

行业解决方案

基于零信任的安全远程访问解决方案



北京2022年冬奥会官方赞助商 Official Sponsor of the Olympic Winter Games Beijing 2022



基于零信任的安全远程访问解决方案-远程访问场景的安全需求

远程访问典型场景

互联网远程访问

移动终端访问

开发测试访问

运维访问

办公系统、报账系统、邮件等

众测,远程开发,系统调试,特权运维等

现有场景痛点

非法人员进入

非法终端访问

业务暴露面过大

安全合规难满足

敏感数据泄露

安全能力分散

终端受控需求

风险: 非法终端接入访问, 勒索/后门恶意软件通过访问

扩散传播

需求:阻止/限制不受控终端业务访问,终端安全状态可感知控制,并根据终端安全状态较短的控制,并根据终端安全状态控制其访问

人员可信需求

风险:弱密码、认证手段单一易仿冒,恶意访问难发现

难阻断

需求:验证策略灵活可控, 访问过程持续监控,实时阻 断,最小权限、人员动态访 问控制

业务保护需求

风险: 互联网/外部网络端口 开放遭受扫描渗透, 谁都可 连接探测, 业务沦为跳板横 移扩散, VPN被打穿

需求:收缩业务暴露面、隐藏网络端口,缓解渗透攻击,仅对受控终端/人员开放

数据保护需求

风险: 敏感数据/机密文件终端落地后被非法共享、数据

泄露

需求:敏感数据不落地,或

落地全程安全隔离

安全合规需求

风险:国密隧道、国产化平台迁移代价高、业务兼容性难保证

需求: 国密隧道支持, 国产

化与Windows兼容

安全能力整合需求

风险:端、网、业务应用安全能力分散。无法形成一体化能力

需求: 打通端到端各环节安全能力,构建最小权限、动态权限,形成动态访问控制



基于零信任的安全远程访问解决方案-方案建设思路

北京2022年冬奥会官方赞助商 Official Sponsor of the Olympic Winter Games Beijing 2022

①终端安全

阻止/限制不受控终端业务访问, 终端安全状态可感知控制,并根据 终端安全状态控制其访问。

②人员可信

用户验证策略灵活可控,访问过程持续监控,可实时阻断,最小权限、人员动态访问控制。

③业务保护

收缩业务暴露面、隐藏网络端口 缓解渗透攻击,仅对受控终端/人员 开放。

④数据保护

敏感数据不落地,或落地全程 安全隔离。

⑤合规需求

国密隧道支持,国产化与 Windows兼容。

6安全整合

打通端到端各环节安全能力, 构建最小权限、动态权限,形成安 全联动。 解决方案针对远程访问场景的各项安全需求,按照零信任原则进行安全能力组合设计,形成技术路线。

场景 需求 解决 方案 能力

准入 漏洞补丁 可信设备清单 终端安全 桌面管控 终端环境感知 杀毒 人员身份管理 多因子认证 动态授权引擎 认证授权 自适应认证 访问策略管理 会话管理 端口收缩 应用层隧道 应用代理 端口隐藏 业务隐藏与 保护 API代理 运维代理 单包授权 数据安全策略 沙箱容器 数据隔离 数据加密 安全桌面 应用加固 国密隧道 浏览器安全 国密/信创 支持 信创软硬平台适配 动态授权引擎 信任评估引擎 策略编排引擎 动态访问控制 风险分析模型 信任评估模型 外部平台集成





基于零信任的安全远程访问解决方案-方案整体架构

终端安全能力

终端合规安全

浏览器安全

信创/国密

终端数据隔离

数据加密

应用加固

户

设

环境身份

化

终端基础安全

漏洞补丁

准入

桌面管控

可信设备清单管理

终端可信环境感知

业务隐藏与保护能力

2.所有访问流量收口,安全策略得以强制实施

业务接入安全

端口收缩

网络准入 单包授权 业务访问安全

应用代理 运维代理

API接口代理

传输安全

TLS/国密 4层隧道

应用层隧道

数据平面 控制平面

客体资源身份

3.打通终端各层安全能力, 贯穿业务访问全程

动态访问控制能力

认证管理

多因子认证 会话管理

自适应认证

访问控制

动态授权引擎

访问策略管理

人员/设备/资源身份

安全策略

终端安全策略 数据安全策略

运维安全策略

4. 持续信任评估、动态访问控制闭环达成

信任评估能力

风险策略与编排

策略编排引擎

风险分析模型

持续信任评估

信任评估引擎

信任评估模型

外部服务

基础支撑

身份管理

其它风险管理平台

普通业务应用 邮件 OA 敏感业务应用 CRM订单 GIT库 运维资源 数据库 服务器/VM 数据服务 API接口

传统IDC、云/数据中心



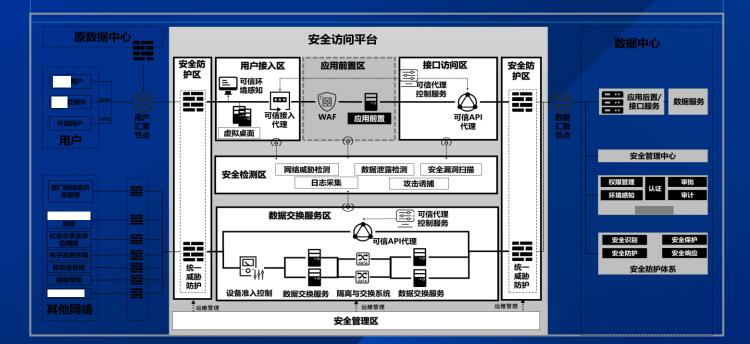
某大型部委数据中心零信任访问场景

项目情况

背景需求:

业务覆盖部、省、市、县等多级行政机构,面临数据共享开放,交叉使用的场景,大数据应用面临的安全 威胁和攻击种类多,攻击行为具有隐蔽性、攻击特征变化快,单纯依赖传统信息安全防护技术来防范大数 据攻击存在一定局限性。

- 接入网的用户汇聚节点和数据汇聚节点之间需保障用户与外部网络的数据交换和对数据中心的安全访问。
- 现有安全措施缺乏对用户身份的持续认证和控制,无法有效应对内部和外部威胁、数据泄露风险。
- 缺乏对外来设备的设备发现、病毒防护、安全基线等安全状态的管控,导致业务网络随意延伸到不可控 区域,直接带来安全风险点。



方案成果

解决方案:

- 基于零信任切分用户汇聚节点和数据汇聚节点
- 持续监测终端设备环境、云桌面应用环境监测
- · 建设应用系统代理、API代理收缩服务器暴露面
- 以终端环境感知、访问行为、威胁检测等综合能力形成动态访问控制

用户价值:

- 业务应用隐藏,确保用户流量不直接进入数据区。
- 人员、终端、业务/数据、安全策略一体化动态访问控制。
- 从应用、接口层面收缩大数据对外暴露面。
- 用户业务流量强制加密,避免用户侧信息泄露。
- 覆盖用户访问、数据交换两类场景。

产品配置:

- 可信应用代理TAP、可信API代理
- · 可信访问控制台TAC、智能身份分析平台
- 终端环境感知TESS、移动端环境感知MTESS



THANKS!

让冬奥更安全 让世界更精彩



