CSA GCR cloud security alliance®
GREATER CHINA REGION

零信任落地案例集

2021.06

目 录

一、前　言.....6

二、落地案例清单.....8

三、落地案例.....10

1、安恒信息温州市大数据发展管理局零信任实践案例.....10

2、任子行零信任安全防护解决方案护航海事局移动/远程办公安全.....14

3、奇安信零信任安全解决方案在部委大数据中心的实践案例.....18

4、吉大正元某大型集团公司零信任实践案例.....20

5、格尔软件航空工业商网零信任安全最佳实践.....28

6、厦门服云招商局零信任落地案例.....37

7、深信服山东港口集团零信任多数据中心安全接入.....41

8、杭州漠坦尼物联网零信任安全解决方案.....42

9、易安联中国核工业华兴建设有限公司 EnSDP 零信任安界防护平台.....45

10、虎符网络国家电网某二级单位基于零信任架构的远程安全访问解决方案.....49

11、奇安信某大型商业银行零信任远程访问解决方案.....55

12、蔷薇灵动中国交通建设股份有限公司零信任落地解决方案.....60

13、缔盟云中国建设银行零信任落地案例.....68

14、联软科技光大银行零信任远程办公实践.....71

15、云深互联阳光保险集团养老与不动产中心零信任落地案例.....75

16、上海云盾贵州白山云科技股份有限公司应用可信访问.....79

17、天谷信息 e 签宝零信任实践案例.....85

18、北京芯盾时代电信运营商零信任业务安全解决方案落地项目.....89

19、云深互联零信任/SDP 安全在电信运营商行业的实践案例.....94

20、启明星辰中国移动某公司远程办公安全接入方案.....99

21、指掌易某集团灵犀·SDP 零信任解决方案.....105

22、美云智数美的集团零信任实践案例.....112

23、360 零信任架构的业务访问安全案例.....118

24、数字认证零信任安全架构在陆军军医大学第一附属医院的应用.....120

25、山石网科南京市中医院云数据中心“零信任”建设项目成功案例.....125

©2021 云安全联盟大中华区-版权所有

26、九州云腾科技有限公司某知名在线教育企业远程办公零信任解决方案.....133
四、关于云安全联盟大中华区..... 136

©2021 云安全联盟大中华区-版权所有

CSA GCR cloud security alliance ®
GREATER CHINA REGION

©2021 云安全联盟大中华区-版权所有

@2021 云安全联盟大中华区-保留所有权利。你可以在你的电脑上下载、储存、展示、查看、打印及，或者访问云安全联盟大中华区官网（https://www.c-csa.cn）。须遵守以下：（a）本文只可作个人、信息获取、非商业用途；(b) 本文内容不得篡改；(c) 本文不得转发；(d)该商标、版权或其他声明不得删除。在遵循中华人民共和国著作权法相关条款情况下合理使用本文内容，使用时请注明引用于云安全联盟大中华区。

©2021 云安全联盟大中华区-版权所有

一、前　言

零信任这一概念提出到现在已有十一年了。作为新一代的网络安全防护理念，零信任（Zero Trust）坚持 “持续验证，永不信任”，基于身份认证和授权重新构建了访问控制的基础。

当前，零信任已经从一种安全理念逐步发展成为网络安全关键技术，受到了各国政府的认可。

由于传统网络安全模型逐渐失效，零信任安全日益成为新时代下的网络安全的新理念、新架构，甚至已经上升为国家的网络安全战略。2019 年，在工信部发布的《关于促进网络安全产业发展的指导意见(征求意见稿)》的意见中，“零信任安全”被列入“着力突破网络安全关键技术”之一。同年，中国信通院发布了《中国网络安全产业白皮书》，报告中指出：“零信任已经从概念走向落地”。国家也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。

我们欣喜地看到，从 2020 年云安全联盟大中华区召开了“十年磨一剑，零信任出鞘”为主题的零信任十周年暨首届零信任峰会，越来越多的 IT 安全厂商投入到了零信任产品的开发和实施中来。从 2021 年 5 月底云安全联盟大中华区征集零信任案例以来，在短短十多天的时间内，我们就收到了 29 家厂商的落地案例，这个速度大大出乎我们的意料，而收集到的案例数量也比去年丰富了不少，可见零信任实践的火爆程度。与 2020 年的 9 个方案相比，今年的方案有了 300%的增长。最后基于“讲技术不讲概念，强调落地不空谈方案”的原则，最终筛选了 24 个案例，涉及 9 个行业，涵盖了政企、能源、金融、互联网、医疗等多个行业，充分说明了零信任技术的广泛适用性。在征集案例的过程中，有的客户尽管提供了授权，但不希望自己的公司名出现在案例中。因此，对于这部分客户，我们在案例中进行了匿名处理。

NIST 在《零信任架构标准》白皮书中列举了 3 个技术方案：1)SDP，软件定义边界;2)IAM，身份权限管理;3)MSG，微隔离。从我们收到的案例来看，绝大部分案例都是 SDP 的案例，聚焦于远程办公的场景。这可能与新冠疫情带来的办公模式的变化有关，与云安全联盟最早推广 SDP 有关，也与 SDP 的技术复杂度较低有关。MSG 和身份权限管理案例的匮乏一方面说明调整传统网络架构以适应零信任架构充满挑战，仍然有很多工

©2021 云安全联盟大中华区-版权所有

作要做，另一方面，很多企业虽然接受零信任的理念，但对于系统转换可能的风险持审慎态度，更愿意从边缘系统开始试水。

因此，云安全联盟大中华区汇编这本《2021 零信任落地案例集》，收集各厂商的成功案例及实施过程中的经验教训，一方面是希望给众多厂商和客户以参考，让大家知道零信任离我们并不遥远；另一方面是鼓励更多的企业投入零信任的探索中来，进入零信任的深水区，打造更先进的零信任平台。

随着企业数字化转型的深入，传统边界逐渐消失，企业以传统安全防护理念应对安全风险暴露出越来越多问题，而零信任理念为我们提供了新的安全思路。我们希望今后会看到越来越多更具代表性的零信任应用场景和探索涌现出来。

《2021 零信任落地案例集》包含了去年和今年入围的案例。云安全联盟大中华区在今后仍密切关注零信任应用实践并更新这一案例集，我们计划每年都发布一份《零信任落地案例集》，收录从 2020 年以来不同行业的零信任实践典型案例，供广大从业用户了解这一领域的最新实践，并协助推动零信任技术的发展。

感谢案例提供的全体单位，经过多次修改及调整，力争为行业呈现单位最优的解决方案。

感谢 CSA 大中华区零信任工作组组长陈本峰、专家姚凯以及研究助理夏营对本次《2021 零信任落地案例集》汇编的大力支持。

如文有不妥当之处，敬请读者联系 CSA GCR 秘书处给与雅正！联系邮箱：info@c-csa.cn；云安全联盟 CSA 公众号

©2021 云安全联盟大中华区-版权所有

二、案例名单

序号	案例所属行业	零信任技术	案例用户名称	案例提供单位
1	政企	SDP	温州市大数据发展管理局	安恒信息
2	政企	SDP	某市海事局	任子行
3	政企	SDP	部委大数据中心（2020 年案例）	奇安信
4	政企	IAM	某大型集团公司	吉大正元
5	政企	SDP	中国航空工业集团有限公司	格尔软件
6	政企	微隔离	招商局集团	厦门服云
7	交通	SDP	山东港口集团	深信服
8	能源	SDP	某省电力公司直属单位	漠坦尼
9	能源	SDP	中国核工业华兴建设有限公司	易安联
10	能源	SDP	国家电网有限公司某二级直属单位	虎符网络
11	金融	SDP	某大型商业银行	奇安信
12	金融	微隔离	中国交通建设股份有限公司	蔷薇灵动
13	金融	SDP	中国建设银行	缔盟云
14	金融	SDP	光大银行	联软
15	金融	SDP	阳光保险集团养老与不动产中心	云深互联
16	互联网	SDP	贵州白山云科技股份有限公司	上海云盾
17	互联网	IAM	e 签宝	天谷信息
18	运营商	SDP,IAM	电信运营商	芯盾时代
19	运营商	SDP	电信运营商（2020 年案	云深互联

©2021 云安全联盟大中华区-版权所有

			例）	
20	运营商	IAM	中国移动某公司	启明星辰
21	制造业	SDP	某集团	指掌易
22	制造业	SDP	美的集团	美云智数
23	制造业	SDP	某国家高新技术企业	360
24	医疗	SDP	陆军军医大学第一附属医院	数字认证
25	医疗	微隔离	南京市中医院	山石网科
26	教育	IAM	某知名在线教育企业	九州云腾

©2021 云安全联盟大中华区-版权所有

三、具体案例

1、安恒信息温州市大数据发展管理局零信任实践案例

1.1 方案背景

温州市大数据发展管理局一直来在以大数据赋能智慧城市、智慧国企、智慧健康等方面走在前列，已建成的一体化智能化公共数据平台为该市下属的委办单位、企业、公众提供良好的大数据业务支撑服务，以数据智能赋能数字经济和民生。

十四五规划中，数据相关产业将成为未来中国发展建设的重点部署领域，相关的数据安全也变得更加重要。随着数据开放面逐渐扩大、数据访问量不断增加，温州市大数据发展管理局预见到了开放共享过程中潜在的数据安全防护及溯源问题，例如数据访问无法追溯到最终用户、API 自身脆弱性带来的安全配置错误及注入风险、API 异常高频访问带来的数据暴露风险等，为此温州市大数据局启动了一体化智能化公共数据平台零信任安全防护体系的建设任务，并引入安恒信息作为零信任安全供应商。

1.2 方案概述和应用场景

基于零信任的理念，本次方案强调“永不信任、始终确认”，在业务访问的全流程中引入身份认证的能力，对管控的客体对象“用户”、“应用”的身份进行持续校验，并针对防护对象 API 资源，实现“先认证、再授权、再访问”的管控逻辑，通过为公共数据平台构建虚拟身份安全边界，最大程度上收窄公共数据平台的暴露面，保障业务安全开展。

©2021 云安全联盟大中华区-版权所有

图 1 温州市一体化智能化公共数据平台零信任安全防护体系逻辑架构

温州市一体化智能化公共数据平台零信任安全防护体系由以下几个关键组件构成：

1.统一控制台：作为零信任架构中的 PDP，维护用户清单、应用清单及资源清单，集成 SSO 系统，并负责零信任体系内访问控制策略的制定和 API 安全代理的控制。其中用户清单来源于浙江省数字政府 IDaaS、浙政钉等多源用户身份目录的合并，追踪和更新温州全市 12 万余用户信息的变化，所有用户具有唯一标识，用户清单为零信任体系中的 UEBA 行为分析引擎提供信息；应用清单维护所有接入零信任体系的应用系统的身份信息，通过与温州市建设的目录系统联动，实现全网应用身份统一，并为应用生成零信任安全接入工具；资源清单维护所有要保护的客体对象信息（在温州场景下即 API 接口资源），通过手动配置或从流量中分析的方式建立。

2.API 安全代理：作为零信任架构中的 PEP，以“默认拒绝”的模式接管所有面向公共数据平台的访问请求，针对每条请求进行身份鉴别和权限鉴别，仅放通通过统一控制台验证的合法请求，同时输出其他 API 安全防护能力。

3.UEBA 行为分析引擎：负责采集零信任体系中的用户行为数据，并对用户行为、应用行为进行大数据建模匹配分析，为统一控制台的访问控制策略制定提供输入依据。应商。

1.3 优势特点和应用价值

1.3.1 统一身份、安全认证

统一控制台通过 SSO 系统为政务外网所有的应用系统提供认证门户，接入应用的用

©2021 云安全联盟大中华区-版权所有

户在通过统一认证的合法性校验后将会生成包含用户、应用身份唯一信息的访问令牌，作为获得后续访问资源的授权凭证之一。

统一控制台在认证过程中，通过对接浙政钉体系、短信体系等，提供多因子认证手段，并通过门户获取登录环境信息，综合判定用户身份，并在发生异常访问事件时对用户登录进行快速处置。

1.3.2 收缩资源暴露面

API 安全代理逻辑串行在公共数据平台的访问通道上，默认拒绝所有请求。统一控制台为注册应用生成访问工具，实现只有集成了访问工具的应用系统服务器可以建立安全连接，同时在应用层叠加用户身份凭证的验证，实现只有授信用户、通过授信应用服务器才能够访问 API 资源，极大强化了公共数据平台对抗潜在的扫描攻击等威胁的能力。

1.3.3 全流量加密

API 安全代理为所有访问公共数据平台的请求加载 TLS 加密通道，保障流量在通道上的安全加密、防篡改。

1.3.4 用户及 API 调用行为分析

API 安全管控系统支持对 API 访问过程中产生的访问日志进行智能分析，并发现潜在的违规调用行为。统一控制台支持按场景扩展异常行为特征匹配规则，根据用户、应用、IP、入参、出参等完整的 API 请求日志信息，帮助安全团队发现凭证共享、疑似拖库、暴力破解等行为。

1.3.5 API 敏感信息监控及溯源

为调用方发起的所有访问请求形成日志记录，记录包括但不限于调用方（用户、应用）身份、IP、访问接口、时间、返回字段等信息，并向统一管控平台上报。

API 安全管控系统将按配置对 API 返回数据中的字段名、字段值进行自动分析，发现字段中包含的潜在敏感信息并标记，帮助安全团队掌握潜在敏感接口分布情况。

©2021 云安全联盟大中华区-版权所有

1.4 经验总结

项目的实施准备阶段，交付团队首先在统一控制台上拉通多方身份及认证体系、注册一体化智能化公共数据平台服务，准备好零信任安全防护体系的上线和基础。在该阶段，需要注意对多方身份目录的梳理，涉及到多方用户信息整合的，需要提前获取各方所提供的数据同步文档、接口文档，确认同步方案，以确保用户信息能够及时同步、保持一致。

搭建好基础架构后，统一控制台即对应用系统开放单点登录及访问工具集成能力，优先选择了开发中的和新上线的业务系统进行单点登录对接，并将 SSO 能力形成标准文档，作为后续政务外网应用开发、接入一体化智能化公共数据平台服务前的必选项之一。

需要尤其注意的是在现有的访问体系下，如何向新的安全访问控制体系迁移。因此项目组在一体化智能化公共数据平台侧，对接口的访问迁移也采用分步骤的方式。在项目实施前期阶段，公共数据平台上已有接口并没有做强制的访问策略切换，只针对新上线的接口，在公共数据平台上启用源 IP 白名单，只接收 API 安全代理转发来的请求；同时，由 API 安全代理兼容公共数据平台的认证能力，不再向新上线的应用提供公共数据平台自身的认证凭证，使其必须通过 API 安全管控系统访问，完成遗留的通道切换后，再处理网络策略的连通性。

另外，在运维流程上实现资源目录的统一管理运维，对后期维护来说也非常重要，一次项目组通过将温州市用户统一登录中心（统一控制台）对接温州市资源目录系统，打通新应用接入的标准化流程，实现业务资源的统一运维。

在访问过程中，统一控制台收集 API 安全代理上报的日志，对 API 的访问频度、调用方分布、异常行为、API 敏感数据进行分析和展示，根据分析结果、API 重要程度逐渐进行白名单策略的切换。

©2021 云安全联盟大中华区-版权所有

2、任子行零信任安全防护解决方案护航海事局移动/远程办公安全

2.1 方案背景

2.1.1 用户需求及方案必要性

随着网络技术在海事业务如船舶驾驶控制、货物装卸、推进系统、旅客管理、通信系统等方面的应用不断提升，越来越多的对外信息交互，使海事业务遭受网络威胁的隐患也不断加剧，这些潜在的威胁可能导致有关的操作、安全或安保系统的破坏或信息的泄露。

网络安全是某海事局开展海事安全管理体系建设中的重要组成部分，自公安部2018年组织国家级的网络攻防实战演练以来，某海事局作为实战检验的重点单位，其信息交互、网络环境、信息设备系统等复杂性对网络安全综合防御能力提出重要挑战。

同时，网络安全将是2021年符合证明（DOC）年度审核的一个重点领域，迫切需要建立由内到外的安全架构体系，保障海事业务信息系统安全稳定运行，满足移动办公、审批、执法等应用场景需求。

2.2 方案概述和应用场景

2.2.1 用户需求与解决方案

用户存在的安全需求总结如下：

1.系统直接暴露在互联网上，导致攻击目标明确，采用VPN存在漏洞和连接终端使用不顺畅问题；

2.存在来自于互联网的肉鸡恶意扫描、恶意攻击；

3.用户在互联网上注册时使用简单好记密码或多个业务使用统一密码，导致访问主体的身份安全无法保障；

©2021 云安全联盟大中华区-版权所有

4. 系统和应用程序的漏洞属于致命威胁。

任子行结合海事局的实际需求与面临的挑战，助力海事局建立综合防御能力更强的网络安全体系，具体实施方案如下：

1. 建立统一工作台，多业务系统统一门户，在解决业务访问主体身份安全问题的同时实现单点登录；

2. 采用细腻动态的访问控制策略，弱化内网安全事件发生的风险，仅允许合法的请求和合法的客户端访问业务系统，拒绝非法请求，屏蔽非法流量的攻击；

3. 业务系统隐身，同时隐藏程序漏洞，将企业内网应用暴露的攻击面降到最低；

4. 持续的安全信任评估，及时发现用户的异常登录和异常访问行为。

2.2.2 用户使用部门及规模

安全监督科、工会、组织人事科、办公室等 12 个科室。（基于信息安全需求，此处不一一列举）

©2021 云安全联盟大中华区-版权所有

图 1 方案架构示意图

2.3 优势特点和应用价值

任子行智行零信任远程接入安全防护解决方案，采用 SDP 的技术架构，以安全浏览器的方式将认证客户端与 Web 应用访问工具相结合，在实践零信任核心安全理念的同时为用户带来了方便快捷的使用体验。这种“轻量级”的实施方案，有助于企业快速落地零信任安全模型，使得零信任访问控制系统成为企业安全防护架构中最基础的防护设施。

2.3.1 技术优势

1.基于七层应用隧道技术，可完美替换传统 VPN

1）覆盖的安全能力更全面，理念更先进，拥有更强的身份认证和细粒度访问控制能力。

2）适用场景更多，不局限于网络远程访问，企业内网零信任安全访问也可以做到。

3）因只需要通过浏览器快速发布，则可实现快速扩容，对网络链路质量要求没有 VPN 严格。

2、让企业应用彻底“隐身”，将攻击暴露面降至最低

1）零信任网关可以将企业内网所有核心资产和业务“隐藏”起来。

2）只有通过专用安全浏览器才能够与零信任网关建立通信隧道，并进而访问到受保护的业务。

3、采用“零信任”理念，对用户动态按需授权和动态调整权限

1）任何用户都必须先进行认证后再接入，对于接入的授权用户，根据最小权限原则只允许用户访问其允许访问的业务系统。

2）除了应用的维度之外，还可以对用户的访问设备、访问位置、访问时间等维度进行安全限制。

3）系统可为不同用户配置不同的安全策略，并且基于来自终端环境、身份信息、审计日志等多源数据建立用户的信任模型，对用户的访问风险进行实时评估，根据结果

©2021 云安全联盟大中华区-版权所有

动态调整其安全策略。

2.3.2 应用效果

将零信任身份安全能力内嵌入业务应用体系，构建全场景身份安全便捷，升级企业安全架构。其主要价值交付有：

1. 信息安全加强

身份管理体系作为信息安全加强的重要举措，可有效保障公司机密及业务数据的安全使用，保护其信息资产不受勒索软件、犯罪黑客行为、网络钓鱼和其他恶意软件攻击的威胁，加强内部人员规范管理；平均减少了 31%的重复身份。

2. 业务流程风险控制

业务流程风险控制作为管理核心，身份治理体系可加强内外部相关人员访问的硬件设备及业务系统进行集中管控，同时从管理制度、合规性、审计要求进行内部风险控制；通过自动化的账号创建、变更、回收及重复密码工作，提升 IT 部门 91%的运维效率。

3. 提高企业生产力

为有效满足信息系统对业务的快捷响应能力，减少保护用户凭证和访问权限的复杂性及开销，打造一套标准化、规范化、敏捷度高的身份管理平台成为经营发展的基础保障，可极大提高企业生产力。通过集中的用户管理模块，访问认证模块及合规审计模块的统一建设，有效减少 88%的信息化重复投入。

4. 降低运营成本

实现身份管理和相关最佳实践，可以多种形式带来重大竞争优势。大多数公司需要为外部用户赋予到内部系统的访问权限。向客户、合作伙伴、供应商、承包商和雇员开放业务融合，可提升效率，降低运营成本。用户从打开网页到登录进系统的访问时间，通过统一认证与 SSO，提升 73%的用户访问效率。

2.4 经验总结

项目实施过程中，零信任团队面临客户环境多样性、网络复杂性等多方面挑战。零信任产品上线可在不破坏原有客户环境的情况下进行，因此需要对客户外接设备进行逐

©2021 云安全联盟大中华区-版权所有

一对接，对客户网络环境进行深度适配。对接流程规范化、对接接口标准化是任子行零信任产品后续提升的必经之路。

3、奇安信：零信任安全解决方案在部委大数据中心的实践案例

奇安信零信任安全解决方案，基于以身份为基石、业务安全访问、持续信任评估和动态访问控制四大核心特性，有效解决用户访问应用，服务之间的 API 调用等业务场景的安全访问问题，是适用于云计算、大数据等新业务场景下的新一代动态可信访问控制体系。解决方案已经在部委级客户、能源企业、金融行业等进行正式的部署建设或 POC 试点。下面以某部委大数据中心安全保障体系为例进行阐述。

3.1 方案背景

1.数据集中导致安全风险增加，大数据中心的建设实现了数据的集中存储与融合，促进了数据统一管理和价值挖掘；但同时大数据的集中意味着风险的集中，数据更容易成为被攻击的目标。

2. 基于边界的安全措施难以应对高级安全威胁现有安全防护技术手段大多基于传统的网络边界防御方式，假定处于网络内的设备和用户都被信任，这种传统架构缺乏对访问用户的持续认证和授权控制，无法有效应对愈演愈烈的内部和外部威胁。

3.静态的访问控制规则难以应对数据动态流动场景大数据中心在满足不同的用户访问需求时，将面临各种复杂的安全问题：访问请求可能来自于不同的部门或者组织外部人员，难以确保其身份可信；访问人员可能随时随地在不同的终端设备上发起访问，难以有效保障访问终端的设备可信；访问过程中，难以有效度量访问过程中可能发生的风险行为并进行持续信任评估，并根据信任程度动态调整访问权限。如上安全挑战难以通过现有的静态安全措施和访问控制策略来缓解。

©2021 云安全联盟大中华区-版权所有

图 1 大数据中心安全场景

为应对上述安全挑战，基于零信任架构构建安全接入区，在用户、外部应用和大数据中心应用、服务之间构建动态可信访问控制机制，确保用户访问应用、服务之间 API 调用的安全可信，保障大数据中心的数据资产安全。

3.2 部署方案

奇安信零信任安全解决方案应用于某部委的整体安全规划与建设之中，在新建大数据共享业务平台的场景下，访问场景和人员复杂，数据敏感度高。基于零信任架构设计，数据子网不再暴露物理网络边界，建设跨网安全访问控制区隐藏业务应用和数据。解决方案通过构建零信任安全接入区，所有用户接入、终端接入、API 调用都通过安全接入区访问内部业务系统，同时实现了内外部人员对于部委内部应用以及外部应用或数据服务平台对于部委数据中心 API 服务的安全接入，并且可根据访问主体实现细粒度的访问授权，在访问过程中，可基于用户环境的风险状态进行动态授权调整，以持续保障数据访问的安全性。

©2021 云安全联盟大中华区-版权所有

图 2 奇安信零信任安全解决方案部署图

3.3 优势特点和应用价值

目前奇安信零信任安全解决方案在某部委大数据中心已经大规模稳定运行超过半年，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，每天的数据流量超过 600G，有效保证了相关大型组织对大数据中心的安全。奇安信零信任安全解决方案，能够帮助客户实现终端的环境感知、业务的访问控制与动态授权与鉴权，确保业务安全访问，最终实现全面身份化、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，构建组织的“内生安全”能力，极大地收缩暴露面，有效缓解外部攻击和内部威胁，为数字化转型奠定安全根基。

注：本案例为 2020 年案例

4、吉大正元某大型集团公司零信任实践案例

4.1 方案背景

随着信息化技术不断发展，企业智慧化、数字化理念的不断深化已经深入各个领域，云计算、大数据、物联网、移动互联、人工智能等新兴技术为客户的信息化发展及现代化建设带来了新的生产力，但同时也给信息安全带来了新挑战。企业急需一套安全、可信、合规的立体化纵深防御体系，确保访问全程可知、可控、可管、可查，变静态为动态，变被动为主动，为信息化安全建设提供严密安全保障。

客户已经建立了自己的内部业务访问平台，通过部署边界安全等实现了一定程度的安全访问。但是，随着业务访问场景的多样化和攻击手段的升级，当前的安全机制存在一些局限性，需要进行升级改造。其中的主要问题如下：

1. 传统安全边界瓦解

传统安全模型，仅仅关注组织边界的网络安全防护，认为外部网络不可信，内部网络是可以信任的，企业内部信息化已不再是传统 PC 端，各种设备可随时随地进行企业

©2021 云安全联盟大中华区-版权所有

数据访问提高了企业运行效率，同时也带来更多安全风险。

2.外部风险暴露面不断增加

企业数据不再仅限于内部自有使用或存储，随着云计算、大数据的发展，数据信息云化存储、数据遍地走的场景愈加普遍，如何保证在数据信息被有效、充分利用同时，确保数据使用及流转的安全、授信是一大难题。

3.企业人员和设备多样性增加

企业员工、外包人员、合作伙伴等多种人员类型，在使用企业内部管理设备、家用PC、个人移动终端等，从任何时间、任何地点远程访问业务。各种访问人员的身份和权限管理混乱，弱密码屡禁不止；接入设备的安全性参差不齐，接入程序漏洞无法避免等，带来极大风险。

4.数据泄露和滥用风险增加

在远程办公过程中，企业的业务数据在不同的人员、设备、系统之间频繁流动，原本只能存放于企业数据中心的数据也不得不面临在员工个人终端留存的问题。数据的在未经身份验证的设备间流动，增加了数据泄露的危险，同时也将对企业数据的机密性造成威胁。

5.内部员工对数据的恶意窃取

在非授权访问、员工无意犯错等情况下，“合法用户”非法访问特定的业务和数据资源后，造成数据中心内部数据泄露，甚至可能发生内部员工获取管理员权限，导致更大范围、更高级别的数据中心灾难性事故。

4.2 方案概括和应用场景

4.2.1 实施范围

实施范围为集团总部及各个二级单位的国内员工、国外员工及供应商外协人员共计4.5万人。

4.2.2 实施内容

基于客户现有安全访问能力以及其面临的安全挑战，我们决定为用户建设以下几个

©2021 云安全联盟大中华区-版权所有

层面的安全机制：

1.将身份作为访问控制的基础

身份作为访问控制的基础，为所有对象赋予数字身份，基于身份而非网络位置来构建访问控制体系。

2.最小权限原则

强调资源的使用按需分配，仅授予其所需的最小权限。同时限制了资源的可见性。默认情况下，资源对未经认证的访问发起方不可见。

3.实时计算访问策略

访问策略决策依据包括：访问发起方的身份信息、环境信息、当前访问发起方信任等级等，通过将这些信息进行实时计算形成访问策略。一旦决策依据发生变化，将重新进行计算分析，必要时即使变更访问策略。

4.资源安全访问

默认网络互联环境是不安全的，要求所有访问链必须加密。

可信访问网关提供国密安全代理能力，保障访问过程中的机密性。

5.基于多源数据进行信任等级持续评估

访问发起方信任等级是零信任授权决策判断的重要依据。访问发起方信任等级根据多源信任信息实时计算得出。

6.动态控制机制

当访问发起方信任等级发生变化后，策略执行引擎将向各个策略执行点进行策略下发。再由各策略点执行控制动作。

©2021 云安全联盟大中华区-版权所有

4.2.3 总体架构

图 1 零信任总体架构图

1.动态访问控制体系

动态访问控制体系主要负责管理参与访问的实体身份管理、风险威胁的采集，以及动态访问控制策略的定义及计算，动态访问控制的主要产品组件如下：

1）IAM

作为动态访问控制的基础，为零信任提供身份管理、身份认证、细粒度授权及行为感知能力。

身份管理及认证能力：身份管理服务对网络、设备、应用、用户等所有对象赋予数字身份，为基于身份来构建访问控制体系提供数据基础。认证服务构建业务场景自适应的多因子组合认证服务。实现应用访问的单点登录。

细粒度权限管理能力：权限服务基于应用资源实现分类分级的权限管理与发布。实现资源按需分配使用，为应用资源访问提供细粒度的权限控制。

2）安全控制中心

作为策略管理中心：负责管理动态访问控制规则。作为策略执行引擎：负责基于多数据源持续评估用户信任等级，并根据用户信任等级与访问资源的敏感程度进行动态访问控制策略匹配，最后将匹配到的结果下发到各个策略执行点。

3）用户实体行为感知

通过日志或网络流量对用户的行为是否存在威胁进行分析，为评估用户信任等级提

©2021 云安全联盟大中华区-版权所有

供行为层面的数据支撑。

4）终端环境感知

对终端环境进行持续的风险评估和保护。 当终端发生威胁时，及时上报给安全策略中心，为用户终端环境评估提供数据依据。

5）网络流量感知

实现全网的整体安全防护体系，利用威胁情报追溯威胁行为轨迹，从源头解决网络威胁；威胁情报告警向安全控制中心输出，为安全控制中心基于多源数据进行持续信任评估提供支撑。

6）可信访问网关

代理服务是可信架构的数据平面组件，是确保业务访问安全的关口，为零信任提供支持建立国密算法与 RSA 算法的安全通路，基于动态安全，制的会话阻断移动终端与客户端登录均通过安全通道访问服务。

2.策略执行点

主要负责执行由安全控制中心下发的动态访问控制策略，避免企业资源遭到更大的威胁。主要包括以下动态访问控制能力：

1） 二次认证

当用户信任等级降低时，需要使用更加安全的认证进行认证，确保是本人操作。效果：当用户信任等级降低时，需要使用生物识别技术和数字证书技术组合的方式才能完成认证。

2） 限制访问

当用户信任等级降低时，限制其能访问的企业资源，避免企业敏感资源对外暴露的风险。效果：当用户信任等级降低时，通过动态权限的变化，使其不能访问到企业敏感资源。

3） 会话熔断

当用户访问过程中信任等级降低时，立即阻断当前会话。最大程度上降低企业资源受到威胁的时间。效果：当用户下载文件时，如果信任等级降低，会导致下载失败。

4)身份失效

当用户信任等级过低时，为避免其进行更多的威胁活动。将其身份状态改为失效。

©2021 云安全联盟大中华区-版权所有

效果：身份失效后，不能访问任何应用。

5)终端隔离

当终端产生严重威胁时，对被隔离的终端进行网络层面上的隔离，效果：被隔离后断网；

3.密码支撑服务

密码支撑服务为零信任提供底层的密码能力，负责保障所有访问的机密行和完整性。

4.2.4 逻辑架构

图 2

安全控制中心基于访问发起者的身份及终端环境、实体行为、网络态势等多源数据，实时计算信任等级，并将信任等级与安全策略自动匹配，决定最终访问方式。

与云计算平台（公有云/私有云/混合云）结合保护企业资源

©2021 云安全联盟大中华区-版权所有

图 3

为客户构建动态的虚拟身份边界，解决内部人员访问、外部人员访问、外部应用访问、外部数据平台问安全问题。

4.2.5 远程办公

客户远程办公主要包含以下几条路径：

1.用户直接访路径

通过零信任方案的落地，实现了国内外用户多网络位置、多种访问通道、多种脱敏方式的自适应无感安全访问流程。

图 4

2.VPN 访问路径

将原有 VPN 访问场景迁移到用户直接访问。导致用户下定决心进行前的迁移的主要原因如下：

1）安全问题

VPN 是为了解决连接的问题而设计的，其架构本身没有考虑资源安全问题。通过 VPN 链接，与资源在同一网络后，资源就面临直接暴露的风险。

2）权限控制问题

传统 VPN 在鉴定用户身份后即开放相应权限，缺乏整体的安全管控分析能力，容易受到弱口令、凭证丢失等方式的安全威胁。

©2021 云安全联盟大中华区-版权所有

3）部署问题

VPN 的部署一般需要考虑网络的拓扑结构，升级往往要做设备替换，因为是网络层的应用因而客户端侧容易出现各种连接不上的问题，需要管理员投入大量精力。

迁移后效果：

4）安全问题

零信任架构是基于安全设计的，其设计的目的就是解决应用访问的安全，具备减少应用暴露面积的能力，这样黑客就很难找到攻击点。

5）权限控制问题

零信任在每次对用户认证时会进行动态访问控制，动态访问内容包括：动态认证控制，动态权限控制和动态阻断控制。以信任评估等级决策授权内容。

6）部署问题

可信上云的部署不需要改变现网结构，同时可以随时根据需要，通过增加设备或虚拟机弹性扩容。大大减少管理员的人工成本。

4.2.6 云桌面访问路径

将用户的云桌面作为一个特殊的 CS 应用与零信任进行对接，对接后使云桌面访问路径得到了更强的安全保护。改造后具备了单点登录、动态认证，实时阻断能力，并使用国密算法进行通道保护。

4.2.7 特权账号

集中管理所有特权帐户，提供密码托管服务、动态访问控制和特权账号发现等能力。管理范围包括：操作系统特权账号、网络设备特权账号、应用系统特权账号等。

4.3 优势特点和应用价值

本方案与同类方案相比的主要优势在于：能够根据客体资源（应用、服务等）的敏感程度，对客体进行分级管理，降低应用改造难度；建立细粒度动态访问控制机制；支持国密与 RSA 通道自适应。

©2021 云安全联盟大中华区-版权所有

4.4 经验总结

零信任项目不是交钥匙工程。除了有好的方案与好的产品做支撑外，还需要对客户的访问方式方法、进行全面而细致的调研，紧密结合用户应用场景不断的迭代零信任动态访问控制策略，才能最大程度上兼顾安全与易用性。

5、格尔软件航空工业商网零信任安全最佳实践

5.1 方案背景

中国航空工业集团有限公司（简称“航空工业”）是由中央管理的国有特大型企业，是国家授权的投资机构，于 2008 年 11 月 6 日由原中国航空工业第一、第二集团公司重组整合而成立。集团公司下辖百余家成员单位及上市公司，员工逾 40 万人。

2019 年，航空工业深入贯彻落实习总书记关于网络安全和信息化工作的系列重要讲话精神，推动集团内部各成员单位之间的办公协同和数字化转型，建设了覆盖全集团所有成员单位的商密网移动办公平台。平台使用阿里专有云架构建设，企业 OA、邮件、即时通、招采平台等内部应用业务系统相继上云，促进跨地区、跨部门、跨层级的数据资源共享和业务协同。随着移动办公和业务系统的逐渐云化，商网的业务架构和网络环境随之发生了重大的变化，访问主体和接入场景的多样化、网络边界的模糊化、访问策略的精准化等都对传统基于边界防护的网络安全架构提出了新的挑战。目前在商网移动办公安全架构中存在的问题主要包括：个人移动办公终端从注册、使用到删除的设备全生命周期难掌控，移动办公终端中的运行环境监控、恶意应用安装和数据保护难管理；使用移动办公终端的人员身份冒用和越权访问难预防；现有的移动终端一次性认证通过后即取得了安全系统的默认信任，而移动终端的运行环境是随时可能发生变化的，第三方恶意应用系统的安装和病毒感染随时可能造成正在访问的敏感数据被窃取；业务系统采用云化部署，以容器化和 API 化提供服务，但对 API 接口和服务的访问防护仍停留在访问认证层面，尚无对 API 和服务调用进行权限控制；业务系统中存储的敏感数据访问

©2021 云安全联盟大中华区-版权所有

尚未有明确的分级分类访问机制，对于访问敏感数据的应用和用户无从控制和审计。

针对商网移动办公应用中存在的上述新安全风险和新安全挑战，航空工业坚持新问题新解决思路的原则，引入全新的网络安全理念-零信任解决方案。从新的角度出发，零信任解决方案以“持续信任评估”、“动态访问控制”和“软件定义边界”的理念应对集团商网新的网络挑战，创造新的安全模式，构建零信任与传统安全防御互相协同的安全技术新体系。

5.2 方案概述和应用场景

5.2.1 零信任安全模型

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。

图 1 零信任安全模型

©2021 云安全联盟大中华区-版权所有

5.2.2 项目总体架构设计

图 2 零信任架构设计

1. **密码基础设施**

依托商网现有的密码基础设施对其网络平台提供密码密钥管理服务；电子认证基础设施（PKI/CA）对不同对象，如人员、设备、应用、服务等提供基于国产商用密码算法的数字证书管理服务。

2. **可信身份管控平台（身份管理基础设施）**

依托密码支撑体系，以身份为中心，提供不同对象的规范化统一管理服务、多类型实体身份鉴别服务、细粒度的授权管理与鉴权控制服务、安全审计服务。

3. **零信任网关管理平台**

支持多因子认证机制，结合动态上下文环境监测，实现不同接入通道下为用户提供细粒度的统一访问控制机制，支持多台分布式部署网关的集中管理和统一调度。自动编排策略并下发至各网关执行点，实现动态访问控制和内部网络隐藏，支持前端（客户端到网关）流量加密、后端（网关到应用）流量加密。

4. **环境感知中心**

©2021 云安全联盟大中华区-版权所有

负责对终端身份进行标识，对终端环境进行感知和度量，并传递给策略控制中心，协助策略控制中心完成终端的环境核查。通过用户行为分析中心和环境感知中心，建立信任评估模型和算法，实现基于身份的信任评估能力。

5. 策略控制中心

负责风险汇聚、信任评估和指令传递下发；根据从环境感知中心、权限管理中心、审计中心和认证中心等获取的风险来源，进行综合信任评估和指令下发；指令接收及执行的中心是认证中心，以及安全防护平台和安全访问平台。

5.2.3 项目逻辑架构设计

图 3 零信任逻辑架构

零信任服务体系架构分为主体区域、安全接入区、安全管理区、及客体。整个逻辑结构展示了主体访问到客体的动作，通过安全接入区对主体的访问进行安全接入控制与策略管理。最终实现动态、持续的访问控制与最小化授权。

©2021 云安全联盟大中华区-版权所有

5.2.4 总体部署结构

图 4 总体部署结构

5.2.5 业务应用场景

5.2.5.1 基于数字证书的移动办公场景

本项目中有超过 20 万的用户使用移动终端访问商网移动办公系统，如何保证移动终端用户身份认证安全和重要数据完整性安全是移动办公安全的基础和重点。通过在内

©2021 云安全联盟大中华区-版权所有

部云建设部署 PKI/CA 体系，为移动终端提供移动发证服务。用户通过 PKI/CA 体系提供的密钥分离、协同签名等防护技术，可自助申请个人证书和设备证书，实现基于密码技术的数字证书认证和数据完整性保护。移动终端中不会存储完整的密钥信息，可以防止个人移动终端丢失造成的身份冒用、数据泄密等风险。

5.2.5.2 基于终端环境感知的持续信任评估场景

通过终端设备安装的环境感知模块，零信任平台可持续感知终端设备的物理位置、基础环境、系统环境、应用环境等多维度的安全环境，并根据终端环境变化和安全策略配置，评估终端设备的可信任程度，根据信任程度对终端执行二次认证、升级认证及阻断连接等访问控制行为。

5.2.5.3 纵深防御场景

在纵深防御场景下，在每个执行点都要进行动态鉴权。动态鉴权主要提供权限的动态自动授予，动态鉴权综合考虑终端环境、用户行为、身份强度等多种因素进行动态计算，为访问控制引擎提供动态的授权因子。权限系统根据动态的授权因子，对外部授权请求进行实时授权处理，基于授权库的多维属性和授权信息引擎提供的实时信息反馈进行授权判断。

©2021 云安全联盟大中华区-版权所有

5.3 优势特点和应用价值

5.3.1 方案实现效果

方案采用领先的零信任安全架构解决集团数据访问的安全性问题，为集团树立行业安全标杆，重构信息安全边界，从根源上解决数据访问的安全性问题。在建设完成之后，可以实现如下的安全能力：

1.具备终端环境风险感知能力

办公终端安装终端环境感知 Agent（Windows 版本、VMware 云桌面版本），通过终端环境感知 Agent 对员工的办公终端提供覆盖基础安全、系统安全、应用合规、健康状况的四大类感知，一旦检测到安全风险，立即上报至智能身份分析系统。

2.具备多维度身份安全分析能力

通过构建智能身份分析引擎，结合各类系统的登录日志、访问日志、态势感知平台的异常事件、终端环境感知中心报送的环境风险等信息，提供信任评估能力。依据建立的行为基线，对所有用户的访问请求进行综合分析、持续评估。

3.具备动态访问控制能力

通过构建安全认证网关作为数据层面业务访问的统一入口、动态访问控制策略的执行点；构建零信任网关控制台作为控制层面的访问控制策略决策点；通过环境感知 Agent 对用户的终端进行全方位多维度感知，确保用户的终端环境安全及安全风险感知上报；构建智能身份分析系统的用户行为进行多维度分析，进行信任评估并上报至零信任网关控制台进行决策，实现动态访问控制的整体逻辑，具备动态访问控制能力。

4.具备全链路的访问安全加密授权能力

所有的访问请求都会被加密，采用 TLS 传输加密技术，可通过传输数据的双向认证防止中间人攻击。所有的访问请求都需要认证，每个访问请求都需要携带 token 进行身份的认证，认证通过后在下一次访问仍然会重新认证，避免了原有的一次认证就可以访问所有资源带来的安全风险，达到持续认证持续授权，实现访问的最小化原则。

©2021 云安全联盟大中华区-版权所有

5.3.2 项目运行状态

1.业务持续优化

自 2020 年 2 月航空工业商网零信任安全管理平台正式投入使用以来，截至目前，平台注册单位四百余家，覆盖全部三级（含）以上单位，注册用户已超过 20 万人，日活（每天登录平台使用）超 10 万人。疫情防控期间，更是通过云报送功能，时刻掌握每位员工疫情期间的体温信息。

2.安全防护提升

航空工业商网零信任管理平台部署投入使用后，互联网的攻击接踵而至，绝大部分是针对移动办公业务系统的。截止目前，共处置突发事件 3 起，均对攻击行为完美监控并及时阻断和持续监测。在事件处理过程中，基于零信任技术架构的主动防护体系提供了较传统网络安全防护架构所不具备的安全性。其中，基于密码技术的身份鉴别与数据保全起到重要作用。攻击者针对业务系统及数据库，从身份上已经不具备访问业务系统及数据库的权限。即使通过数据库注入的方式，产生注入的行为流量被数据库审计及态势感知平台第一时间定位告警。其次，通过密码技术对重要数据进行了机密性和完整性保护，使攻击者即使成功完成注入，也无法获取业务系统数据信息及篡改商网的数据内容。

对各类攻击的源 IP 地址进行分析后发现，大部分为国外 IP 地址，明显的说明国外的黑客组织视我国军工行业敏感数据为首要攻击目标。而零信任技术的应用，针对的就是用户主体对客体的持续信任评估和动态的访问控制，有效的保证了集团数据的安全性和业务应用的持续性。

5.3.3 项目推广价值

1.首个零信任应用示范项目

航空工业商网零信任管理平台作为中航工业集团乃至军工行业及大型中央企业集团总部内首个采用新型“零信任”技术部署应用来统一支撑全集团日常办公的平台，为军工行业和中央企业响应落实国家“数字化转型”战略，迈出了坚实的第一步，其示范意义重大。

各军工集团和大型中央企业集团总部通过借鉴“零信任”架构的应用模式，

©2021 云安全联盟大中华区-版权所有

结合自身集团的业务现状、管理手段、生产管控机制、信息化建设及防护措施，将新技术应用到集团的业务工作开展中，提高企业的办公效率。同时，加快推进全行业的数字化转型进度，为未来新型基础设施建设中的大数据中心及工业互联网建设中，提供更加安全的主动防御网络架构。

2.支撑疫情常态化防控

疫情防控期间，航空工业依托商网办公平台、视频会议系统等数字化技术为集团提供有效沟通联络渠道，充分运用信息化手段，提升信息传达能力，快速支撑集团掌握全员基本信息、分布区域及身体状况；为响应疫情防控要求，减少召开现场会议，降低人员聚集感染风险，实现随时音视频连线功能，快速掌握疫情防控、复工复产等情况；帮助各单位有效落实疫情防控部署、支持各单位快速有序推进复工复产。

商网零信任架构模式可在各军工集团和大型中央企业集团总部推广，在疫情防控常态化的态势下，推行零信任安全架构建设，改造提升传统产业，培育数字产业，落实落地数字化转型战略，围绕办公、党建、教育培训、业务协同等场景，开发实施云会议、在线学习、云直播、云党建、云工会、移动考勤、安全巡检、访客登记管理等应用，满足远程办公、移动办公、业务协同等高效、便捷的工作场景需求。

5.4 经验总结

本项目完全践行零信任理念开展建设，工期短、任务重、可借鉴经验少，对集团信息化建设部门和格尔公司都是极大地挑战，同时也是完善集团商网全新安全架构体系的最佳机遇。在集团和格尔公司的共同努力下，在规定建设时间内完成了零信任体系的全面建设，实现了集团商网用户的统一身份管理、统一授权、统一认证、统一审计，同时融合 PKI 体系，提供移动端 APP 证书签发、签名验签、证书登录等功能。零信任平台整合了商网资源及业务系统，打造成为统一身份中台功能，给集团及成员单位提供应用上云的身份集成服务，实现以商网办公平台为基础的安全可靠的业务访问，在实际使用中获得了领导和同事的一致好评。

在零信任平台建设成功的同时，我们也总结经验，展望新的技术实现和新的业务拓展。商网零信任平台后期将向平台容器化部署模式逐步转化，同时也考虑

©2021 云安全联盟大中华区-版权所有

与应用的深度联动，实现应用敏感操作的二次认证等拓展业务，更好的为商网提供安全、便捷、贴心的服务。

6、厦门服云招商局零信任落地案例

6.1 方案背景

数据中心承载的业务多种多样，早期数据中心的流量，80%为南北流量，随着云计算的兴起，业务上云成为了趋势，在云计算时代80%的流量已经转变为东西向流量，越来越丰富的业务对数据中心的流量模型产生了巨大的冲击。云环境中南北向的数据经过防火墙，可以通过规则做到网络隔离，但是东西向的数据无需经过防火墙，也就是绕过了防火墙设备，另外，防火墙生命周内基本不做调整，难以实时更新策略，无法适应现代多变的业务环境，所以无法做到业务的精细化隔离控制，网络威胁一旦进入云平台内部，可以肆意蔓延。

传统的网络隔离有 VLAN 技术、VxLAN 技术、VPC 技术。VLAN 是粗粒度的网络隔离技术，VxLAN 技术、VPC 技术采用 Hypervisor 技术实现网络隔离，但是远没有达到细粒度的网络隔离。

2020 年发生了微盟删库重大恶意事件。在事件发生前，微盟已经有了一些安全管控手段如个人独立的 VPN、堡垒机，而当时删库的内部员工通过登陆内网的跳板机，进而删除微盟 SAAS 业务服务的主备数据库。此次删库事件导致微盟损失巨大，SaaS 服务停摆导致微盟平台约 300 万个商家的小程序全部宕机，公司信誉形象大打折扣。财务损失方面，除拟用于赔付客户的 1.5 亿元外，其股价下跌超 22%，累计市值蒸发超 30 亿港元。纵观微盟删库事件，其内部安全管理与防护存在严重的问题，缺少科学、高效、安全的隔离策略，对开发环境、测试环境和生产环境进行严格微隔离。

2017 年 5 月 12 日，WannaCry 勒索病毒事件全球爆发，以类似于蠕虫病毒的方式传播，攻击主机并加密主机上存储的文件，横向覆盖整个内部网络，然后要求以比特币的形式支付赎金。WannaCry 爆发后，至少 150 个国家、30 万名用户中招，造成损失达 80 亿美元，已经影响到金融，能源，医疗等众多行业，造成

©2021 云安全联盟大中华区-版权所有

严重的危机管理问题。中国部分 Windows 操作系统用户遭受感染，校园网用户首当其冲，受害严重，大量实验室数据和毕业设计被锁定加密。部分大型企业的应用系统和数据库文件被加密后，无法正常工作，影响巨大。

根据《网络安全法》、等保 2.0 的相关要求，各组织与企业在等级保护的对象、保护的内容、保护的体系上要从被动防御加强为事前、事中、事后全流程的安全可信、动态感知和全面审计。另外除了对传统信息系统、基础信息网络的覆盖外还要囊括云计算、大数据、物联网、移动互联网和工业控制信息系统。

只有以攻击者的角度换位思考攻击者的目的，识别攻击者眼中的高价值目标，进而定义防御目标，才是有效应对之策。在近几年的大型攻防演练或者实战中，可以发现，企业对网络安全的认识只停留在应付性的表面工作，安全意识停留在“重外敌，轻内鬼”的阶段，缺乏全局视角下发现实际环境中安全风险的能力。招商局集团内部存在弱口令风险、老旧资产可能成为攻击跳板、网络缺乏细粒度隔离措施、服务器普遍零防御等安全问题，这些问题在日后都会成为致命弱点。

6.2 方案概述和应用场景

针对当前招商局集团网络防护体系突出的问题，我们引入零信任架构作为防护的。零信任安全防御核心思想是不再区分内、外网，要求对任何试图接入信息系统的访问进行持续验证，消灭特权帐户。将以网络为中心的访问控制改变为以身份为中心的动态访问控制，遵循最小权限原则，构筑端到端的逻辑身份边界，引导安全体系架构从“网络中心化”走向“身份中心化”，可以有效的避免内部人员的恶意操作。

方案主要使用安全狗云隙微隔离系统和云眼主机安全检测与管理系统，采集工作负载之间的网络流量，自动生成访问关系拓扑图，根据可视化的网络访问关系拓扑图，看清各类业务所使用的端口和协议，并以精细到业务级别的访问控制策略、进程白名单、文件访问权限等安全手段，科学、高效、安全地实现对开发环境、测试环境和生产环境严格微隔离。各个模块进行联动，模块间数据联通，形成闭环系统，整体方案赋予业务资产安全体系攻击防御、精细化的访问控制能力以及行为合规能力，落实零信任安全理念。

云隙微隔离系统的组成由业务可视化、流量控制、Agent 部署与管理三个功

©2021 云安全联盟大中华区-版权所有

能模块，各个模块进行联动，模块间数据联通，形成闭环系统，下图为微隔离系统架构示意图：

图 1

微隔离系统包括如下组件模块：

1. 业务拓扑

通过显示工作组位置、数量、工作负载信息，动态展示出工作组下工作负载的业务流量及访问关系，直观的展示东西向和南北向的访问关系。同时还可在拓扑图上选择访问关系并设置访问规则策略。可指定工作负载查看与该工作负载相关的流量日志，查看访问者的 IP、端口、访问时间、访问次数。

2. 工作组及工作负载管理

将工作负载进行分组，用位置、环境和应用来确定工作组的唯一性，显示用户相关的工作负载及工作组信息包括基础信息、服务信息及策略信息，并提供编辑标签。

3. 策略信息管理

管理策略集基础信息，对策略集范围和规则进行操作管理，策略可分为组内策略和组间策略，策略应用可根据工作组、标签角色或工作负载。

4. IP 列表管理

可将单个或多个 IP 定义为 IP 列表，通过对 IP 列表添加允许操作，达到对南北向流量集中化处理。

©2021 云安全联盟大中华区-版权所有

云隙微隔离采用 Agent 工作负载采集服务器和主机的流量信息，并将相同特征的工作负载，标记上相同的标签。依据实时流量和角色标签，自动生成可视化的业务拓扑图，集中、自动、灵活地配置策略规则；通过策略和策略对象解耦，策略范围确定策略对象，以此实现动态改变服务器上的安全规则，实现对主机全方位业务流量访问控制。

6.3 优势特点和应用价值

1. 流量可视化，流量可视化有利于进行业务分析，使得业务分析更加灵活和简便，辅助运维人员“看清情况”，进而设计精准的规则策略。

2. 采用同一个轻量级 agent 以及云+端的架构，不占用工作负载资源的同时能够覆盖公有云、私有云、混合云模式下的服务器工作负载。

3. 可控范围足够广泛，能够对应急事件做出合理的、迅速的处理。

4. 多维度的隔离能力，全面降低东西向的横向穿透风险。

5. 具备策略自适应能力，能根据虚拟机的迁移、拓展实现安全策略自动迁移。

6. 自适应的防护能力，实现对实时变化的网络环境，实时更新策略。

7. 把策略从每一个分散的控制点上给拿出来，放在一个统一集中的地方进行设计，实现集中管理和维护。

6.4 经验总结

基于深度剖析客户的安全体系，对其体系中的“隐患”要抓准，抓全面，要“对症下药”。零信任方案落地不单单靠使用安全设备做网络隔离，持续性的安全监测、可视化的业务访问态势、动态的策略调整等安全运营能力也需要加强。只有兼顾提升安全防护能力和安全运营能力，才能在设备防护层面以及安全意识层做到面全的提升，进而完善整个安全体系。

©2021 云安全联盟大中华区-版权所有

7、深信服山东港口集团零信任多数据中心安全接入

7.1 方案背景

山东港口集团拥有青岛港集团、日照港集团、烟台港集团、渤海湾港口集团四大港口集团，经营金控、港湾建设、产城融合、物流、航运、邮轮文旅、装备制造、贸易、科技、海外发展、职教等十一个业务板块，在日常业务开展过程中，遇到一些安全挑战：

1.业务系统分布在不同的数据中心，员工需要同时移动接入多个数据中心访问业务系统；

2.一些业务系统直接暴露在互联网上，且明文传输，需要收缩业务系统暴露面，实现数据安全传输；

3.不同港口、业务板块的人员难以区分用户权限；

4.有大量的 H5 应用需要通过移动终端、PC 访问，缺乏统一的门户入口。

山东港口集团希望找到一套合适的方案来解决上述问题。

7.2 方案概述和应用场景

通过市场调研和交流，山东港口集团认为深信服零信任远程接入方案非常符合他们的需求。

1.在集团总部部署了深信服零信任控制中心，在各数据中心分阶段部署深信服零信任安全代理网关，实现多数据中心的同时接入；

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.引入办公门户 APP，实现 H5 应用的统一入口，并新建统一认证平台，实现所有员工的统一身份管理、业务系统统一认证，以及单点登录；

4.通过策略配置，将零信任与办公门户 APP、统一认证平台的对接，实现办

©2021 云安全联盟大中华区-版权所有

公门户 APP 的安全接入和单点登录；

5.通过权限策略配置，实现动态权限管理。

7.3 优势特点和应用价值

山东港口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数据中心的业务系统，提高的经营生产效率；

通过 SDP 的分布式部署方案，实现多数据中心业务系统的同时访问和灵活扩容，解决了传统的 VPN 的方案无法实现多数据中心业务系统同时访问；

通过办公门户 APP、统一认证平台建设，并与零信任结合，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。

7.4 经验总结

项目实施过程面临的挑战一是涉及众多业务系统对接，复杂度较高，比如零信任设备要与办公门户 APP 以及统一认证平台对接，需要厂商具备丰富的对接案例和经验；二是人员角色众多，人员访问业务系统的权限梳理难度较大；三是数据中心分布在不同的城市，设备的安装部署需要有丰富的经验。

8、杭州漠坦尼-物联网零信任安全解决方案

8.1 方案背景

近年来，能源行业全力推进“互联网+智慧能源”战略贯彻，引入“大云物移智链 5G”等新技术，新技术的应用使网络内部的设备不断增长，尤其新型业务发展接入了海量的物联网，使网络“边界”越来越模糊，已经突破了传统能源网络安全防护模型。这些新兴业务的出现所带来的新问题，让安全防护要求变得更为错综复杂。

©2021 云安全联盟大中华区-版权所有

8.2 方案概述和应用场景

平台设计采用以端到端安全防护为核心的零信任安全理念，建立以身份为中心，基于持续信任评估和授权的动态访问控制体系，同时结合现有安全防护措施实现网络安全防护架构演变，形成持续自适应风险与信任评估网络安全防护体系。

图 1

1. 动态授权服务系统

提供权限管理服务，同时对授权的动态策略进行配置，包括动态角色、权限风险策略等。

2. 智能身份分析系统

针对人员认证提供动态口令、人脸识别、指纹识别等身份鉴别技术；针对终端设备提供基于设备属性的‘身份’认证。

3. 访问控制平台

能够接收终端环境感知系统推送的风险通报，能够接收智能身份分析系统与动态授权服务系统提供的身份与权限信息，反馈执行相应的权限控制策略。能够为网关分配密钥，下发通信加密证书。

4. 终端环境感知系统

具备智能终端环境实时监测能力，从各类环境属性分析安全风险，确定影响

©2021 云安全联盟大中华区-版权所有

因素提高对终端信任度量准确度，为信任度评估提供支撑。

5.终端 TEE（安全可信执行环境）

提供终端侧的行为监测、安全认证、内生安全防护等功能，为终端构建安全隔离执行环境。

目前，平台覆盖了能源行业用户的典型应用场景，如远程办公、外部协作、物理网防护场景等，同时相关关键技术与产品也可逐步拓展应用到石化、铁路、水利、轨道交通等多个工业控制领域，具备在全国其他关键信息技术设施进行大规模推广的前景。

8.3 优势特点和应用价值：

漠坦尼物联网零信任安全防护平台可以帮助能源行业用户面对大规模复杂物联网环境时保障业务与数据的安全通过对零信任安全防护体系建设，以动态信任评估体系为核心将安全技术和安全设备融为统一技防体系，降低安全风险概率，增强终端防护能力，打破空间和时间的限制，以身份为中心为业务与数据提供全方位持续防护，在保证安全性的同时为业务创新提供强有力的网络架构支撑，更有效的挖掘数据价值，释放数据潜能。

8.4 经验总结

在项目实施过程中遇到过物联终端设备、哑终端设备管控等一系列挑战与问题，下一步项目将继续进一步完善，丰富可接入纳管的终端类型，优化安全感知与响应能力，在更多的业务场景中提供可靠的安全防护。

©2021 云安全联盟大中华区-版权所有

9、易安联中国核工业华兴建设有限公司EnSDP零信任安界防护平台

9.1 方案背景

中核华兴承担过众多核工程、国防军工工程的建设，参加了国内及出口的大部分核电站的工程建设。业务系统具有较高的安全等级要求，为响应相关部门及集团的安全管理要求，参加“HW行动”，检验自身在应对安全威胁的应对能力、防控能力。

在了解到EnSDP零信任安界访问方案后，中核华兴采用EnSDP来保障业务系统安全，有效防止攻方针对业务系统发起的渗透攻击等安全威胁。

9.1.1 网络现状和安全需求

1.业务系统暴露在互联网，成为黑客攻击、入侵的入口之一；

2.人员类型复杂，需要同时满足本地用户、下属企业及移动办公用户的远程安全接入；

3.老旧的业务系统自身组件如中间件、数据库等存在漏洞，无法妥善处理，被网安部门通报。

4.员工终端设备没有进行全面管理，终端设备随意接入公司网络，缺乏终端防护手段，导致增加网络暴露面。

5.缺少对业务系统的保护措施，以勒索病毒为例，黑客一旦边界进入到内网，会进行渗透扫描，寻找有价值的业务服务器，对服务器进行定向攻击。

©2021 云安全联盟大中华区-版权所有

9.2 方案概述和应用场景

9.2.1 方案

图 1

易安联结合自身产品，根据对企业的调研，以及中核华兴的安全需求情况，提供了易安联 EnSDP 零信任安界访问解决方案。

9.2.2 应用场景

1. 远程办公

可完美替换 VPN，解决 VPN 漏洞多、管理繁、回溯难的问题；可支持普通浏览器和钉钉/微信小程序接入，提供便捷安全的远程接入方式。

2. 护网行动

基于应用网关的应用隐藏机制，可百分百保障护网行动，应用网关隐藏业务和自身，红队扫描不到，无从发起攻击，解决客户应对护网的问题。

3. 数据泄露防护

可对端侧工作域内的数据隔离/加密，解决端侧数据泄露的问题。

©2021 云安全联盟大中华区-版权所有

4.内部审查

可对用户行为和应用访问深度分析，通过网状关联，即时发现异常给出告警和策略联动，解决客户内部数据泄露的问题；可有效管控运维人员，解决运维人员的权限难控制和数据易泄漏的问题。

5.业务上云

支持公有云、私有云及混合云，有效保障云上应用的东西向安全，助力客户业务安全上云。

9.3 优势特点和应用价值

9.3.1 优势特点

本方案充分考虑了系统的可用性、可靠性、及可扩容性。具体的方案优势如下：

1、暴露面收敛

EnSDP 默认屏蔽任何非授权的访问请求，不响应任何 TCP、UDP 等形式的报文，只响应通过可信设备且使用 EnAgent 客户端登录的请求，所以对于任何人来讲不能利用端口扫描、漏洞扫描等工具进行渗透攻击。

2、阻断直接访问形式的安全威胁

非可信账号、非可信设备无法得到业务系统的直接响应，导致攻击方无法尝试利用 WEB 系统 SQL 注入、XSS 攻击等方式造成攻击。

3、核心业务系统一件断网

提供最为便利的远程管理工具，EnSDP 可实现对特定应用一键关闭，解决重要时期或紧急情况的业务系统断网处理。

4、统一身份管理

打通业务系统之间账号信息，员工不需要记住多套账号密码，为方便维护和管理，弱口令、弱密码等安全问题得到有效解决。

5、智能权限控制

通过 EnSDP 实现对用户鉴定及授权，单次访问仅授予最小权限，并通过用户身份，终端类型，设备属性，接入网络，接入位置，接入时间等属性来感知用户

©2021 云安全联盟大中华区-版权所有

的访问上下文行为，并动态调整用户信任级别。

6、设备管理

主要确保用户每次接入网络的设备是可信的，系统会为每个用户生成唯一的硬件识别码，并关联用户账号，确保用户每次登陆都使用的是合规、可信的设备，对非可信的设备要进行强身份认证，用户通过后则允许新设备入网。

7、可信环境感知

对发起访问者所使用设备（手机、电脑等）的软环境进行检测，如设备所使用操作系统的版本、是否安装制定的杀毒软件、杀毒软件是否开启、杀毒软件的病毒库更新到新版本等。

8、异常行为审计

从用户请求网络连接开始，到访问服务返回结果结束，使所有的操作、管理和运行更加可视、可控、可管理、可跟踪。实现重点数据的全过程审计，识别并记录异常数据操作行为，实时告警，保证数据使用时的透明可审计。

9、洞察访问态势

实时同步全球安全威胁情报，及时感知已知威胁，全方位多维度安全数据挖掘，支持用户、设备、应用等维度数据采集，对用户行为、设备等信息进行全面统计并输出多维度报表。

9.3.2 应用价值

1.提升中核华兴安全接入管控能力，所有业务系统都通过 EnSDP 进行安全防护，实现真正意义上的唯一入口，便于管控。

2.增强中核华兴业务系统安全防护能力，提上应对攻方发起的内网扫描、嗅探等渗透攻击方式的应对能力，有效屏蔽 XSS 攻击、SQL 注入攻击等安全威胁。

3.管理人员利用 Web 终端功能实现便捷的远程管理维护，同时可以对特定应用一键断网，实现秒级关闭访问通道。

4.员工访问通过 EnSDP 业务统一安全访问入口，使用统一身份认证账号，无需记住多套账号密码。

©2021 云安全联盟大中华区-版权所有

9.4 经验总结

我司系统版本经常迭代，用户在版本升级的同时，进行业务发布，未成功保存，导致业务发布不成功。

10、虎符网络国家电网某二级单位基于零信任架构的远程安全访问解决方案

10.1 方案背景

当前安全态势下，网络黑产的产业化、集团化应用趋势明显；网络成为某些恶意组织作恶的主要工具或者武器装备，网络威胁种类也更加复杂多变，现有安全解决方案难以应对高级、持续、集团化、武器化的威胁。主要配套的 APT 检测防御等设备应用门槛高，落地效果一般，并不能够保证业务实时的安全性。

近些年来，随着国家对网络安全的重视程度大幅度提升，尤其是国网、中石油、铁路等国有重大型企业，国家对其尤为重视。对此，习近平总书记也特别强调，要加强对信息基础设施网络安全防护，加强网络安全信息统筹机制、手段、平台建设，加强网络安全事件应急指挥能力建设，积极发展网络安全产业，做到关口前移，防患于未然；其次，落实关键信息基础设施防护责任，行业、企业作为关键信息基础设施运营者承担主体防护责任。因此，确保关键基础设施能够稳定运行，构建零信任远程访问，保护敏感信息不被泄露极为重要。

国家高度重视电力等关键信息基础设施的网络安全工作。《中华人民共和国网络安全法》将抵御境内外网络安全威胁、保护关键信息基础设施、数据安全防护等工作上升至法律的层面，严格相关责任和处罚措施。国网公司作为国家特大型公用事业企业，被公安部列为国家网络安全重点保卫单位。各省公司作为国网公司的重要子公司承担着确保网络与信息安全的重要职责，如有其中某一点被攻破，整个电网体系将面临巨大的挑战。

虎符网络专注于零信任技术架构下的防护体系建设，构建外防攻击、内护数

©2021 云安全联盟大中华区-版权所有

据的新安全体系实践。在国网公司已落地多个项目，其中以 2 个典型用户场景作为 2021 年零信任落地案例申报：

1. 国家电网有限公司某二级直属单位教育培训终端零信任技术应用

国家电网有限公司某二级直属单位作为国家电网领导干部培训主阵地，其自主研发的教育培训终端将通过互联网侧对国网系统内领导干部开展培训教育工作，其重要性由此可见一斑。所以该单位对于派发的教育培训终端的数据传输、数据运行以及数据维护等工作保密程度也极为看重。

虎符网络针对该单位的实际业务需求以及对各地的教学培训终端的远程管控要求做了整体的调研分析，发现以下几点实际需求：

1）该终端系统具备一套成熟的账号体系，能够清晰的定位每台设备对应的所属物理位置及所属单位，用户侧只限于该终端系统内指定开放的应用进行远程学习；

2）该终端系统实际访问用户较为明确，面向对象也是针对国网公司系统内单位，主要通过互联网侧开展相应的培训工作。

2. 国家电网有限公司某二级产业单位公司电力仿真实验室零信任技术应用

国家电网有限公司某二级产业单位公司为应对国际各类网络攻击事件以及新型攻击手段进行研究，并提供国网系统内网络安全工作安全防护提升解决方案。其下创立了电力仿真实验室，针对电力系统经常被使用的供电系统、IT 设备、中控设备等仿真环境开展技术研究，并设定攻防演练平台供信息安全红队人员开展场景性攻防演练工作。为提供便利的业务服务环境，该单位部分应用部署在实验室边界防火墙后的 DMZ 区，通过大量安全防护设备进行权限管理。

运维人员意识到远程访问无法针对操作者的审计以及操作人员的身份甄别，缺乏更安全更方便的远程访问方式，甚至应有一些对抗手段，比如攻击检测和预警。其典型业务需要包括：

1）提供一种比较隐匿的远程访问方式，同时又不能被潜在的网络攻击者通过互联网出口嗅探到，减少暴露面。

2）能够实时有效的接入的实验室人员终端设备做管控，通过可信的终端才能够访问到远程访问设备，其他终端自动拒绝；同时异常访问行为能被感知并预警，以方便甲方应急响应事件。

©2021 云安全联盟大中华区-版权所有

3）实验室中部署的攻防演练平台，在比赛期间需要对指定的信息安全红队人员临时开放账户，同时需要限制这些临时账户的访问权限，只允许访问特定的靶标系统，不能访问实验室内网中的其他应用。攻防演练比赛结束后，这些临时账户的权限能够自动回收，减少由于忘记删除账号而导致的数据泄漏风险。

4）解决传统 VPN 无法解决的问题。例如，传统 VPN 不支持自定义路由配置。如下图所示，甲方需要在其实验室的办公内网访问部署在公网上的培训系统，但办公内网使用 172 网段，无法直接通过防火墙开放到外网，需要系统支持路由配置。这种自定义路由配置，在传统 VPN 上实现难度较大。

图 1

针对上述需求和痛点，甲方采用了虎符网络的虎盾零信任远程访问系统（简称“虎盾 ZRA”）。虎盾 ZRA 是可替代传统 VPN 设备的下一代远程安全访问系统，在提供远程访问通道的同时提供多种安全保障。

10.2 方案概述和应用场景

针对远程访问实验室内部服务资源的全业务流程，虎盾 ZRA 提供基于设备侧环境信息和网络侧行为信息，覆盖网络层、登录层、访问层的一体化零信任防御体系。

©2021 云安全联盟大中华区-版权所有

图 2

用户访问实验室内网应用时，将会经过以下验证和授权过程：

图 3

1. 用户通过互联网使用虎盾 ZRA 客户端进行 SDP 敲门；

2. 虎盾 ZRA 网关验证敲门信息，验证通过则返回响应包至客户端主机，同时允许客户端所在的外网 IP 访问 TCP 服务端口；

3. 客户端提交用户/终端信息至虎盾 ZRA 网关进行验证；

4. 虎盾 ZRA 网关验证用户/终端信息，验证通过后授予客户端主机相关应用的访问权限；

5. 客户端接入到虎盾 ZRA 网关，访问授权的内网应用；

©2021 云安全联盟大中华区-版权所有

6. 虎盾 ZRA 网关将客户端的访问请求转发至应用系统；

7. 应用系统响应虎盾 ZRA 网关转发的请求；

8. 虎盾 ZRA 网关转发应用系统的响应内容至客户端主机。

部署完成后，所有流量均由虎盾 ZRA 代理进行访问，实验室内部应用需要与虎盾 ZRA 进行对接，同时虎盾 ZRA 通过企业内部、云端身份体系对用户访问应用权限按需分配。

图 4

1. 采用流量代理模式对内部应用和数据访问流量进行收口，隐藏内部业务系统，收缩资产暴露面，整个网络去除匿名流量。同时仅对公网开放一个 UDP 端口，对于非法请求，端口保持静默，达到“隐身”的效果，让扫描器无从下手。以上措施解决了甲方所关心的“服务隐身”问题。

2. 基于访问设备指纹信息的可信设备认证，结合对认证行为、访问行为、访问内容的审计，让访问可控、可感知。对于网络攻防演练场景，虎盾 ZRA 提供重保模式，非可信设备无法敲开网络，有效缓解各种网络扫描探测、漏洞攻击等风险；同时对凭证盗用、暴力破解、网络敲门暗语滥用等行为都有预警和相应的处置策略。以上措施解决了甲方所关心的接入设备有效管控问题。

3. 在对外部人员临时开放实验室的内部攻防演练平台期间，虎盾 ZRA 允许通过 Excel 批量导入攻防演练参赛人员名单，将此批次人员加入到特定的用户组，并将该组的权限设置为仅访问攻防演练平台。该批次人员的身份和权限生效时间均可定制，赛后将该用户组的权限自动收回。以上措施解决了甲方所关心外部人员临时接入内网的账号和权限控制问题。

©2021 云安全联盟大中华区-版权所有

4.虎盾 ZRA 支持自定义路由条目。对于部署在公网上的培训系统的访问，通过在虎盾 ZRA 上添加路由条目以及在上一级路由器上配置路由策略，使得内网办公用的 172 网段也能被远程访问到，就可以让办公内网用户通过虎盾 ZRA 也可以访问培训系统。以上措施解决了甲方所关心的传统 VPN 部分功能不满足实际业务需求的问题。

10.3 优势特点和应用价值

电力仿真实验室通过部署虎盾 ZRA，解决了远程访问内网资源业务场景下所面临的风险隐患。对于运维人员，通过统一的安全访问策略集中管理所有内网资源，极大的降低了网络边界重新规划的复杂性和时间成本；简化业务合并管理，提高远程访问安全性的同时降低运维成本。虎符网络独家提出的重保模式，能够比较好的应对网络攻防演练场景下针对蓝队设备的检测、渗透和攻击。

作为升级版的下一代 VPN 和零信任框架下更安全的远程访问解决方案，虎盾 ZRA 可在互联网上为企业架设一层以身份为边界的逻辑私有网络，实现四大安全目标：自身服务隐身、人员身份明确、可信设备防御、动态评估授权。

与传统的 VPN 设备相比，虎盾 ZRA 具有以下优势：

对比项	传统 VPN	虎盾 ZRA
产品理念	创建 IP 传输隧道，创建加密通道，传统 VPN 还是网络产品	在加密传输隧道基础上，执行多点验证和检查，保障访问用户身份的真实性，持续监控风险，虎盾 ZRA 是网络安全产品。
可信设备&设备准入	基于用户凭证(用户名+密码)，无设备和环境因素	对接已有身份认证体系，必须完成可信设备绑定，融合设备身份和行为身份，在应用层完成统一设备准入和管控
自身服务暴露面	对互联网暴露服务端口，可能成为攻击的突破点	只对外开放一个 UPD 端口，完成 SDP 敲门之前不会响应任何客户端连接请求，服务端口在互联网上隐藏
权限控制	无法对接入用户执行统	结合访问者身份、访问设备和访

©2021 云安全联盟大中华区-版权所有

对比项	传统 VPN	虎盾 ZRA
	一管控，权限管理和分配难度大	问环境等多维度因素进行动态评估，基于判定结果对用户授予最小访问权限
行为审计	无法对用户的业务和数据访问行为执行深度审计	不仅提供远程访问通道，还可对通道上内容执行深度审计
用户体验	VPN 隧道通常采取长连接，对网络质量要求高，易断线	微隧道代理，短连接，基于网关的流量代理转发，连接稳定，网速更快

10.4 经验总结

从产品定位来讲，虎盾 ZRA 可以不仅局限于用于企业内部访问的 VPN 替代品，而是作为一个“网络入口”工具。接入虎盾 ZRA 后，用户应可以访问到与网关建立信任关系的任何资源，不限于公司内部资源。

从产品功能来讲，虎盾 ZRA 内部应支持创建自定义 DNS 配置，让用户连接到网关后，可以通过自定义域名访问企业内部资源。这种方式相当于为企业创建一个私有的“暗网”，即可以满足业务的便利性，同时由于这些自定义域名在公网上并不存在，也最大程度的降低了网络攻击和信息泄露的风险隐患。

11、奇安信某大型商业银行零信任远程访问解决方案

11.1 方案背景

某银行行内主要是以办公大楼内部办公为主，员工通过内网访问日常工作所需的业务应用。为满足员工外出办公的需要，当前主要的业务流程是通常情况下，用户申请 VPN+云桌面的权限，在审核通过后，管理员为用户开通权限范围内的应用。在远程访问时，员工采用账号密码方式登录 SSL VPN 客户端及云桌面拨入

©2021 云安全联盟大中华区-版权所有

行内办公网络，访问行内办公系统。

随着该行业务发展以及数字化转型的需要，远程办公已经成了行内不可缺少的办公手段，并日渐成为该行常态化办公模式。同时，受疫情影响，使得行内有些业务必须对外开放远程访问。为了统筹考虑业务本身发展需求以及类似于此类疫情事件影响，该行着手远程办公整体规划设计。保证远程访问办公应用、业务应用、运维资源的安全性及易用性。

图 1 客户业务现状

业务痛点：

1.用户远程访问使用的设备存在安全隐患

员工使用的终端除了派发终端还包括私有终端，安全状态不同，存在远控软件、恶意应用、病毒木马、多人围观等风险，给内网业务带来了极大的安全隐患。

2.VPN 和云桌面自身存在安全漏洞

VPN 和云桌面产品漏洞层出不穷。尤其是传统 VPN 产品，攻击者利用 VPN 漏洞极易绕过 VPN 用户验证，直接进入 VPN 后台将 VPN 作为渗透内网的跳板，进行肆意横向移动。

3.静态授权机制无法实时响应风险

当前的网络接入都是预授权机制，当访问应用过程中发生。发生用户登录常用设备、访问地理位置、访问频次、访问时段、用户的异常操作、违规操作、越权访问、非授权访问等行为时，无法及时阻断访问降低风险。

11.2 方案概述和应用场景

为应对上述安全挑战，同时满足其远程访问的要求，奇安信基于“从不信任并始终验证”的零信任理念，为其构建“以身份为基石、业务安全访问、持续信任评估、动态访问控制”的核心能力，从设备、用户多个方面出发，通过立体化

©2021 云安全联盟大中华区-版权所有

的设备可信检查、自适应的智能用户身份认证、细粒度的动态访问控制，可视化的访问统计溯源，模型化的访问行为分析，为为该行提供按需、动态的可信访问，最终实现访问过程中用户的安全接入及数据安全访问。同时，结合其现有安全管控的能力，与现有的分析系统进行安全风险事件联动，进一步提供动态访问控制能力。

图 2 零信任远程访问整体解决方案逻辑图

图 3 零信任远程访问整体解决方案部署图

解决方案由可信访问控制台（TAC）、可信应用代理（TAP）、可信环境感知系统（TESS）等关键产品技术组件构成。该方案在访问的业务系统前部署可信应用代理 TAP，提供链路加密、业务隐藏、访问控制能力。通过部署可信环境感知产

©2021 云安全联盟大中华区-版权所有

品提供终端风险感知作用，并通过可信访问控制台提供动态决策能力。

通过部署和使用奇安信零信任远程访问解决方案，该银行构建了安全、高效和合规的远程访问模式，实现了以最小信任度进行远程接入，对应用权限的“最小授权”，数据的安全传输，达到了远程访问的动态访问目的。

11.3 优势特点和应用价值

奇安信零信任远程访问解决方案适用于业务远程访问、远程运维、开放众测等多种业务场景，对应用、功能、接口各个层面形成纵深的动态访问控制机制，既适用于传统办公访问场景，在云计算、大数据中心、物联网等新 IT 场景也具备普适性。

11.3.1 用户价值

1.业务隐藏、收缩暴露面

可信应用代理 TAP 将云平台中数千个桌面云彻底“隐身”，不对外暴露桌面云的 IP、端口。同时，TAP 采用 SPA 单包授权技术，默认情况下全端口全隐身（连不上、ping 不通），只对合法用户合规终端开放网络端口。

2.终端检查、确保终端环境安全

通过可信环境感知系统 TESS 对用户访问终端进行全方面安全扫描（设备信息、病毒扫描、漏洞扫描、补丁检测、运行软件）和持续监测，不满足检测要求的终端将被禁止登录。

3.持续验证、提升身份可信

通过自适应多因子认证能力，根据人员、终端、环境、接入网络等因素动态调整认证策略，兼顾安全与易用，访问过程中，根据风险情况，持续验证用户身份是否可信。

4.按需授权、细粒度访问控制

遵循最小权限原则，基于场景化应用对业务人员进行细粒度的访问控制。基于角色、访问上下文、访问者的信任等级、实时风险事件动态调整访问权限。

5.安全加固，防止设备被打穿，自身安全

内置 WAF 模块，有效缓解漏洞注入、溢出攻击等威胁；内置 RASP 组件，可

©2021 云安全联盟大中华区-版权所有

抵御基于传统签名方式无法有效保护的未知攻击，同时具备基于自学习的进程白名单和驱动级文件防篡改能力。

6. 无缝体验

解决方案使得员工拥有内外网一致的办公体验，无需用户重复登录，不会因为网络的连通性而影响办公效率。

11.3.2 方案优势

1. 访问控制基于身份而非网络位置

解决方案以身份为逻辑边界，基于身份而非网络位置构建访问控制体系，为网络中的人、设备、应用都赋予逻辑身份，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。基于身份进行细粒度的权限设置和判定，能够更好地适应多类终端接入、多方人员接入、混合计算环境下的数据安全访问及共享问题。

2. 业务访问基于应用层代理而非网络层隧道

解决方案在应用层对所有访问请求进行认证、授权和加密传输，将业务暴露面极度收缩，避免网络层隧道导致的暴露面过大和权限过度开放。传统业务代理实现时由于业务暴露面过大，经常发生安全事故。

3. 信任基于持续评估而非人为预置

解决方案对终端、用户等访问主体进行持续风险感知和信任评估，根据信任评估对访问权限进行动态调整。受控终端具备安全状态可信环境感知能力，能够根据终端上的各种安全状态信息，如漏洞修复情况、病毒木马情况、危险项情况、安全配置以及终端各种软硬件信息，采用“可信加权”原则，将所有风险项产生的权值进行相加，以百分制提供给可信访问控制台。

4. 访问权限基于动态调整而非静态赋予

静态权限难以对风险进行实时响应和处理，解决方案基于持续信任评估和风险感知对权限进行动态调整，遵循基于持续信任评估的动态最小权限原则，实时对风险进行闭环处置。

©2021 云安全联盟大中华区-版权所有

11.4 经验总结

在方案推进过程中，奇安信安全专家发现，其实产业界多数用户均已经在关注并认同零信任的核心理念，但在实际落地迁移中，确实也会存在一些顾虑。比如，目前政策导向不足，零信任建设能否得到公司领导层的有力支持；需要真正实现安全与业务的融合，对运维要求高，需具备一定的技术能力，又要熟悉自己的业务；认为零信任建设存在建设周期长、开发成本高的问题等等。

其实，企业何时、如何进行零信任工程规划和推进并无放之四海而皆准的标准。用户可根据自身的特点以及业务场景的需要，与方案供应商进行深入沟通和交流，共同设计满足自身安全需求的零信任解决方案，并根据方案选择相关产品或组件。引入零信任安全的最佳时机是和企业数字化转型保持相同的步伐，对于不更新基础设施的企业，遵循零信任安全基本理念，结合现状，逐步规划实施零信任；无论全新建设或者迁移，都需要基于零信任进行整体安全架构设计和规划；同时建议，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，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，并取得所有参与人的理解和支持，尽量减少对员工工作的影响。此外，对于运维能力有一定的要求，需要运维人员掌握零信任的基本概念和产品组件，方案供应商也需要积极主动配合，才产生更好的安全效益。

12、蔷薇灵动中国交通建设股份有限公司零信任落地解决方案

12.1 方案背景

目前中国交通建设股份有限公司（以下简称中交建）数据中心内部千台主机所采用的网络安全防护手段主要有边界类以及终端类等产品，现有的安全防护产品无法实现数据中心、公有云等上千规模的虚机访问关系可视化、不同介质环境

©2021 云安全联盟大中华区-版权所有

的统一精细化管理、点对点白名单式的访问控制，访问控制策略的管理现状主要采用人工梳理的方式梳理数据中心内部各主机相关联的业务主机，人工梳理各主机所需开放的业务端口，采用人工方式设置每台主机的访问控制策略，当主机业务发生变化或主机迁移时，需人工更新访问控制策略。这种人工管理访问控制策略的管理方式耗时长且策略梳理困难，亟需实现基于业务的访问控制关系和端口的自动化梳理、实现基于业务的访问控制策略的设置、实现策略的自适应更新及实现不同介质环境的统一管理。

12.2 方案概述和应用场景

12.2.1 现状描述

1.第一阶段

我司在中交建完成了对 vpc 间防火墙的部分替换，利用微隔离策略替代原有 vpc 间的防火墙策略的替换。

2.第二阶段

对中交下属 50 余家二级单位进行纳管，做到分级授权、分散管理，分数部署方式，避免边界防火墙压力过大；

3.第三阶段

完成对 4A 身份系统的对接；

完成与 CMDB 的对接，进行配置、策略的同步更新；

12.2.2 蔷薇灵动 5 步实现数据中心零信任

1.明确要实施微隔离的基础设施，确定管理范围

中交建部署我司集群版管理中心，最大管理范围可达 25000+的终端。对纳管范围内的虚拟机进行客户端部署，同时通过独特的身份标签技术对每一台机器进行描述。

2.利用可视化技术对业务流进行梳理

©2021 云安全联盟大中华区-版权所有

图 1

3. 根据业务特征，构建零信任网络架构

图 2

4. 生成并配置微隔离策略，对被防护系统实施最小权限访问控制

©2021 云安全联盟大中华区-版权所有

图 3

5.对主机网络行为进行持续监控

图 4

12.3 优势特点和应用价值

12.3.1 优势特点

12.3.1.1 分级授权、分散管理

大型企业规模庞大、分层过多造成管理及运维困难，各部门协同工作效率不

©2021 云安全联盟大中华区-版权所有

高，很难及时作出有效决策。

能力体现：蔷薇灵动蜂巢自适应微隔离安全平台能对不同权限用户提供细致到功能点的权限设置，区分安全、运维与业务部门的权限划分，结合微隔离 5 步法更好地实现数据中心零信任。

12.3.1.2 高可靠、可扩展集群

微隔离产品属于计算密集型产品，随着点数的增多计算量成指数型增长，在应对超大规模场景时如何保持产品的稳定性、抗故障率等是一种巨大挑战。

能力体现：蔷薇灵动蜂巢自适应微隔离安全平台支持集群模式，支持更多的工作负载接入，降低系统的耦合性，更以扩展，解决资源抢占问题，提升可靠性，有更好的抗故障能力。

12.3.1.3 大规模一步通信引擎

随着超大规模场景的需求日益增多，管理中心和客户端之间通信能力迎来巨大挑战。

能力体现：蔷薇灵动蜂巢自适应微隔离安全平台可做到高效并发通信，通过软件定义的方式，从各自为战彼此协商走向了统一决策的新高度。

12.3.1.4 API 联动、高度可编排

超大规模情况下，资产信息、网络信息、安全信息、管理信息、运维信息等各自独立，不能紧密结合。

能力体现：蔷薇灵动蜂巢自适应微隔离安全平台面向云原生，API 全面可编排，便于融入客户自动化治理的体系结构里，讲个信息平面打通并精密编排在一起，促进生态的建设。

12.3.1.5 高性能可视化引擎

随着云计算时代的来临，网络流量不可见就不能对业务进行精细化管控，同时也不能进行更高层的网络策略建设。

©2021 云安全联盟大中华区-版权所有

能力体现：蔷薇灵动蜂巢自适应微隔离安全平台对全网流量进行可视化展示，提供发现攻击或不合规访问的新手段，为梳理业务提供新的视角；同时平台可与运维管理产品对接，便于对业务进行管理。

12.3.1.6 高性能自适应策略计算引擎

随着业务不断增长，企业网络架构不断演进、内部工作负载数量也呈指数型增长。超大规模场景下，海量节点、策略量大增、策略灵活性不足等问题日益显著， 而企业往往缺少有效的应对方式。

能力体现：蔷薇灵动蜂巢自适应微隔离安全平台可以自动适应云环境的改变。面向业务逻辑与物理实现无关，减少策略冗余。为弹性增长的计算资源提供安全能力。软件定义安全，支持 DevSecOps，安全与策略等同。

12.3.2 应用价值

12.3.2.1 业务价值

1.满足数据中心中各业务对东西向流量管控的要求。

针对现有业务场景，根据业务实际的访问情况，配置点对点白名单式安全策略；需对内网服务器（虚拟机）细分安全域。对于高危端口、异常来源 IP、异常主机，需在网络层直接关闭、阻断。防止攻击者进入网络后在数据中心内部横移；在上千点主机的业务规模下，当主机的业务、IP 等发生变化时，需能够实现访问控制策略的自适应更新；需实现针对物理机、虚拟机及容器的统一管理。

2.攻击面缩减。

数据中心内部存在大量无用的端口开放，存在较大风险。

3.发现低访问量虚机。

目前数据中心内部存在有些虚拟机访问量较少，使用频率不高的情况，这造成了资源浪费，并且可能成为僵尸主机，增加安全风险。

4.内部异常流量发现。

目前数据中心内部缺少对于内部东西向流量的监测能力，内部存在不合规的访问行为。

©2021 云安全联盟大中华区-版权所有

5.简化安全运维工作。

目前数据中心内部由于历史原因及人员的更迭，现有很多规则已与需求不符，但由于不清楚业务访问逻辑，安全策略调整十分困难，需要能够减少安全策略总数，并对策略调整提供依据。

6.投资有效性需求。

目前数据中心内部采用传统物理服务器，虚拟化云平台也在持续建设中（按照规划，云平台将发展为混合云架构），以及不排除未来会采用容器技术进行业务搭建。考虑到投资的有效性，具体要求如下：

1）既适用于物理机、也适用于不同技术架构的云平台。

2）可以对容器之间的流量进行识别和控制。

3）物理机、不同技术架构的虚拟机、容器均可在同一平台进行可视化呈现及安全管理。

7.协助满足等保2.0的要求。

等保新规中“能够识别、监控虚拟机之间，虚拟机与物理机之间的流量”等要求。

12.3.2.2 功能分析

1.内部流量可视化

1）需要在一个界面中绘制全网业务流量拓扑，并能实时更新访问情况；

2）需识别物理机之间、虚拟机之间、虚拟机与物理机之间的流量；

3）需识别流量的来源IP、目的IP、访问端口即服务；

4）需能够查看虚拟机所开放的服务、服务所监听的端口，及服务对应的进程；

5）需能够记录服务及端口的被访问次数；

6）需能够记录被阻断的访问，包括来源IP、访问的服务及端口、被阻断的次数等信息；

7）拓扑图需可以标识出不符合访问控制策略的访问流量；

8）拓扑图中的元素需支持拖动、分层，实现业务逻辑的梳理。

2.对未来可能涉及到的容器环境提供微隔离防护能力

©2021 云安全联盟大中华区-版权所有

1）需能够识别容器之间的访问流量；

2）需识别流量的来源 IP、目的 IP、访问端口及服务；

3）需能够实现容器之间的访问控制。

3.微隔离策略管理

1）需实现全网物理机、虚拟机、容器的访问控制策略统一管理；

2）通过 web 页面需实现访问控制策略的增加、删除、调整；

3）需可以进行精细化访问控制策略的设置，包括访问的来源、目的、访问的端口及服务；

4）需可配置逻辑业务组的组内规则及组间规则。

4.访问控制策略自适应调整

1）当物理机、虚拟机、容器的 IP 发生变化时，产品需能够自动调整所有与其相关主机的访问控制策略；

2）在虚拟机迁移的过程中访问控制策略需能随之迁移；

3）当虚拟机发生复制时，系统能需识别并自动将原虚拟机的角色及访问控制策略应用到新复制的虚拟机上；

4）产品需能够自动发现新建虚拟机，并自动匹配预设访问控制策略。

5.兼容性要求

1)需支持 Windows sever2008R2 和以上 Windows 全系 64 位服务器操作系统，及 CentOS、Ubuntu、Redhat 等主流 Linux 发行版本；

2）需支持实体服务器、VPS 和云主机等混合环境；

3）需支持 OpenStack 等云操作平台，Xen、Hyper-V、VMware、KVM 等虚拟化架构。

6.产品安装

1）客户端支持一键快速安装，可利用统一运维工具，一键批量安装；

2）客户端的安装、升级、删除无需重启虚拟机。

12.4 经验总结

实施过程中的挑战：客户要求虚拟机模板内置客户端镜像形式部署，由于部署时间紧张且需要对不同的虚拟机内的文件进行修改，故没有采取此安装方式。

©2021 云安全联盟大中华区-版权所有

13、缔盟云中国建设银行零信任落地案例

13.1 方案背景

建设银行高层领导提出了数字经济时代，要破现代商业银行的两大困：1.“数据之困”，拥有数据很重要，但更重要的是将数据充分“聚起来”“用起来”“活起来”，这样才能使数据成为基础性战略资源和重要生产要素。2.“安全之困”，防范现代科技带来的数据泄露、违规经营、服务中断甚至系统崩溃等风险。

建设银行作为大型商业银行数字化转型的代表，近年来，一直在产品创新、新技术应用、业务流程变革、开放银行建设以及监管体系等方面大力推进数字化发展。基于对缔盟云领先产品性能及创新能力的认可，建设银行终端数据安全防泄露项目选定缔盟云“太极界”零信任安全产品为金融数据的安全高效流通保驾护航。

13.2 方案概述和应用场景

零信任网络访问产品“太极界”被规模化应用到建行及其全球分支机构，服务数十万终端。

图 1 太极界技术架构示意

©2021 云安全联盟大中华区-版权所有

以零信任客户端、零信任分布式网关、零信任控制器为主要组件，构建终端-互联网-云的弹性安全区域。由缔盟云 ESZ®Cloudaemon 平台出品。

图 2 一图看懂太极界如何防止金融企业源代码泄露

图 3 一图看懂太极界远程办公接入

©2021 云安全联盟大中华区-版权所有

图 4

13.3 优势特点和应用价值

1.连接、开放、敏捷的数据流通---太极界破”数据”之困

用好、用活外部公共信息和内部经营数据是数字经济时代对金融行业的全新要求。但由于对网络安全极高标准的要求，商业银行在进行互联网数据、办公网数据以及更高安全级别数据的跨网络传输时需要经过冗长的审批流程，并需要通过专用加密设备进行中转。这极大地限制了数据流通性和办公运营效率。

太极界在终端建立一个安全可信的工作空间，在此空间内，被授权的员工可以实现在办公环境、互联网环境以及更高密级别的环境之间自由切换，访问已授权的内部信息及外部资源，真正发挥数字经济的连接、开放、便捷等特征。同时管理平台可以对员工在终端的操作行为进行监管和控制，杜绝非法泄露。

2.灵活、无缝、安全的员工访问---太极界破“安全”之困

新冠疫情的持续蔓延，让商业银行面临前所未有的挑战，金融业务的移动化、线上化和电子化亟待全面推进。员工远程接入办公、非管控设备临时访问、互联网接入开发环境、敏感数据授权提取等常见场景无形中扩大了不可信身份接入的风险以及来自外部攻击者的攻击面。

太极界通过零信任网络对用户、设备、应用、报文进行持续验证，确保访问的安全可信，同时让整个数字生态系统在互联网上隐藏，从而降低被攻击的风险。最终帮助商业银行实现各类设备都能随时随地访问业务系统、服务、数据等，实现灵活、无缝、安全的访问体验。

©2021 云安全联盟大中华区-版权所有

14、联软科技光大银行零信任远程办公实践

14.1 方案背景

疫情前光大银行主要使用 VPN 进行远程办公，VPN 设备在开发网、测试网、办公网均有部署。去年疫情期间，远程办公常态化，运维部门的工作强度增大，而 VPN 也频频暴露出来漏洞，增加了远程接入的风险。并且在参加护网行动中，由于 VPN 带来的风险，一般会直接关停 VPN，而野蛮关停 VPN 影响业务的正常运行。光大银行近年来高度重视网络安全建设，为了增强网络安全体系安全性与先进性，决定使用联软 UniSDP 零信任远程办公解决方案替换现有 VPN 接入方式。

14.2 方案概述和应用场景

14.2.1 方案概述

联软 UniSDP 零信任远程办公解决方案为企业应用提供安全、高效、面向未来的企业安全架构平台。基于零信任安全理念设计，践行零信任网络访问核心原则，包含控制器、安全网关、客户端三大核心组件，采用控制平面与数据平面分离架构，在用户访问受保护资源之前，通过 SPA 单包授权机制与多种身份认证手段，先进行身份校验，确保身份合法后才可与安全网关建立加密连接，并赋予最小访问权限；提供统一安全策略配置及下发，基于评分机制，从环境、行为、威胁三大维度对业务访问生命周期进行动态访问控制及持续信任评估；向管理员提供审计日志、系统监测信息、可视化管理视图，可对系统进行可视化统一运维。

光大银行实际落地方案采用了三套联软科技 UniSDP 系统分别在开发网、测试网、办公网采用负载均衡模式部署，包括 6 台 SDP 控制管理平台和 8 台 SDP 服务网关。

©2021 云安全联盟大中华区-版权所有

图 1 光大银行部署架构图

在两个数据中心分别部署 3 台硬件设备，1 台管理平台（controler、mysql、redis 一体机）和 2 台网关设备；DMZ 区的两个网关通过行方负载均衡进行服务负载，同时两个数据中心的管理平台与各自的网关绑定，通过负载均衡对管理平台进行健康检查，当发现某一数据中心管理平台服务异常，负载均衡会将对外的服务完整切换至另一个数据中心的网关和管理平台，保证系统的高可用性；两个数据中心的 MySQL 和 Redis 分别建立集群，实现数据的同步。

具体建设内容：

1. 联软 UniSDP 软件定义边界系统采用转控分离的部署架构将控制层面与隧道转发分离，提升架构安全性；

2 通过 SPA 单包授权机制，实现互联网暴露端口隐藏，屏蔽非法用户接入，阻止网络攻击；

3. 采用多因素认证方式，对接入用户的身份唯一性进行可信校验，确保仅有合法用户允许接入访问

4. 通过终端安全检查基线，实现接入终端合规性检测；

5. 通过应用水印和现有 VDI，实现数据落地安全。

通过以上能力，建立以认证和授权为核心的零信任远程安全接入系统。通过部署联软 UniSDP 软件定义边界系统，客户使用 SDP+VDI 方案，联软科技 UniSDP

©2021 云安全联盟大中华区-版权所有

软件定义边界系统通过可信身份、可信终端、可信网络、可信服务四个方面为此银行了基于零信任的打造新一代远程解决解决方案。

14.2.2 应用场景

1.远程办公

替换传统 VPN，采用控制平面与网关分离部署架构，提升架构安全性。

2.单点登入

认证通过访问一个平台，可自由访问所有可访问业务系统，提升用户使用的便捷性。

3.终端安全基线检查

持续、动态的设备验证，实现接入终端合规性检测，确保客户端接入期间的合规性和安全性。

4.数据防护

采用 SDP 与原有 VDI 结合方式访问内网业务系统，身份校验通过后，使用 VDI 实现数据不落地，结合数字水印，实现对屏幕数据的保护及溯源。

14.3 优势特点和应用价值

14.3.1 优势特点

1.多因素身份认证

多因素（用户口令+短信口令+设备硬件特征码），提升安全强度。

2.细粒度访问控制

基于用户、设备、应用、等细粒度访问控制，实现最小权限管理。

3.业务安全保护

所有终端通过加密通道访问业务，对所有流量进行访问控制，未经认证用户不可视，减少业务攻击面。

4.安全与业务融合

用户只需要访问一个门户，可以自由访问所有可访问系统，最大限度的保证了用户接入体验效果。

©2021 云安全联盟大中华区-版权所有

5.适应弹性网络

以用户为中心重构信任体系，用户可灵活在任意位置接入，使用 BYOD、办公等终端访问。

6.简化 IT 运维流程

适应移动办公、远程运维、移动业务办理等业务场景，助力企业数字化转型，简化身份部署，提供业务部署、迁移的灵活性。

14.3.2 应用价值

安全：

1.SPA 机制隐藏服务，暴露面收敛，天然抗攻击

2.应用级加密隧道技术，避免内网全面暴露，并保障数据传输安全

3.多因素身份认证机制，确保用户身份合法性及唯一性

4.终端接入安全检查，保障接入设备安全合规，避免接入设备成为攻击跳板

高效易用：

5.提供灵活、便捷的多因素认证方式

6.支持 SSO 单点登录，无需反复认证

7.统一门户，统一访问入口，规范用户访问行为

8.部署简单、运维简单

9.用户行为记录分析，提供丰富的决策依据

扩展：

10.微服务架构，按需灵活扩展模块

11.标准 API 接口，轻松集成第三方系统

12.统一后台架构，支持扩展移动平台接入

14.4 经验总结

联软 UniSDP 系统是零信任安全架构的完美落地，为客户提供了高安全、易用的远程办公解决方案，用户在建设过程首先要立足规划，注重落地，逐步替换，在替换 VPN 的过程中要紧密和业务部门沟通，保障业务运行的连续性。

©2021 云安全联盟大中华区-版权所有

15、云深互联阳光保险集团养老与不动产中心零信任落地案例

15.1 方案背景

阳光保险于 2005 年 7 月成立，历经十余年的发展，已成为中国金融业的新锐力量。公司成立 5 年便跻身中国 500 强企业、中国服务业 100 强企业。集团目前拥有财产保险、人寿保险、信用保证保险、资产管理、医疗健康等多家专业子公司，国内前十大保险公司。

阳光保险自成立以来，累计承担社会风险 1290 万亿元，开启“四五”发展新征程之际，阳光保险启动了“一聚三强”的发展新战略，即以阳光文化为引领，以价值发展为主线，聚焦保险主业核心能力及核心优势提升，持续强化大健康产业布局，强化大资管战略落地,强化科技引领和创新驱动，有效推动集团的高质量可持续发展。

面向未来大健康战略挑战，集团养老与不动产中心，立足康养业务云化、智能化的发展需求，亟需新一代安全理念的解决方案支持未来数字化建设过程的安全建设。经多方评估与技术论证，优先选择基于零信任（ZTNA）理念，打造基于新一代 SDP 的云网一体化平台，实现企业内网、公有云、SaaS 方式的系统安全域防护域管理的需求：

1. 解决错综复杂云+网环境下的信息安全防护

2. 互联网暴露面收敛：暴露在互联网上的明源 ERP、康养运营平台、康养智联云平台、商业租赁系统等企业应用访问通道安全

3. 数据安全： 业务系统一直有端口暴露，存在 IT 资产暴露，被扫描、探测的风险。

©2021 云安全联盟大中华区-版权所有

15.2 方案概述和应用场景

15.2.1 深云 SDP 解决方案

深云 SDP 整体解决方案如下

图 1 深云 SDP 整体解决方案

15.2.2 深云 SDP 方案说明

1. 深云 SDP 方案支持通过客户端跟浏览器【无端】接入云端的 SDP 网关，然后通过网关访问企业内部应用及企业私有云服务器，打造云网一体化部署。

注：浏览器访问仅支持访问 B-S 应用

2. 在 SDP 大脑配置私有 DNS，加速了 DNS 解析，防止 DNS 劫持，默认所有云端网关所有的端口都是 Deny,只有云深客户端（带身份认证、数字签名）进行 SPA 端口敲门，网关验证身份后，才会针对合法用户的 IP 暂时放行 tcp 端口，保证了企业数据“隐身”于互联网，避免端口暴露，防止被攻击。

3. 用户认证通过后会建议 https 加密隧道，保障数据传输安全，进行应用的访问。这里的应用需要在大脑提前配置，只有在白名单的应用才可以被访问

4. 无端模式，深云浏览器强大的兼容模式支持企业使用统一入口登录，减少运维成本，且通过单点登录，一次登录后可以访问被授权的所有应用，在安全基础上实现快速办公。

©2021 云安全联盟大中华区-版权所有

15.2.3 阳光保险应用场景

1. 场景一、浏览器登录入口—统一门户（单点登录及待办集成）

图 2

阳光保险采用融合版深云浏览器进行无端访问，既可以统一入口快速访问，又可以保证客户端安全。

2. 场景二、应用级访问准入：只允许用户访问业务系统，不暴露其他内网资源，避免将风险引入内网

SDP：用户只能访问自己被授权应用，其他内网资源完全不可见

图 3

©2021 云安全联盟大中华区-版权所有

15.3 优势特点和应用价值

15.3.1 产品优势

阳光保险集团主要采用了深云的融合版浏览器+SaaS 模式接入深云 SDP 网关，进行统一认证、远程安全访问、数据隐身技术及最小粒度应用授权来保障企业数据在互联网上高效安全地交互。

图 4

15.3.2 应用价值

整体安全风险降低、办公效率提升、数据可视化、认证系统等级提升、网络访问安全级别提升。

图 5

©2021 云安全联盟大中华区-版权所有

15.4 经验总结

在项目实施过程中，涉及到公司标准的 SaaS 解决方案与客户定制需求的一些冲突，公司项目初期，未能及时考虑到客户的定制场景导致了项目验收过程中的一些问题。

为了解决这些问题，深云 SDP 不仅支持 SaaS 接入，也可以提供 SDK 集成以及融合版浏览器等解决了客户的定制性的需求。未来，我们更多的会通过 SDP 大脑配置来兼容或者解决部分客户定制的需求。提高客户交付及验收效率，加快深云 SDP 产品的落地。

16、上海云盾贵州白山云科技股份有限公司应用可信访问

16.1 方案背景

16.1.1 方案背景

随着云计算、大数据、物联网、移动互联网等技术的兴起，适用于不同行业的“私有云”或者“公有云”解决方案层出不穷，很多政务系统、OA 系统、重要业务系统以及其他对外信息发布系统逐渐向“云”端迁移。这无疑加快了很多企业的战略转型升级，企业的业务架构和网络环境也随之发生了重大的变化。

目前，绝大多数企业都还是采用传统的网络分区和隔离的安全模型，用边界防护设备划分出企业内网和外网，并以此构建企业安全体系。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，但是在高级网络攻击肆虐、内部恶意事件频发的今天，传统基于边界防护的网络安全架构很难适应新环境，对于一些高级持续性威胁攻击无法有效防御，内网安全事故也频频发生。传统安全架构已不能满足企业的数字化转型需求，传

©2021 云安全联盟大中华区-版权所有

统的网络安全架构需要迭代升级。

16.1.2 风险分析

16.1.2.1 过度信任防火墙

防火墙提供了划分网络边界、隔离阻断边界之间的流量的一种方式，通过防火墙可以提供简单、快速有效的隔离能力。然而传统防火墙是基于 IP、VLAN 手工配置访问策略，这意味着管理员需要将所有的防火墙策略进行持续维护，不但工作量巨大容易出错，而且基于区域隔离的 ACL 授权太严格，限制了生产力。一旦攻击者使用合法权限（如口令、访问票据等）绕过防护机制，则内网安全防护形同虚设。

16.1.2.2 内网粗颗粒度的隔离

我们知道风险已不只来自于企业外部，甚至更多是来自于内部。而传统的基于网络位置的信任体系，所有策略都是针对边界之外的威胁，在网络内部没有安全控制点，导致边界一旦被攻破之后，既无法应对攻击者在企业内部的横移，也无法有效控制“合法用户”造成的内部威胁。

16.1.2.3 远程办公背后的挑战

近年来 APT 攻击、勒索病毒、窃密事件、漏洞攻击层出不穷，日趋泛滥，云化和虚拟化的发展，移动办公、远程访问、云服务形式又突破了企业的物理网络边界，而接入网络的人员、设备、系统的多样性呈指数型增加，参差不齐的终端接入设备和系统，具有极大的不确定性，各种接入人员的身份和权限管理混乱，更使安全战场不断扩大，信任区域日趋复杂。企业同时面临着安全与效率的双重挑战，边界消失已经成为必然。

16.1.2.4 攻击面暴露

随着公有云市场占有率不断提升、企业上云是共同的趋势。在这一趋势下，企业的关键业务会越来越多地部署在公有云上，那么其暴露面和攻击面势必变大，

©2021 云安全联盟大中华区-版权所有

原本只能在内网访问的高敏感度的业务系统不得不对互联网开放。与此同时军工级攻击工具的平民化，又让风险不断加剧。

16.2 方案概述和应用场景

16.2.1 平台架构

YUNDUN-应用可信访问解决方案提供零信架构中“无边界可信访问”的核心能力。基于“从不信任、始终校验”的架构，重构企业安全能力建设，将过去的基于网络边界的模型，转变为以身份为核心的新的安全边界，助力企业数字化转型。

图 1

16.2.2 应用场景

16.2.2.1 无边界移动办公场景

据第三方调查数据显示，2020 年春节期间，中国有超过 3 亿人远程办公，以前只能在办公室开展的工作全部搬回了员工的家中，不仅仅局限在日常工作协同沟通、视频会议等，越来越多的企业将很多 IT 功能都搬上了远程办公平台，远程开发，远程运维，远程客服，远程教学等等都已变成现实。为了支撑远程移动办公，原本只能在内网访问的高敏感度的业务系统不得不对互联网开放。目前远程移动办公使用最多的是两种接入方式，一种是通过端口映射将业务系统直接

©2021 云安全联盟大中华区-版权所有

开放公网访问；一种是使用 VPN 打通远程网络通道。无论哪种方式，都是对原本脆弱的网络边界打上了更多的“洞”，敏锐的攻击者一定不会放过这些暴露面。

在 YUNDUN 零信任解决方案中，默认网络无边界，无论访问人员在哪里，使用什么终端设备，访问是内网办公应用或是业务资源，都无需使用 VPN，同时支持细粒度的鉴权访问控制，真正实现无边界化安全办公场景。

16.2.2.2 多云业务安全管控场景

越来越多的企业业务应用构建在云端大数据平台中，使得云端平台存储了大量的高价值数据资源。业务和数据的集中造成了目标的集中和风险的集中，这自然成为黑产最主要的攻击和窃取目标。从企业数字化转型和 IT 环境的演变来看，云计算、移动互联的快速发展导致传统内外网边界模糊，企业无法基于传统的物理边界构筑安全基础设施，基于网络边界的信任模型被打破，企业的安全边界正在消失。

同时近年来外部攻击的规模、手段、目标等都在演化，有组织的、攻击武器化、以数据及业务为攻击目标的高级持续攻击屡见不鲜，且总是能找到各种漏洞突破企业的边界并横向移动，可以说企业的网络安全边界原本就已经很脆弱，而随着“全云化”的覆盖可以说是让这种脆弱性雪上加霜。

YUNDUN-应用可信访问解决方案利用边缘安全网关技术隐藏用户的真实业务资产，如真实 IP、端口等等，用户在通过边缘安全网关访问业务时，会进行身份认证，只有经过身份认证并授权访问的应用才被准许访问，这样就极大的隐藏了攻击暴露面。保障业务部署于任何环境下的访问安全性，有效防御数据泄露、DDoS 攻击、APT 攻击等安全威胁。

16.2.2.3 统一身份、业务管理场景

单点登录要解决的就是，用户只需要登录一次就可以访问所有相互信任的应用系统，目前，YUNDUN-应用可信访问解决方案已经支持与第三方身份认证如钉钉、企业微信、微信等集成，同时支持标准的 OIDC、SAML 等协议，可与客户应用轻松集成。云端控制台可进行精细的权限管控，保障权限最小化，访问控制策略可实时下发至边缘安全网关。边缘安全网关可持续对用户的访问行为进行信任

©2021 云安全联盟大中华区-版权所有

评估，动态控制和调整用户访问权限。同时企业的应用将收敛于应用门户，统一工作入口，方便统一管理。

16.3 优势特点和应用价值

16.3.1 方案优势

16.3.1.1 SaaS 部署

无需机房、服务器等开销，降低建设、维护硬件成本，使用浏览器就可以连接到平台中，省时省力。

16.3.1.2 综合的解决方案及产品

YUNDUN-应用可信访问解决方案除了提供单独的应用可信访问功能，同时支持灵活扩展，包含云 WAF、云抗 D、云加速、DNS 防护等综合安全能力，全面提高应用性能和可靠性。

16.3.1.3 安全检测分析平台联动

传统的边界防护模型通常不介入到业务中，因此难以还原所有的轨迹，不能有效关联分析，导致安全检测容易出现盲点，应用可信访问平台支持针对所有访问审计，UEBA 异常行为分析弱身份凭据泄漏，同时支持与 SOC/SIEM/Snort 等平台数据对接、联动分析、持续审计访问。

16.3.2 客户价值

16.3.2.1 传统 VPN 的缺陷

1. 安全性不足

仅一次用户鉴权，没有持续安全监测，当出现用户证书被盗或用户身份验证强度不足的情况，无法解决合法用户的内部安全威胁；

2. 稳定性不足

©2021 云安全联盟大中华区-版权所有

当使用弱网络（如小运营商，丢包率高），海外网络（跨洋线路，延迟大）时，频繁断线重连，访问体验差；

3.灵活性不足

大部分企业的 VPN 产品是第三方采购，采购和部署周期长，容量，带宽也受限于先前的规划，难以在突发需要的时候进行快速的弹性扩容。

整个方案目标旨在为用户提供更多场景的远程访问服务，内网应用快速 SaaS 化访问，灵活性更强，同时拥有更强的身份认证和细粒度访问控制能力，弥补了内部 VPN 安全性、稳定性、灵活性不足的问题。

16.3.2.2 提高安全 ROI，降低 IT 复杂度

整体方案基于零信任思想："默认情况下不信任网络内部和外部的任何人/设备/系统，以身份为中心进行访问控制，身份是安全的绝对核心"。将过去的基于网络边界的模型，转变为以身份为核心的新的安全边界，无需做过多的改造，降低 IT 复杂度。

16.3.2.3 精细灵活的安全管理

管理员可对用户访问进行精细化控制，包括 URL 过滤、带宽控制、DNS 过滤，优先保证组织内重要商务应用的访问，提升企业办公效率，并可视化所有网络流量，提供各维度统计报表，帮助管理员更好地实施合规策略。

16.4 经验总结

产品是基于零信任这个概念，是国内最近才火起来的，客户接受度不高，市场缺乏教育，以产品方式去推动时，客户更多的是处于观望和了解状态。

©2021 云安全联盟大中华区-版权所有

17、天谷信息 e 签宝零信任实践案例

17.1 方案背景

随着数字化的普及移动办公和云服务使用日益广泛，企业或政府内部薄弱系统无防护，网络边界不再局限于个人设备和系统的运行环境。企业内部应用存在多而分散，登录认证不统一，员工的账号的恶意行为很难被分析，部分员工使用自己的设备在公司办公等多种问题，内部网络不再是应用可以无防护开放的安全环境。对于缺乏安全防御管理的应用，天谷零信任平台对访问的来源设备、用户登录凭证等进行细粒度的访问控制，基于多重因素的持续认证可以大幅度减少应用被扫描，爆破，内部资料外传等风险。e 签宝作为 saas 公司存在其场景的特殊性，主要包含以下：

1. 采用多云服务，云服务账号管理比较痛苦，无法接入内部用户体系，风险极大

2. 内部应用域名混乱，缺乏统一登录，业务不愿意适配接入统一认证

3. 第三方应用如 wiki，jira，Jenkins 等无人维护，无法二开，更无法接入统一登录平台

4. 外采 saas 账号无法接入内部用户体系，风险极大

©2021 云安全联盟大中华区-版权所有

17.2 方案概述和应用场景

图 1

在天谷零信任平台的设计中，用户必须通过零信任网关才能访问到后台的应用系统，同时集成风险引擎、信用评级、安全态势等安全能力，打造基于基于身份体系的安全管控平台。

天谷零信任平台包含如下的组件：

1.零信任网关

零信任网关作为代理，用户必须通过零信任网关才能访问到后台的应用系统，后台业务做隐身保护，同时提供精细粒度的、基于请求的策略防护，非法访问敏感信息的审计日志，打通 RBAC 鉴权网关

2.DNS 指向

打通内部 cmdb，DNS 服务，把业务域名切到零信任网关

3.IAM

IAM 的统一卡点，实现所有应用登录环节中身份体系的统一身份收拢

4.RBAC 权限控制模型

实现了应用访问的应用级权限访问控制，基于用户部门岗位等，进行权限的全生命周期管理

5.UEBA 统一审计

©2021 云安全联盟大中华区-版权所有

实现了用户跨应用的统一行为审计，针对用户的历史访问行为进行画像，并且将当前用户的行为进行匹配，UEBA 基于 LSTM，多采用层次检测和集成检测两种思路，层次检测指的是搭建多个简单模型对全量数据进行粗筛，之后在用性价比高、可解释性好的模型进行精准检测

6.文件追踪

网关对于所有系统的文件下载行为，对其中的敏感文件进行统一管控到文件管理平台，并在下载前添加下载人的身份追踪标识，来追踪这份敏感文件的打开记录目前阶段，零信任网关已经接入公司内部绝大多数部分系统，包括但不限于基于开源搭建、自研、三方私有云部署、三方 Saas 服务部署等

17.3 优势特点和应用价值

1.e 签宝零信任团队只有 2 个同学，应用无需任何改造，只要域名切换到网关，进行部分简单配置，就能接入，用户使用除登录界面变化外，基本无感。方便快捷的接入方式 使得天谷零信任平台已经接入 30+以上的内部系统，全面实现公司的统一登录以及身份认证，堵住数据泄露的缺口，抓住公司内鬼。

2.突出优势是能够为所有应用插件化赋能，比如统一添加文件追踪能力，对于数据流的导出，可以进行全生命周期的追踪。

3.天谷零信任平台通过系统化，确保零信任能够在总部以及全国各分办进行扩展， 过程不会对系统使用、技术支持或用户使用造成负面影响。

4.零信任结合 UEBA 将保护资源的目标聚焦到人与数据安全，通过策略与控制排除不需要访问资源的用户、设备与应用，使得恶意行为受到限制，缩小被攻击面，大大降低了安全事件的数量，能够节约时间与人力资源来迅速恢复少数的安全事件。

©2021 云安全联盟大中华区-版权所有

图 2

图 3

17.4 经验总结

零信任系统看着很美好，其实坑超级多，下面罗列几点遇到的坑：

1. 跨域问题

零信任由于是劫持域名，域名不统一就会存在跨域问题，要做到单点登录，就需要解决跨域问题，这块我们投入大量时间去解决，我们现在正在推内部应用统一域名

2. 跳转问题

零信任要判断登录状态，做到实时拦截，拦截后重定向到登录页，由于现在大部分业务都是前后端分离，但部分老业务又没有做到前后端分离，导致跳转方式各种各样，有的是前端跳转，有的是 302 跳转，有的是业务后端跳转，需要零信任网关做大量适配。

©2021 云安全联盟大中华区-版权所有

3.对接麻烦

由于每个系统都有自己的登录认证体系，有些是遵守标准接口，但是现实很骨感，大部分应用不遵守标准，这样零信任需要对接每个认证协议，才能实现单点登录，比如分享逍客,FINDBI 等等

4.验证麻烦

我们采用的零信任架构是劫持域名，这样的话，会造成测试比较麻烦，上线虽然也有灰度，但是如果有些应用是写死后端 IP 的话，这种问题根本测试不出来，由于这种模式，造成了各式各样的线上故障

5.https 流量

我们零信任采用的 nginx 反向代理模式，拿不到 https 就麻烦进行流量解析，这块要么申请二级域名，找供应商要证书，要么就是采用正向代理，需要客户信任证书

6.团队协作

零信任需要切域名，业务接入等，依靠各个支撑部门的配合，安全部门、运维部门、内部用户中心、IT 部门、行政部门以及人事部门等部门的合作，这块存在巨大的沟通和协作成本

18、北京芯盾时代电信运营商零信任业务安全解决方案落地项目

18.1 方案背景

随着 5G、人工智能、云计算和移动互联网等技术的发展，企业不断深化信息化建设，云应用、移动办公等越来越普及，关键业务越来越多地依托于互联网开展，移动成为设备、业务和人员的显著特点，企业 IT 架构进入无边界时代。任意人员在任意时间，可以通过任意设备，在任意位置对企业内部任意应用进行访问。给企业管理、企业安全、员工使用都带来了巨大的挑战。

根据 NIST 零信任架构白皮书的相关说明，完整的零信任解决方案将包括增

©2021 云安全联盟大中华区-版权所有

强身份治理、逻辑微隔离、基于网络的隔离等三部分。埃森哲《2019 年网络犯罪成本研究报告》中显示，通过对上百家企业采访和统计得出，排在首位的安全威胁是来源于粗心和不知情的雇员，其次是过期的安全访问控制策略，第三是未经授权的访问。

可以看出，安全风险较大的场景都与数字世界中“人”相关，安全体系架构从“网络中心化”向”身份中心化”转变将成为必然，本质诉求是围绕数字世界中的“人”为中心进行访问控制，在不可信的网络环境中，基于风险进行认证、授权访问和控制管理，从而重构可信且安全的网络框架，满足当下网络的安全需求，降低乃至消除因网络环境开放、用户角色复杂引发的各种身份安全风险、设备安全风险和行为安全风险。

具体安全风险如下：

1. 员工账户

员工需要记住多个应用系统的密码，在登录每个应用系统时都需要输入用户名和口令；简单密码容易被破解，复杂密码难以记忆，如果在多个应用系统中使用一套密码，会带来更大的安全隐患。

2. 系统管理员

因为用户的账号和权限在各应用系统中是分散独立的，系统管理员需要在每个系统中进行创建、维护、注销以及用户管理和权限管理等一系列操作，这些工作繁琐并容易出现纰漏，更重要的是各应用系统审计功能独立，管理员很难通过分散的日志系统识别全局性的安全风险。

3. 业务发展

随着业务的发展，越来越多的新应用或新系统需要接入，而业务应用开发商的开发重点在业务功能实现，对于业务安全部分往往考虑较少，存在诸多安全风险和漏洞，所以业务方考虑到安全原因不愿草率上线，即使上线，一旦漏洞被人利用，损失很大，这造成业务系统上线周期和风险不可控，影响了业务发展。

4. 业务风险

随着企业信息化建设的不断发展，企业中几乎所有数据均通过电子信息的方式传播、利用和处理，并在这一过程中不断累积。在这些信息中，既有业务系统收集到的用户信息，也有组织内部的敏感商业数据，如：财务报表，招投标方案，

©2021 云安全联盟大中华区-版权所有

采购计划，业务战略规划等。由于重要信息固有的商业价值和经济价值，总会被不法份子采取各种手段所谋求如盗取账号，冒名进入业务系统，甚至直接与组织内部人员里应外合，或内部人员监守自盗，团伙作案，最终损害组织利益或公众利益。企业需要对用户的操作行为进行实时监控和分析，并快速识别安全风险。

作为国内领先的零信任业务安全厂商，芯盾时代拥有强大的研发团队和敏捷的技术创新能力，并积累了大量黑灰产相关行业的对抗经验，这是领跑零信任业务安全领域的有力保障。芯盾时代零信任业务安全解决方案，覆盖人与业务交互全流程，自登录开始直至登出全过程进行持续的判断和风险评估，并具备对不同风险结果的及时处置能力，帮助企业解决来自外部业务风险和内部身份欺诈，为用户构建智能、自适应的业务安全保障体系和基础设施，避免因黑灰产和恶意网络攻击造成的企业高额经济损失。目前，芯盾时代零信任业务安全解决方案已经在近 1000 家金融、政府、运营商、大型企业、互联网等行业用户落地实践。

18.2 方案概述和应用场景

芯盾时代零信任业务安全解决方案，以保护企业资源安全为目标，通过保护数字世界中“人”的安全，实现保护企业核心信息资产和金融资产的安全目标。零信任的核心是基于身份的信任链条，芯盾时代零信任安全体系核心功能包括：企业身份管理平台（EnIAM）和零信任业务安全平台（SDP）等。实现身份/设备管控、持续认证、动态授权、威胁发现与动态处理的闭环操作，实现企业业务场景的动态安全，解决当今企业 IT 环境下的业务风险问题。

在某运营商零信任业务安全解决方案项目落地过程中，实施部署遵循松耦合、模块化的原则，需保证与传统的纵深体系没冲突，而是互补和增强；同样的安全模型可以在云上进行构建；项目落地后除了安全性能提升以外，要兼顾用户体验。

具体建设需求总结：

1. 移动端多因素认证

采用密钥分割、设备指纹、白盒算法、环境清场等技术，与移动安全认证系统协同，实现在移动终端的密钥、数字证书全生命周期管理及密码运算。

2. 企业身份管理平台（EnIAM）

增加应用资源动态访问控制功能，实时监控用户所有业务行为，连续自适应

©2021 云安全联盟大中华区-版权所有

风险与信任评估，能够适应复杂组织架构的用户角色，实现分级管理、细粒度授权等功能。并且能够根据用户客户端的安全环境和自然环境（如：时间、地点登录）确定用户使用何种认证方式是最优的，并根据风险情况自动调整认证策略，解决企业内部身份统一管理难题。

3. 零信任业务安全平台（SDP）

对网络环境中所有用户采取“零信任”的态度，针对前期收集的用户信息，在已有规则基础上，针对实际业务特点开发定制深入的违规检测规则；持续通过信任引擎对用户、设备、访问及权限进行风险评估，实现动态访问控制。

4. 零信任风控决策引擎

即引入人工智能引擎，针对用户行为习惯进行大数据分析并根据业务场景建模，通过历史数据发现新规则，建立与专家规则互补并行的分析评估引擎。

5. 国产化

所用技术以及产品系统均符合国产化要求，使用国密算法并兼容国产化芯片及操作系统。

零信任业务安全解决方案实现效果：

1.远程办公

不再区分内外网，在人员、设备及业务之间构建基于身份的逻辑边界，针对不同场景实现一体化的动态访问控制体系，不仅可以减少攻击暴露面，增强对企业应用和数据的保护，还可通过现有工具的集成大幅降低零信任潜在建设成本，满足员工任意时间、任意地点、任意设备安全可控的访问业务

2.多云/多分支环境

企业使用本地服务、云计算等技术架构，构建多分支跨地域访问，导致企业服务环境越来越复杂，通过零信任访问代理网关将访问流量统一管控，基于动态的虚拟身份边界，并通过计算身份感知等风险信息，建立最小访问权限动态访问控制体系，这样可以极大的减少企业内部资产被非法授权访问的行为，实现在任意分支机构网络环境下的内部资源访问

3.护网/攻防

随着大数据、物联网、云计算的快速发展，愈演愈烈的网络攻击已经成为国家安全的新挑战，护网或攻防已逐步常态化、持续化，范围越来越广。护网或攻

©2021 云安全联盟大中华区-版权所有

防的核心目的是寻找网络安全中脆弱的环节，从而提升安全建设能力。通过“网络隐身”技术，对外隐藏业务系统，防止攻击方对业务系统资产的收集和攻击，进而确保业务系统的安全

4. 跨企业协同

企业有时需要第三方合作伙伴为其提供服务，实现数据或服务共享，开放的业务系统为企业带来极大的安全隐患，通过零信任网关，对外隐藏业务服务，针对协同的合作伙伴进行有效的权限管控，安全审计和可控的访问通道，确保业务和数据安全。

图 1

从建设零信任安全网络的角度来看，在完成基础网络体系后，根据自身特点和业务情况逐步有序的进行建设。另外，在建设零信任安全网络的过程中，随着控制节点的增加，正常员工和外部用户的访问体验趋向于无感知，但对恶意用户而言是愈加严厉的认证策略。

18.3 优势特点和应用价值

1. 资源隐藏，基于 SPA 协议进行预认证，并与动态访问控制平台协同，实现

©2021 云安全联盟大中华区-版权所有

应用预授权列表下发。

2. 高强度设备指纹，采用设备硬件和相似度模型相结合的自主研发专利算法，完美适配主流机型，经过上亿现网用户使用认证无误。

3. 满足合规要求，适配国产化芯片、操作系统、数据库，同时满足国密改造需求。

4. 无需业务改造，通过零信任网关代理业务应用，支持业务系统无改造的情况下，完成单点登录、细粒度授权、基于风险的动态授权等。

5. 多因素认证，支持移动端多种认证方式，包括扫码、动态令牌、人脸、指纹等 10+认证方式。

6. 持续信任计算，基于规则引擎与机器学习引擎高效联动，实时计算访问的风险等级。

7）细粒度访问控制策略，按需配置所需权限，最小权限原则，动态调整访问策略

18.4 经验总结

在项目实施过程中，整个项目团队与客户紧密合作、积极沟通并分析探讨业务场景，创新并解决疑难问题。

芯盾时代坚持服务用户应该以人为本，用技术持续推动，全流程保障用户的业务安全。大量用户的累积证明专业的技术服务能力+优质的产品功能+高效专业的售后保障才是获得用户青睐的原因，将用户放在第一位、将需求放在第一位、将服务放在第一位才能加快市场推广进度。

19、云深互联零信任/SDP 安全在电信运营商行业的实践案例

19.1 方案背景

电信运营商营业厅的业务支撑系统的安全访问一直以来都存在诸多挑战。

©2021 云安全联盟大中华区-版权所有

由于营业厅地理位置分散、人员结构复杂等因素，运营商通常把某些支撑系统开放在公网上直接访问，某些系统通过 VPN 来拨网访问。然而，这样给安全运维部门带来很大的困扰。以国内某大型省级运营商为例，该运营商将营业厅常用的 10 多个业务系统（包括：2G/3G/4G 移动客户端体验管理平台、综合外呼平台、渠道销售实况监控、BSS3.0 等）开放在公网上。如图 1 所示。

图 1 客户现状问题

这种方式面临如下的安全挑战：

1.攻击面暴露

暴露公网上业务服务器、VPN 服务器经常受到来自全球各地黑客的网络爬虫以及黑客的 7x24 小时的扫描和攻击。这些核心业务支撑系统一旦被黑客扫描和攻破，则将会给运营商企业带来巨大的损失和造成不良的社会影响。

2.运维复杂

访问业务支撑系统的的人员结构比较复杂，包括员工、装维人员、渠道代理商、外呼人员、施工监理单位等“四方”人员。由于每个人的电脑水平参差不齐，VPN 经常性的掉线给运维部门带来很大的负担，而且 VPN 也可能会把设备上的恶意软件引入内网。此外，VPN 对于权限的分配和管理难度极大，很难进行精细化授权管理，导致可能访问权限被滥用，造成数据泄露。

3.设备安全风险高

由于人员结构复杂，办公电脑上的软件环境无法严格管控。加上业务人员的电脑水平普遍较低，极有可能中了病毒也未必及时发现。终端电脑上的病毒木马

©2021 云安全联盟大中华区-版权所有

不断会窃取终端的数据，而且会通过 VPN 通道渗透进内网，进而造成严重的安全风险。

4.弱口令导致账号劫持

代理商、上下游供应商的员工安全意识薄弱，登录验证的方式较为单一，容易发生被黑客撞库攻击。

19.2 方案概述

深云 SDP 解决方案是一个基于零信任网络安全理念和软件定义边界（SDP）网络安全模型构建的业务系统安全访问解决方案。方案基于互联网或各类专网分别建立以授权终端为边界的针对特定应用的虚拟网络安全边界，基于用户身份提供特定应用的最小访问权限；对于特定应用对虚拟边界以外的用户屏蔽网络连接，同时在传统网络安全设备上最大化设置严谨的安全策略以减少隐患、最小化开放网络端口以减少因为网络协议自身漏洞造成的攻击，可有效缩小网络攻击面，提高全域网络安全。

深云 SDP 包含三个组件----深云 SDP 客户端、深云 SDP 安全大脑、深云隐盾网关（如图 2 所示）：

图 2 深云 SDP 三大组件

©2021 云安全联盟大中华区-版权所有

1. 深云 SDP 客户端

深云 SDP 客户端主要面向企业办公场景，为保护数据安全、提升工作效率而设计，全面支持企业当前 C/S 及 B/S 应用。在深云 SDP 中，深云 SDP 客户端用来做各种的身份验证，包括硬件身份，软件身份，生物身份等。

2. 深云 SDP 安全大脑

深云 SDP 安全大脑是一个管理控制台，用来对所有的深云 SDP 客户端进行管理，制定安全策略。深云 SDP 安全大脑还可以与企业已有的身份管理系统对接。

3. 深云隐盾网关

所有对业务系统的访问都要经过 SDP 网关的验证和过滤，实现业务系统的“网络隐身”效果。

深云 SDP 可以有效解决应用上云带来的安全隐患，减少业务系统在互联网上的暴露面，让业务系统只对授权的深云 SDP 客户端可见，对其他工具完全不可见，以避免企业的核心应用和数据成为黑客的攻击目标，保护企业的核心数据资产（如图 3 所示）。

图 3 深云 SDP 解决方案

深云 SDP 部署在 DMZ 和云资源池，业务系统分别部署在内网和云资源池，外网用户通过隐盾网关访问业务系统。部署架构如图 4 所示

©2021 云安全联盟大中华区-版权所有

图 4 部署架构图实践。

19.3 优势特点

1. 网络隐身、最小化攻击面

深云隐盾网关实现了将 10 多个业务系统从互联网上彻底“隐身”。另外在内部及外部开展的威胁监测处置工作中，持续对深云 SDP 进行安全监测，目前为止未发现任何安全风险的出现。

2. 按需授权，细粒度授权控制

深云 SDP 安全大脑对业务人员进行细粒度的访问控制，具体到哪些人员可以访问哪些业务系统，只有拥有相对应业务系统授权的用户才能够访问相对应的业务系统，其余无授权的业务系统，无法进行访问。此外，通过深云 SDP 企业浏览器还可以控制用户是否可以进行复制、下载等操作。

3. 身份安全增强

深云 SDP 客户端通过短信验证、硬件设备绑定等功能，使原来业务系统的身份验证更加安全。

4. 提升效率，降低运维成本

深云 SDP 摈弃了传统 VPN 长连接的模式，因此不会掉线，上手简单，同时还有 SDP 安全大脑进行远程管理升级，提升了工作效率的同时又降低了运维成本。

5. 高并发，稳定运行

深云 SDP 自上线实施后，每天支撑营业厅超过一万以上的业务人员同时办公，保障每天数千万元的业务操作的安全。

注：本案例为 2020 年案例

©2021 云安全联盟大中华区-版权所有

20、启明星辰中国移动某公司远程办公安全接入方案

20.1 方案背景

电信运营商作为大体量通信骨干企业，承担着国家基础设施建设责任，具备为全球客户提供跨地域、全业务的综合信息服务能力和客户服务渠道体系。电信运营商安全体系建设相对于其他行业，具有专业深、覆盖广、安全能力丰富等特点，整体覆盖数据安全、应用安全、网络安全、基础安全等多方面。始终以搭建体系化、常态化、实战化的安全防护体系为抓手。尤其是在账号、权限的统一管理上，已经搭建了一套 4A 平台上，建设了一套适合电信运营商自身业务发展的统一安全管理平台。

但随着互联网与电信网的融合、新技术新业务的发展、传统业务模式与新业务模式并存使得业务网络复杂性增加、人员的复杂性增加，进而显现了诸多安全隐患。同时电信运营商安全体系面临的外部网络攻击事件数量持续上升，外部网络攻击的方式愈加智能化、体系化、有组织化。这两方面因素，给电信运营商安全体系建设带来的巨大的挑战，如：

1.终端接入风险，终端的安全防护能力参差不齐，由于未安装或及时更新安全防护软件，未启用适当的安全策略，被植入恶意软件等原因，可能将权限滥用、数据泄露、恶意病毒等风险引入内部网络。

2.人员结构复杂风险，内部业务系统越来越多，人员访问造成的泄密风险增加。

3.对外业务风险，部分业务暴露在会联网上的同时，也会暴露一些高危的漏洞，因此很有很能危及内部业务系统。

4.对内业务风险，数据的集中，大数据技术的应用，使数据成为更容易被“发现”的大目标，数据安全成为安全防护的重点，如用户的的非授权操作、越权操作、脱库、爬库等行为将会导致数据中心的敏感数据被非法获取。

©2021 云安全联盟大中华区-版权所有

20.2 方案概述和应用场景

电信运营商很早就意识到数据安全防护的重要性，在面临接入人员结构复杂、对接的设备和应用多、分布范围广、数据量巨大的问题上，通过抓住第一道安全访问关口，即：对人员身份、接入设备的身份进行验证，确保每一个接入平台人员和设备都是安全可信，拒绝未通过认证的任何人员或实体设备入网，此 4A 安全管控平台的诞生。

4A 安全管控平台自 2008 年建立，通过与绕行阻断结合，建设一套以身份为中心的，基于身份的认证、授权、审计体系，使得所有账号以及操作可管、可控、可审。电信运营商 4A 访问层次主体为人员和设备，客体为应用、服务器、数据库。整体架构分为控制层和能力执行层，控制层主要以安全统一管理为主，包括统一证管理、统一账号管理、统一授权管理、统一资源管理、统一策略管理、统一金库管理、统一审计管理、安全运营管理。执行层主要体现到具体的用户的执行操作。比如某用户执行某个敏感操作，会触发某某金库的动作，其操作是由执行层去执行的。

图 1 4A 安全管控平台信任逻辑示意图

4A 安全管控平台：

1. 统一认证，先认证，后连接，作为主体访问客体的唯一路径，包括单点登

©2021 云安全联盟大中华区-版权所有

录、强身份认证、集中认证、认证安全性控制；

2.统一账号管理，客体账号管理，包括主从账号管理、特权账号管理、密码策略管理、账号安全性控制；

3.统一授权控制，按照 RBAC 权限管理，原子授权、实体级授权、角色级授权、细粒度授权，以及针对高危数据操作场景和敏感数据访问场景的二次化授权金库控制、基于敏感操作的敏感数据实时脱敏控制、水印等；

4.统一审计管理，基于规则分析、关联分析、统计分析、实施分析、建模分析技术，以数据为中心，针对所有在网用户操作审计。

零信任架构，可解释“从零开始建立信任”，“零”是“尽可能小”的相对概念，而非“无或没有”这样的绝对概念。零信任架构打破了传统的认证即信任、边界防护、静态访问控制、以网络为中心等防护思路，建立起一套以身份为中心，以识别、持续认证、动态访问控制、授权、审计以及监测为链条，以最小化实时授权为核心，以多维信任算法为基础，认证达末端的动态安全架构。

零信任架构的关键在于持续不断的去分析终端、环境、行为的风险或是证明网络中“我是我”（这个“我”指的是网络中存在的访问主体）的问题。它通过一系列的动作或参数去评估网络中的“我”是否是“我”，是否是“我”在操作，“我”所处的网络环境存在怎样的安全风险，“我”是否有权限操作等的问题。总体概括就是一个持续认证和动态授权的过程。

图 2 零信任架构逻辑示意图

©2021 云安全联盟大中华区-版权所有

零信任架构通过改变原有的静态认证和静态的权限控制的方法，用一种新的持续的可度量的风险参数作为评判的依据，加入到访问主体的过程中，以达到网络访问的可信，实现整个零信任架构的建设。

零信任架构与电信运营商建设的 4A 平台的建设理念如出一辙，电信运营商限制所有账号的登录路径，这使得管控的访问入口更集中，用户必须通过先认证后连接的方式才能访问到具体的资源权限，其次，4A 针对每个实体账号设置独立的细粒度化的访问权限，为了操作的安全性，在敏感操作或是高危操作情况下需要进行二次授权金库控制，最后，4A 对所有的用户行为进行审计，及时发现未授权操作违规行为、越权操作行为、未经金库审批行为、非涉敏人员访问涉敏权限违规行为等。通过事前、事中、事后多维控制，建设构建面向关键信息基础设施的集中化安全管理。

4A 到零信任架构，能力进一步提升，主要体现在：

1. 在 4A 认证的基础上+访问网络隐藏、通道加密、可信接入组件

4A 的认证管理模块包括了强身份认证、单点登录、基于 IP、Mac 地址和时间段的认证安全访问方式，以及先认证后连接的机制。零信任主要在 4A 的认证基础上进行了扩展，增加了网络隐藏机制，将被保护的资源隐藏，通道加密，缓解了中间人渗透攻击、数据泄露等风险，零信任中的可信接入，将原有 4A 基于 IP、MAC、时间信息的认证访问方式，进行了强化，通过一种可度量的计算方法，应用到认证过程中，实现对访问主体运行状态的周期性信任评估，从而确定账号的唯一性和有效性。如，当终端开发高危端口时，或是未安装杀毒软件，信任评估中心根据终端环境持续做分析，当安全分值未达标时，则不允许进行访问。

2. 在账号的基础上+终端环境感知

零信任架构中，判断用户的信息不再以账号和密码为唯一基准，在日常运维和业务操作中，单一的判断标准会出现账号共用的行为，即多个用户使用同一账号，共享账号会给审计带来很大的影响，同时如果用户终端出现问题，存在病毒之类，会将风向带入内网。零信任正是摒弃了这种单一的判断依据，通过针对访问客体建立详细的终端指纹信息，终端环境状态的判断，从而判断其访问客体的有效性。终端环境包括，采集运行进程状态、注册表、系统版本、关键文件存在与否等环境信息。

©2021 云安全联盟大中华区-版权所有

3. 在静态权限基础上+动态权限控制

4A 的权限控制都是基于静态的授权或是策略进行控制。零信任主要通过改变原有的静态的权限控制的方法，用一种新的持续的可度量的风险参数作为评判的依据，加入到访问主体中，作为客体访问的依据，以达到网络访问的可信，实现整个零信任架构的建设。

4. 在审计基础上+基于用户行为的实时分析能力

4A 的审计都属于事后行为审计，即违规行为已经发生，而零信任的本质是将事后行为审计提前，通过大数据分析技术，针对每个访问主体提前预制行为基线，将访问行为框定到具体的操作行为范围内，当访问主体发生异常操作时候，通过用户行为实时分析模块，针对访问主体操作进行控制，已达到动态授权的行为。由于电信运营商各自的业务特点，以及业务访问需求，需结合自身实际情况，以及管理要求，酌情进行控制。

通过差距分析，再结合 4A 平台，构建了电信运营商独有的零信任架构，打破传统以“人”为中心的认证方式，构建以“人+设备+环境”的认证体系，即统一安全管理平台（4A）+持续、动态的“用户+设备（环境）”的检测与授权，实现访问主体的身份可信，确保数据安全访问，达到对数据“可用可见、可用不可见、不可用不可见”等状态的统一安全管控。

图 3

零信任架构包括零信任客户端、零信任网关、安全管控中心（4A）、以及信

©2021 云安全联盟大中华区-版权所有

任评估中心。

1）零信任客户端，实现单点登录、终端采集和链路加密；

2）零信任网关，执行组件，包括可信接入网关、可信运维网关、可信 API 网关，提供网络隐藏和应用系统访问入口，主要做认证和访问策略执行，提供身份的零信任策略执行、访问的零信任策略执行、提供动态访问控制处置和应用系统访问代理，以保证应用访问的安全性；

3）安全管控中心，在原有 4A 的账号、认证、授权、审计基础上，增加访问控制服务，以实现动态身份管理控制、动态权限控制、终端访问控制等策略；

4）信任评估引擎，零信任架构中实现持续信任等级评估能力的核心组件，和访问控制引擎联动，持续为其提供主体信任度评估，作为访问控制策略判定依据。

20.3 优势特点和应用价值

1.让数据更安全

针对业务访问、办公访问、运维访问等不同场景，零信任从数据的采集、存储、传输、处理、交换、销毁等维度，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，从而让数据更安全。

2.让办公更便捷

随着全球化进程的推进，大型公司全球多地协同办公的现象很普遍，零信任通过分布式、弹性扩容、自动容灾、终端环境感知等技术，解决了多地办公性能问题、时差问题及安全与用户体验的矛盾，从而让办公更便捷。

3.应对演习更从容

近年来，网络演习活动在各监管机构、主管部门的组织下，呈现出常态化趋势。社工、近源攻击等高级渗透手段也屡见不鲜，红方攻击人员一旦进入蓝方内网，或拿到了蓝方人员的弱口令，将对蓝方的防守工作造成巨大威胁。演习期间，蓝方人员往往杯弓蛇影，压力巨大，甚至不惜下线正常业务。

零信任架构立足于 SPA+默认丢包策略，网络连接按需动态开放，体系设计

©2021 云安全联盟大中华区-版权所有

满足先认证后连接原则，在网络上对非授权接入主体无暴露面，极大的消减网络攻击威胁。除此之外，需合法用户使用合法设备，且在合法设备的安全基线满足预设条件的情况下，接入主体的身份才被判定为可信。可有效防护多种网络攻击行为，从而让蓝方防守更有效。

20.4 经验总结

目前项目已经完成实施部署，但是还存在一些问题，一方面主要体现到持续的动态授权认证和授权方面，还需要针对具体的场景进行分析、细化数据访问控制，比如远程登录访问敏感数据场景、批量下载敏感数据场景等，在落地实施时候，需要同时关注针对数据的分级分类，制定相应的策略防护，同时结合行为实时分析，才共同支撑零信任动态授权；一方面是在推广层面，零信任会增加针对终端的信任评估内容，依据终端采集的信息进行相应评分，评估终端是否能够按照要求接入。所以在推广时，会遇到各种登录不上去的问题，解决办法，需要制定相关的制度要求，以及相应的手段进行落地。

21、指掌易某集团灵犀·SDP 零信任解决方案

21.1 方案背景

随着移动信息化的高速发展，以智能手机，智能平板为代表的移动智能设备逐步深入到企业办公领域。基于当前移动办公的趋势，某集团也逐步将业务从 PC 端向移动端进行迁移。一方面，移动技术的发展让移动办公成为常态，疫情进一步加速了移动办公、线上协作的常态化进程。另一方面，为使线上协作、移动办公更高效便捷，越来越多的应用和数据在互联网上发布，数据和应用访问面临更高的风险。

随着数字化转型的不断深入，某集团将越来越多的核心应用迁移到云计算平台和互联网，企业的服务范围已经远远超出了原有内部网络边界，企业业务系统

©2021 云安全联盟大中华区-版权所有

走向了更开放的生态模式，由此面临的来自互联网的恶意威胁越来越大。主要包括：

1.员工自带设备办公，存在数据泄露风险

大部分员工使用自带的手机、笔记本进行移动/远程办公，企业数据在不可控的个人设备上面临以下风险：办公过程中，难免会流转敏感文件，若被员工下载到个人设备中、随意转发到互联网，会造成敏感文件泄露事件；业务应用展现了重大审批流程、公司等，一旦被拷贝、截屏并转发到微信等社交平台上，损失将不可估量。

2.业务应用服务器暴露在互联网上，终端、应用与某集团内网业务服务器之间通过互联网连接方式，网络无边界、接入无认证，将业务数据置于随时能被攻击或截获的环境中，存在很大的安全隐患。

综上，传统的安全方案已经不能满足企业要求。多种因素促使该企业一直在寻求更完善的信息安全解决方案，有效防护企业 IT 资产和数据安全，并帮助全球员工安全地接入业务系统，便捷的开展日常工作。

21.2 方案概述和应用场景

某集团业务种类众多、数据资产庞大，且已经构建了复杂的网络体系，企业网络安全防护体系在满足业务发展需求的同时，面对应用实践仍然较少的零信任理念转型需求，如何保障数据的合法合规访问和使用，以及如何选择最贴切集团业务安全需求的方案提供商成为重要挑战。指掌易在详细了解了该集团客户所面临的的挑战和实际需求之后，为客户提供了一套切实可行的零信任解决方案。通过一年多的持续考察论证，某集团的零信任网络架构建设已经取得了显著的成效。

©2021 云安全联盟大中华区-版权所有

图 1

指掌易 SDP 零信任解决方案基于零信任模型实现，以基于身份的细粒度访问代替广泛的网络接入，为用户提供安全可靠的访问业务系统方案。帮助客户实现 OA、门户、邮件等办公系统在互联网上进行隐身，同时要求基于零信任理念，保证员工在内、外网访问办公系统时，都必须首先通过零信任系统进行认证，避免以往当员工处于内网时的隐形信任问题。

指掌易通过和集团现有 IAM 系统进行对接，保证在 PC 端和移动端是实现用户的统一身份认证及 SSO 单点登录机制。

图 2 指掌易零信任整体解决方案架构图

本项目总体设计架构图如上图所示，指掌易 MBS 移动业务智能安全平台是一套“云-管-端”三位一体构建立体纵深的移动设备、业务的安全防护、管理运维的综合平台。平台主要由安全工作空间、SDP（软件定义边界）零信任接入网关、

©2021 云安全联盟大中华区-版权所有

运维管理平台三部分组成。

MBS 移动业务智能安全平台支持在 Android 和 iOS 移动设备上，建立移动安全工作空间，实现个人数据和企业数据的完全隔离，实现应用级的 DLP 策略，如应用水印、禁止复制粘贴、禁止截屏等功能，所有集团内部办公应用可以发布在安全工作空间内的应用商店中。

MBS 移动业务智能安全平台支持在 Windows 和 Mac 系统上安装 PC 安全浏览器，在安全浏览器内可以实现包括水印、禁止复制、禁止另存为等功能。

支持多类型终端通过 SDP（软件定义边界）方式连接入某集团内网，外网员工通过部署在新、老 DMZ 区的不同 SDP 网关接入内网业务系统，内网员工通过部署在内网的 SDP 网关连接到业务系统。所有员工访问内网业务系统都需要首先通过 SDP 认证。

通过运维平台，能够实现态势感知、运维审计等功能，支持对攻击行为、应用情况、用户情况、设备情况等进行记录和审计。

1. 零信任安全接入

图 3

指掌易 SDP 安全网关解决方案由客户端、安全网关和控制器三大组件构成。SDP 客户端负责用户身份认证，周期性的检测上报设备、网络等环境信息，为用户提供安全接入的统一入口。SDP 控制器负责身份认证，访问策略和安全策略分发，并持续对用户进行信任等级的动态评估，根据评估结果动态调整用户权限，并对用户的接入、访问等行为进行全面的统计分析。SDP 安全网关根据控制器的策略与客户端建立安全加密的数据传输通道。

©2021 云安全联盟大中华区-版权所有

1）网络隐身避免外部攻击

关键的应用服务端口不再向外暴露，由零信任网关代理访问。基于 UDP 协议的 SPA 单包授权认证机制，默认“拒绝一切”请求，仅在接收到合法的认证数据包的情况下，对用户身份进行认证，对非法 SPA 包默认丢弃。认证通过后，接入终端和网关之间建立基于 UDP 协议的加密隧道，支持抗中间人攻击、重放攻击等。SPA 协议和加密隧道协议技术实现对外关闭所有的 TCP 端口，保证了潜在的网络攻击者嗅探不到灵犀 SDP 安全网关的端口，无法对网关进行扫描，预防网络攻击行为，有效地减少互联网暴露面。

2）可信接入实现安全访问

根据“零信任”的安全理念，通过对包括用户、设备、网络、时间、位置等多因素的身份信息进行验证，确认身份的可信度和可靠性。在默认不可信的前提下，只有全部身份信息符合安全要求，才能够认证通过，客户端才能够与安全网关建立加密的隧道连接，由安全网关代理可访问的服务。针对异地登录、新设备登录的等风险行为，系统将追加二次验证，防止账号信息泄露而导致的内网入侵。

3）零信任环境检测

包括进行身份信息检测、设备信息检测、访问位置信息检测、访问网络信息检测、访问时间信息检测等。

4）最小化授权

图 4

当用户行为或环境发生变化时，指掌易 SDP 会持续监视上下文，基于位置、时间、安全状态和一些自定义属性实施访问控制管理。通过用户身份、终端类型、

©2021 云安全联盟大中华区-版权所有

设备属性、接入方式、接入位置、接入时间来感知用户的访问上下文行为，并动态调整用户信任级别。

对于同一用户需要设定其最小业务集及最大业务集，对于每次访问，基于用户属性、职务、业务组、操作系统安全级别等进行安全等级评估，按照其安全等级，进行对应的业务系统访问。

5）零信任持续认证

通过强大的身份服务来确保每个用户的访问，一旦身份验证通过，并能证明自己设备的完整性，赋予对应权限访问资源。SDP 进行持续的自适应风险与信任评估，信任度和风险级别会随着时间和空间发生变化，根据安全等级的要求、网络环境等因素，达到信任和风险的平衡。

指掌易 SDP 零信任解决方案架构中，所有用户的请求都必须通过组织信任的设备发起，用户的身份需要鉴定确认是否合法，并且通过遵循控制端下发的安全策略才能访问隐藏在安全网关后面的特定的内部资源。

在持续认证过程中，通过上下文分析和基于计分的信任算法提供更加动态和细粒度的访问控制能力。

2. 安全工作空间

针对集团员工的 BYOD 办公场景，基于指掌易自主研发的 VSA 技术，无需获取应用源代码、无需对操作系统进行 Root 或越狱情况下，对应用进行容器化，建立一个可管理的、相对隔离的安全工作空间，作为构建在应用和系统、应用和应用之间的桥梁。集团内部的办公应用均通过应用商店下发和安装到安全工作空间内。安全办公空间内的办公应用和数据与空间外的个人应用和数据相互隔离，个人应用无法访问办公应用和数据，保障办公应用的安全。同时，安全工作空间通过容器化封装对办公应用提供数据防泄漏能力，防止应用层数据外泄。DLP 赋能企业移动业务，无需改造移动 APP。提供包括应用水印、截屏/录屏保护、复制黏贴保护、数据/文件保护、数据隔离、应用数据透明加解密等安全保护策略。

3. 态势感知

支持对用户、设备、应用、网络攻击、服务器状态等信息的统计、分析、上报能力。能够对用户情况、设备类型、数量、应用安装情况、使用情况、网络攻击类型、IP 地址、攻击来源等进行分析展示，帮助客户了解各类信息。

©2021 云安全联盟大中华区-版权所有

21.3 优势特点和应用价值

1.安全工作空间

提供移动化办公统一协作空间和应用入口，基于指掌易独创的VSA（虚拟安全域）技术，支持在移动设备上创建虚拟的安全工作空间。在BYOD场景中，实现用户个人数据与工作业务数据的安全隔离，既保障了工作数据的安全性，同时极大提升了移动办公的用户体验。实现了一个设备兼备“个人”和“工作”两套“区域”，兼顾工作数据安全以及个人生活隐私。

2.基于“零信任理念”的安全接入系统

围绕无边界零信任网络安全架构理念建设安全网关，零信任安全针对传统边界安全架构思想进行了重新评估和审视，并对安全架构思路给出了新的建议，零信任架构建议组织围绕业务系统创建一种以身份为中心的全新边界，旨在解决“基于网络边界建立信任”这种理念本身固有的安全问题。零信任模型不再基于网络位置建立信任，而是在不依赖网络传输层安全机制的前提下，有效地保护网络通信和业务访问。

3.轻量化安全框架

轻量化的移动安全框架，适配99%的应用及近千款主流移动设备，移动应用安全封装后安全控制能力近百项，同时支持Android、iOS两大主流移动平台。开箱即用，简化配置，无需繁琐的设备注册，增强移动办公效率。打消BYOD场景中个人用户对安装使用安全保护应用，可能造成个人隐私信息泄露等众多疑虑，降低移动办公安全的推进难度。

4.高可扩展性设计

系统支持高可用集群部署，具有合理、高效、灵活的体系结构，便于管理系统的处理能力、容量的扩充、以及多种业务的接入。支持企业移动业务不断新增扩展，安全能力向后兼容，不断扩展新的安全功能或能力，同步支持企业移动业务安全赋能。

21.4 经验总结

零信任理念是未来企业网络安全防护体系的重要发展方向，从实施推进的具

©2021 云安全联盟大中华区-版权所有

体路径上，以及覆盖的业务系统范围来看，目前该集团的零信任架构重点关注于OA 系统、邮件系统、移动办公平台等使用范围广泛，用户级别较高的业务，且已经覆盖了庞大的用户群体。未来，可通过安全态势感知和智能、动态的安全策略调整，逐步实现整体信息安全智能化，助力某集团构建全面信息化安全规划。

22、美云智数美的集团零信任实践案例

22.1 方案背景

在全球疫情驱动下，美的集团数字化工作空间，需要满足内部员工分布式接入、合作伙伴、客户等各类人员，使用各类设备，从任何时间任何地点访问企业服务资源及硬件资源，日常数据传输量大，网络环境不一致，业务资源复杂且分散，集中管控难度变大，对于企业办公网络的稳定性、安全性、可控性提出了更高要求，传统的边界网络（例如 VPN 等）解决方案越来越难以满足现在的需求。

业权一体化（BPI），让权限回归业务本质，让 IT 聚焦数字智能！ 基于美云智数自主研发的业权一体化产品，为每个应用系统和企业资源建立起一道权限安全边界，通过策略授权、自动回收，动态鉴权，实现所有业务动作皆有权限控制的安全屏障，根据用户业务需要自动开通，自助申请与审批，可见即有权，不需要时权限自动取消回收，这些过程都由业务驱动自动完成。

Midea-BPI-SDP 项目，基于美云智数零信任网络平台构建一个全网互联的全新身份化网络，该组件采用了软件定义边界（Software Defined Perimeter，SDP）的安全框架，在用户中通过构建叠加虚拟网络（Overlay Network）的方式重建以身份为中心的零信任安全体系，满足了企业当前无边界网络的安全需求，为客户提供按需、动态的可信访问。即将分布于各地域环境下的数万个终端，以及部署在各种云平台和数据中心的各类应用都接入到统一的安全网络，并采用端到端加密方式跨越互联网进行业务访问，快速解决超大规模远程安全协同办公问题。

©2021 云安全联盟大中华区-版权所有

22.2 方案概述和应用场景

22.2.1 方案概述

Midea-BPI-SDP 由许多组件相互协作组成，确保只有通过严格认证的设备和用户才能访问被授权的企业应用服务器和应用。“图 1：总体架构”是 Midea-BPI-SDP 的解决方案总体架构示意图。

该方案通过基于传统的物理网络，构建基于 SDP 技术构建零信任安全叠加网络 TM-Cloud，该叠加网络（Overlay）是由“信域客户端-TMA、信域网关-TMG、信域控制台-TMG”组成。TM-Cloud 是一种在物理网络(Underlay)架构上叠加的虚拟化网络的技术，具有独立的控制平面和数据平面，使终端资源、云资源、数据中心资源摆脱了物理网络限制，更适合用在多云混合、云网互联网络环境中进行统一集中的身份认证、授权与访问控制。只有通过叠加虚拟云网的认证的用户和终端，才能访问到起上的应用服务（公有云，私有云，本地应用服务），在细粒度权限管理层，通过 BPI（业权一体化）的支撑架构实现权限的弹性开放与回收，以达到动态授权的目的。

图 1 总体架构

“图 2：SDP 架构”是 Midea-BPI-SDP 的解决方案中的 SDP（软件定义边界）实现技术架构图。该架构方案解决了如下问题：

©2021 云安全联盟大中华区-版权所有

1. 更强大的隐身能力

增强的 SDP 架构，客户无需任何公网 IP，所有业务系统和信域组件都隐藏在私有的安全云网络中，最大限度减少互联网暴露面。

2. 以身份为中心的访问控制

执行以身份为中心的访问控制策略，通过预认证、预授权的方式，仅允许已认证和授权的访问源接入叠加网络，并只允许访问已授权的业务。

3. 超大规模访问控制策略

基于身份属性的细粒度访问控制策略，安全关口前移，支持超大规模访问控制策略，同时保持高性能流量转发能力。

4. 无隧道，无限制

不建立网络隧道，而是搭建完整的 IPv4 网络，端到端加密传输，可大范围部署，比 VPN 更安全、更快、更稳定，用户体验更好。

图 2 SDP 架构

“图 3：BPI 架构”是 Midea-BPI-SDP 的解决方案中的 BPI（业权一体化）实现技术架构图。该架构方案解决了如下问题：

5. 大规模运维减负

通过驱动程序进行远程连接与控制，实现大规模服务器端的去插件化。支持

©2021 云安全联盟大中华区-版权所有

运维用户自助化的权限申请。提升权限开通效率，同时，实现了用户入转调离的权限自动化赋予与回收。

6.多样化、碎片化、动态化权限管理能力

以零信任网络安全为基础，强调从不信任，即动态身份认证与动态授权。BPI（业权一体化）是从权限管理基础设施上带来的企业级业务变革，满足企业多样化、碎片化、动态化的场景需求而生的权限管理体系，支撑企业落地有限元的极细粒度授权单元管理与业务场景的动态匹配。

7.远程办公、轻松运维

支持任何环境下开展用户和终端和远程接入，从不信任，始终认证，细粒度授权和弹性控制。

图 3 BPI 架构

22.2.2 痛点场景

序号	痛点描述	解决方案
1	原有身份管理系统老旧，界面易用性不高，不能分级分权管理，并权限控制粒度较粗，不能控	使用美云智数业权一体化产品，从功能级到数据级权限控制一步到位，并且支持不同维度的分级管理，同时，实现大部分岗位标准权限的自动化开通、

©2021 云安全联盟大中华区-版权所有

	制到指令级	转移与回收，大大提升管理效率的同时，降低安全风险。
2	现有十万级服务器需要大量的运维持续投入，原有身份管理系统不能设置定期更新密码策略，服务器安全存在较大隐患	使用美云智数业权一体化产品，可以设置定期更换的复杂密码策略，定期自动更新，实现管理大规模应用服务器密码的自动维护
3	原有身份管理系统管理不同类型服务器，都需要在每台机器上安装插件且不稳定，造成运维工作量较大提升	使用美云智数业权一体化产品，干掉各类型服务器端安装的客制化插件，使用连接器驱动管理服务器资源与细粒度权限资源
4	原有网络环境下，运维工作只能在物理办公网络进行，出现紧急情况时，故障恢复效率不高	使用美云智数零信任网络平台（信域安全云网）构建一个全网互联的云端办公网络，基于软件定义网络 SDP 基础架构实现远程办公安全协同与可信互联

22.3 优势特点和应用价值 I 架构办公问题

22.3.1 优势特点

本研究成果主要目标市场为全国中大型企业资源安全访问控制，解决传统模式下的资源统一管理难、分级管控难、安全能力不足、效率低下等问题，提供了一套满足企业多业务场景的业权一体与零信任安全运维的解决总体方案（即“既要守前门，也要守后门”的双重安全加固），是保障企业数字化转型下的基础设施安全的必要部分，具有巨大的市场空间和广阔的市场前景。

©2021 云安全联盟大中华区-版权所有

22.3.2 应用价值

随着企业数字化转型步入深水区，以及国家在信息安全监管方面的力度加强，安全边界越来越模糊，基于业权一体化的零信任安全应用方案（即“既要守前门，也要守后门”的双重安全加固），将在各大企业中具有非常广的应用前景。

22.4 经验总结

22.4.1 经验总结

经过本项目的实践，总结出如下的经验：

创新点一：业权一体化产品的高效实践方法论

创新点二：远程办公、轻松运维

创新点三：无边界的端到端加密私有安全网络

22.4.2 效果反馈

经过本项目的实施，真正做到网络层可控、授权层可管的细粒度高效运维。效果截图如下：

图 4

©2021 云安全联盟大中华区-版权所有

23、360 零信任架构的业务访问安全案例

23.1 方案背景

某公司是国家高新技术企业，主要从事复合材料与环保建材的研制、开发、生产、销售等，产品广泛用于房地产开发、旧城改造、民用建筑、工业厂房建设、室内外装修、城市公用配套设施等领域。秉承"善用资源，服务建设"的理念，坚持科学发展、和谐建设，经过十多年的发展历程，在国内外拥有多家合资合作公司，享有自营进出口权，是中国民用复合材料行业的领军企业。

随着该企业的数字化转型，同时业务也开始扩展到国内多个城市，分支机构对业务的访问和安全需求随之而来。同时，疫情导致的远程办公常态化，诸多内部员工采用远程访问的方式进行业务操作。

在此背景下，给该企业安全带来了双重挑战：

挑战 1：业务和数据的访问者超出了企业的传统边界。分支机构散布全国，网络、人员、设备都无法精确识别与控制

挑战 2：企业的业务和数据也超出了企业的认知边界。数据流向安全管理人员无法控制的范围

23.2 方案概述和应用场景

以 360 连接云软件定义边界系统为核心，基于零信任架构，遵循零信任核心理念。包含环境感知、可信控制器、可信代理网关三大组件，具备以身份为基础、最小权限访问、业务隐藏、终端监测评估、动态授权控制等几大核心能力。实现企业终端统一管理、用户统一管理、应用统一管理、策略统一管理、数据统一管理、安全统一管理。

©2021 云安全联盟大中华区-版权所有

图 1

23.3 优势特点和应用价值

23.3.1 方案效果

1. 企业用户终端只能通过 360 安全浏览器进行身份认证，满足企业“轻办公”入口需求；

2. 浏览器携带用户身份通过可信网关进行认证并建立国密数据通道；

3. 可信网关根据用户权限鉴别开放其身份可见的业务系统；

4. 用户浏览业务系统文件时实现了防复制、防截屏、防打印、防下载等数据安全能力；

23.3.2 方案价值

1. 安全

1）端口隐藏，减少攻击暴露面；

2）国密数据通道加持，安全可靠；

©2021 云安全联盟大中华区-版权所有

3）持续感知动态鉴权，及时发现风险并有效抑制；

4）数据不落地有效防止人为泄露；

2.高效

1）全面支持 SSO 单点登录，无需反复认证；

2）不改变用户使用习惯，打破无形的技术门槛；

3）统一用户访问入口，规范用户访问行为；

23.4 经验总结

零信任的环境感知持续评估对后期运维带来挑战：客户原有 VPN 用户认证成功后后续再无安全动作，零信任强调的持续感知会要求对访问终端的环境进行持续的评估，发现安全风险后可动态对访问进行干预，这导致刚开始推广时，运维管理员接到不少用户咨询访问被干预的原因。建议在落地前整理对应问题解决 FAQ，并通过企业内部统一 IT 工作流进行问题上报/跟踪/处理整体流程。

24、数字认证零信任安全架构在陆军军医大学第一附属医院的应用

24.1 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。

©2021 云安全联盟大中华区-版权所有

24.2 方案概述和应用场景

24.2.1 方案概述

本方案主要建设目标是为西南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。

根据对西南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：

图 1 西南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、零信任访问控制区结合，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。

24.2.2 陆军军医大学第一附属医院零信任安全架构主要构成

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

©2021 云安全联盟大中华区-版权所有

端安全引擎，由统一身份认证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.安全控制中心

安全控制中心分为访问策略评估服务和统一身份认证服务两个部分。统一身份认证模块对接入的医院用户、医疗终端设备、医疗应用资源、访问策略进行集中化管理。访问策略评估服务对医院用户账号、终端、资源接入进行访问策略进行评估和管理，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.安全基础设施中心

本零安全基础设施中心分为证书服务模块和签名服务模块两个部分。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。签名服务模块主要针对安全控制中心和零信任网关在传输、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。

©2021 云安全联盟大中华区-版权所有

24.3 优势特点和应用价值

24.3.1 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。

24.3.2 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

©2021 云安全联盟大中华区-版权所有

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。

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。

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。

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

24.4 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

©2021 云安全联盟大中华区-版权所有

全引擎和终端模块前，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。

25、山石网科南京市中医院云数据中心“零信任”建设项目成功案例

南京市中医院成立于 1956 年，是南京中医药大学附属南京中医院、南京市中医药研究所、全国肛肠医疗中心、国家级区域诊疗中心；医院现占地面积 92 亩，建筑面积 31.1 万㎡，编制床位 1500 张；在职职工 1900 人，其中硕博士 456 人，高级职称卫技人员 423 人，是一所中医特色明显，集医疗、教学、科研、预防保健、康复和急救功能为一体的、具有中国传统文化特色的花园式、现代化大型三级甲等中医院。

医院现有 1 个主院区（大明路院区）和 1 个分院区（城南分院），2019、2020 年分别新增两个紧密合作型医联体：浦口分院（浦口区中医院）、高淳分院（高淳中医院），2021 年 4 月新增一个市外紧密合作型医联体：滨海分院（盐城市滨海县中医院）。有全国老中医药专家学术经验继承工作指导老师 5 人，江苏省名中医 10 人，江苏省名中西医结合专家 4 人，南京市名中医 37 人，南京市名中西

©2021 云安全联盟大中华区-版权所有

医结合专家 2 人，秦淮区名中医 12 人；有全国名老中医工作室 5 个，省级名中医工作室 3 个，市级名中医工作室 27 个。

医院科室设置完善，现有国家级重点学科 1 个（中医肛肠病学）、重点专科 7 个，省级重点学科 1 个（中医脑病学）、重点专科 8 个，市级重点专科 14 个，市级重点专科建设单位 2 个。肛肠中心为国家级区域诊疗中心、部省共建中医肛肠疾病临床医学研究中心。医院设立院士工作站、江苏省研究生工作站、江苏省博士后创新实践基地、南京市中医药现代化与大数据研究中心、南京市中医药转化医学基地、南京市普外科临床医学中心、南京市医学重点实验室、南京市临床生物资源样本库等。

医院拥有院内自制制剂 122 种。拥有国家级非物质文化遗产代表性项目：丁氏痔科医术；江苏省非物质文化遗产项目：“洪氏眼科”“金陵中医推拿术”；与多名国医大师、国医名师达成合作协议；与美国、比利时等多所大学开展院校间科研、教学、人才培养全面合作。在全国率先创立多专业一体化诊疗平台，并作为典范向全国推广建设经验。

抗疫期间，医院涌现出一批先进工作者，先后有 4 人次荣获全国抗击新冠肺炎疫情先进个人和全国优秀共产党员等国家级荣誉，20 人次荣获省抗疫先进个人、省百名医德之星等省级荣誉，42 人次荣获市优秀共产党员、市五一劳动奖章、人民满意的卫生健康工作者等市级荣誉。2020 年，肛肠科被评为“2020 届中国中医医院最佳临床型专科”。顾晓松院士工作站经批复成为江苏省级院士工作站。医院顺利通过“三级中医医院复核评审”，通过医院信息“互联互通标准化成熟度四级甲等测评”，摘得 2020 年度“全国医院质量管理案例奖·卓越奖”。

25.1 方案背景

2017 年 6 月实行的《中华人民共和国网络安全法》，第二十一条明确要求：国家实行网络安全等级保护制度。而针对医疗卫生行业，卫生部早于 2011 年分别发布《卫生部办公厅关于全面开展卫生行业信息安全等级保护工作的通知》和《卫生行业信息安全等级保护工作的指导意见》，明确要求全国所有三甲医院核心业务信息系统的安全保护等级原则上不低于三级；2016 年，国家卫健委《2016

©2021 云安全联盟大中华区-版权所有

三级综合医院评审标准考评办法（完整版）》规定了医院的重要业务系统必须达到信息安全等级保护三级标准才满足三级医院评审标准中对于网络安全的要求。

医疗行业越来越多的业务系统比如：HIS、LIS、PACS 等迁移至虚拟化平台中运行，但是安全建设依然沿用之前的传统安全解决方案来应对当前主流的安全威胁。在云环境中，传统安全的解决方案会造成云内安全的空白，从而影响将关键业务应用转移至灵活低成本云环境的信心，同时业务系统面临的安全威胁也越发凸显。南京市中医院于 2020 年启动了《云数据中心“零信任”建设项目》，对于南京市中医院虚拟化环境，虽然外部部署了入侵防御设施，但依然存在上述的情况。因为传统的安全模型仅仅关注组织边界的网络安全防护，认为外部网络不可信，内部网络是可以信任的，遵循“通过认证即被信任”。一旦绕过或攻破边界防护，将会造成不可估量的后果。零信任安全模型理念，改变了仅仅在边界进行防护的思路，把“通过认证即被信任”变为“通过认证、也不信任”。即任何人访问任何数据的时候都是不被信任的，都是受控的，都是最低授权的，同时还将记录所有的访问行为，做到全程可视。

微隔离技术，是 SDDC（软件定义数据中心）、SDS（软件定义安全）的最终产物。当微隔离技术与 NFV 相结合，配合 Intel DPDK 技术的高速发展，这与零信任安全模型的思路完全契合。在业界诸多领先厂商的不断努力下，我们看到在云计算环境中微隔离产品是零信任安全模型的最佳实践。

25.2 方案概述和应用场景

25.2.1 方案概述

山石网科为用户带来“零信任”安全模型的最佳实践方案，基于 SDN 的网络微隔离可视化方案—山石云·格。山石云·格在云计算环境中真正实现了零信任安全模型，精细化按云内核心资产进行管理，可以将用户虚机的不同角色划定不同的安全域。山石云·格更能做到 L2-L7 层的最低授权控制策略，且全面适配 IPv6 环境。 凭借山石网科十多年来在应用识别、入侵防御、网络防病毒、Web 访问控制的积累，不论是借用 80 端口的 CC 攻击，还是隐藏在文件中的“病毒”

©2021 云安全联盟大中华区-版权所有

都会被发现、阻断！

南京市中医院采用山石云•格方案分别部署在医院外网（前置服务区）和办公区域（内网区）。

图 1 用户数据中心网络拓扑

医院外网虚拟化数据中心，山石云•格部署在 VMware-vSphere（非 NSX）环境内，为医院官方网站、移动支付、院感系统等应用提供 L2-L7 层安全防护及业务隔离能力。办公区域虚拟化数据中心内部，山石云•格部署在 VMware- NSX 环境内，通过 NSX 服务编排方式引流，山石云•格提供了灵活的策略编排，详细的云内流量展示以及入侵防御和防病毒功能，加固了整套虚拟化数据中心的安全能力。

25.2.2 微隔离技术的实践

南京市中医院的云数据中心中运行的众多应用，分别由不同的供应商开发并维护对应的系统，不同应用系统之间有一定的服务调用，在安全方面，在整个教据中心的外侧边界采用了下一代防火墙、IPS 等设备进行防护，并做了基本的管理、应用系统的网络划分。由于配置难度、保证系统快速上线和应用迭代等原因，云内未划分更多安全城。为了业务快速开发、迭代和互相调用，采用了大二层组网的方式。系统存在的最大风险是，不同外包开发商引入的安全风险，如关键数据的泄瀚，或是外包人员以报复社会为目的的恶意攻击。

在帮助用户采用微隔离技术实现零信任安全模型时，微隔离技术的使用也是

©2021 云安全联盟大中华区-版权所有

遵循 ISO 27001 标准中的 PDCA 循环，即 Plan(计划)、Do(实施)、Check(检查) 、Act(措施)实现的。

1.明确云内核心资产，是实现零信任安全模型的基础，从内向外设计网络，划分安全域的第一步。在 PDCA 的循环中，这是一个动态的过程，不要奢望一劳永逸。！我们一步步围绕，现有以及未来增加的数据，计算核心资产，来划分 MCAP 进行防护，即使采用了 NFV 技术，但在进行深度安全防护时，计算资源依旧宝贵、稀缺、按需对虚机进行防护才是正确的方式，做好这一步有利于将“好钢用在刀刃”上。

图 2 采用全分布式架构的微隔离方案

2.学习和可视。建议初期，我们采用旁路虚拟网络流量到山石云·格，也可以暂时设为全通策略。每次学习和可视的周期最好大于正常的业务周期。利用山石云·格的可视化能力，刻画云内虚机之间的通信轨迹，有哪些应用、有没有威胁。对各个应用系统之间数据和服务交互情况，云内威胁情况. 管理员会有个实际的认识。

©2021 云安全联盟大中华区-版权所有

图 3 云平台全局流量可视

3.确定低授权策略。根据学习可视阶段的成果。可以制定接下来的防护策略。比如 MCAP 如何划分，MCAP 间全局的访问控制策略和一些已知高危漏洞的防护策略 … …

MCAP 的划分可以有多种方式，比如说按照应用的部门进行划分。也可以按照一类虚机进行防护，把一类虚机作为高危资源，设定防护策略。

图 4 按照虚机身份自由划分微安全域

在这些防护策略的制定上，除了在山石云·格上进行相关防护外. 也可以结合外部的下一代防火墙一同进行协调配合。比如在外部防火墙上可以对不同的外包服务商设定 VPN 账号，将该账号与可访问内部虚机进行限定。同时对不同外包供应商负责的虚机，分别再划分 MCAP，设定最低授权策略。

到下一个 PDCA 周期的时候，安全管理员可以将外包供应商登陆 VPN 的情况，山石云·格可以行到的 MCAP 内部，MCAP 之间通信情况、威胁情况，在统一的时

©2021 云安全联盟大中华区-版权所有

间维度上进行分析。借助山石云·格的策略助手，可以学习 MCAP 需要配置的安全策略，并邀请主机管理员、应用开发人员一起，循序渐进，设定好每个 MACP 的最低授权策略，避免错误设，也避免不敢设置导致的漏洞。

图 5 多维度立体的安全域划分，实现最低授权访问

4. 制定实施的计划。协调相关部门进行防护的实施。

微隔离技术在初次实施部署时，由于涉及到一些计算资源和网络资源，需要网络安全部门和系统部门进行细致的协调配合，确定最佳的上线时间和协调相关的资源。

在系统上线之后，虽然微隔离技术大量采用了 SDDC / SDS《软件定义数据中心 / 软件定义安全》，大大提升了生产力，只需要轻点鼠标就能完成相关安全防护工作。但是，最好有明确实施计划和细节。在应用、系统部门进行通告和协调、避免可能带来的业务风险。

同时微隔离产品的设计初衷，并不是让操作者在一个协作团队中成为“上帝”，我们希望可视化的效果能够成为多个部门良好协作的“契约”！

5. 实施。

实施之后，将会回到第一和第二步，一方面检查策略是否实施有效，另外是重新新审视内部情况，制定下一步的行动计划. 我们建议采用一个循序渐进的思路，在云内实现零信任安全模型。

©2021 云安全联盟大中华区-版权所有

图 6 持续监控

25.3 优势特点和应用价值

大多数的数据泄漏事件是突破了边界防护，利用内部防护、管理的漏洞达成。零信任安全模型，提出了一个安全防护的新思路。微隔离技术不仅让云计算中可以实现零信任安全模型，同时也是零信任安全模型提出以来获得的最佳实践，微隔离技术可以实现：

1. 从内到外设计网络，安全融入网络 DNA
2. 更精准的最低授权策略
3. 更清晰的流量、威胁可视化
4. 更高的性能和可扩展性
5. 更高的安全生产力

25.4 经验总结

在本次的案例中 VMware NSX 和山石云·格配合在云中实现零信任安全模型，通过多个 PDCA 循环实现最优化配置的。

初期通过明确核心资产发现，各种业务网络是多个核心数据资产，情况不清晰，且还有细化的空间。

南京市中医院的云数据中心面临的最大挑战是内部不可视，特别是虚机间、应用系统间交互关系不清楚；这些系统间跑哪些应用，使用哪些已知端口或自定义端口不清楚；网络通信中是否有攻击有违规应用，也不清楚。不可视带来的难题是，想实现微隔离，核心资产及其安全域的边界不明晰；不清楚跑哪些应用，调用哪些端口号，无法确定最低授权策略……

整体需要经历多个 PDCA 循环，完成 NSX 和山石云·格的部署，安全域的划

©2021 云安全联盟大中华区-版权所有

分和调整，最低授权策略的部署和调整优化。在多个 PDCA 循环过程中，分两个大的阶段实施：

第一阶段目标是“明确”。利用山石云·格的可视和学习，明确资产、最低授权策略。可以充分利用山石云·格的“透视镜”、“策略助手”等功能。NSX 向山石云•格的引流策略可以较粗，或者选择分区域抽样引流。山石云•格具备云内资产发现功能，配合山石云•格的多维度过滤功能，网络管理员可以区分哪些流量来自云数据中心之外，哪些是内部但未防护的区域。在这一阶段中，既可以勾勒出云内不同业务系统、租户间网络交互的情况，也能及时发现并阻断威胁。

第二阶段目标是优化。逐步将一些经过验证，可以由 NSX 完成 L2-L4 层访问控制策略从山石云·格上转移到 NSX 上实施，山石云·格则集中在一些 L5-L7 层的安全防护上，实现性能、全面防护的有效结合。

26、九州云腾科技有限公司某知名在线教育企业远程办公零信任解决方案

26.1 方案背景

2020 年，突发疫情，企业纷纷开启远程办公模式。

对在线教育企业来说，则面临着更加严峻的挑战。大量学生，“停课不停学”，更加频繁的通过在线教育平台进行学习，企业的业务比非疫情期间还要繁忙。

某知名在线教育企业，数万员工集体远程办公，超过二十万台设备接入企业内网，企业面临着诸多的安全挑战：

1. 大量员工远程办公，缺少有效的安全管控体系，存在数据泄漏风险；

2. 有 20 多个应用，包括本地部署应用和 SaaS 应用。员工远程办公，通过公网在多个系统间切换，重复登录验证体验差。弱口令、重复口令，存在着巨大的安全隐患；

3. 大量使用 iPad 移动终端授课，现有的 IT 方案，无法自动识别并进行有效管理；

©2021 云安全联盟大中华区-版权所有

4. 员工数量众多，安全力量有限，员工入职、调岗、离职权限管理压力巨大，稍有不慎，则会带来巨大的安全隐患；

5. 如何在最短的时间内，以最小的改动，满足疫情下的远程办公需求，兼顾安全与效率，是该企业必须全盘考虑的问题。

九州云腾远程办公零信任解决方案，以身份认证为基石，通过细粒度的动态的身份验证及授权，确保仅有授权的用户可以访问授权的业务。丰富的应用模块，可快速对接各类企业应用，实现系统的快速上线，满足企业需求。

另一方面，九州云腾丰富的超大规模客户经验，可轻松应对各类场景下的大规模访问及认证请求。良好的扩展性，为企业零信任战略的推进，提供坚实的身份基础。

26.2 方案概述和应用场景

九州云腾远程办公零信任解决方案，以可信、动态为核心，经过可信认证体系的 IP、设备、应用，在进入办公网络进行权限获取和数据调用时，凭借可信认证获取权限，实现动态安全检测防护。

图 1 零信任远程办公方案

1. 远程终端安全管理

提供终端的可信认证以及身份管理，通过认证才能访问内部系统。同时采集分析终端安全数据，实时而非静态的判断入网设备的安全性。客户网络直播课程中，为保证网络传输速度，提出了需要通过有线网络连接大规模大批量使用 iPad

©2021 云安全联盟大中华区-版权所有

的终端资产管理和网络安全需求，解决方案通过控制入网组网，实现了对移动设备转接头入网情况的突破性识别，同时监控设备状态，针对设备可能出现的异常状态做好动态分级的权限管理，结合终端安全检测与杀毒，实现全生态的移动设备管理。

2. 云端动态决策管控

多因素强认证，采用包括人脸识别、指纹识别、人声识别、动态二维码、手机短信、令牌等交叉安全认证方式来提升整个身份认证的强度。并以智能模型分析可信验证结果，综合判断访问身份的可信等级，实现用户权限的动态分配。例如：若某位员工偏离了日常登录地址，突然有一天显示海外登录，那么系统就会给出不同的身份认证，匹配不同的访问权限。

3. 统一可信网络

通过 IDaaS 产品打通了不同应用系统间的账户认证和授权体系，通过智能管理中心和多种安全管控节点，实现集中权限管理以及全面审计能力，使企业的所有应用系统可信接入办公网络，帮助企业提升安全性与便利性。

4. 动态最小授权

对进入系统的任何人和动作进行持续的安全监控和审计，无需配置内网准入和 VPN，使用公网即可接入办公网络，避免了繁琐配置和技术本身限制带来的网络延迟。

九州云腾远程办公零信任解决方案，通过 IDaaS 打通所有的员工和应用，并通过安装在设备上的客户端，实现终端的安全检查，通过可信身份、可信设备、可信网络、可信应用、可信链路，构建零信任可信远程办公体系，让员工随时随地安全接入内部业务，在安全和效率之间达到最佳的平衡。

26.3 优势特点和应用价值

九州云腾远程办公零信任解决方案，在不改变客户原有网络架构的基础上，快速实现大规模的远程办公部署：

1.自动覆盖所有员工，联动管理

基于 IDaaS 平台的集中式身份管理服务，为客户建立统一身份管理中心，基于设备和人的绑定关系，批量覆盖所有员工的联动管理，确保员工所有访问行为

©2021 云安全联盟大中华区-版权所有

的可视、可管、可审。

2.跨应用免验证高速切换提升体验

IDaaS 平台内预置了多种模板应用，同时平台自带开发者服务功能模块，可快速与企业的各类应用对接，实现对各种业务的统一免密验证登录，员工在应用之间无缝切换。并结合上网行为管理和终端数据防泄漏能力，确保落地数据安全。

3.持续监控确保全链路可信

分段、隔离和控制网络的能力，仍然是零信任网络安全的关键点，九州云腾远程办公零信任策略组合利用了多种现有技术和方法，以持续的访问控制、安全监控和审计，帮助客户实现远程访问过程中网络链路的可信。

4.分布式微服务设计，高性能，易扩展

分布式微服务设计，支持快速水平扩展，在系统访问量波峰波谷时段，都能保持一致的性能，满足各类突发场景下的需求。

26.4 经验总结

突发疫情，需要在极短的时间内，快速完成对接，实现数万员工的无感接入，因此采用了最小集合的解决方案，通过可信终端+可信身份实现安全远程办公。

而这也刚好符合了企业推进零信任战略的逻辑，零信任不是部署一个统一身份认证，或一套 SDP，而是一套全新的安全理念和架构，需要基于企业的特点，进行持续的升级改造，循序渐进的构建与业务需求匹配的安全又高效的信息安全体系。

©2021 云安全联盟大中华区-版权所有

四、关于 CSA 大中华区

云安全联盟 CSA 于 2009 年正式成立，是全球中立权威的非营利产业组织，旨在为推广云计算和新兴数字技术提供安全保障的最佳实践，并致力于国际云计算安全和下一代数字技术安全前沿研究和全面发展，研究领域包括云安全、数据安全、零信任、区块链安全、物联网安全、人工智能安全、个人信息保护与隐私安全、云应用安全、5G 安全、工业互联网安全、量子安全等。CSA 目前在全球设立四大区，包括美洲区、欧非区、亚太区和大中华区，全球会员共有 600 多家及 6000 多名国际高级专家。

云安全联盟大中华区（Cloud Security Alliance Greater China Region，“CSA GCR”）于 2016 年在香港注册成立，并在中国上海注册上海代表处，聚焦信息技术领域的基础标准和安全标准研究及产业最佳实践，牵引与推动国家及国际标准的接轨，打造国际标准、技术联接器与沟通桥梁，开展业务的地域范围覆盖中国（含港澳台）、俄罗斯、蒙古国、哈沙克斯坦、吉尔吉斯坦、乌兹别克斯坦等欧亚国家。

CSA GCR 在中国的成员单位包括中国信通院、华为、中兴、腾讯、浪潮、OPPO、顺丰科技、深信服、360 集团、奇安信、绿盟科技、启明星辰、安恒信息、天融信、工商银行、国家电网、数字认证、金山云、金蝶、海尔集团、中国银联、中国科学院云计算中心、北京大学等 160 多家机构，个人会员近 2 万人，已成为构建中国数字安全生态的重要力量。

©2021 云安全联盟大中华区-版权所有

CSA GCR cloud security alliance ®
GREATER CHINA REGION

零信任落地案例集

CSA大中华区公众号

下载案例集电子版

官网：http://c-csa.cn

微信号：csagcr

邮箱：info@c-csa.cn

电话：18024312752