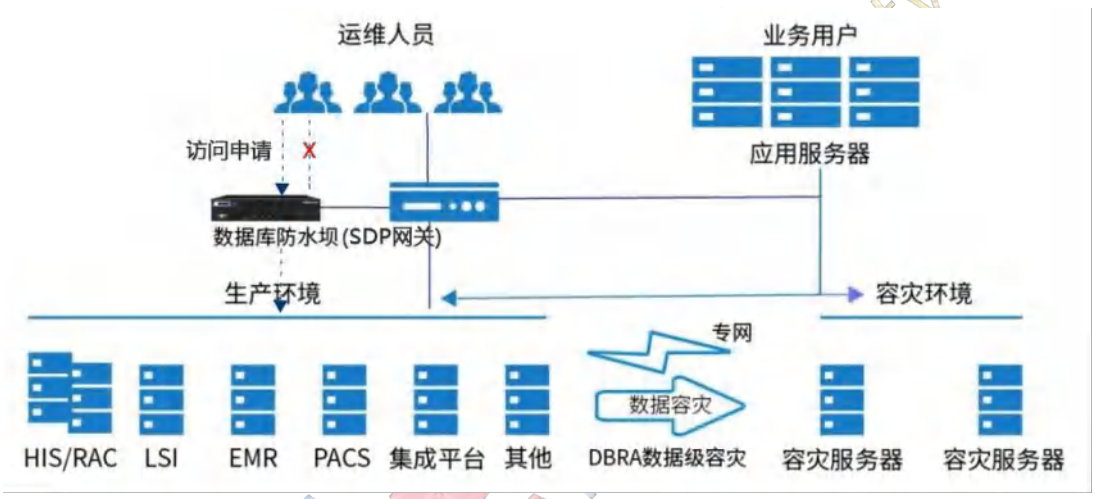
美创的安全产品以资产和身份为核心，从资产出发，以身份为中心，建立安全访问体系。安全从资产的定义开始，明确保护对象，由内而外地确定资产的动态访问边界，实时调整访问边界，实现最小访问原则；以身份为中心进行身份治理，建立动态身份体系，通过身份行为分析、关联分析识别身份、识别风险，为身份圈定动态、虚拟的访问边界，将安全问题降到最低。



6.5.2 方案概述和应用场景：

针对中国科学院大学附属肿瘤医院（浙江省肿瘤医院）的需求，美创科技从内部运维风险管控的角度出发，提出如下解决方案：

运维侧的安全管理，是数据安全防护的有效手段，我们通过先定义高价值目标——敏感数据，然后定义访问边界，以杜绝超级用户访问，根据 SDP 架构，数据的保护边界可以实现最小化，比如到数据库内的每张表，甚至每个字段。通过将资源隐藏在 SDP 网关后面，所有希望发起访问的用户都要进行授权和认证，然后才能正常访问被授权的资源，实现数据保护。美创数据库防水坝系统基于以上逻辑架构，实现敏感数据管控、身份识别、数据库准入、行为阻断、授权管理、监控预警等功能，补齐数据安全短板。



部署示意图

该方案解决了如下问题：

1）敏感数据管控

敏感数据分类是数据和运维安全的基础性工作，同时也是重点工作，可以通过表格、Schema、业务单元三个层面进行分级分类。清楚保护目标才能实施更加安全的保护措施，数据安全和运维安全真正需要保护的在于 1%~10%左右的敏感数据，必须把敏感数据从普通业务数据中脱离出来进行独立管理，SDP 将敏感信息隐藏在用户自己的黑云里，使得这些关键 IT 资产对外不可见。

2）准入控制

SDP 要求在获得对受保护服务器的网络访问之前，先对端点进行身份验证和授权。身份管理通过应用程序名、IP 地址、主机名、操作系统账户、数据库账户、数据库实例名、

时间、U 盾等因素进行任意组合，形成新的登陆认证规则，同时支持签名登陆验证和数字证书认证方式，符合规则予以准入，反之则阻断；对于应用防假冒，识别真实应用特征，防止人为恶意将其他的应用改成业务系统应用，假冒应用访问数据库，进行非法操作；对于撞库攻击，建立用户信息白名单，限制同一个 IP 的请求次数和请求频率来防止；对于直连控制，在反向代理部署模式下，可对直连数据库的行为进行控制；免密登陆实现通过安全客户端免密登录数据库，避免密码泄露。

3）敏感数据访问控制

针对敏感数据集合的访问，通过授权才可访问，不具备访问权限的操作，明确阻断拒绝。敏感数据集合支持设置访问规则，访问规则中可设定精细化的访问因子，如应用程序名、IP 地址、操作系统账户、数据库实例名、时间、U 盾等条件，满足条件方可访问敏感数据集合。通过隐藏网络资源，SDP 可减小攻击界面，并清除用户扫描网络和在网络中横向移动的可能性。

4）高危性操作防护

数据库存在众多特权账号，如系统管理员、数据库管理员、开发人员等，可执行 DDL、DML、代码类的高危操作，并存在误操作的可能。为解决此类问题，结合访问控制功能，执行 delete、update 等高风险操作时要求携带 where 条件，符合要求才可进行操作，从而起到误操作防范的作用。

5）全面运维审计

可对数据库查询、新增、修改、删除等行为进行监控，可对事件进行搜索、管理，并能够锁定操作终端，可基于单个会话进行事件回溯，符合等保三级的核心要求，符合网络安全法关于对个人隐私数据信息的保护，符合 HIPAA 法案、PCI-DSS 法案、SOX 法案、GLBA 法案的要求，保护敏感数据资产的安全审计，为运维管理提供极大的便利。

6）实时安全风险感知

实时展示数据库的安全情况，出现风险时可快速定位当前被攻击的数据库及发起攻击的

客户端，同时对注入攻击、漏洞攻击、敏感访问、系统运行、流量等进行 24 小时实时监控，让数据库更安全，让运维更轻松。

7）遵循法规提供报表

内置支持各种法规遵循所需的管理性报表，简化法规遵循管理和审计流程。总计提供众多安全报表，全方位覆盖运维安全各层面的需求，同时提供由 N 张报表所合并而成的综合性报表，提高报表的可读性。针对等级保护、企业内控条例、SOX、PCI、HIPAA、GLBA 等多种法规遵循还提供不同的分类报表，使合规更简单。

6.5.3 优势特点和应用价值：

1、通过美创数据安全产品，数据库运维访问环节得到强力有效的管控保障，建立医院内部数据安全使用管控体系、完善了整体的信息安全架构。

2、基于人员与数据资产的内部数据安全管控能力，有效防止数据从运维端内部泄露，提升医院整体数据安全防御能力。

3、满足《中华人民共和国网络安全法》、《中华人民共和国数据安全法》（草案）以及医疗行业等相关政策法规要求。

6.5.4 经验总结：

作为用户方，数据安全的价值体现度、参与度还有提升空间。因此要从管理层到每一位工作人员，需要充分了解数据安全的重要性，数据安全不仅仅是合规事项、IT 内部控制事项，而是关系到每个业务领域每个职能领域每个科室每个人的事项，在数据安全建设方面要保证充足的资源投入，跨业务部门合作，全员参与，保障数据安全工作在医疗行业有效落地。作为数据安全建设支撑单位，需要深入了解用户的使用场景，充分考虑影响因素，为用户提供整体数据安全建设方案，结合行业发展动向和技术发展趋势，提供高兼容性、高可扩展的产品。

7. 致谢

感谢所有参与此次全景图的单位，以及联盟相关的专家和志愿者，全景图的发布离不开大家的支持和共同努力：

顾问指导：李雨航、贾良玉

专家团队：周杰、谢琴、姚凯、郭鹏程、王金红

志愿者：夏营、牛俊生

联合发布单位：天融信、深信服、数字认证、白山云、美创科技

《2021 中国零信任全景图》难免存在遗漏之处，敬请各界朋友指正，烦请扫描下方二维码进行反馈。同时，欢迎广大零信任相关单位共同参与零信任全景图的持续迭代和更新，若有单位不在该全景图之列，欢迎随时联系我们，我们将在下一个版本进行补充和完善。

联系人：CSA 大中华区秘书处 叶女士 18024312752 info@c-csa.cn。

2021

CSA公众号

微信号

官网：https://c-csa.cn

邮箱：info@c-csa.cn