志翔科技
ZSHIELD INC

远程办公安全管控解决方案

使能远程办公，保障数据安全

2020. 02. 14

远程办公的两大主要问题

如何防止黑客攻击

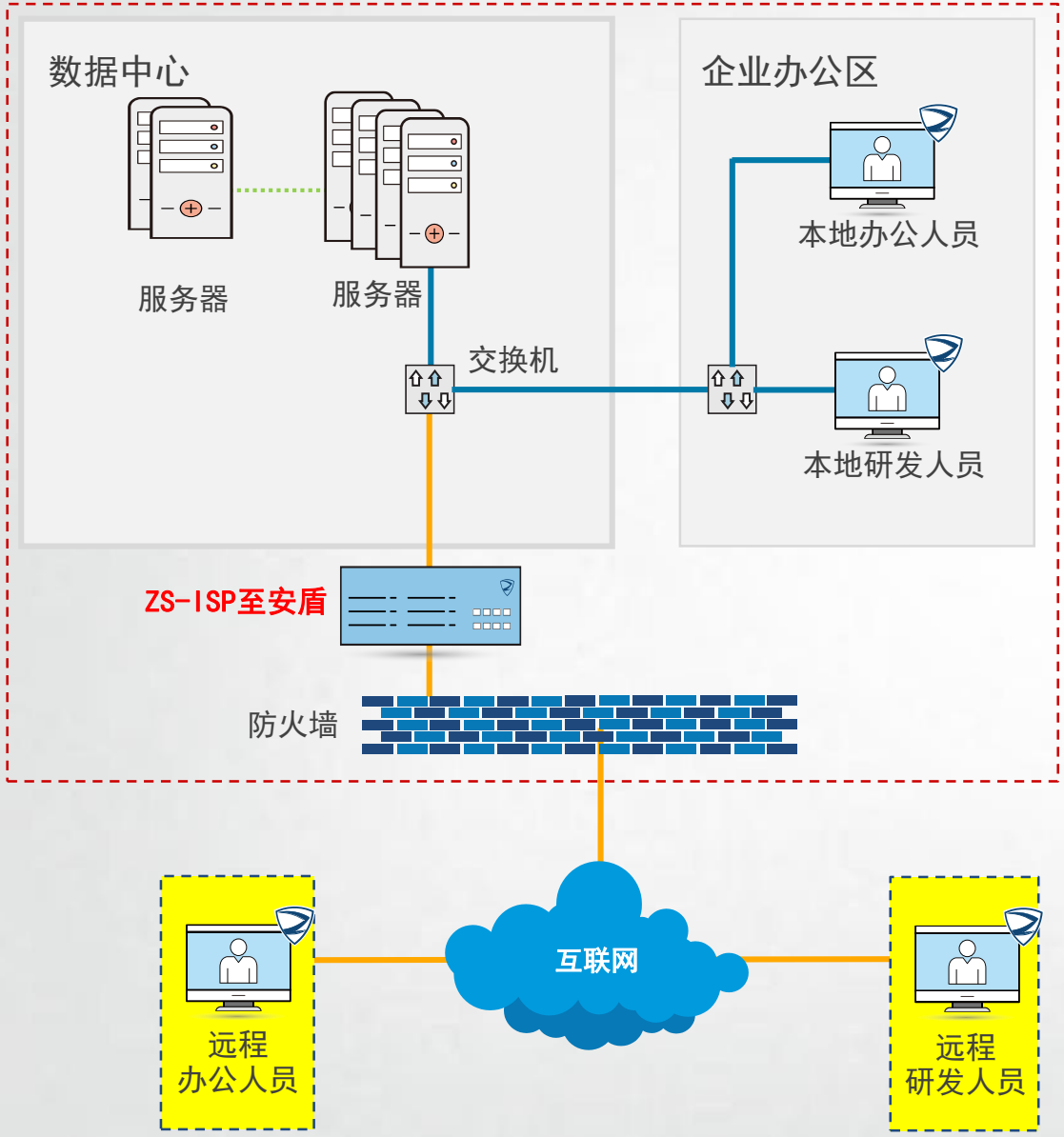
- 远程设备本身不够安全，传输过程面临黑客攻击等风险，进而威胁到内网的安全

如何防止数据外泄

- 员工缺乏监督，数据可能下载至本地，拷贝截屏和违规操作难管控，很难监管审计，数据外泄风险大

志翔的解决方案完美地解决了这两个问题

解决方案——概要

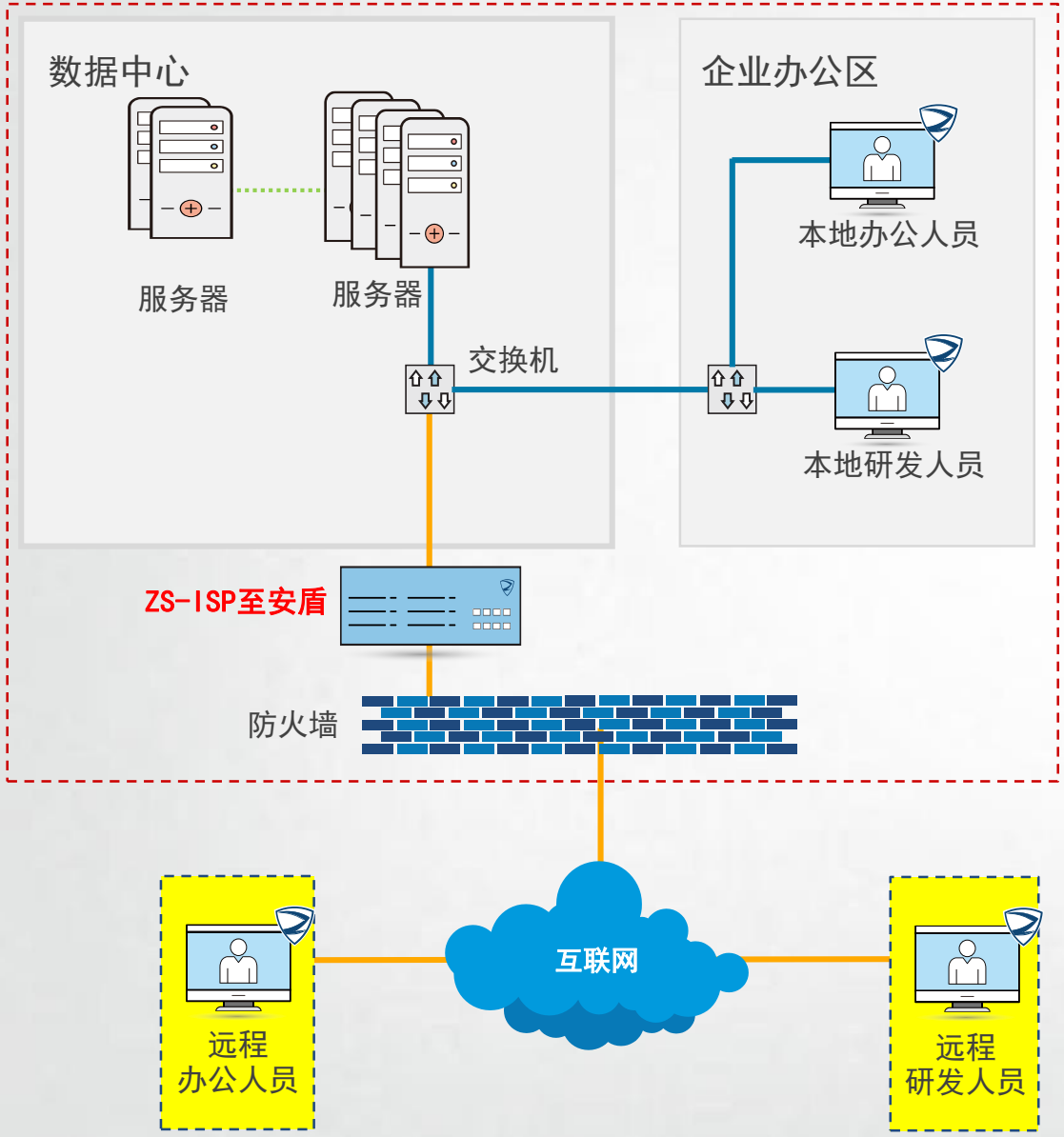


方案概要：

本方案为企业提供了极为高效且安全的远程办公环境，可以将企业内部的PC电脑、虚拟机、工作站、应用服务器等运行的系统桌面交付给远程用户，在家办公像跟在公司办公一样，操作及性能均“类似本地”，尤其适合中小型企业的远程办公及远程研发工作。

1. 数据安全有保障，数据不外泄，可灵活对用户开启和禁止数据上传、数据下传、剪切板复制粘贴等权限；不怕黑客攻击。
2. DPD高效传输协议，远程访问速度极快，连接带宽占比小，在低带宽情况下连接稳定。
3. 会话暂停和恢复功能确保在远程连接中断或远程访问客户端崩溃时不会丢失任何工作；用户可随时在一台设备上挂起工作，之后在另一台设备上恢复之前的工作。

解决方案——使能远程办公



使能远程办公：

1. 至安盾部署在企业防火墙后接入内部网络。
2. 将至安盾桌面服务映射到互联网。
3. 远程用户下载并安装客户端。
4. 远程用户通过客户端登录至安盾，即完成接入公司数据中心服务器工作。

注：

a) 至安盾融合了网络安全接入、数据安全管理、桌面调度和虚拟桌面系统。用户可按需灵活选择整体解决方案；如果用户已自有桌面系统，也可基于其现有桌面系统来使用至安盾的安全接入、数据安全管理和桌面调度等功能。

b) 至安盾不依赖于VPN，用户既可以登录VPN后再登录至安盾，也可以直接登录至安盾接入（取决于公司安全规则）。

c) 如果企业内网有多张子网，至安盾能让用户按不同权限分配远程接入多张网。

解决方案——保障数据安全

志翔科技 ZSHIELD INC

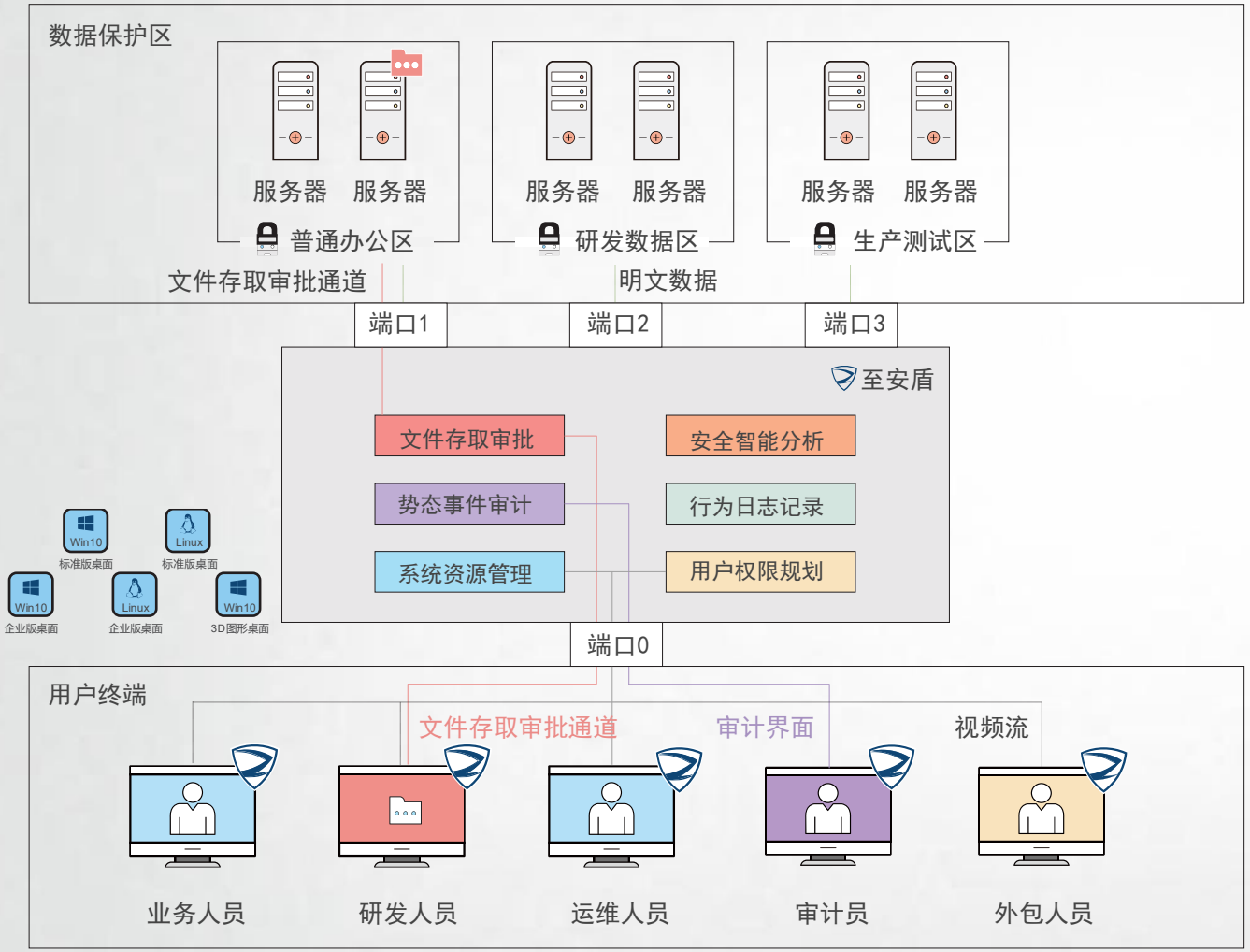
数据不外泄：

- 文件被隔离：
  - 保持企业工作环境与远程终端的隔离，企业办公文档、研发资料始终存储在企业内网，无法泄露。
- 数据不落地：
  - 远程终端只以视频流方式显示桌面操作的影像，实际数据不会传输和存储到远程终端上。
- 内容出不来：
  - 远程用户无法对核心数据区内容进行复制粘贴、截屏、录屏等操作，内网工作内容无法保存到终端。
  - Windows虚机支持桌面水印功能，防止用户进行屏幕拍摄。

不怕黑客攻击：

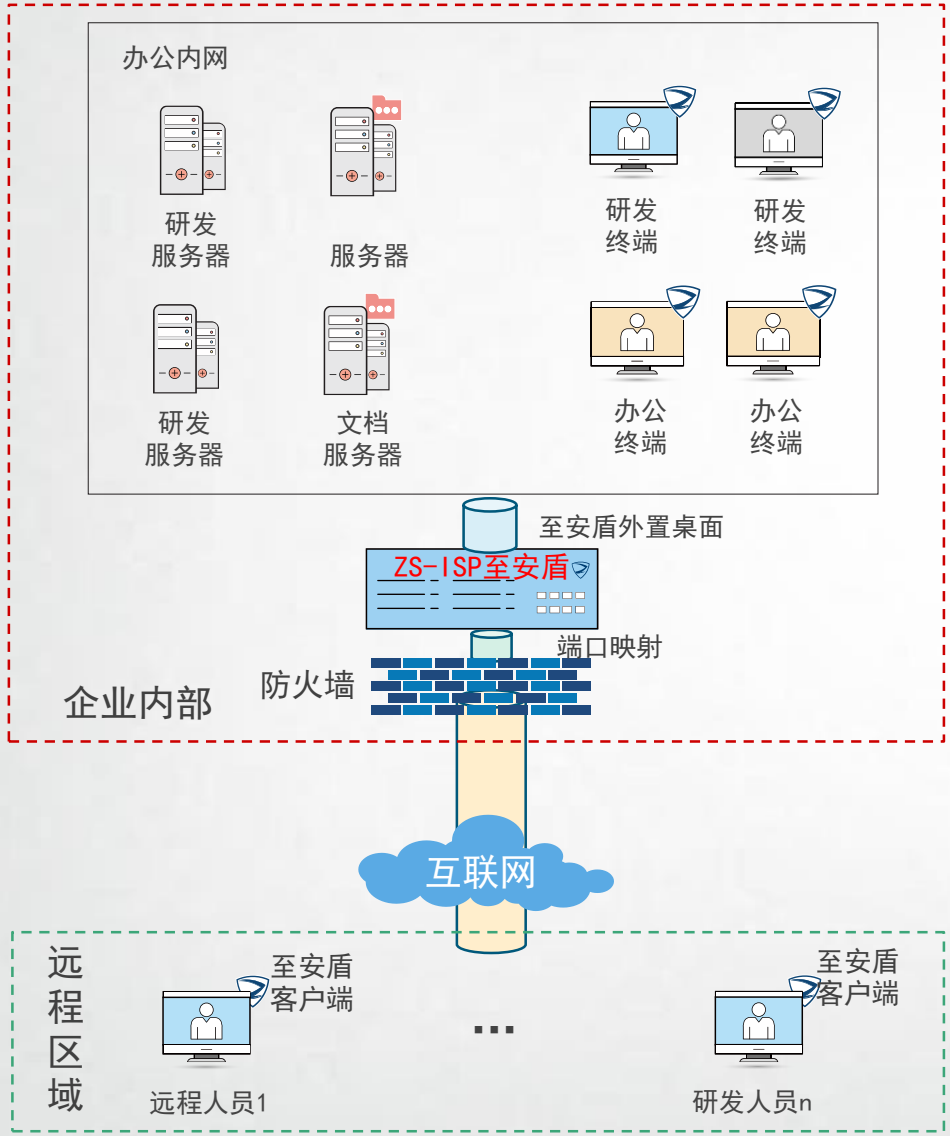
- 内部三道防线提升网络攻击防御能力
  - 内置防火墙
  - 私有状态登录协议防止各种针对桌面服务端口的攻击
  - 客户端不在线自动关闭桌面服务，降低攻击可能
- 信道加密
  - 防止信道窃听
- 控制攻击来源
  - 通过限制用户、登录时间、登录地点来降低攻击来源
- 记录登录行为，安全看得见

解决方案——附加功能



- **多区隔离**：将人员与业务系统和数据相隔离；支持多个安全区域，区域之间彼此隔离。数据访问过程中数据不落地。
- **文件流转**：对不同人员之间的跨安全区域文件流转进行审批管理，文件流转可控且高效。保留日志记录，支持流转文件备份。
- **安全审计**：持续不间断监控，保留完整的日志记录，并利用大数据技术进行可视化智能分析和审计，保证行为可追溯。安全事件自动推送报警、用户日志可回溯10年。
- **外设支持**：同时支持底层及上层两种USB重定向技术，可快速适配U-KEY、U-link仿真器等USB终端设备，也可支持网络打印机等常用外设。
- **四权分立**：业务人员、系统管理员、审批员和安全审计员四方各司其职，相互制约。

案例1：远程直接接入企业员工内网主机



客户环境：

- 某新兴高科技企业300人。至安盾系统对接企业原有的员工主机，并提供安全接入、数据安全管理和桌面调度等功能。
- 至安盾在企业内网旁路部署，在防火墙配置规则仅允许接入至安盾。
- 企业无VPN设备。
- 在员工内网主机上打开Windows RDP远程访问服务。

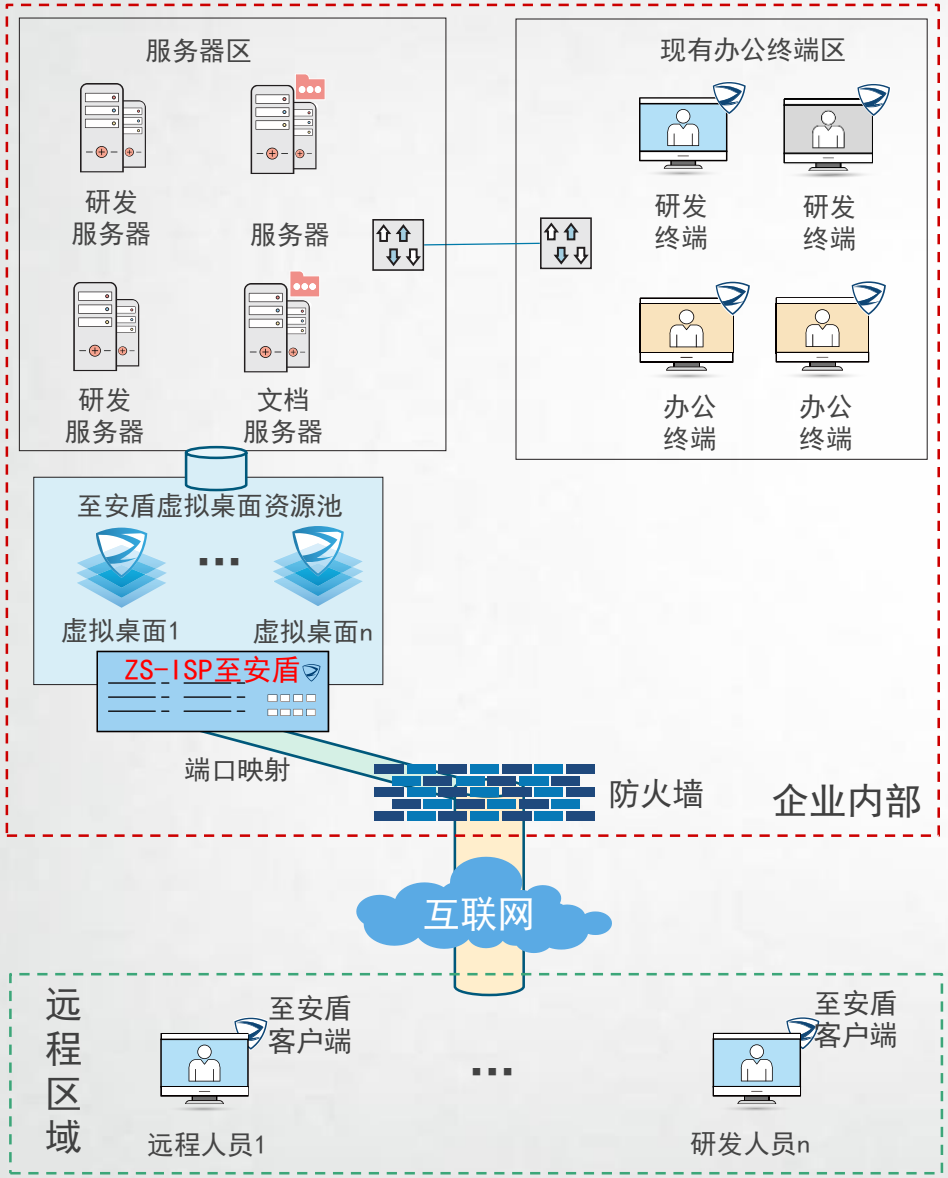
用户操作：

- 远程用户启动至安盾客户端，输入企业外网固定IP地址和用户名密码，登录至安盾桌面开始办公。

使用效果：

- 员工从远程终端直接登录原有内网主机，等同于在企业内网工作，并且保障数据没有泄漏风险。

案例2：远程直接接入至安盾虚拟桌面



客户环境：

- 某软件开发企业远程用户500人，新购配有虚拟桌面的至安盾集群系统。
  - 办公人员400人，每人配置4c8g的Win10桌面；
  - 研发人员100人，每人配置8c16g的Win10桌面。
- 至安盾在企业内网旁路部署，在防火墙配置规则仅允许接入至安盾。
- 企业无VPN设备。

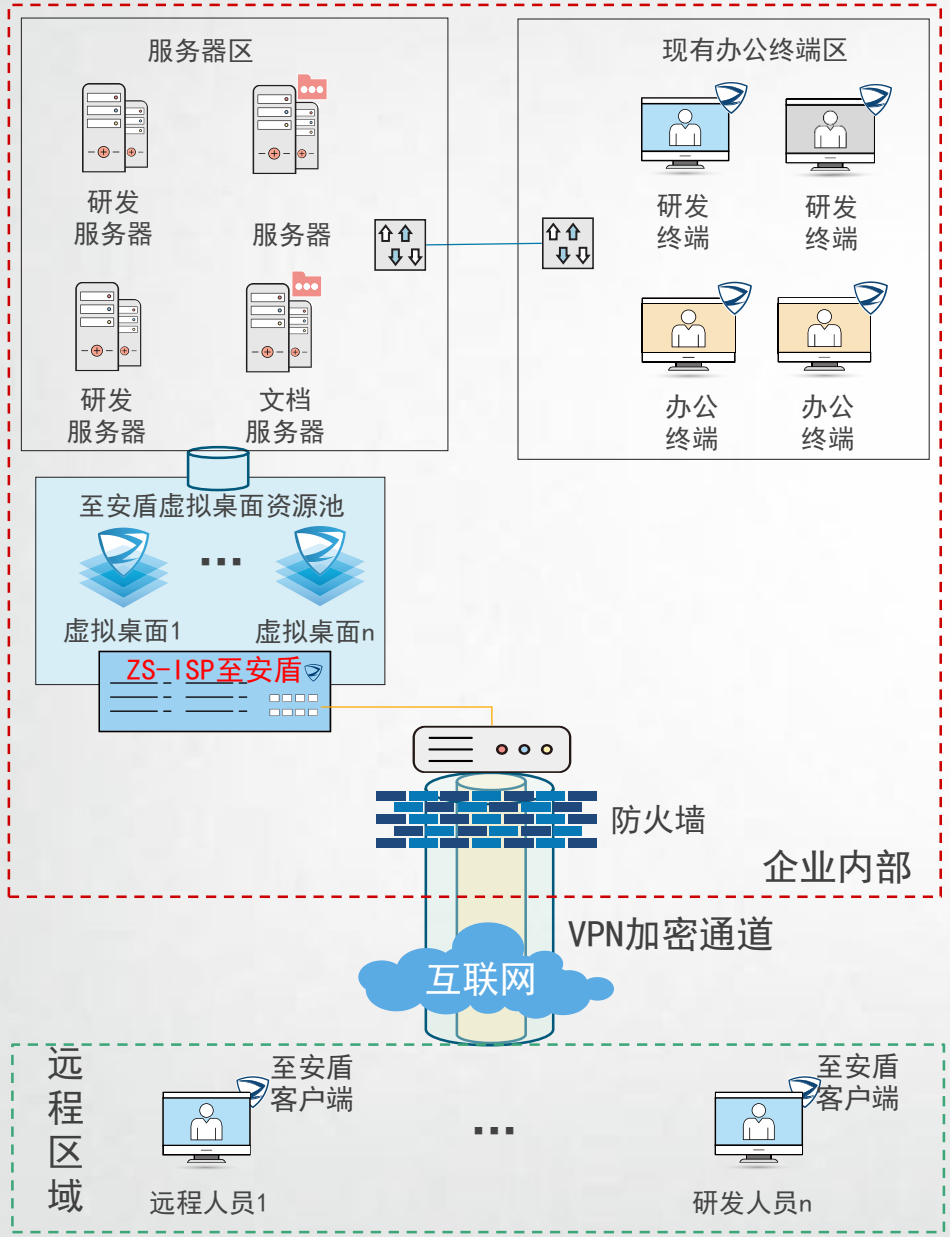
用户操作：

- 远程用户启动至安盾客户端，输入企业外网固定IP地址和用户名密码，登录至安盾桌面开始办公。

使用效果：

- 远程工作，数据不泄露：远程研发人员能使用IDE工具进行代码开发，远程办公人员能使用U-KEY来来访问ERP等企业核心系统。
- 数据没有泄漏风险，并增加文件存取审批、行为审计等安全功能。
- 不改变内部用户从内网终端对服务器网段的访问方式和使用习惯。

案例3：配合VPN远程接入至安盾虚拟桌面



客户环境：

- 企业原有VPN设备及开通了远程接入服务。
- 某新兴高科技企业研发部近百人，新购配有虚拟桌面的至安盾集群系统，每人配置8c8g的Win10桌面。
- 至安盾旁路部署，在防火墙配置规则确保远程用户与服务器网段相隔离状态。

用户操作：

- 远程用户通过VPN接入至企业办公内网虚拟网段10.0.0.X。
- 然后启动至安盾客户端，输入至安盾集群IP地址和用户名密码，登录至安盾桌面开始办公。

使用效果：

- 远程工作，数据不泄露：远程研发人员能使用IDE工具进行代码开发，远程办公人员能使用U-KEY来来访问ERP等企业核心系统。
- 数据没有泄漏风险，并增加文件存取审批、行为审计等安全功能。
- 不改变内部用户从内网终端对服务器网段的访问方式和使用习惯。

关于志翔

志翔科技 ZSHIELD INC

专注做大数据安全

基于AI的数据安全保护和业务风险管控
基于“零信任”安全理念
“无边界”安全的倡导者
产品国内首创，技术壁垒高，细分市场占有率居首

豪华全面的团队

多次成功创业经验
全球视野、技术实力雄厚
涵盖前政府官员、中外名企高管、行业专家
核心团队均毕业于中美顶级名校

安全界的新星

2019 Gartner CWPP市场指南入选厂商
2018、2019连续两年蝉联中国网络安全企业50强(安全牛)
2017中国大数据安全领域创新者(IDC)

安全产品资质齐备

国家保密局：涉密信息系统产品检测证书
公安部：计算机信息系统安全专用产品销售许可证
中国网络安全审查技术与认证中心（CCRC）：IT产品信息安全认证证书
中国信息安全测评中心（ITSEC）：信息技术产品安全测评证书
军用信息安全产品认证证书

志翔科技
ZSHIELD INC

疫情来临怎么办？远程办公家里干！
远程安全怎么管？志翔产品解忧烦！

电话：4008198880（7*12小时快速响应）
邮箱：contact@zshield.net