SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

深信服零信任“VPN”方案

“以身份为中心
构建可信访问、智能权限、极简运维的零信任安全架构”

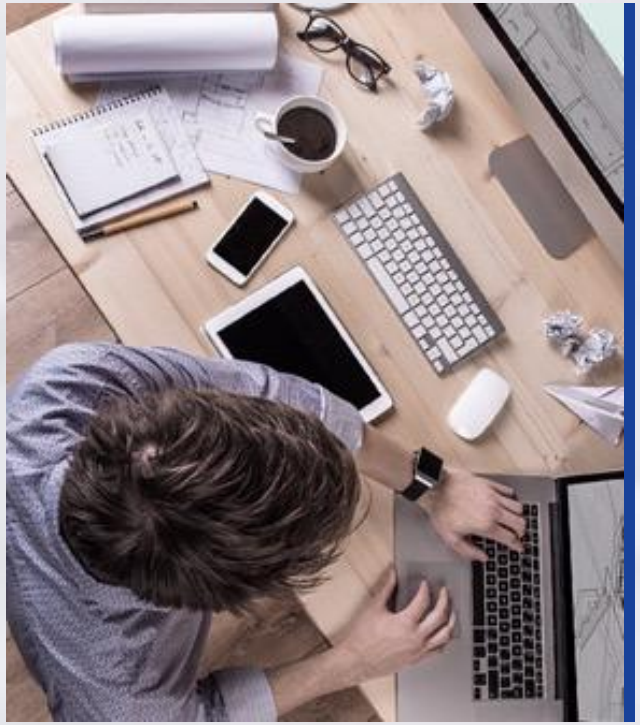
深信服科技

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

目录

规模化远程办公需求升级与新挑战

远程办公规模化、常态化带来新变化



接入角色多样化

从运维人员、部分高管变成各业务人员、各级主管、职能人员、开发人员、第三方供应商等；

使用场景多样化

从远程运维、流程审批变为远程办公、远程开发、远程协同、居家坐席等多样化场景

接入环境复杂化

办公大楼、办事处、居家、出差途中、机场咖啡厅等场所，环境复杂，边界模糊。

接入终端复杂化

业务接入的终端从内网的PC、统采的PC 变成了各类BYOD个人终端，安全隐患大幅增加

然而传统的安全接入方案遇到瓶颈

1、缩小暴露面效果欠佳

3、访问权限固化，访问行为不可控

2、缺少接入终端全周期检测手段

4、使用体验差，运维挑战大

挑战1：缩小暴露面效果欠佳

- 敏感业务、核心业务对外发布，安全风险陡增
- 通过传统SSL方案发布如OA业务，OA业务虽然隐藏，但仍然对公网暴露SSL认证页面，任意终端、任意人员、任意位置都可发起认证请求，仍存在利用SSL认证页面的漏洞扫描、注入攻击等风险

挑战2：缺少接入终端全周期安全检测手段

- ✓ 针对BYOD终端缺少轻量、灵活的安全检测手段；BYOD终端很难推行较重量级的终端安全管控软件
- ✓ 缺少业务访问全周期的检测能力，接入时候安全可信，不代表访问业务过程一直是安全可信的

- ✓ 有没有安装防病毒软件?
- ✓ 有没有打上系统补丁?
- ✓ 有没有危险进程?
- ✓ ……

访问业务全周期中，接入终端和身份一直是安全的吗?

挑战3：访问权限固化，访问行为不可控

1 接入访问权限固化

静态访问权限
认证通过后业务访问权限不会进行调整
默认接入内网等于进入“安全地带”

2 访问行为不可视不可控

接入后访问业务行为不可视不可控
异常行为、可疑行为无法及时发现及处置

挑战4：使用体验差，运维挑战大

员工使用体验要求高

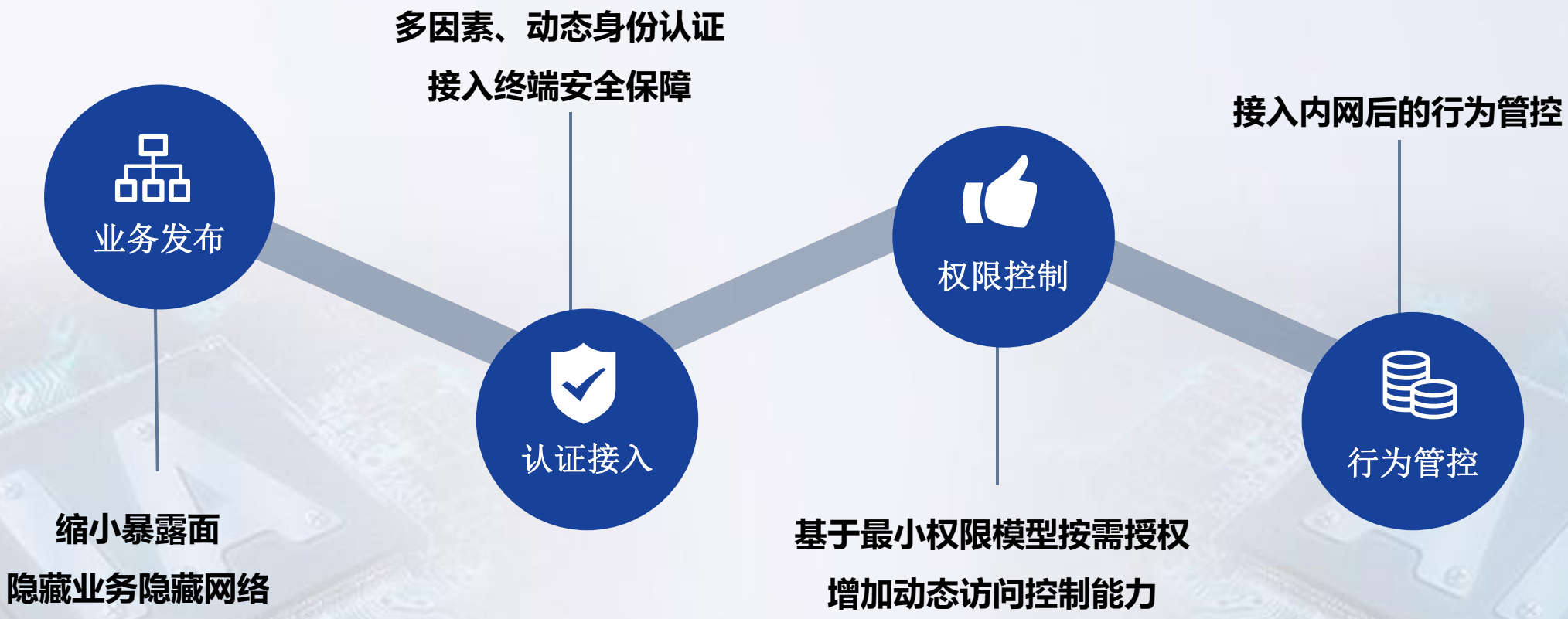
- ✓ 访问业务需要强制安装客户端插件，使用繁琐，常出现兼容性、插件冲突等问题影响使用
- ✓ 访问业务外网通过VPN客户端接入，进入内网需要切换登录方式，使用繁琐

IT运维挑战大

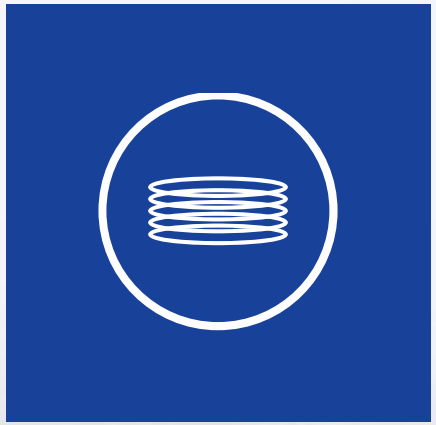
- ✓ 规模化远程办公，终端运维压力大，员工抱怨投诉多，需要给员工更简单、无插件无客户端的接入方式，轻量化运维。
- ✓ 规模远程办公，使用角色复杂，权限申请繁琐、权限管理难，既不能分配过大权限带来业务暴露风险，又不能权限过小影响员工正常业务访问。

如何应对远程办公升级需求的挑战

远程访问业务全流程安全控制点



利用零信任思想和相关技术满足远程办公全流程安全保障



身份可信

- 基于身份建立边界
- 基于条件变化自动调整认证强度

环境可信

- 终端环境持续动态检测
- 终端进程可信识别

行为可信

- 从零开始建立信任，最小权限授予
- 异常访问行为识别和控制

持续评估动态控制

基于环境/行为/身份等进行持续信任评估，动态调整访问权限

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

零信任“VPN”-新一代远程办公安全方案

深信服零信任“VPN”--融合零信任思想及VPN领域多年积累与创新

以身份为中心，构建可信访问、智能权限、极简运维的零信任安全架构

零信任“VPN”--提供远程访问全周期安全保障

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

动态自适应认证与业务准入

动态自适应认证
终端动态环境检测
终端进程可信
业务动态准入

多源信任评估，异常行为管控

集成第三方安全能力，多源信任评估
访问行为安全审计、分析异常行为，
动态处置、灰度处置。

业务发布

认证接入

权限控制

行为管控

网络隐身

SPA机制缩小业务暴露面

动态权限控制

基于身份、环境、行为变化，动态收缩权限
不同敏感度业务采取不同级别访问控制

零信任“VPN”--提供远程访问全周期安全保障

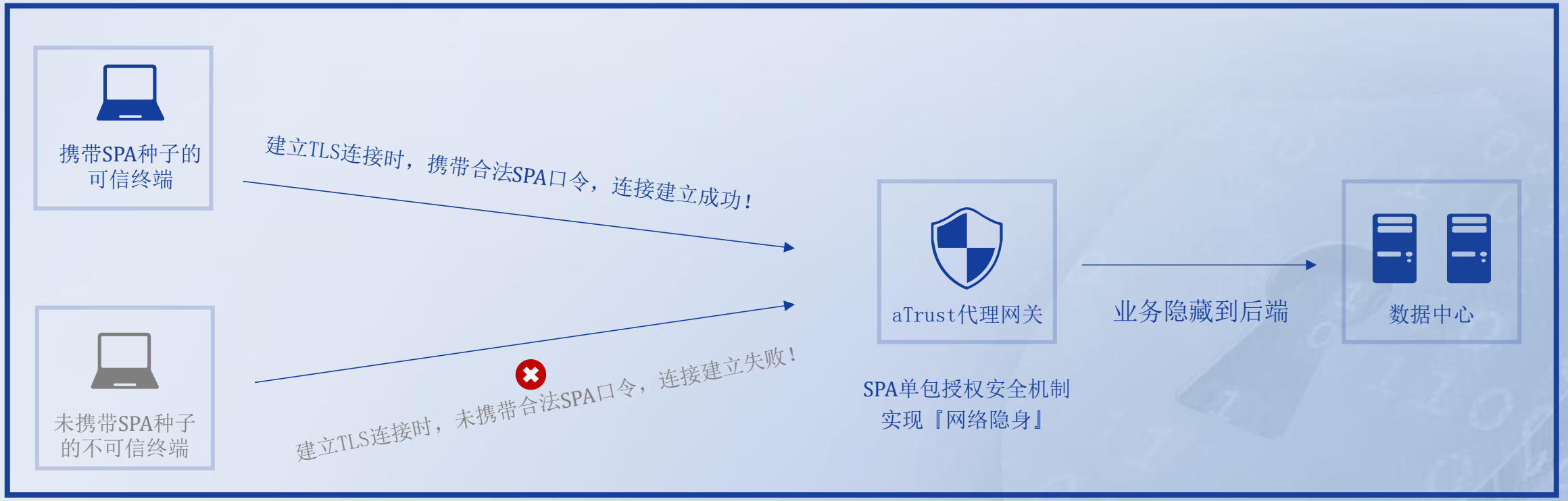
业务发布

网络隐身

缩小业务暴露面

业务发布—网络隐身（SPA机制）最大程度收缩业务暴露面

- ✓ 先受信，再连接、认证：所有终端先进行受信校验才能发起认证请求，通过认证后才能连接业务
- ✓ 非授信客户端登录访问，无法打开登录页面，无法访问任何接口，规避攻击者漏洞扫描、漏洞试探攻击、弱密码爆破
- ✓ 业务完全隐藏到代理网关后端，业务对非法访问/攻击者完全隐身



零信任“VPN”--提供远程访问全周期安全保障

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

动态自适应认证与业务准入

动态自适应认证
终端动态环境检测
终端进程可信
业务动态准入

业务发布

认证接入

网络隐身

缩小业务暴露面

可信访问– 动态自适应认证，平衡安全与体验

安全可信的情况下，简化认证操作，增强访问体验

免二次认证（体验增强）

- 当在**授信终端**登录时，免除二次认证
- 当在**内网环境**下登录时，免除二次认证
- 当在**Windows域环境**登录时，免除二次认证

一键上线（体验增强）

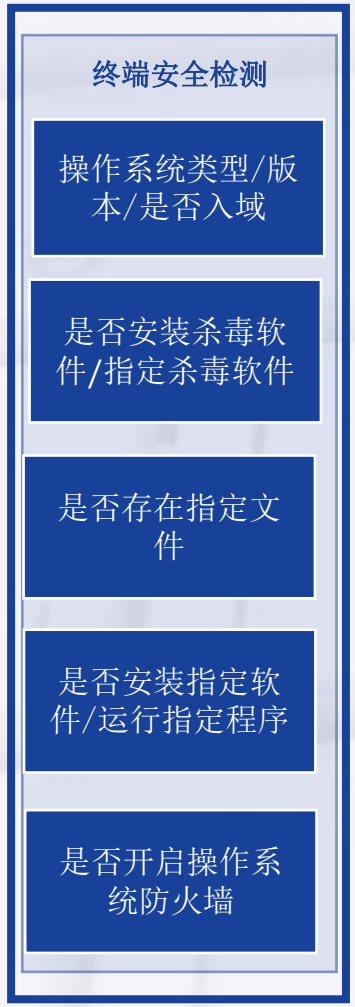
- 当在**授信终端**登录时，客户端可以一键上线
- 当在**内网环境**下登录时，客户端可以一键上线
- 当在**Windows域环境**登录时，客户端可以一键上线

身份、环境异常存在安全隐患时，自动进行增强认证

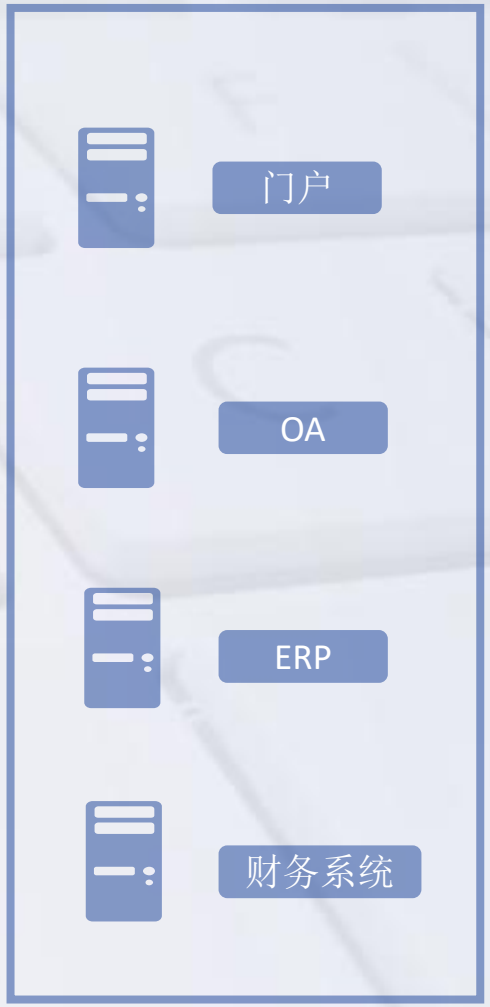
增强认证（安全增强）

- 当用户使用**弱密码登录**时，必需进行增强认证
- 当用户在**异常时间段登录**时，必需进行增强认证
- 当用户在**异地登录**时，必需进行增强认证

可信访问 - 终端环境动态检测与业务准入



- ✓ 要求终端必需打齐**操作系统补丁**才允许访问OA系统；
- ✓ 要求终端必需安装**防病毒软件并更新到最新版本才能访问ERP系统**
- ✓ 要求终端必需**安装运行指定软件**才允许访问财务系统；



- ✓ 从粗粒度准入走向精细化准入
- ✓ 从粗暴网络准入走向业务准入
- ✓ 从仅登录环节检测到全访问周期持续检测

可信访问-- 可信应用策略，保障终端的进程可信

可信应用核心价值

- ✓ **发现、阻止终端不可信进程访问高敏感核心业务**
- ✓ **只允许特定可信白名单进程访问业务，保护高敏感核心业务**

零信任“VPN”--提供远程访问全周期安全保障

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

动态自适应认证与业务准入

动态自适应认证
终端动态环境检测
终端进程可信
业务动态准入

业务发布

认证接入

权限控制

网络隐身

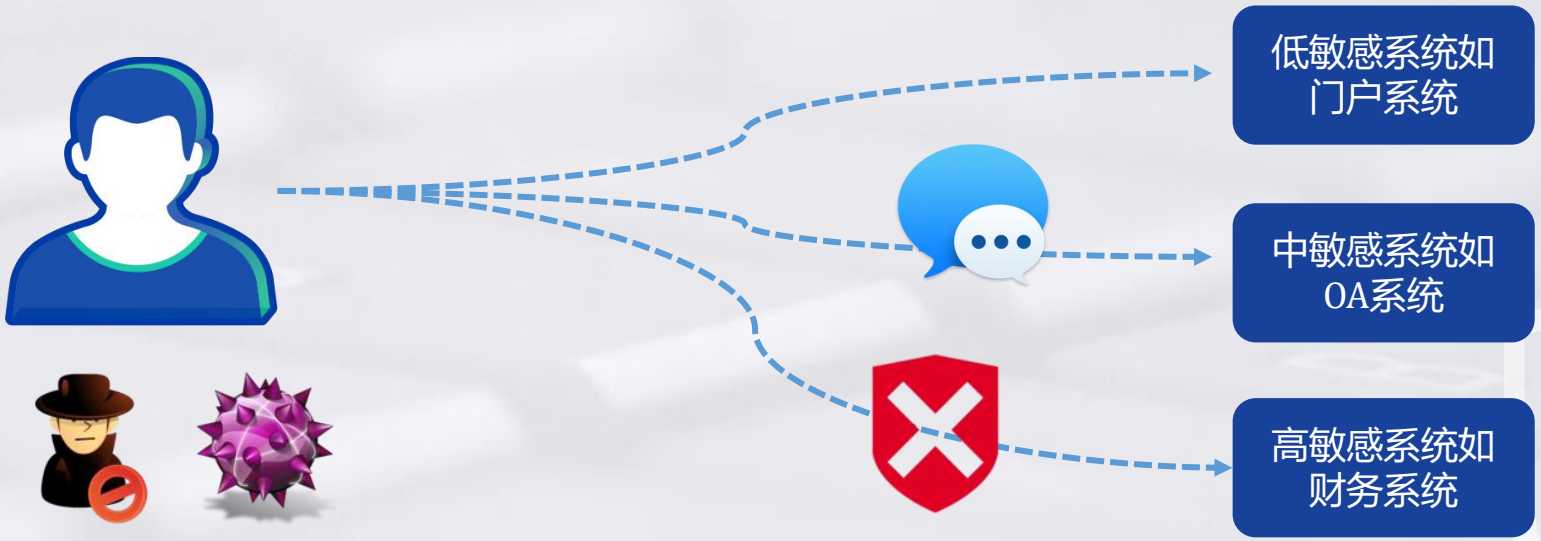
缩小业务暴露面

动态权限控制

基于身份、环境、行为，动态调整权限；
不同敏感度业务采取不同安全访问条件

智能权限-- 动态访问控制（安全基线）

通过“信任引擎”发现环境/行为/身份存在风险时，收缩用户的访问权限，缩小内网业务暴露面



当环境、身份、行为存在风险，收缩权限，
如中敏感业务需要二次身份增强认证，高敏感业务则可阻止访问。

智能权限-- 动态访问控制（安全基线）

不同敏感度业务采用不同安全级别的动态访问控制策略

需安装杀毒软件

低敏感系统如门户系统

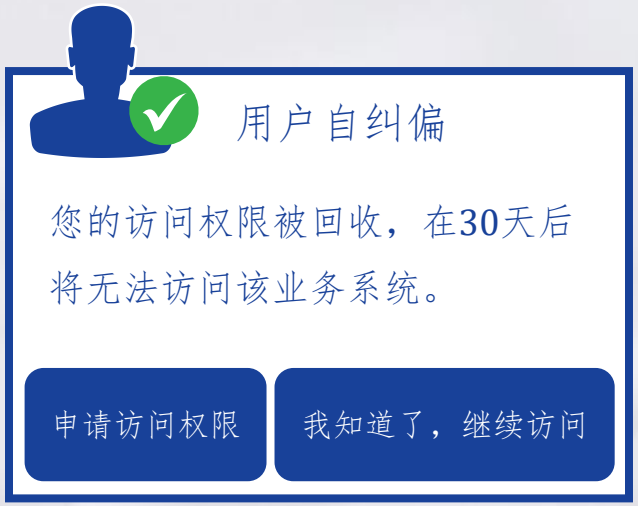
只允许通过Chrome浏览器访问

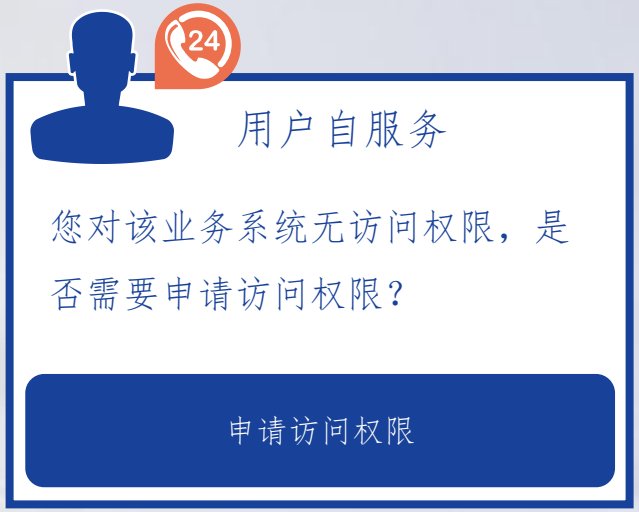
中敏感系统如OA系统

需安装指定软件、只允许通过Chrome浏览器访问、需要进行二次身份认证

高敏感系统如财务系统

智能权限– 权限梳理工具，帮助实现最小化权限的落地





1 采集

- ✓ 可通过采集阶段帮助搭建基础的用户权限模型
- ✓ 根据用户/角色访问业务频次等智能推荐权限基线

2 试运行

- ✓ 基于最小权限原则逐步纠偏，用户可自助申请，IT/主管审核

3 正式运行

- ✓ 正式运行，提供权限自服务通道，确保权限准确、可靠

零信任“VPN”--提供远程访问全周期安全保障

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

动态自适应认证与业务准入

动态自适应认证
终端动态环境检测
终端进程可信
业务动态准入

多源信任评估，访问行为管控

集成第三方安全能力，多源信任评估
访问行为安全审计、分析异常行为，
动态处置、灰度处置。

业务发布

认证接入

权限控制

行为管控

网络隐身

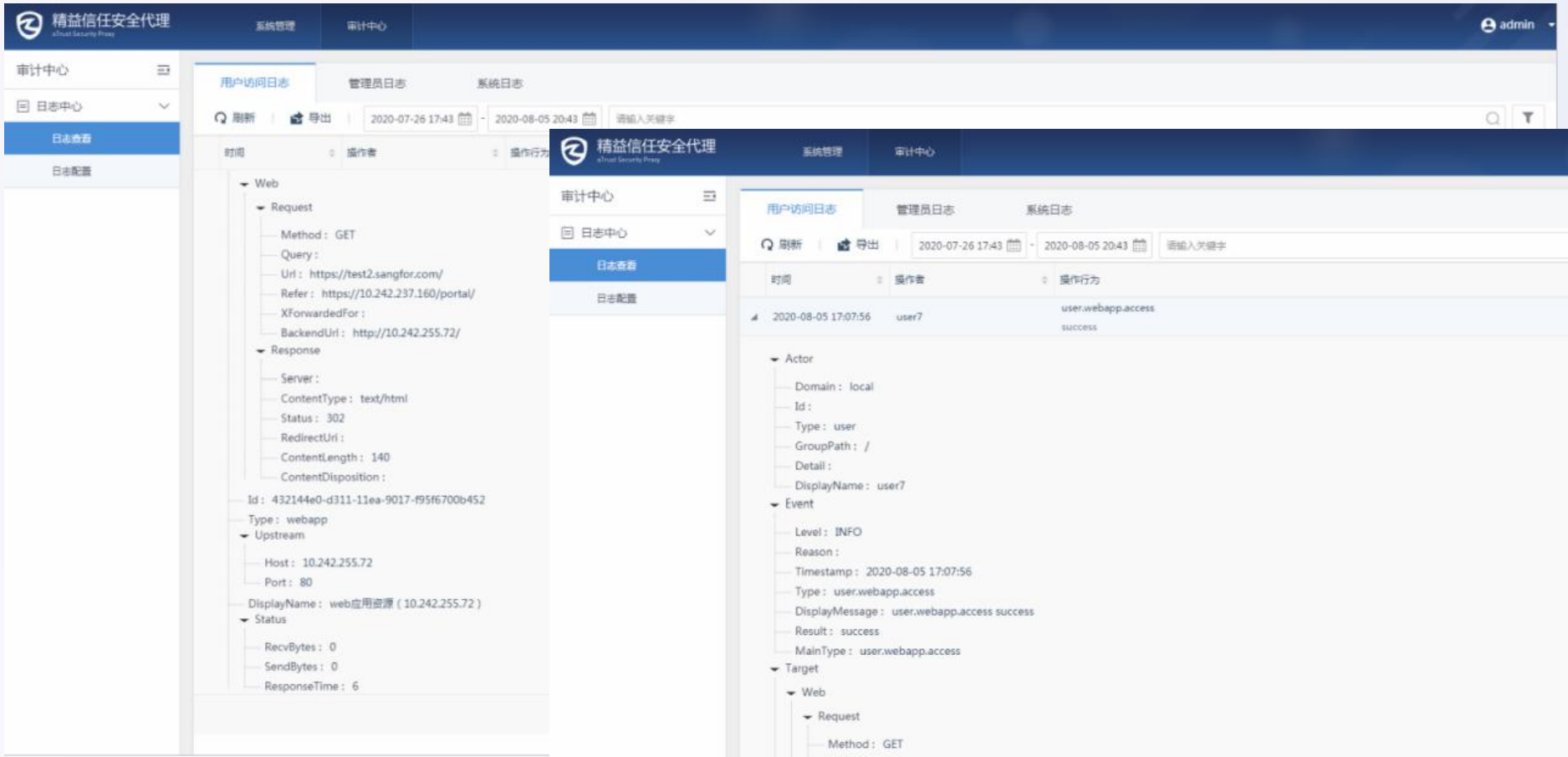
SPA机制缩小业务暴露面

动态权限控制

基于身份、环境、行为变化，动态收缩权限
不同敏感度业务采取不同级别访问控制

访问行为安全审计

访问行为完整审计，为安全溯源与UEBA分析提供支撑



智能权限--第三方安全能力集成与多源信任评估

结合第三方安全能力，多源信任评估并实现灰度处置，对可疑行为有效处置，兼顾安全与体验

极简运维 – 多项技术改进提升用户访问及运维管理体验

1 **B/S业务免客户端**

提升用户访问体验

降低终端运维工作

2 **内外网一致访问体验：**

内网接入与外网接入实现一致的访问体验

3 **权限申请自服务**

业务访问权限自助申请，IT人员自主审批

简化权限运维管理工作

4 **终端运维工具**

提供终端运维工具，终端一键排障、日志收集，简化终端运维工作。

5 **传输技术优化**

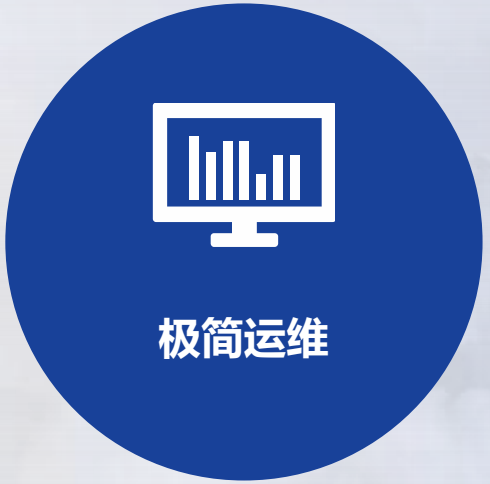
远程接入传输技术改进，提升访问体验。

零信任“VPN“核心优势及价值

更安全，体验更好的新一代远程办公安全解决方案

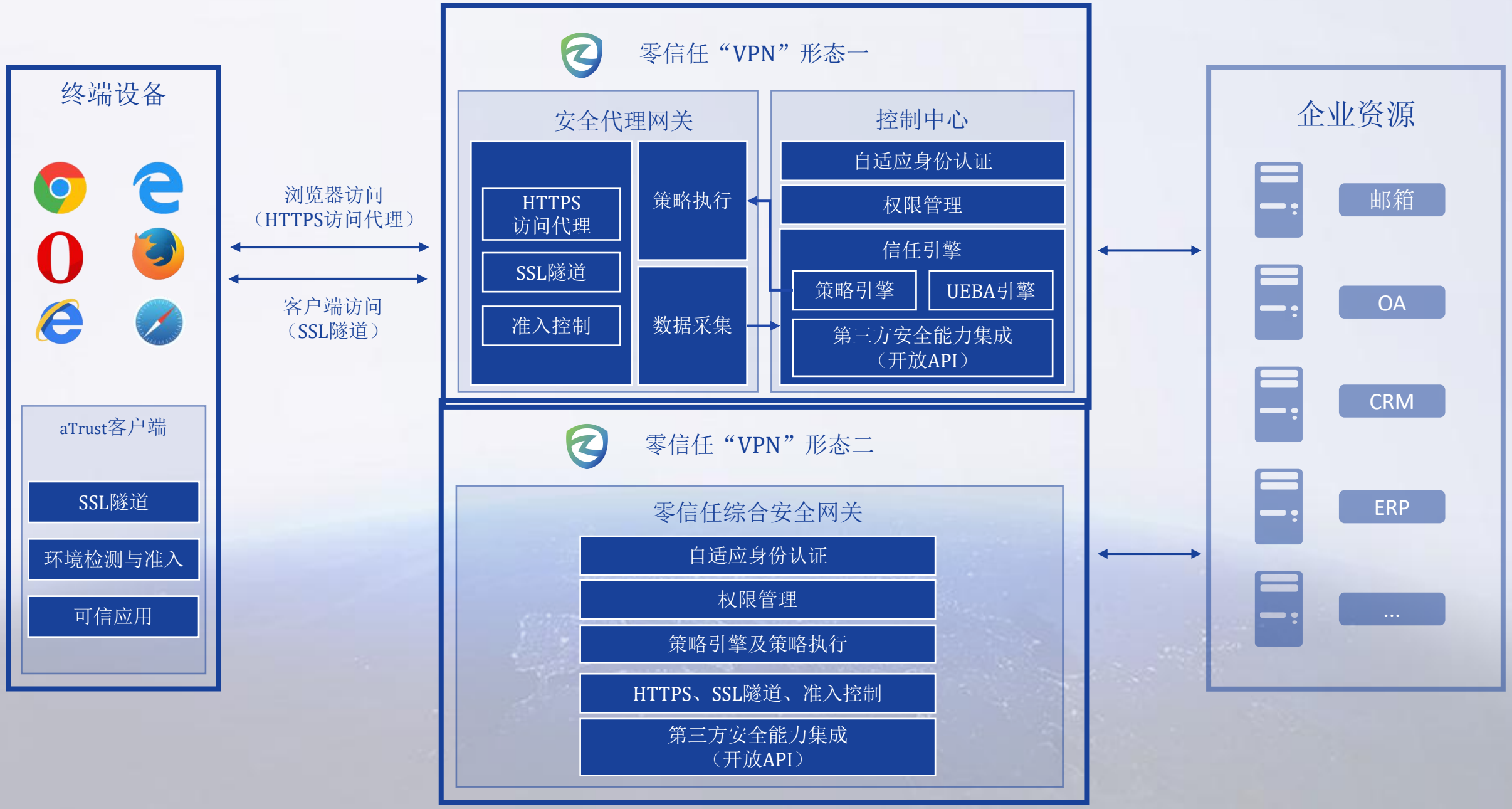
核心优势：
动态自适应认证
网络隐身，第二代SPA单包授权机制
动态全周期环境检测与全局业务准入
可信应用

核心优势：
安全基线（动态权限）
智能权限基线工具
灰度处置



核心优势：
B/S业务免客户端
权限自助服务
内外网一致体验

深信服零信任”VPN”方案形态



深信服零信任“VPN”访问数据流程

深信服零信任”VPN”对比传统VPN 的关键能力升级

关键能力维度	传统SSL VPN	零信任“VPN”
业务发布	业务收缩进内网，通过SSL发布，但默认都可以连接SSL发起认证请求	✓ 业务收缩隐藏到代理网关（或综合网关）后 ✓ 采用SPA单包授权机制，实现网络隐身
认证接入	双因素多因素认证 终端登录时静态准入	✓ 动态自适应认证，增加动态增强认证能力 ✓ 全周期终端环境动态检测，动态业务准入
权限控制	基于角色的静态访问控制	✓ 动态访问控制，基于环境、身份、行为等多源条件动态调整访问权限
访问行为安全	日志审计，通过SYSLOG、外置数据中心记录访问资源等行为	✓ 全量、更精细的访问日志审计 ✓ 结合第三方安全能力，多源评估，识别异常访问行为，快速处置 ✓ 灰度处置能力
访问体验	通常采用客户端接入	✓ B/S业务免客户端接入 ✓ 内外网一致体验 ✓ 传输技术改良，兼容性与快速性更优
运维体验	客户端运维工作较大 权限变更、申请依赖于运维人员，权限运维难度较大	✓ B/S业务免客户端 ✓ 权限自服务申请与自主审批 ✓ 权限；提供智能权限工具

深信服远程办公的积累与实践

深信服VPN领域近20年的技术和实践积累

深信服SSL VPN连续12年国内市场第一（IDC）
国内唯一入围Gartner魔力象限

深信服大量的客户积累

90%	80%	80%	85%	90%	95%
政府部委	全球500强 中资企业	银行/证券/保险	985/211高校	医疗百强	三大运营商

深信服VPN领域近20年的技术和实践积累

VPN技术领域近20年积累与创新

- ✓ **国家SSL/IPSEC VPN技术标准核心制定者**
- ✓ **2005年全球率先推出SSL、IPSEC一体化的VPN 安全网关**
- ✓ **VPN领域的专利技术积累：**

一种基于WEB的线路自动选择方法、
利用网页进行动态寻址的方法和系统专利、
多路复用VPN隧道的连接方法等专利积累等

零信任相关标准及生态实践

参与技术标准与指南制定

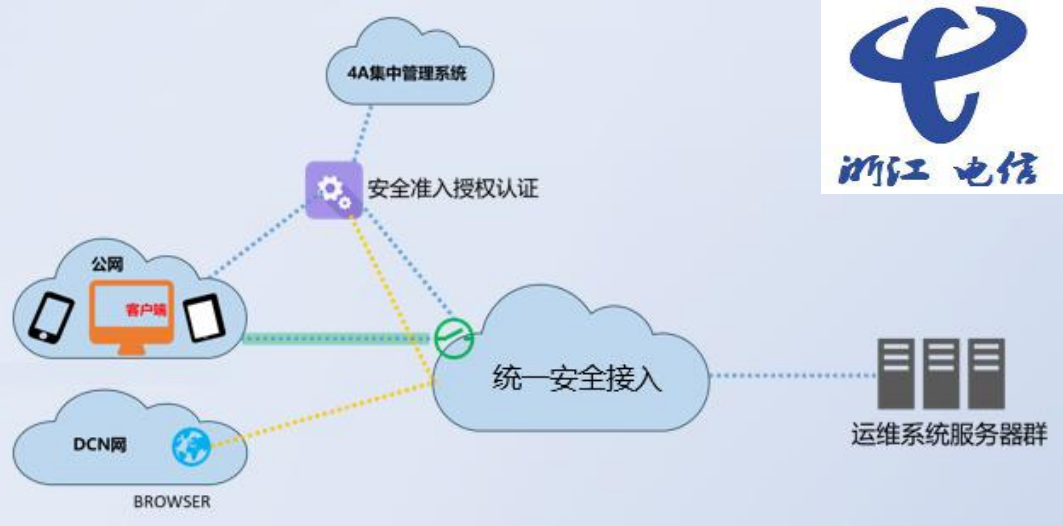
✓ 《信息安全技术 零信任参考体系架构》（制定中）
标准参编单位

✓ 《网络安全实标准践指南-零信任参考架构及安全应用指引》（制定中）
核心参编单位

CSA SDP工作组首批参与单位

为提高SDP在中国企业的应用，在中国云安全联盟的支持下，CSA GCR成立SDP工作组。工作组于2019年3月成立，深信服成为首批参与单位之一。

• 浙江电信零信任最佳实践案例



浙江电信共有网管系统、办公系统、业务后台管理系统等200个网络及应用运维系统，6000余名运维人员，有大量的业务系统需要通过内网和外网（SSL VPN方式）访问。

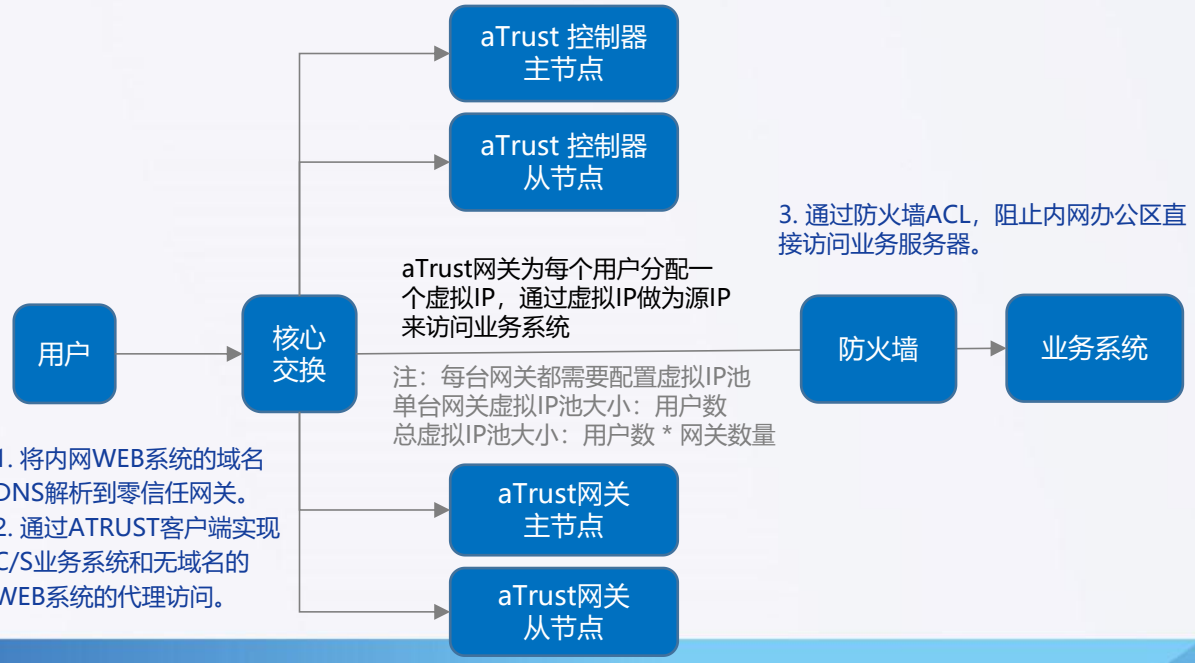
需求背景

- **业务暴露面过大：**内网有大量配置固定IP的终端，通过这些终端可以访问所有业务系统；为SSL VPN接入的用户发布了大量的业务系统，如果远程接入的是非法用户，或者接入终端环境不安全，存在极大安全隐患。尤其是HW期间，过大的业务暴露面带来极大的挑战。
- **访问权限不可控：**无论是运维人员还是领导、或者是第三方人员，均具备访问几乎所有业务系统的权限。HW期间过大的权限将面临随时被钓鱼后攻破内网的风险。
- **内外网使用体验不一致：**一些WEB业务系统在内网可以直接访问，而在外网通过VPN访问时需要强制安装客户端，对于领导、第三方合作人员的使用体验极其不好。
- **访问行为不可控：**DCN网络内缺乏有效的终端检测与准入措施来对终端的环境和行为进行管控，使得终端的接入安全不可控，可能对DCN网内的业务系统造成横向影响。

方案概述

方案设计：

1. 与浙江电信4A系统对接，实现流量身份化及权限管理
2. 通过aTrust安全代理网关代理内外网访问，将业务系统进行隐藏，缩小业务暴露面，降低数据泄露风险
3. 通过aTrust安全代理网关的动态访问策略来强制执行设定的安全基线，实现信任最小化
4. 提供权限基线梳理工具，做到访问请求的精准化、颗粒化控制，保护业务安全
5. 通过aTrust客户端对用户终端环境实现全生命周期检测持续评估



安全策略：

1. aTrust与4A系统对接，实现流量身份化及权限管理
2. 将内网WEB系统的域名DNS解析到零信任网关
3. 通过aTrust客户端实现C/S业务系统和无域名的WEB系统的代理访问
4. 通过防火墙ACL，阻止内网办公区直接访问业务服务器
5. 配置虚拟IP池，aTrust安全代理网关为每个用户分配一个虚拟IP，通过虚拟IP来访问业务系统；
6. aTrust控制器和安全代理网关分别进行集群部署；
7. aTrust控制器配置动态访问控制策略，弱密码、非授信终端拒绝访问业务系统、非法时间段通过短信认证才能访问业务系统。

方案价值和效果

- 为全省6000多运维人员提供统一安全入口，实现内外网运维统一访问控制
- 网络隐身，通过SPA机制缩小业务暴露面
- 接入终端环境动态检测以及基于访问业务的动态业务准入，建立业务系统级的安全边界
- 动态访问控制，并可对风险行为进行灰度处置
- 访问行为可视化，访问行为全量审计，SYSLOG对接日志平台
- 支持Web业务无感知访问，通过浏览器即可轻松接入，有效平衡安全与体验

实践案例– 深信服零信任助力江苏银行第三方商户平台缩小暴露面

江苏银行 BANK OF JIANGSU

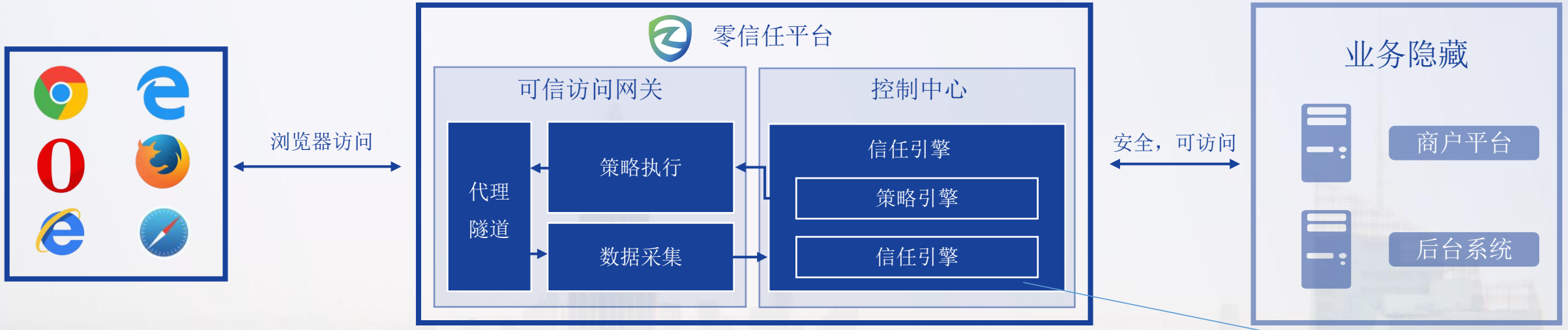
江苏银行简介：

江苏银行于2007年1月24日正式挂牌开业，截至2019年末，总资产2.07万亿元。在英国《银行家》杂志2019年度全球1000强银行排名中，按一级资本列92位，蝉联全球银行百强，国内排名第18位。

需求场景

1. 商户管理平台、商户服务平台、后台管理平台等商户管理平台、商户服务平台、后台管理平台等业务仅允许特定合作商户进行访问，面向互联网发布暴露面过大，且但访问用户为动态IP，无法进行有效访问控制。
2. 业务通过传统方案收进内网会面临用户访问域名发生变化、无法强制商户安装客户端，使用体验较差及运维难度大；
3. 商户接入需进行强身份认证，当用户使用弱密码时需加强认证，异地登录时需要进行增强认证；当有异常暴力破解行为时需要提供防护机制；

实践案例-- 深信服零信任助力江苏银行第三方商户平台缩小暴露面



零信任方案使用效果

1、可信访问：对外发布业务从互联网收缩进内网，隐藏业务，最大程度业务缩小暴露面；

2、动态自适应认证：除提供双因素认证外，提供自适应认证策略，当用户使用弱密码登录时，必须使用增强认证；当用户在异常时间段登录时，必须使用增强认证等。

3、无感接入与极简运维：从互联网发布收缩进内网，不改变用户原有网站域名，不改变商户访问原有使用习惯，纯浏览器免客户端登录，保障商户和合作方使用体验，并且大幅降低行内运维人员终端侧的运维压力。

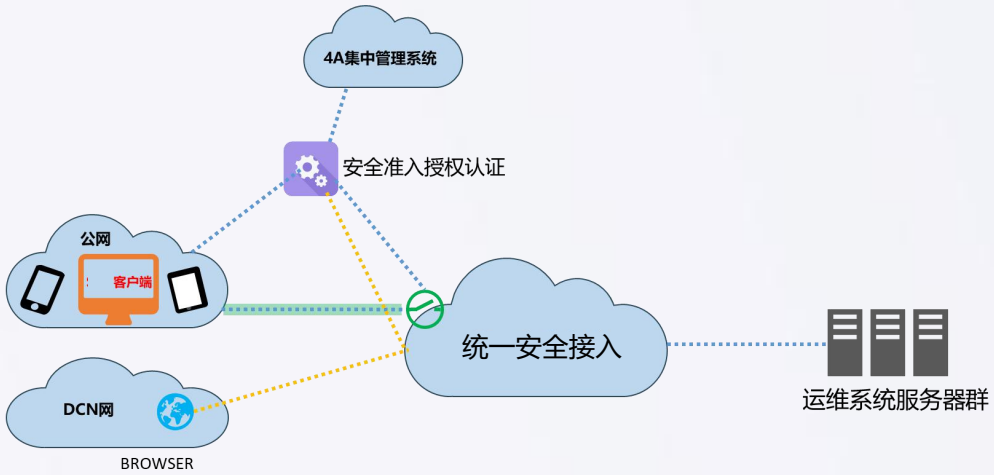
4、智能权限：动态安全基线，基于应用级的动态访问控制，实现一旦接入终端有异常访问行为触及安全基线即可动态识别收缩应用的访问权限。

如只允许通过Chrome访问
在凌晨发起的访问需要增强认证
异地登录访问需要二次认证

信任引擎：动态安全基线

不允许通过以下IP接入
检测到凌晨发起访问，拒绝

实践案例：深信服零信任方案助力浙江电信统一运维接入



● 需求场景

浙江电信共有网管系统、办公系统、业务后台管理系统等200个网络及应用运维系统，6000余名运维人员，需要实现各类网管运维系统统一安全接入，缩小业务暴露面，统一访问控制。

● 零信任方案使用效果

- 为全省6000多人员运维人员提供统一安全接入入口，实现内外网运维统一访问控制
- 网络隐身，通过SPA机制缩小业务暴露面
- 接入终端环境动态检测以及基于访问业务的动态业务准入，建立业务系统级的安全边界
- 动态访问控制，并可对风险行为进行灰度处置
- 访问行为可视化，访问行为全量审计，SYSLOG对接日志平台
- 支持Web业务无感知访问，通过浏览器即可轻松接入，有效平衡安全与体验

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

更多客户案例：

CVTE Dream·Future 视源股份

听 喜马拉雅

上海环境 SHANGHAI ENVIRONMENT

厦门信达 XINDECO XIAMEN XINDECO

上海教育 上海市教育委员会主办

美年大健康 Health 100

中国科学院上海应用物理研究所 SINAP Shanghai Institute of Applied Physics, Chinese Academy of Sciences

山东省计算中心（国家超级计算济南中心） SHANDONG COMPUTER SCIENCE CENTER (NATIONAL SUPERCOMPUTING CENTER IN JINAN)

THANK YOU

2020 深信服科技