联软科技
LEAGSOFT

战疫求“安”
远程办公的新危机如何应对

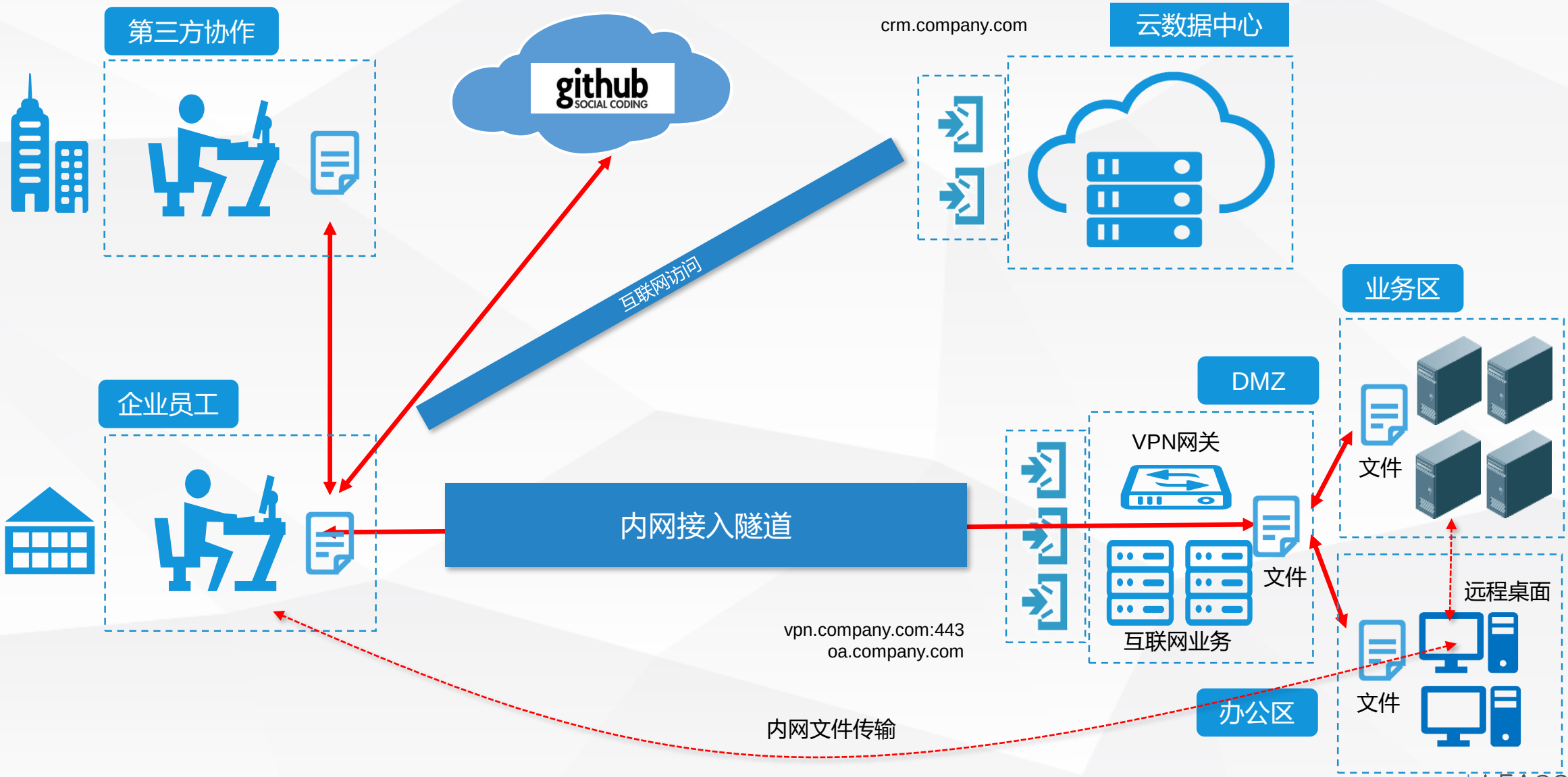
华南区技术总监：郑召坤

构建可控的互联世界

联软科技
LEAGSOFT

远程办公场景下的风险分析

远程办公的几种场景


第三方协作
github
SOCIAL CODING
crm.company.com
云数据中心
互联网访问
业务区
企业员工
DMZ
VPN网关
文件
内网接入隧道
文件
远程桌面
vpn.company.com:443
oa.company.com
互联网业务
文件
办公区
内网文件传输

远程办公场景下的风险分析

远程办公带来了新的安全挑战

终端不再”可控”

终端脱离企业可控范围

数据安全受到挑战

数据离网、交换通道变多，管理变得复杂

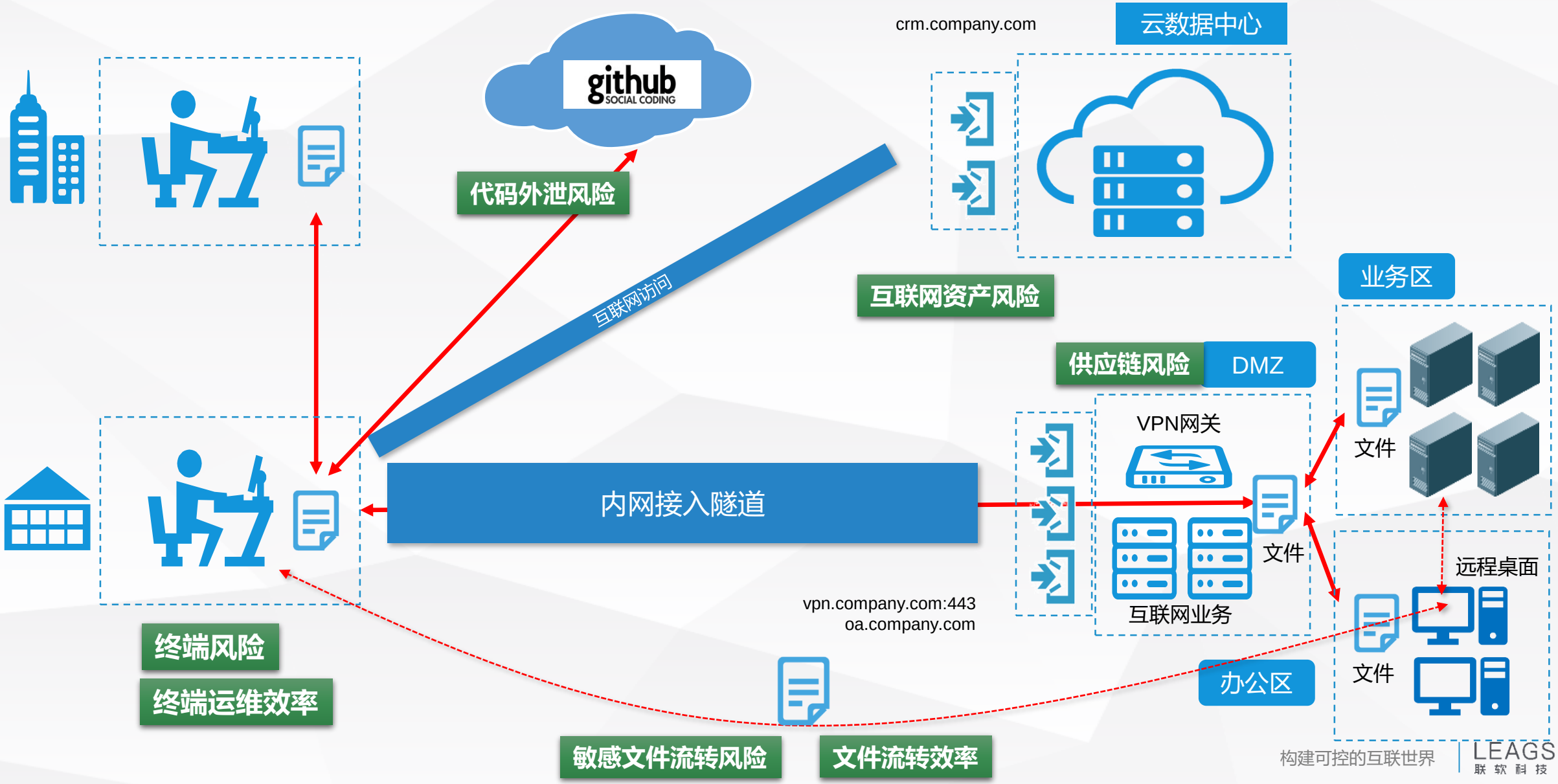
互联网暴露面风险增加

互联网侧到底有多少资产
供应链安全如何保障

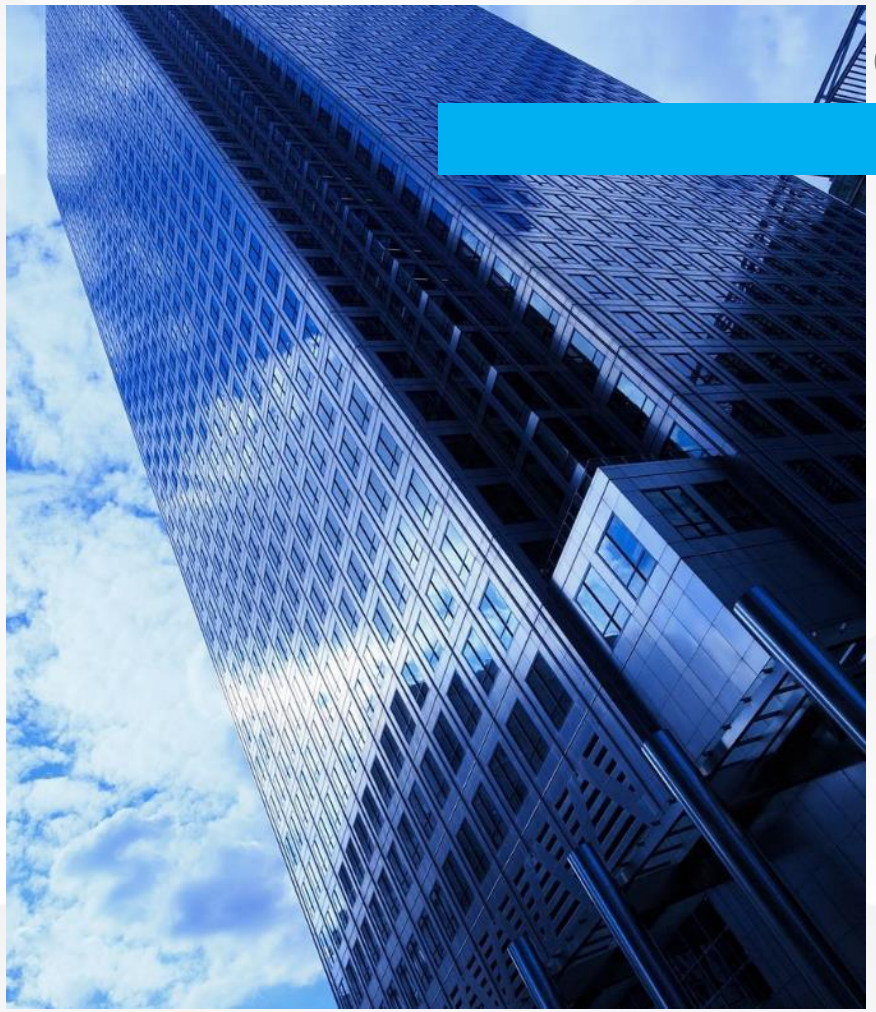
如何安全高效的进行文件交换

多网环境下，文件交换的复杂度都极大增加、安全风险极大提升
效率和安全如何平衡?

远程办公场景下的风险分析



方案目录



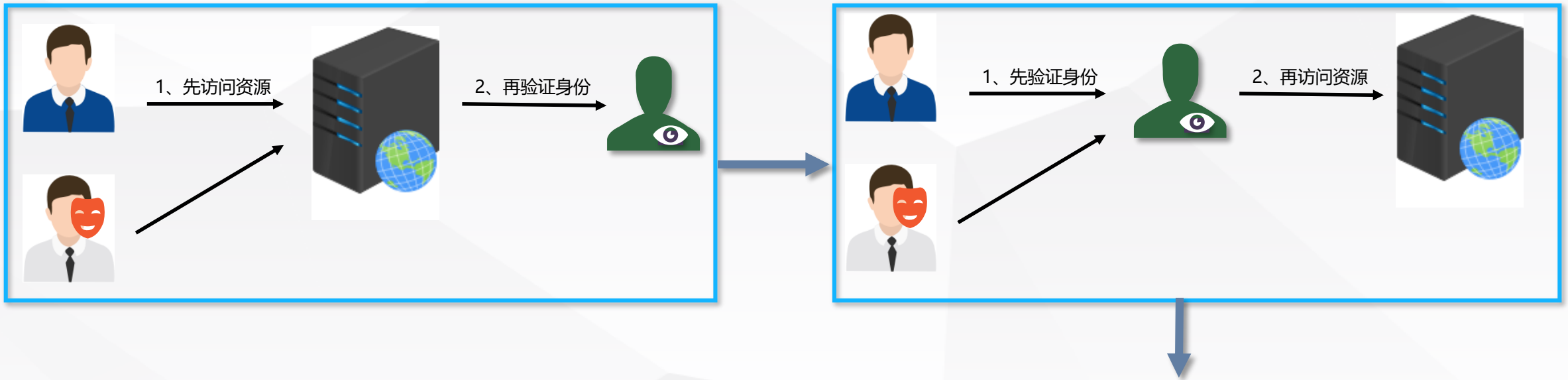
Contents

联软科技
LEAGSOFT

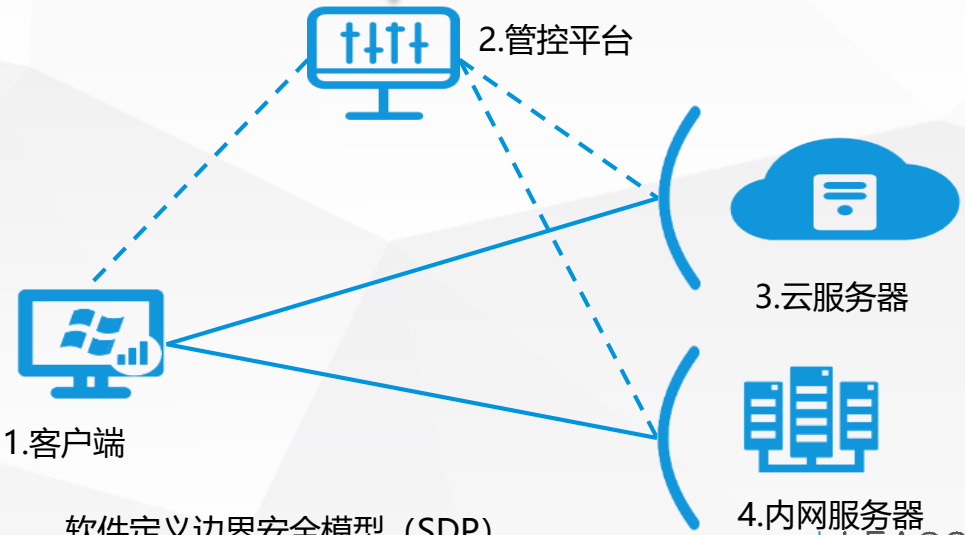
“零信任架构”
远程办公安全解决方案

远程办公

零信任理念的应用



- 1、不再区分内外网，基于安全状态访问控制
- 2、Need to know 的访问控制策略
- 3、访问所有资源都必须认证、授权、加密
- 4、最小化攻击界面，强化防护界面，安全措施尽可能贴近防护界面
- 5、所有网络访问流量必须监控和审计

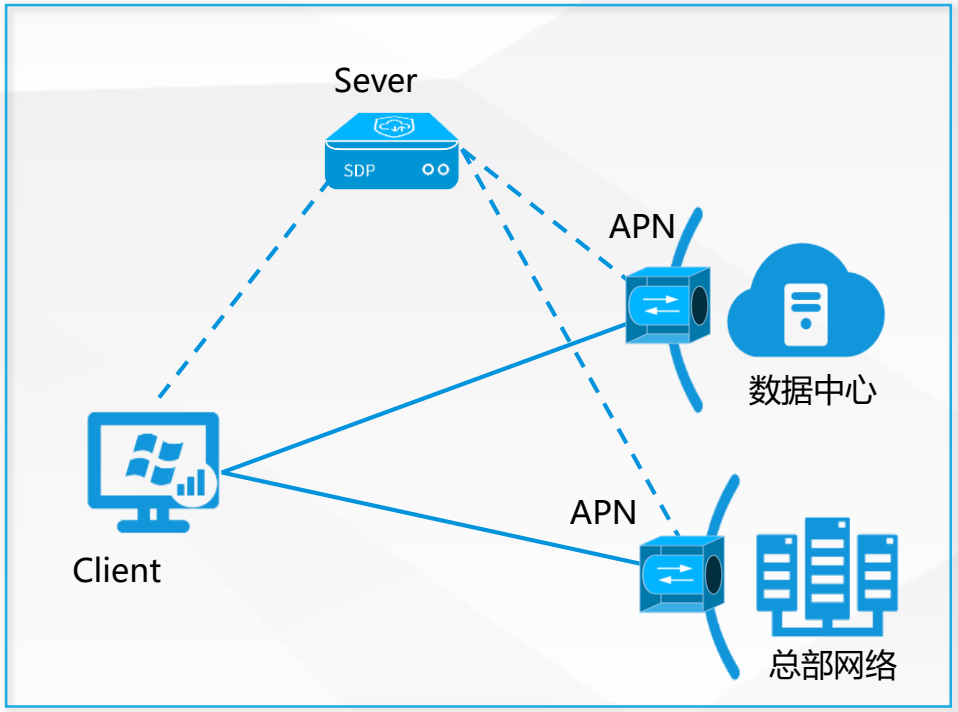


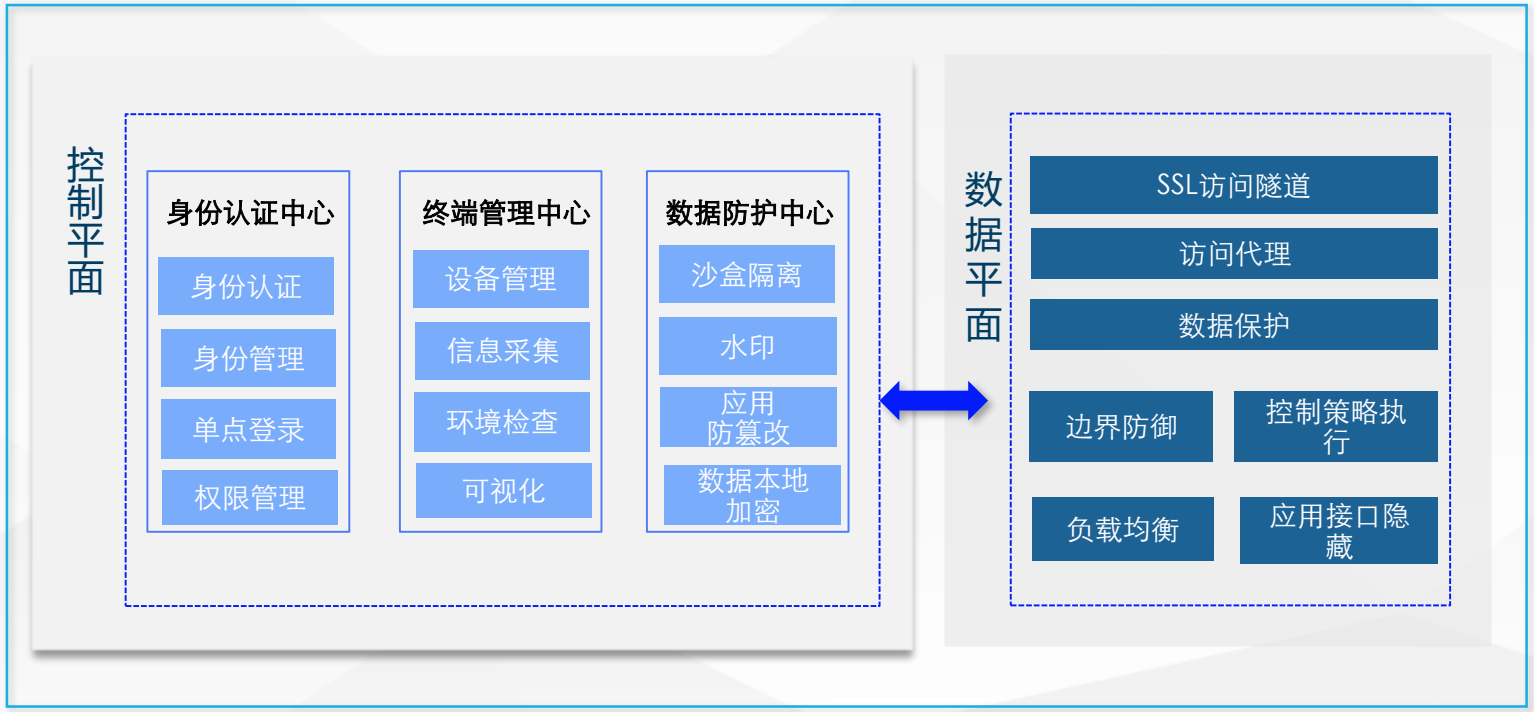
软件定义边界安全模型（SDP）

构建可控的互联世界 | LEAGSOFT 联软科技

远程办公接入平台

架构安全，认证方便，数据可控！





基于零信任架构搭建安全、高效易用、高扩展的远程办公接入平台
支持全平台终端：安卓、IOS、Windows、Linux、MAC OX、麒麟

基于Zero Trust理念的安全架构

可信身份

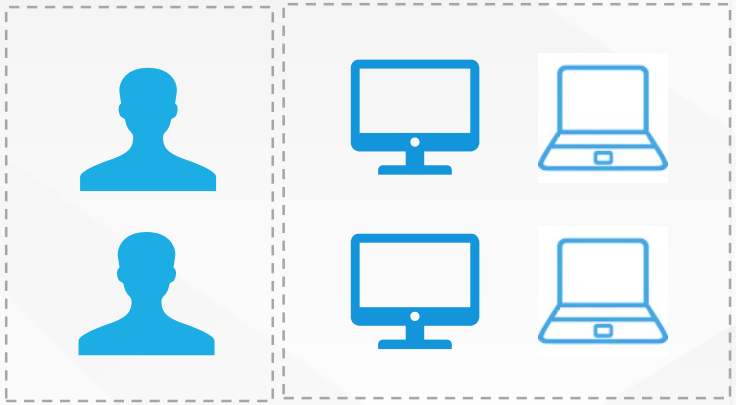
身份认证　多因素认证

SSO单点登录

可信网络

SPA　SSL双向校验

国密支持　独立应用隧道



加密隧道

加密隧道

SSL全程加密

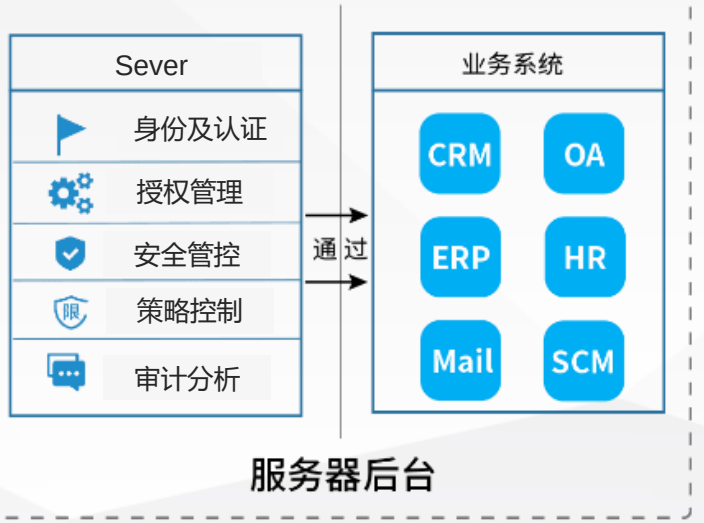
APN

安全网关

内部网络

内部网络

内部网络



服务器后台

可信终端

设备管理　安全沙箱

安全检查　策略总控

可信服务

身份认证中心　日志审计中心

高冗余/高可靠

数据安全-全方位的安全保护确保“可信终端”

沙盒系统
数据隔离

水印模块
防止拍照泄密

本地数据
加密存储

U盘控制
外发控制

行为审计
日志记录

基于应用的
高颗粒度授权控制

粘贴复制
禁止出沙盒

联软科技
LEAGSOFT

远程办公终端安全加固

全方面加固接入终端

网络准入控制
安全检查
补丁管理
安全基线管理
基于角色授权

终端安全

外联管控
外发管理
打印管理
水印控制
外发审计

数据管理

软件商城
软件分发
软件黑白名单
违规卸载
使用统计

软件管理

基于场景策略
资产管理
一键远程协助
消息公告推送
日志审计

运维支撑

终端一体化安全管理平台

数据安全-数据外发通道管理

网络

发帖内容/附件审计
网络共享/网盘/FTP

即时通讯软件

QQ/WEB微信/Client微信/TIM等
文件/图片/聊天内容
全审计/识别接收者

录屏

对用户行为进行录屏

屏幕水印
漏洞修复

邮件

邮件收件人地址/服务器IP黑白名单
邮件标题/正文/附件审计/附件敏感外发阻止

U盘拷贝

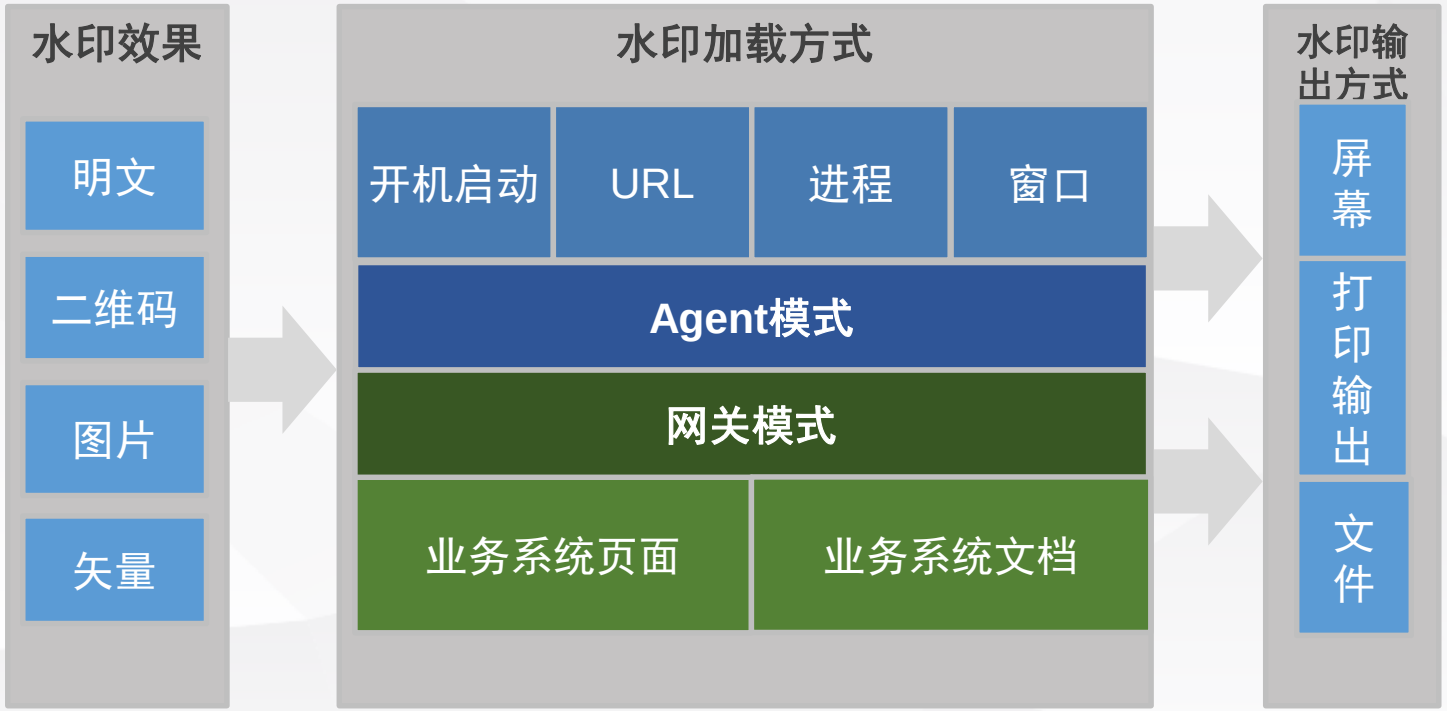
新建/删除/读写/复制粘贴/导入导出/
进程/源文件/目的文件

打印

打印机黑白名单
打印水印
打印内容审计

数据防扩散-水印系统架构简介

方案架构



方案价值

心理震慑：

通过直观的水印效果，以对用户强调行内数据安全目标，并给与心情威慑

审计追溯：

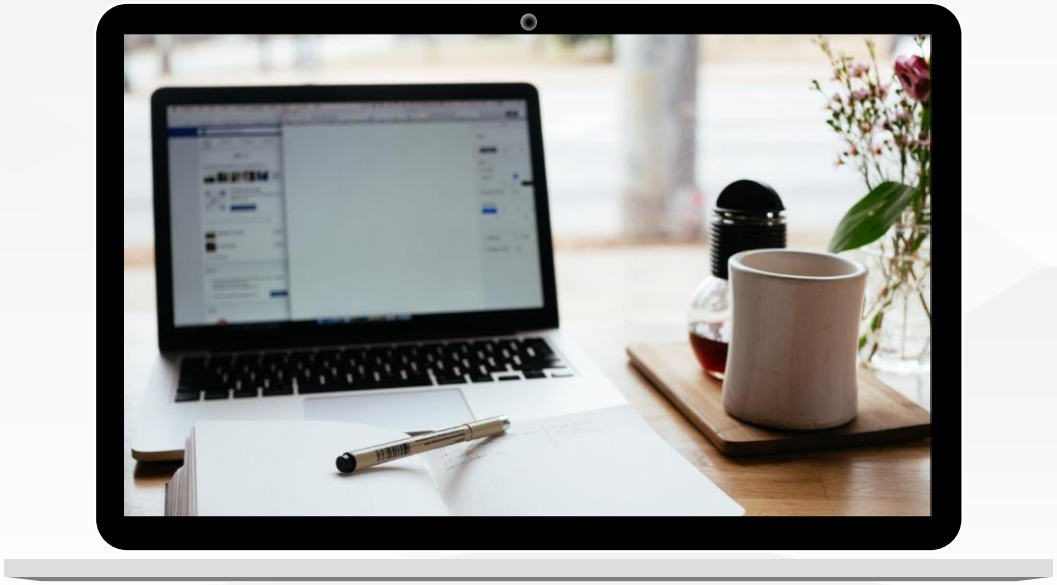
- 通过附带个人信息的水印效果，提供数据外泄的追溯手段
- 通过数据流转管理，协助定位泄露文件的人员

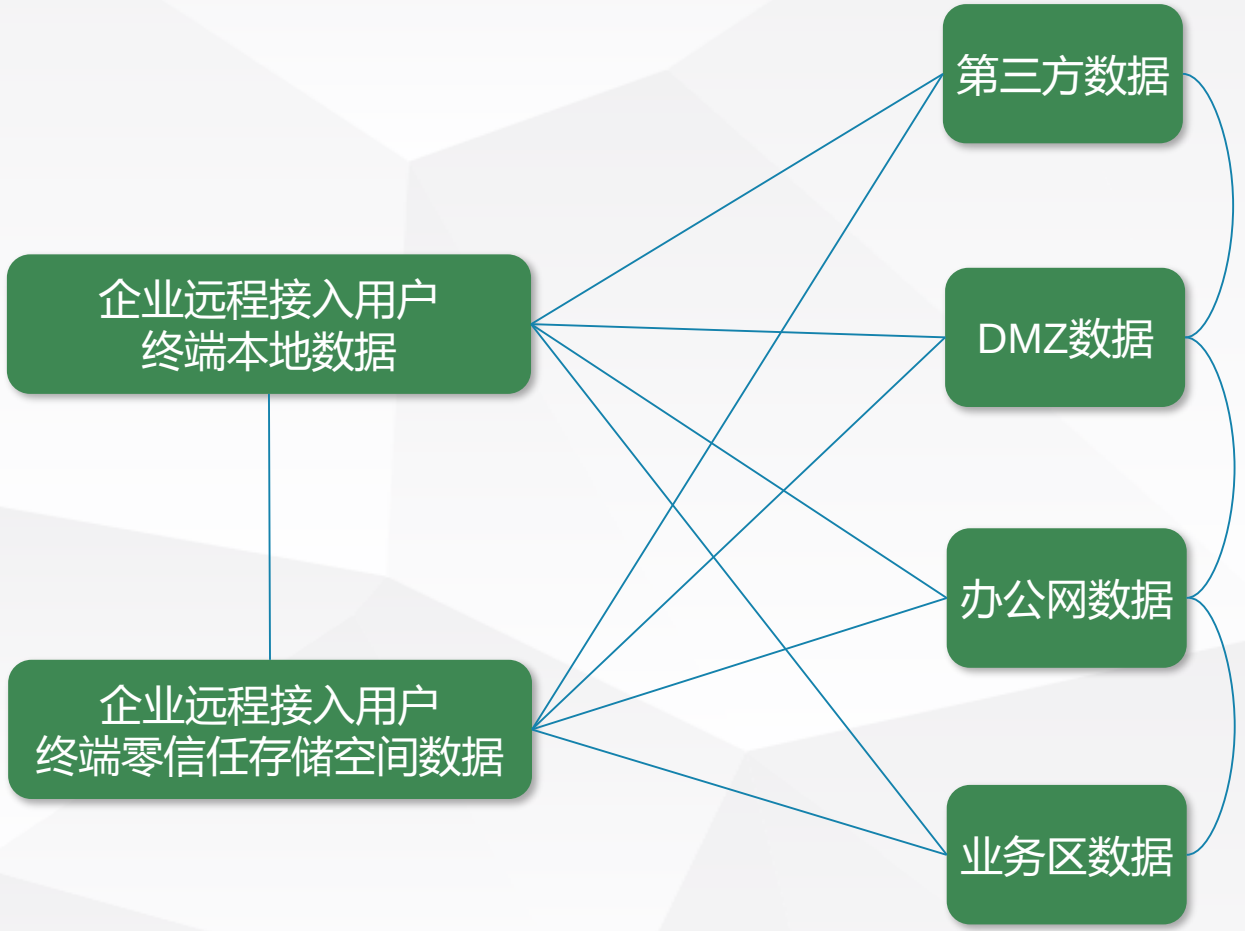
联软科技
LEAGSOFT

安全数据交换系统

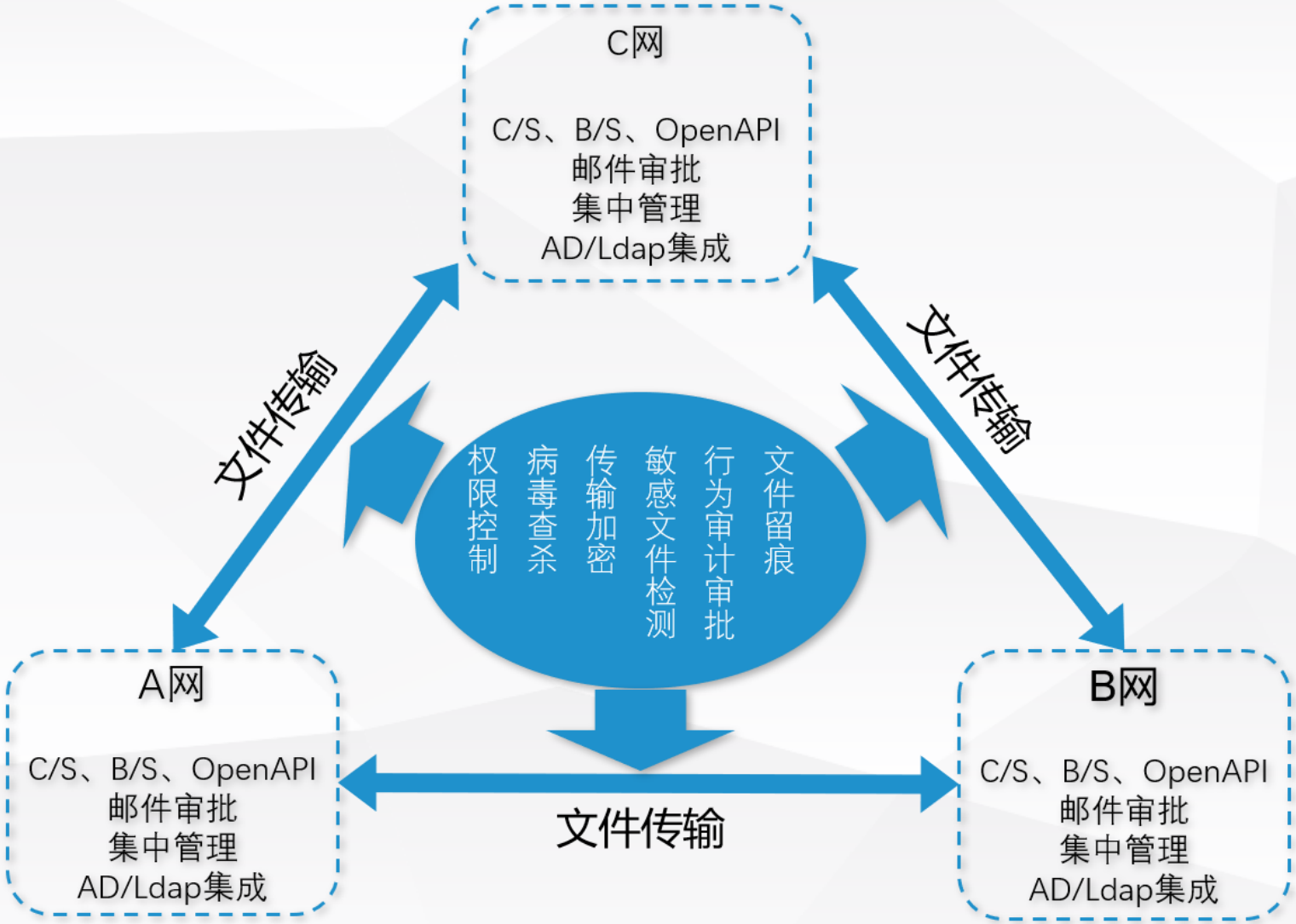
远程办公场景下，文件交换变得复杂

安全、效率成为难题





联软安全数据交换系统



权限控制：

精细化权限控制，基于角色设定在每张网的上传、下载权限

病毒查杀：

集成多套杀毒引擎，确保入网文件无感染

行为审计审批：

提供审批控制，确保权限管理的灵活性

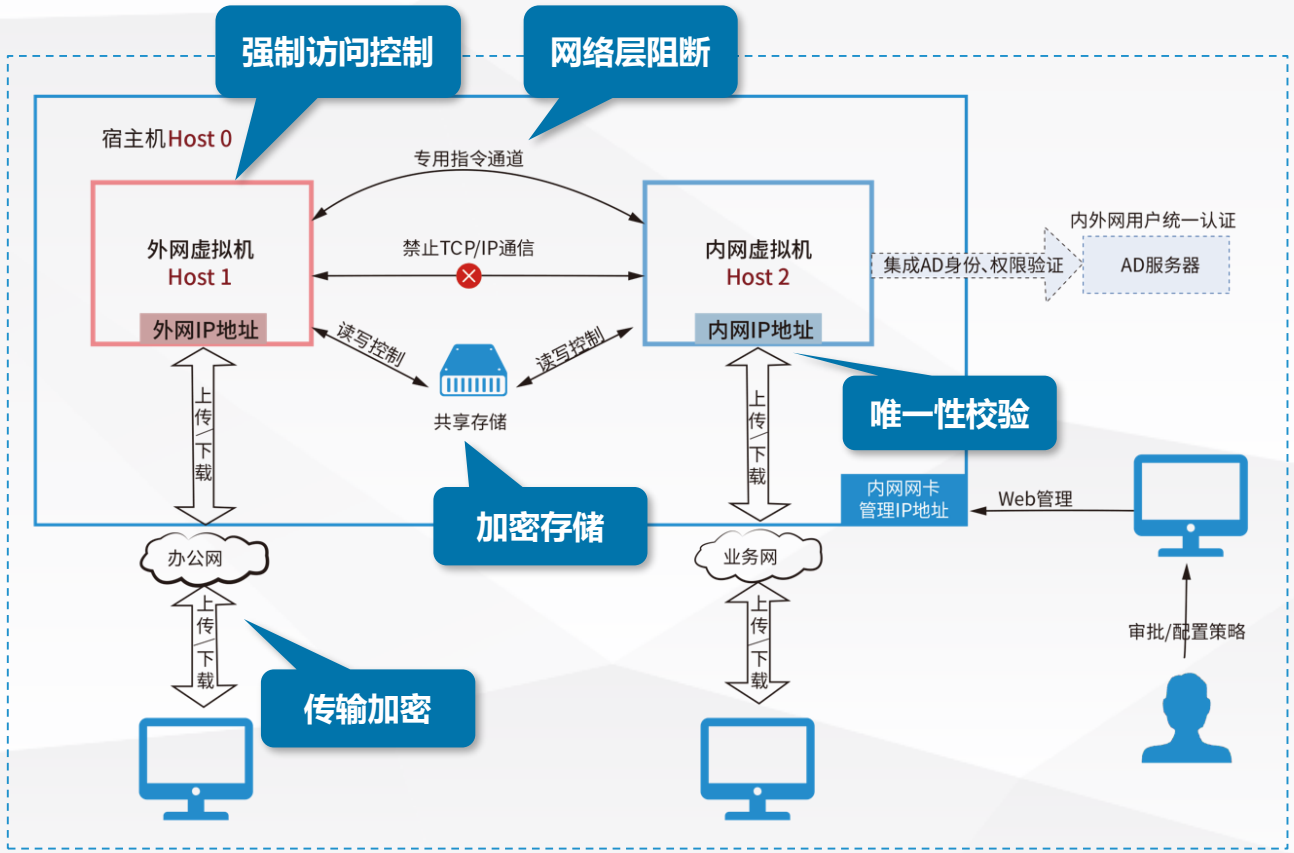
文件留痕：

详细记录用户的文件操作行为，提供事后溯源能力

敏感文件检测：

提供文件敏感信息监测，实现控制策略联动

系统架构安全性设计



01.虚拟化隔离

利用虚拟化隔离技术，阻隔网络层协议传输，文件传输过程中剥离数据包头信息

02.传输通道加密

数据由客户端到服务端间由ssl加密保障传输安全

03.文件落地加密

用户文件传输至UniNXG后，系统自动加密数据，保障非法获取数据也无法解密

04.文件唯一性校验

文件在传输过程中经过多次唯一性校验，防止文件窃取替换发生

05.强制访问控制

特殊环境内可设置强制访问控制，限制系统平台内可以运行的进程，严格杜绝木马病毒

联软科技
LEAGSOFT

互联网资产安全检测服务

远程办公系统引入新的脆弱性

设备引入

- 设备自身风险
- 不安全的方案

系统变更

- 系统级漏洞
- 应用级漏洞

风险暴露面

- Web后台对外
- 远程维护端口

资产风险

- 系统/应用漏洞
- 弱口令/口令爆破风险
- 访问认证缺陷
- 管理后台开放
- 远程访问端口

供应链风险

- 大环境下远程接入设备厂商更易受攻击
- 设备漏洞/风险
- 远程接入设备供应商/SAAS服务商风险预警时效性

数据风险

- 开发人员安全意识不足，上传到Github等开源社区

运维风险

- 跨部门协作/信息打通问题
- 人员操作失误
- 临时策略/沉默策略/不合规策略引起的风险

互联网安全监控解决方案（SaaS）

✧ 互联网资产梳理

- ➢ 互联网资产发现、变动监控
- ➢ 远程办公相关设备、资产、入口，重点关注

✧ 暴露面探测与漏洞扫描

- ➢ 登陆入口与风险暴露梳理
- ➢ 互联网安全漏洞扫描
- ➢ 安全策略有效性检验
- ➢ 远程入口专项安全检测（专家服务）

✧ 信息泄漏监控

- ➢ 开源社区监控
- ➢ 社工库查询
- ➢ 暗网交易平台监控
- ➢ 网盘泄漏监控

✧ 漏洞与威胁情报

- ➢ 远程办公相关厂商漏洞&安全情报通告

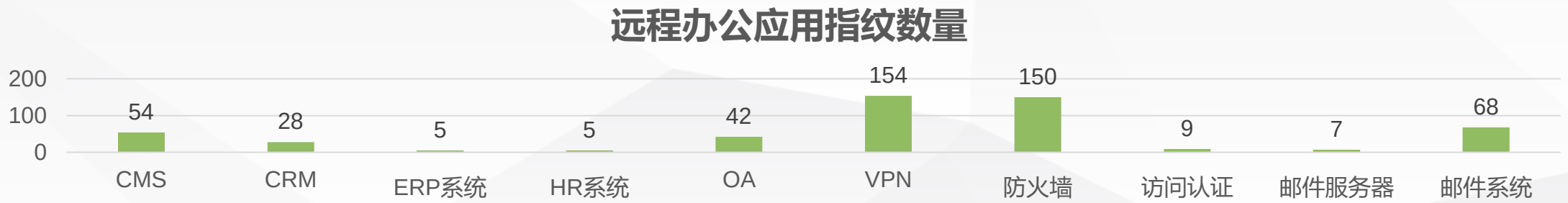
平台监测与检测能力

资产识别
- TCP全端口扫描，常用UDP服务
- 资产指纹113个细类，10000+条
- 域名自动挖掘

风险检测
- POC漏洞插件1200+，
- 风险暴露面，支持自定义添加
- 集成扫描，融入多种安全检测能力

安全情报
- Github开源社区监控、暗网监控
- 社工库查询、网盘泄漏监控

专家运营
- 7*24安全监控运营
- 15分钟内响应



专家服务：7*24运营，确保“远程无忧”

【魔方安全[redacted]报告20200212

service@cubesec.cn 发[redacted]

2020/2/12 13:26 详细信息

各[redacted]的同事，你们好：

[redacted]的周期性例行扫描中，监控[redacted]点存在2处高危漏洞，建议尽快修复。

附件为漏洞验证报告，详情请登录平台https://scan.cubesec.cn进行查看。

安全漏洞简述：

1[redacted]站点存在管理后台弱口令2处，弱口令导致1095条员工信息被泄露，包含员工的姓名、登录账户、性别、部门、职位、手机号及邮箱。

深圳市魔方安全科技有限公司-产品服务中心
总部：深圳市南山区高新中一道9号软件大厦816室
广州研发中心：广州市天河区林和西路157号保利中汇广场A座写字楼1408
Email:service@cubesec.cn

附件(1)

[redacted]验证报告202...

198KB

service@cubesec.cn 2019-11-19
【魔方安全】Apache Solr由于错误配置JMX RMI导致远程代码执行漏洞预警
尊敬的客户： 近日，安全研究人员 JanHøydahl 披露了 Apache Solr 的 8.1.1 和 8.2.0 发行版中的默认配置文件 solr.in.sh ，在其配置文件中 ENABLE_R

service@cubesec.cn 2019-11-07
【魔方安全】Squid缓冲区溢出漏洞预警
尊敬的客户： 近期，Squid官方发布安全更新修复了包括远程代码执行、信息泄露在内的多个漏洞。其中CVE-2019-12526为缓冲区溢出高危漏洞，可能导致远程代码执行，请尽...

service@cubesec.cn 2019-10-31
【魔方安全】Apache Solr Velocity模版注入远程命令执行漏洞预警
尊敬的客户： 近日，国外的安全研究员S00pY在GitHub发布了Apache Solr Velocity模版注入远程命令执行的poc，经研判，该poc真实有效。该漏洞是由于Velocity模板存在注

service@cubesec.cn 2019-10-25
【魔方安全】泛微e-cology OA 数据库配置信息泄漏漏洞预警
尊敬的客户： 2019年10月24日，泛微e-cologyOA被爆出存在数据库配置信息泄露漏洞。攻击者通过访问特定页面，可以直接获取数据库配置信息。如果攻击者可直接访问数据库...

service@cubesec.cn 2019-10-23
【魔方安全】PHP 远程代码执行漏洞预警（CVE-2019-11043）
尊敬的客户： 近期，PHP 官方发布漏洞通告，其中指出：使用 Nginx + php-fpm 的服务器，在部分配置下，存在远程代码执行漏洞。Nginx 上 fastcgi_split_path_inf

service@cubesec.cn 2019-10-18
【魔方安全】泛微e-cology OA SQL注入漏洞预警
尊敬的客户： 2019年10月17日，泛微官方发布了泛微e-cology OA系统存在SQL注入漏洞的预警，漏洞等级高。当服务端使用SQLServer 2012以上版本的数据库进行后端存储时...

service@cubesec.cn 2019-10-16
【魔方安全】WebLogic 高危漏洞预警(CVE-2019-2891)
尊敬的客户： 近日，Oracle 官方发布了 2019 年 10 月的补丁更新 CPU（Critical Patch Update），其中修复了存在于 WebLogic 中的一个高危漏洞（CVE-20

service@cubesec.cn 2019-10-16
【魔方安全】WebLogic 高危漏洞预警(CVE-2019-2891)
尊敬的客户： 近日，Oracle 官方发布了 2019 年 10 月的补丁更新 CPU（Critical Patch Update），其中修复了存在于 WebLogic 中的一个高危漏洞（CVE-20

EAGSOFT
软 科 技

联软科技
LEAGSOFT

联软科技简介

中国企业级端点安全市场的领导者

深耕端点安全领域

2004年成立，15年端点安全管控领域持续耕耘

中国首家网络准入控制厂商

中国首家推出泛端点安全平台化解决方案

终端产品全部拥有自主知识产权

云/边界安全

业内首创产品品类 – 多网文件交换系统

业内最早一批推出网络空间资产探测产品

提供覆盖云、边界、端多场景的平台级网络安全解决方案

企业文化

敬天爱人，诚实正直，不懈努力

公司愿景

构建可控的互联世界

基于TDNA理念的ESPP框架

指挥中心：安全策略管理 | 身份管理 | 整体态势感知 | 事件管理 | 安全运营管理 | 协同响应联动处置

产品体系

端点		边界	云
UniDLP数据防泄露	UniEDR终端检测与响应	UniNAC网络准入控制	UniSIMS云主机安全
UniAccess终端管理	UniEMM企业移动化管理	UniSDP软件定义边界	UniCSM网络空间资产测绘
UniAV防病毒系统	UniNID（IoT安全）	UniNXG网间数据交换	企业互联网安全监控SaaS

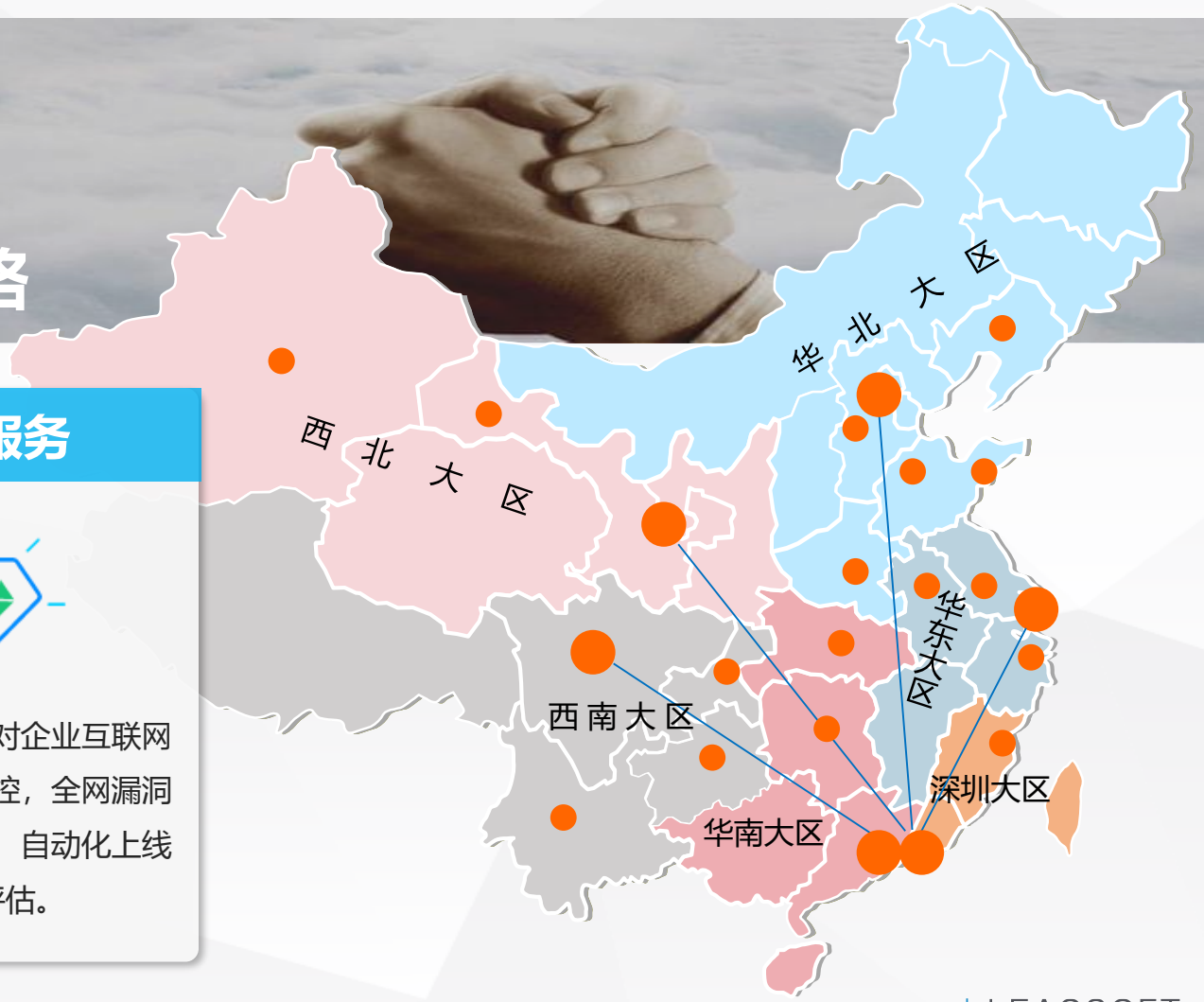
安全能力：行为分析 | 杀毒引擎 | 设备/软件/网站/文档/文件类型识别 | 安全知识库 | 威胁情报

基础组件：认证与授权 | 大数据处理 | 文件安全存储 | 文件分发 | 安全通信 | 水印 | APIs

服务体系

全国统一的服务热线 400-6288-116
ITIL标准国际专业服务流程

遍及全国各地的销售及服务网络



服务范围

公司总部位于深圳，广东省本土网络安全厂商，同时提供覆盖全国的营销和售后服务网络。

技术团队

公司技术主导，500多个技术人员占公司人数80%，专注端点安全十五年服务经验积累，业内大型案例交付实施最多。

安全服务

以攻击者的视角对企业互联网进行持续风险监控，全网漏洞发现与快速预警，自动化上线前安全评估。

联软科技
LEAGSOFT

THANKS

构建可控的互联世界