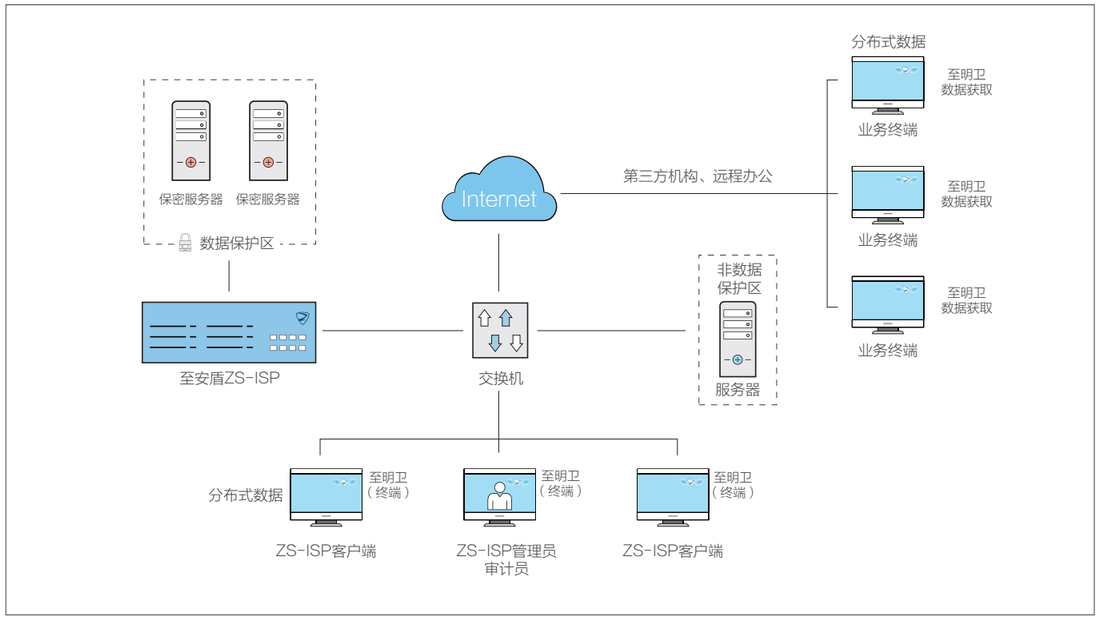
Solution
解决方案

集中式、分布式综合部署

面对复杂部署环境，服务器、用户终端、第三方机构以及远程办公等同时需要数据保护时，通过至安盾隔离管控集中式数据，至明安全探针监测分布式数据，两者联合部署提供完善的无边界智能安全数据方案。方案能够记录行为日志，备份进出文件，快速定位案件，精准锁定证据，有效保障政府和企业的数据资产安全。



关于志翔科技

志翔科技是国内创新型的大数据安全企业，致力于为政企客户提供核心数据保护和业务风险管控两个方向的产品及服务。志翔科技打破传统固定访问边界，以数据为新的安全中心，为企业构筑兼具事前感知、发现，事中阻断，事后溯源，并不断分析与迭代的安全闭环，解决云计算时代的“大安全”挑战。志翔科技是2017年IDC中国大数据安全创新者，2018年安全牛中国网络安全50强企业。2019年，志翔云安全产品入选Gartner《云工作负载保护平台市场指南》。

更多信息

如欲了解有关志翔科技至安盾®ZS-ISP、至明®ZS-ISA安全探针产品的更多信息，请联系您的志翔科技销售代表，或访问官方网站：www.zshield.net

扫码关注志翔

北京志翔科技股份有限公司
www.zshield.net

电话：010-82319123
邮箱：sales@zshield.net

北京市海淀区学院路35号世宁大厦1101
邮编：100191

志翔科技数据安全无边界防护解决方案

新一代网络安全技术，实现无边界的安全统一管控

亮点

- 围绕核心数据资产，提供无边界安全防护
- 全面监控、高效检测、实时预警
- 可视化管理，主动防御，安全状态直观可见
- 节约成本，快捷部署，分钟级上线，支持集群热备
- 安全与效率兼顾，不影响访问及业务操作体验

随着服务虚拟化、分布式计算以及云计算、多形态应用等兴起，企业和政府的工作环境更加便利，网络边界也随之变得更模糊，传统以网络为中心的边界安全模式已经落伍！

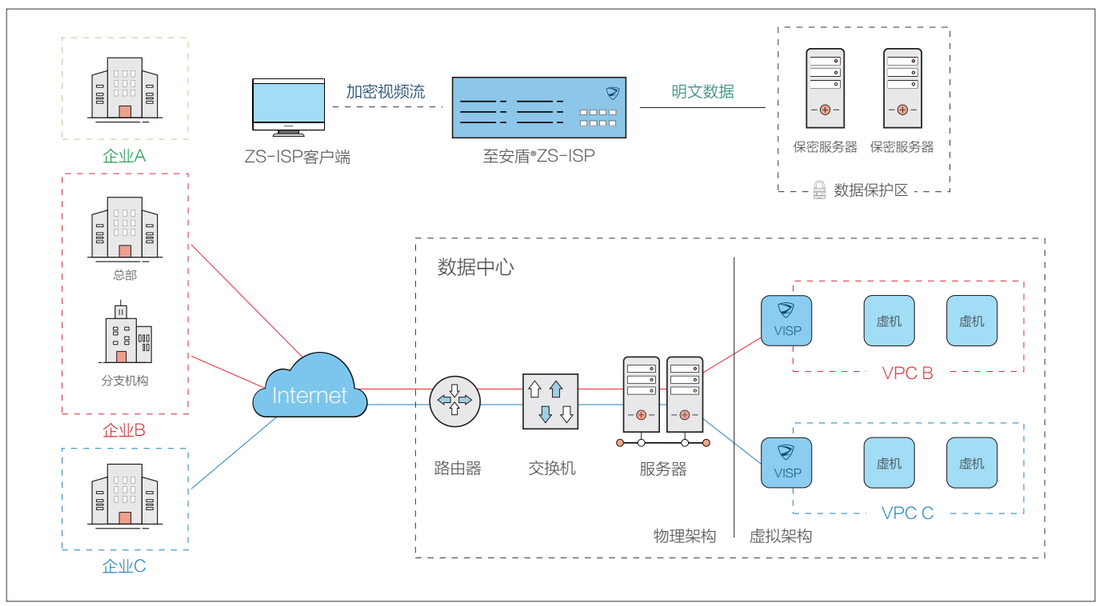
政府和企业核心数据资产包括重要文件、涉密数据、源代码、设计文档等，核心数据资产的泄露不仅会带来不可估量的经济损失，还会严重影响企业社会声誉，甚至带来一系列严重连锁反应。核心数据资产的安全保护上，不仅需要防御潜在的黑客，内部员工及第三方合作机构同样也是巨大隐患。

为核心数据资产提供全面保护

基于至安盾®和至明®安全探针产品，志翔对数据中心与终端提供完整的数据防护机制，有效防范企业核心业务数据泄漏，避免成为下一个数据违规事件的焦点。志翔方案隔离用户与关键数据的接触，精确捕捉并实时记录终端和数据中心上关键数据的操作行为，并可视化展示安全状态。志翔的数据安全方案在安全事件发生之前预警，发生之时及时阻止，发生之后快速追溯、精准定位责任问题到人，并在司法程序中提供有力证据。志翔科技无边界安全解决方案，更先进更全面的保护您的企业数据资产。

集中式数据防护：至安盾®ZS-ISP，虚拟至安盾VISP

将关键数据隔离在数据中心集中管理；数据导入导出需经过严格审批；全面记录并审计数据操作行为，及时预知安全风险，并确保问题可追溯；安全可视化展示，提升企业管理效率。



支持情况：多种系统环境 Windows、win-server、Linux、Mac OS；多种部署方式 企业机房、云端、远程办公、分支机构、外包服务；支持C/S、B/S、混合架构。

隔离管控确保数据不落地

至安盾将办公环境划分为保护区和终端区。敏感数据置于保护区，用户需登录至安盾客户端才能读取和操作。被访问数据经由至安盾服务器，以视频流的形式回传至终端区，终端只呈现其影像，用户无法对其进行拷贝、粘贴、打印、截屏等操作，终端缓存不会留下任何痕迹，杜绝企业内外部用户访问带来的敏感数据泄漏。同时，保护区间相互严格隔离，可根据企业需求动态分配、管理。

审计核查，问题追溯

终端用户在服务器上任何行为都将以系统日志、视频的形式被记录下来，并能按需进行时间点回放，秒杀巡视监查和摄像头监控等原始监控方式。所有数据流转和对数据的操作都会被记录在案，所有审批流程都备案待查，系统可保存10年日志满足审计需要。通过对所有用户行为的实时智能分析，至安盾可精准感知安全风险，第一时间预警违规行为，事中止损。

安全可视化展示，提升企业管理

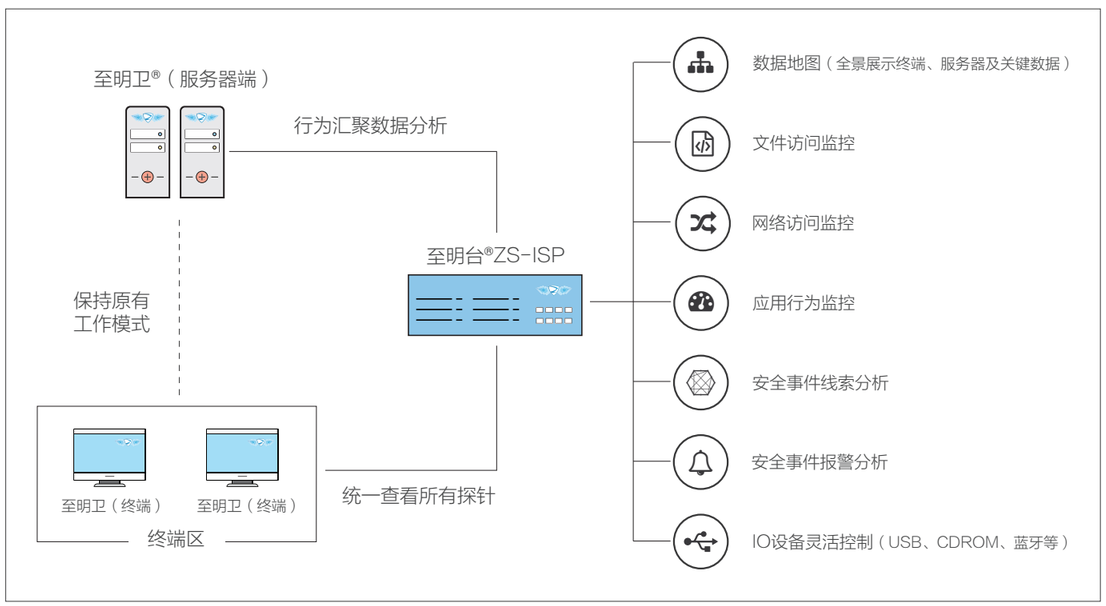
至安盾通过对所记录的日志和数据等进行安全可视化展示，帮助管理人员随时、直观了解企业安全状态，实时预警将导致泄密风险的违规行为。服务器负载可视和历史记录能为IT增加投入提供可执行建议。同时，可对用户工作量进行分析统计，直观化图标展示，给管理层合理分配工作任务提供参考，同时准确监测外包工作量，防止虚报和资源浪费。

保证用户工作效率的同时保证安全

通过领先的技术手段，至安盾可实现远程与本地工作的用户体验一致，并同时做到带宽消耗极低。至安盾通过开辟专门安全上网区，统一管控终端与外网的文件交互，提升研发效率。对于数据的存取，用户需要发起申请，通过审批流程才能上传、下载。同时，可智能鉴别文件类型和设置自动审批策略，节省人工时间，提高工作效率。

分布式数据防护：至明®ZS-ISA安全探针

至明安全探针软件安装于终端、服务器和云主机等设备上，对分布于各设备上的数据进行全方位不间断监控，采集用户行为，形成用于分析的系统日志；可视化数据流向，绘制数据资产地图；对于违规用户行为实时报警；I/O外设智能管理。



支持情况：多种系统环境 Windows、win-server、Linux；多种部署方式 PC、服务器、云主机。

围绕核心数据的智能监控

实时、智能监控核心业务数据文件的使用情况，并对监控获取的日志信息进行过滤和综合分析；监控针对高层有效的用户行为，而非繁琐的的底层进程行为；对可执行的程序进行监控，智能配置管控策略，记录与追踪执行程序来源；对终端用户I/O进行监控，包括网络访问、外设使用情况等。

安全可视化

通过日志分析自动生成核心资产的网络拓扑图，可视化直观显示数据流向关系；对用户行为情况详细展示，包括进程、文件、网络、外设等；　安全状态一目了然，为及时发现违规事件，以及安全隐患提供强有力的技术支撑。

预警违规行为，保护数据

通过志翔大数据智能分析技术，对用户行为进行多维度查询和关联分析，对违规行为实时预警，例如：恶意程序/黑名单程序安装或运行；特定的网络文件下载、移动存储设备文件导出、文件打印；P2P程序的异常使用、网络音频/视频访问等，防止数据泄漏事件发生。

外设智能管控

禁用USB存储，但不影响USB键盘鼠标、U-Key的使用；禁止USB网卡、无线网卡、蓝牙、外设等功能的使用。灵活配置策略可让指定用户使用终端的USB存储功能，操作方便快捷。