CSA GCR cloud security GREATER CHINA REGION alliance ®

ZERO TRUST International Summit

企业安全数字化与零信任

演讲人：周智坚　　单位名称：深信服科技

2022 INTERNATIONAL ZERO TRUST SUMMIT 第三届国际零信任峰会暨首届西塞论坛

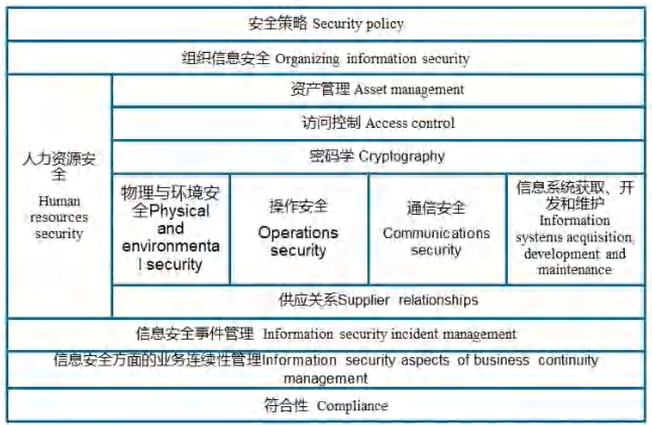
2022 INTERNATIONAL ZERO TRUST SUMMIT
第三届国际零信任峰会
暨首届西塞论坛

目录

CONTENTS

安全1.0

流程+人+少量技术-重点是保密



安全1.5

技术+流程+人，处理攻击、泄密、违规和丢失安全风险-重点是合规+实战

安全2.0

安全能力数字化，实现大部分安全事前防护，风险可视可控可评价，让安全团队做更有意义的事情-合规+真正的能力

目前企业安全面临的问题：

- **外部环境上：** 企业数字化转型，员工围绕系统工作，原有的安全体系无法融入业务，无法看清和收敛风险---高危风险分布在哪些产品上、敏感数据在哪里/哪些人有权限、哪些员工对安全底线有认知能规避...，安全团队与业务团队无休止掐架
- **安全能力上：** 该买的都买了，依然有很多安全问题，系统暴露面大、老旧系统无法整改、影子资产无法及时发现、碎片化的安全产品无法联动、实战成为企业一场场运动
- **人员流动上：** 安全人员流动大，能力无法沉淀，招人成本高
- **价值认可上：** 经常救火、时常背锅、不被认可、安全投资负循环

02. 企业安全能力数字化的方案：自研 or 商业产品，与零信任的关系？

ZERO TRUST International Summit

自研1+1+N安全数字化后，企业CSO的工作状态：

- ✓公司整体是否安全，看安全成熟度指数
- ✓公司实时风险，看风险地图、预警中心
- ✓各资产/产品线、每个员工的安全状况，看安全报表
- ✓安全团队的效能和任务，看效能报表
- ✓各个安全业务过程，看安全ERP各模块

一句话安全	一个安全ERP	安全业务分类
安全的员工-使用安全的设备-经过动态鉴权-精细化授权-访问安全的系统	资产中心，风险管理，稽查中心，数据安全，预警中心，报表中心，员工中心，评价中心	安全合规、员工安全、基础安全、应用安全、数据安全、访问控制、攻防及应急响应

商业产品构建企业安全数字化能力-平台+组件+服务：

数据安全	开发安全	合规及员工安全	安全服务	SRC	BAS
零信任平台		SOAR	XDR平台		

零信任与安全数字化的关系：企业安全数字化底座

✓零信任通过各种身份认证、动态权限、持续评估和日志审计等隔离控制技术，构建企业大部分安全风险的事前防护能力，**为企业其他安全能力构建赢取时间和空间**

✓零信任平台应该具备用户行为及权限的告警分析、行为轨迹、安全报表，风险地图等数字化工具，让企业看清风险在哪里、有什么危害，**为企业提供安全风险管理的决策数据**

02. 企业安全能力数字化的方案，自研：1+1+N安全数字化能力框架

ZERO TRUST International Summit

安全数字化后，企业CSO的工作状态：

✓公司整体是否安全，看评价中心安全成熟度指数

✓公司实时风险，看风险地图、预警中心

✓各资产/产品线、每个员工的安全状况，看安全报表

✓安全团队的效能和任务，看效能报表

✓各个安全业务过程，看安全ERP各模块

自建的步骤：梳理安全业务流程、安全业务信息化、数字化、自动化/AI

自建的代价：完整的产品研发团队+2~3年的时间+志同道合的安全团队

安全业务分类：

- 安全合规
- 员工安全
- 基础安全
- 应用及业务安全
- 数据安全
- 访问控制
- 攻防及应急响应

一句话安全：
安全的员工-使用安全的设备-经过动态鉴权-精细化授权-访问安全的系统

一个安全ERP：
资产中心，风险管理，稽查中心，数据安全，预警中心，报表中心，员工中心，评价中心

人员安全	终端安全	网络/物理安全	服务器/特权安全	应用及开发安全	结构化数据安全	业务安全
安全组织	杀毒	IPS	HIDS	APP加固	数据库加密	不良信息检测与过滤
安全红线	EDR	DDOS	容器安全	代码加固	数据库脱敏	舆情监控
安全培训	终端行为审计	FW	微隔离	灰盒测试	数据库审计	反作弊（如：用工具秒杀）
安全考试	文件泄密审计	NTA	漏扫	黑盒测试	数据库网关	反欺诈（如：用工具秒杀
安全模拟	透明加解密	上网行为管理	蜜罐	安全评审	数据库备份	反爬虫
调查取证	虚拟桌面/应用	无线安全	堡垒机	安全api（XSS、加解密、注入）	大数据安全	
	BRI	VPN	特权平台	动态安全测试	数据蜜罐	
	沙箱	网络准入		WAF	数据库水印	
	文件备份	风火水电雷、门禁、CCTV		邮件安全网关	API安全	
	远程擦除	机房容灾			个人隐私保护	

02. 企业安全能力数字化的方案，商业产品：平台+组件+服务，构建安全数字化能力

ZERO TRUST International Summit

安全业务分类：

- 安全合规
- 员工安全
- 基础安全
- 应用及业务安全
- 数据安全
- 访问控制
- 攻防及应急响应

零信任平台		SOAR		XDR平台		
数据安全	开发安全	合规及员工安全		SRC	BAS	

人员安全	终端安全	网络/物理安全	服务器/特权安全	应用及开发安全	结构化数据安全	业务安全
安全组织	杀毒	IPS	HIDS	APP加固	数据库加密	不良信息检测与过滤
安全红线	EDR	DDOS	容器安全	代码加固	数据库脱敏	舆情监控
安全培训	终端行为审计	FW	微隔离	灰盒测试	数据库审计	反作弊（如：用工具秒杀）
安全考试	文件泄密审计	NTA	漏扫	黑盒测试	数据库网关	反欺诈（如：用工具秒杀
安全模拟	透明加解密	上网行为管理	蜜罐	安全评审	数据库备份	反爬虫
调查取证	虚拟桌面/应用	无线安全	堡垒机	安全api（XSS、加解密、注入）	大数据安全	
	BRI	VPN	特权平台	动态安全测试	数据蜜罐	
	沙箱	网络准入		WAF	数据库水印	
	文件备份	风火水电雷、门禁、CCTV		邮件安全网关	API安全	
	远程擦除	机房容灾			个人隐私保护	

安全服务

- **零信任平台的作用：**
  身份及资产管理、认证和权限、隔离控制、信任评估、增强认证、策略管理、访问行为分析及可视、风险分析及可视、动态策略推荐、风险处置联动

- **零信任适用场景：**
  办公场景、数据中心微隔离、物联网安全、应用安全、数据安全、特权访问...

- **零信任可能的部署路径：**
  办公零信任（远程、内网）、数据中心微隔离、应用安全、数据安全访问控制、物联网零信任...

- 零信任通过各种身份认证、动态权限、策略管理、持续评估和日志审计等隔离控制技术，快速拉高了安全短板，构建企业大部分安全风险的事前防护能力，**为企业其他安全能力构建赢取时间和空间**

- 零信任平台应该具备用户行为及权限的告警分析、行为轨迹、安全报表，风险地图等数字化工具，让企业看清风险在哪里、有什么危害，**为企业提供安全风险管理的决策数据**

03. 全网落地零信任方案的难点及解决办法

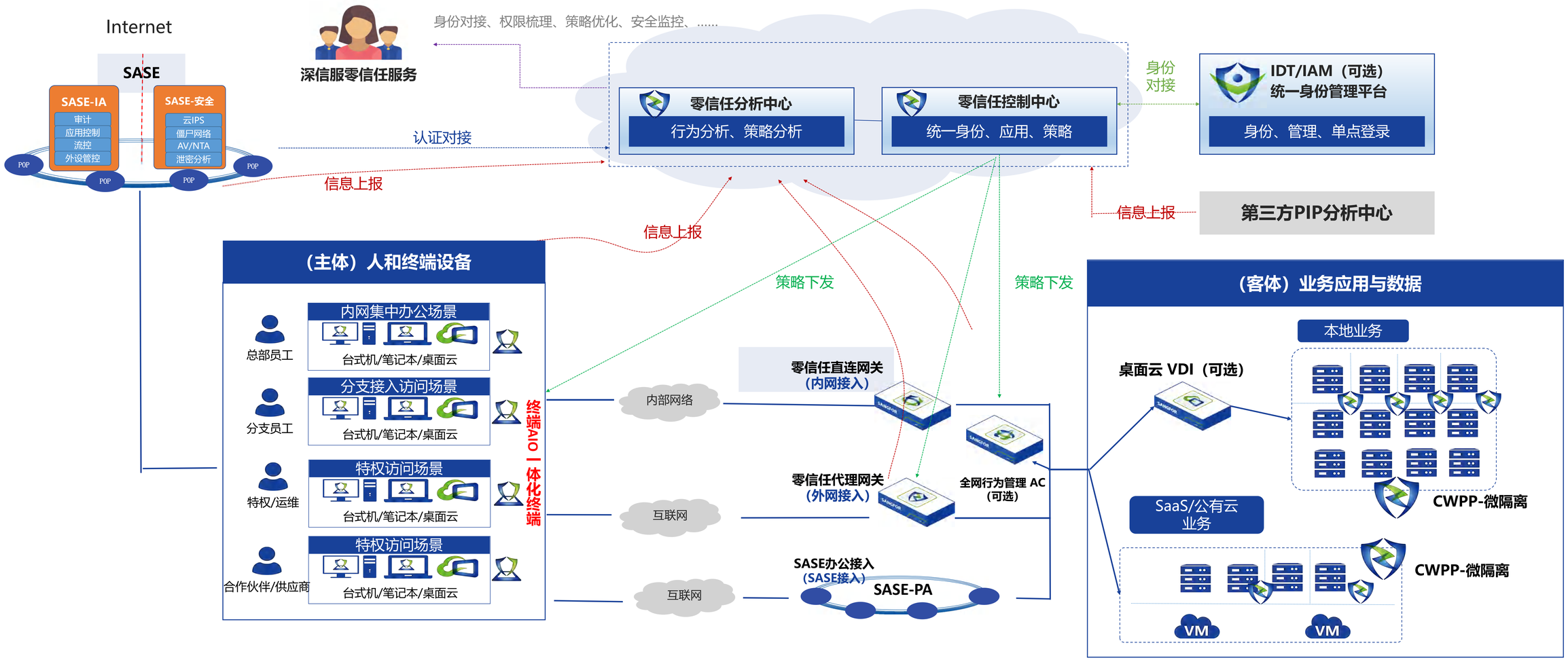
具备规模的企业大部分会保留企业办公内网，落地零信任方案需要考虑为员工提供无边界的办公体验：远程、职场办公无摩擦切换。远程办公落地零信任市场上有很成熟的方案，但是办公内网如何落地零信任，会有哪些坑?

- 需修改已有复杂的ACL策略，**网络改造程度显著提高**
- 加密流量会造成内网原有的监测策略失效，影响**安全追溯**
- 代理和加密情况下，部分应用会有**网络抖动和延时**，对业务原有的通信逻辑有影响，网络兼容性差
- 零信任网关发生故障，无**bypass机制实现逃生**
- 无法同时支持**有端和无端**，用户体验不好
- 加密和代理需要更强的性能，**成本更高**
- 其他未知问题

以下多种网关技术的组合能比较好地解决全网零信任方案落地的难点

场景	使用组件	主要解决问题
远程办公	ZTA+SDP	远程接入办公，基于身份的权限管控
内网办公	ZTA+DGW	内网办公，暴露面隐藏，基于身份的权限管控
混合办公	ZTA+SDP+DGW	远程办公和内网办公一致体验、自动切换
上网+远程办公	ZTA+SASE-IA+SASE-PA	上网统一管控，弹性扩容，远程接入办公
上网+远程办公	ZTA+SASE-IA+SDP	上网统一管控，远程接入办公，数据不上云
上网+远程办公+内网办公	ZTA+SASE-IA+SDP+DGW	上网统一管控，远程接入办公，数据不上云，内外网统一权限管控

04. 深信服如何解决这些问题--全网一个端、一个控制器、一个分析面，多种网关



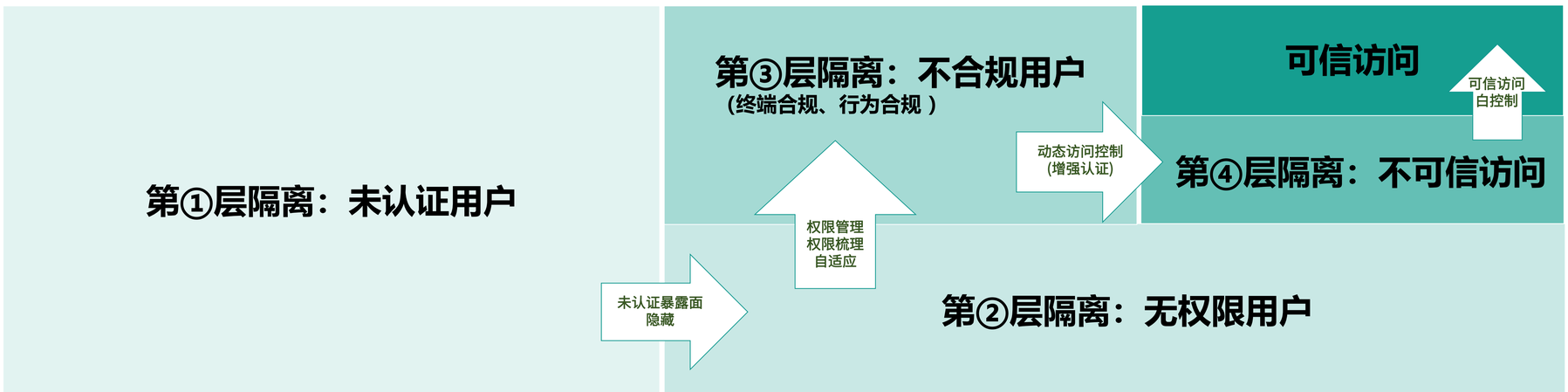
04. 深信服如何解决这些问题-零信任隔离控制的能力图谱

ZERO TRUST International Summit

持续运营

异常行为告警	实时风险地图	数字化报表	用户行为轨迹
•内置风险模版助风险发现 •多维度聚合自定义告警能力匹配不同运营场景需求 •准确化动态权限管控	•组织风险直观展示 •责任主体明确落实 •联合整改有效驱动	•应用/用户视角权限可视 •量化指标辅助持续收敛 •安全建设成果直观反馈	•人机对应行为日志展示 •场景化调查取证能能力 •运营研判基础依据

隔离控制



05. 深信服自身零信任落地分享-零信任部署上线的3个阶段

阶段一：重点保护

优先考虑集团远程办公场景安全接入，收敛业务对外暴露面，构建端到端的零信任隔离控制系统

- 高风险办公场景优先，构建统一访问控制，收缩对外业务的暴露面，避免恶意探测与攻击
- 构建身份、终端、应用、连接、访问、数据端到端访问信任链条
- 通过零信任服务保障安全持续有效

阶段二：场景扩展

通过零信任保护更多业务，逐步扩展到办公内网场景，实现内外网混合零信任

- 将更多业务纳入零信任保护范畴之内，解决用户→业务之间的安全接入问题
- 对业务划分不同密级，通过零信任、VDI、安全沙箱等安全能力构建分级安全访问体系，并提供不同的数据保护能力
- 逐步探索东西向微隔离和身份治理体系IAM建设

阶段三：持续演进

持续优化身份管理体系
建设微隔离、数据安全体系

- 持续优化内部身份管理体系，在保障安全的同时，提升用户接入访问体验，并不断细化权限管理
- 构建微隔离安全体系，梳理内部业务互访关系，实现东西向流量可视化，进一步增强安全能力，实现自适应安全、应对未知威胁
- 实现数据分级分类，基于结构化数据和非结构化数据梳理数据权限，通过技术+管理手段落实数据安全管控手段

从办公场景到全场景零信任逐步落地

《深信服零信任的0号样板点》

项目背景

伴随着业务的快速增长和数字化转型，深信服过去的安全建设也难以满足日益增长的安全需求。接入终端难管控、访问权限难管控、违规行为难管控等一系列问题开始暴露，经过详细的方案论证和业务设计，深信服最终决定开始在内部开展零信任落地实践。

方案效果

实现内外网全面零信任，项目完成后**零信任接入终端数高达40000个，并发在线终端数25000，发布应用2000+，**

安全收益：极大的收缩了业务暴露面，通过零信任构建的动态访问策略，将业务根据不同敏感度分类，结合终端安全产品、桌面云等**实现针对不同敏感度应用的不同安全控制，**并通过扫码、动态口令业务准入时的增强认证等方式减少身份仿冒、钓鱼威胁。

运维收益：仅边界ACL运维一项工作，**就节省5倍以上的人力投入。**过去内网权限管控完全依赖各网络区域边界的ACL来实现，仅策略管理维护都要投入5-6人，全面零信任后，所有策略集中在零信任平台完成，基于用户身份的可视化权限，**日常运维1个人绰绰有余，**不仅释放了运维压力，也避免了过去因为ACL权限不可视导致的权限管理复杂、权限孵化等问题。

业务收益：工作效率大幅提高，包括流程、程序响应速度等，连接内网的时间从**平均10s缩短至平均5s，效率提高了1倍；当前日均并发终端20000+，**保障了业务的不间断运行；

CSA GCR cloud security GREATER CHINA REGION alliance ®

ZERO TRUST International Summit

致力于让所有用户 安全，领先一步

落地有声

第二届零信任用户分享大会

11月4日 14:10-17:30 杭州

扫码报名

2022 INTERNATIONAL ZERO TRUST SUMMIT
第三届国际零信任峰会
暨首届西塞论坛

CSA GCR cloud security GREATER CHINA REGION alliance ®

ZERO TRUST International Summit

THANK YOU !

2022 INTERNATIONAL ZERO TRUST SUMMIT
第三届国际零信任峰会
暨首届西塞论坛