CSA GCR 6th Congress 第六届云安全联盟大中华区大会

CSA GCR cloud security GREATER CHINA REGION alliance®

从局部到全局，深信服内部全面零信任实践

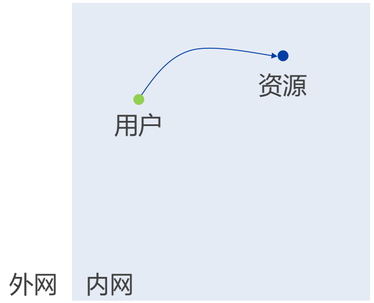
演讲人：杨志刚 深信服科技

CSA GCR 6th Congress 第六届云安全联盟大中华区大会

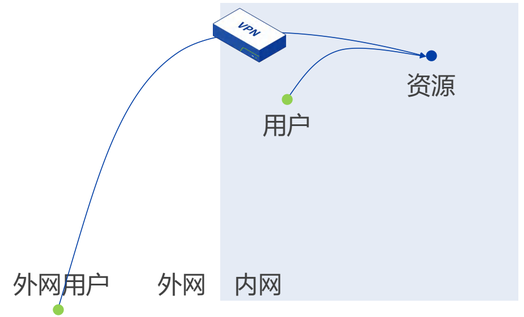
目　录

CONTENTS

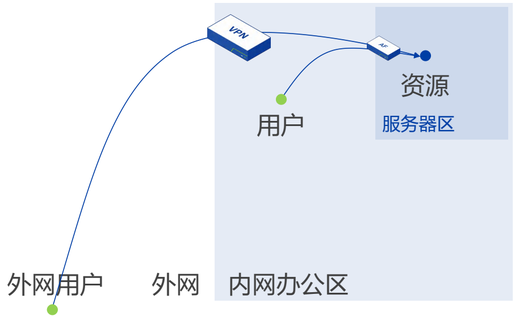
建设背景—业务发展中的分区分域建设



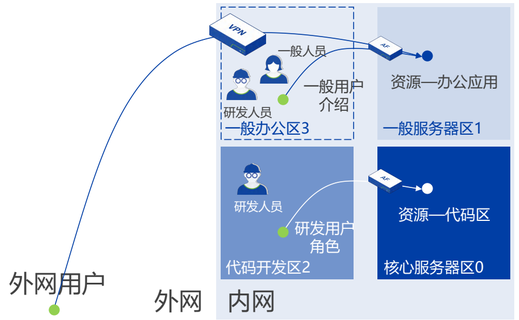
用户访问资源



用户在内外网访问资源



内网分成办公区和服务器区

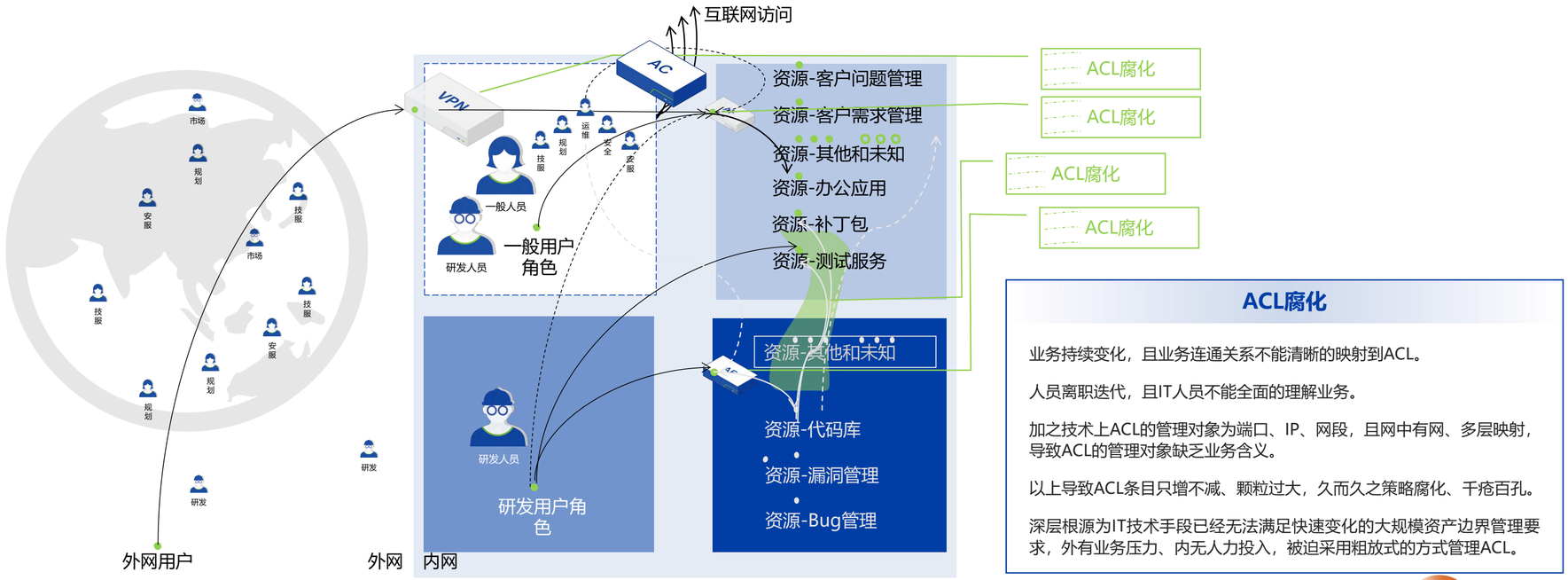


进一步分成不同安全级别的区域
人员按职责分别访问不同区域

建设背景

理想的分区分域面临的挑战

- 用户活动范围广泛
- 人员众多职责切换
- 入职离职太多权限
- ACL腐化混乱



ACL腐化

业务持续变化，且业务连通关系不能清晰的映射到ACL。

人员离职迭代，且IT人员不能全面的理解业务。

加之技术上ACL的管理对象为端口、IP、网段，且网中有网、多层映射，导致ACL的管理对象缺乏业务含义。

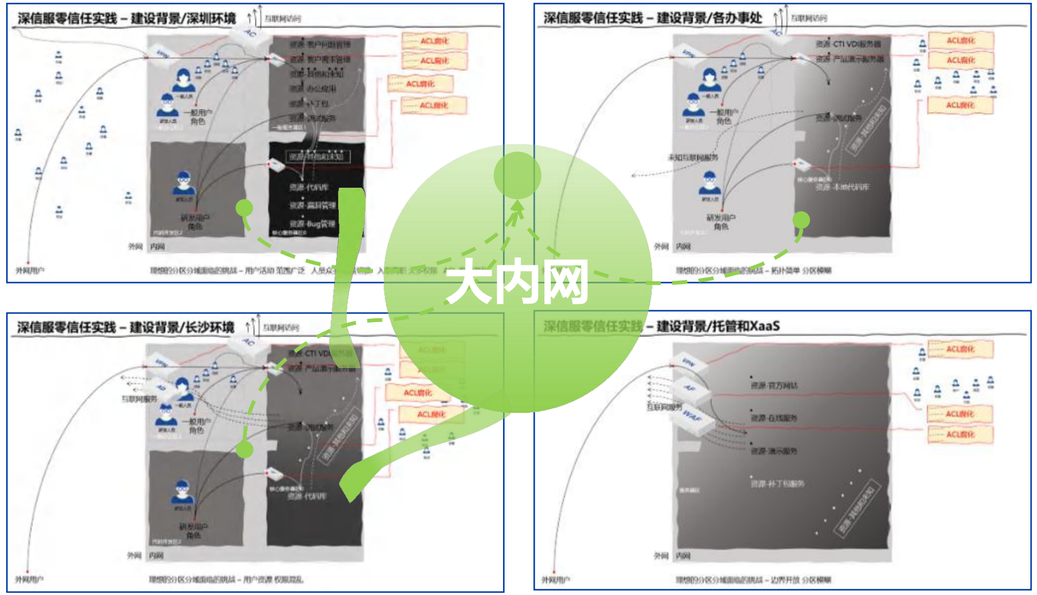
以上导致ACL条目只增不减、颗粒过大，久而久之策略腐化、千疮百孔。

深层根源为IT技术手段已经无法满足快速变化的大规模资产边界管理要求，外有业务压力、内无人力投入，被迫采用粗放式的方式管理ACL。

建设背景

信息化建设和数字化转型

让边界变得更模糊、权限更混乱



安全痛点和根源

安全管理

业务过程是连续的，用户在持续变化且行为多样、资源在持续变化且漏洞难免，同时用户和资源之间，资源和资源之间的的访问关系都在持续变化，而区域边界是离散的、相对静态的。

在少数固定的隔离边界上，以粗颗粒度的、相对静态的安全策略，识别多种多样的用户行为、防护层出不穷的技术漏洞、维护快速变化的访问关系，必然会遇到问题规模和资源投入的矛盾，问题规模大而资源投入小，安全运营往往虚化，痛点很难缓解。数字化转型加剧了这种矛盾。

零信任尝试以多种方式解决这些问题：以SDP灵活的动态边界替代少数固定的边界，并统一维护资源清单、同时大量屏蔽系统漏洞；以增强的IAM统一维护用户身份、持续检测用户环境、持续评估用户行为；

由于统一了资源清单和用户身份，安全策略对象的种类得到简并，有可能减少问题规模、并细化安全策略。

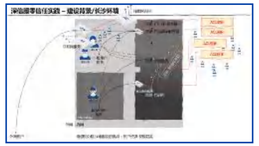
以微隔离控制资源之间的东西向访问，增强流量可见性、并持续回收过期资源访问关系，缓解横向攻击风险。

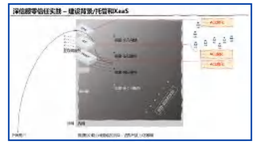
人员管理

岗位管理

终端管理

账号管理





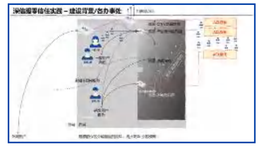
数据管理

应用管理

服务器管理

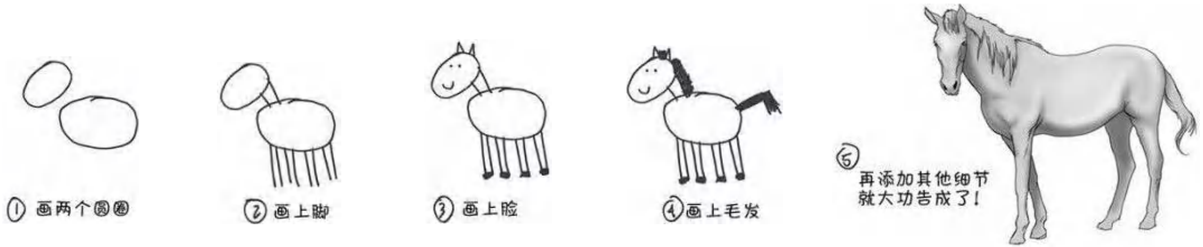
网络管理

机房管理



信息化和自动化支持

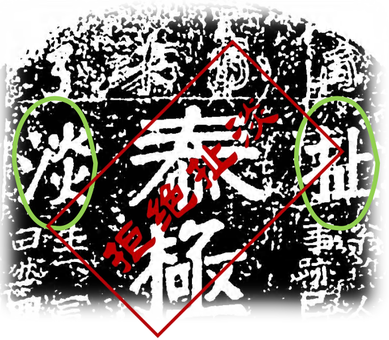
落地实践



5步落地零信任，手把手

- 第一步　深刻学习零信任方法论
- 第二步　认真研究零信任白皮书
- 第三步　积极开展零信任讨论会
- 第四步　敢于设置零信任DEADLINE
- 第五步　就很简单了，落地。

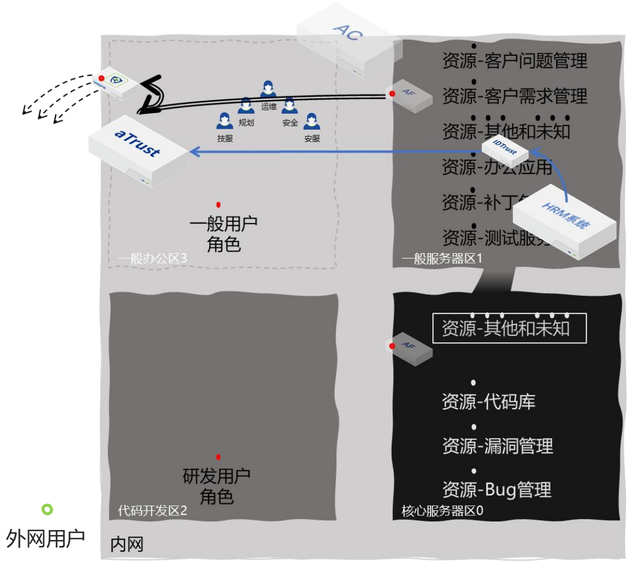
这一步很简单，就交给你来完成了



落地实践—0 平滑切入 减少依赖

在分区分域之上部署零信任 最小化实施：

- 部署组件
- 对接身份
- 发布资源



建设

1. 部署零信任最小组件集 控制中心/代理网关/身份中心
2. 通过LDAP等协议，接入企业人员管理系统
3. 发布了一个资源 “OA报销系统”
4. 用户可在办公内网和互联网，无感知访问 “OA报销系统

运营 （便利性提升/安全性增强）

1. 通过OATH2协议，对接OA报销系统和零信任系统
2. 在零信任系统上配置通配符证书， OA报销系统使用HTTPS
3. 启用零信任安全策略，安装aTrust客户端后才能访问 OA报销系统

在分区分域之上部署零信任 – 建设和运营目标

落地实践—0 平滑切入 减少依赖

√ 本阶段安全效果和痛点缓解

通过最小化的零信任项目实施，我们已经达到以下安全效果

- 大部分人机得到匹配
- 访问报销系统的人员行为可全面留痕、检索
- 人员离职时自动关闭报销系统权限
- 定义了访问报销系统的唯一路径和系统边界
- 避免了报销系统直接暴露给用户，缓解了漏洞风险

- 人机不能匹配
- 行为难以审计
- 权限回收过慢
- 边界难以管理
- 数据分布广泛
- 应用漏洞频出
- 资产信息混乱
- 东西隔离困难
- 黑客手段隐蔽

落地实践—1 横向扩展 确保可用

在分区分域之上部署零信任 横向扩展：

- 双机部署 横向扩展
- 发布更多业务系统

在内部发布的部分应用（脱敏）

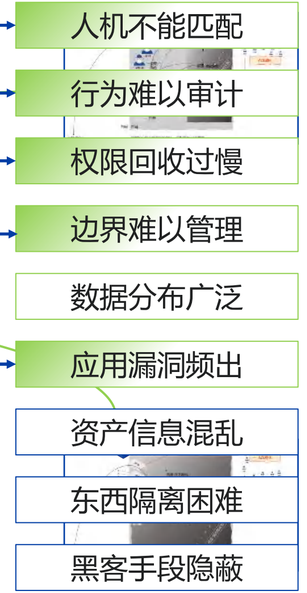
- 知识库系统
- 补丁管理系统
- 质量和满意度运营系统
- OKR系统
- 销售管理系统
- 订单管理系统
- ...

落地实践—1 横向扩展 确保可用

√ 本阶段安全效果和痛点缓解

通过零信任项目的横向扩展，我们已经达到以下安全效果

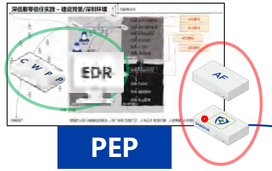
- 绝大部分人机得到匹配
- 访问多数系统的人员行为可全面留痕、检索
- 人员离职时自动关闭多数系统权限
- 定义了访问多数系统的唯一路径和系统边界
- 避免了大部分应用系统直接暴露给用户，缓解了漏洞风险
- 实现了大部分应用系统的双因素认证



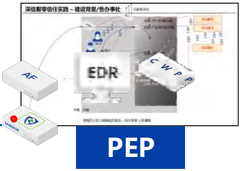
落地实践—2 纵向增强 联动能力

在分区分域之上部署零信任 纵向增强：

- 联动终端EDR、AF，实现多点联动封锁和信息收集
- 联动SIP/NGSOC，实现多源日志分析
- 联动MSS，补充专家能力和情报信息，联动处置



PEP



PEP

建设

- 以零信任组件为挂载点，对接用户终端、网络边界、服务器端点上的安全能力，视其为扩展的PEP/PIP，实现多点的联动封锁和信息收集
- 以零信任组件为挂载点，对接SIP/FutureX运营中心，复用流量信息和多源日志，增大分析深度。视aTrust/SIP/FutureX为更广义的PDP
- 对接云端的MSS/云脑，获取专家能力和情报信息，联动处置事件，视其为PIP和更广义的PDP

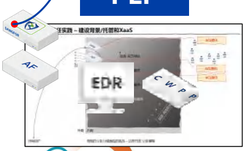
运营

（便利性提升/安全性增强）

0. 启用终端安全策略

PEP

PEP

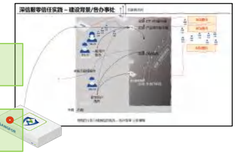


落地实践—2 纵向增强 联动能力

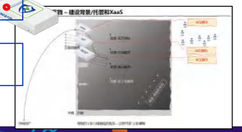
√ 本阶段安全效果和痛点缓解

通过零信任项目的横向扩展，我们已经持续完善以下安全效果

1. 绝大部分人机得到匹配
2. 访问多数系统的人员行为可全面留痕、检索
3. 人员离职时自动关闭多数系统权限
4. 定义了访问多数系统的唯一路径和系统边界
5. 避免了大部分应用系统直接暴露给用户，缓解了漏洞风险
6. 实现了大部分应用系统的双因素认证



- 人机不能匹配
- 行为难以审计
- 权限回收过慢
- 边界难以管理
- 数据分布广泛
- 应用漏洞频出
- 资产信息混乱
- 东西隔离困难
- 黑客手段隐蔽



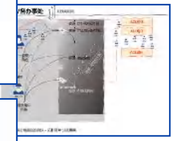
落地实践—3 持续运营 迭代循环

持续运营，从人工处置到SOAR：

- 安全是动态的，主要价值落地在运营阶段
- 运营工作量过大，大部分工作应通过SOAR落地

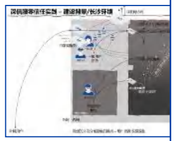
建设

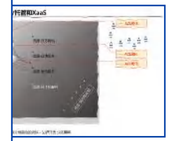
1. 持续按需建设



运营 （便利性提升/安全性增强）

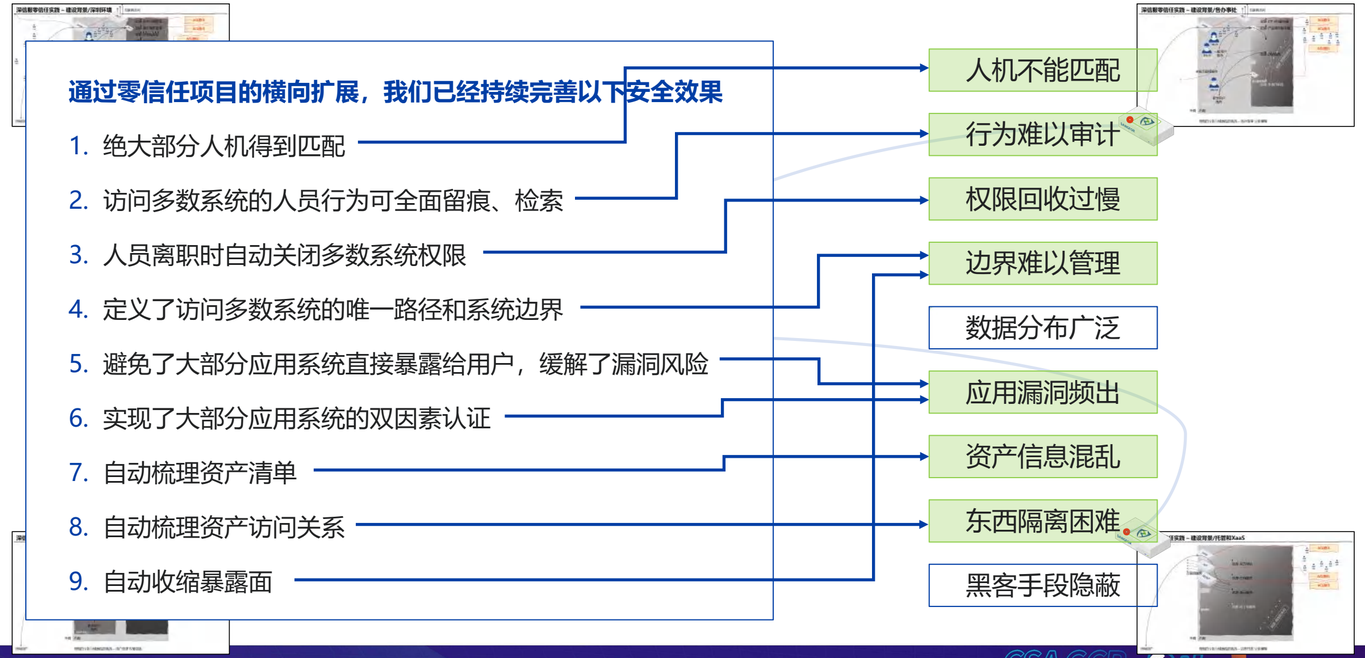
1. 自动梳理资产清单，导入aTrust、AD、SIP、AF流量日志到NGSOC等，自动发现流量中的服务器资产信息
2. (半)自动梳理资产访问关系，导入cwpp流量日志到NGSOC，结合SIP/AF的流量日志信息，自动发现高价值服务器的流量关系
3. 全面生成人员行为应用访问日志，使用NGSOC存储和分析aTrust业务访问体制，对所有发布的应用，免改造实现业务日志能力
4. 自动收缩暴露面，使用NGSOC中存储的aTrust/AD流量日志，联动AD/AF自动封锁内网服务器到互联网的过期接口。按以下规则: a) aTrust中已发布的内网服务器IP和端口，在AD上自动封锁 b) AD中出现过的IP:Port对，3个月无访问流量则自动封锁。 c) 后续结合资产扫描发现工具，驱动规则b进一步发挥作用





落地实践—3 持续运营 迭代循环

√ 本阶段安全效果和痛点缓解



项目收益

安全收益

- 极大地**收缩了业务暴露面**，对业务进行权限收缩，以白名单进行微隔离，极大地**减少了业务遭受恶意攻击的概率**；
- 针对内外部访问，通过零信任构建的动态访问策略，实现不同敏感度应用的不同安全控制，并通过业务访问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**节省5倍以上的人力**投入，原本需要5-6人才能完成的各区域边界ACL运维工作，当前**仅投入1人即可**集中在零信任平台完成，而且完全是基于用户身份的可视化权限，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、权限腐化**等问题。

业务收益

- 全渠道、全业务的**一致性**的免密办公体验；
- 内网业务接入时间**缩短50%以上**
- 远程接入**效率提升100%**，提高了业务人员的响应速度，客户问题响应**提升30%**；
- 为**3000+**合作伙伴提供了随时随地接入能力。

CSA GCR 6th Congress 第六届云安全联盟大中华区大会

CSA GCR cloud security alliance® GREATER CHINA REGION

THANK YOU.