志翔科技
ZSHIELD INC

公有云服务安全解决方案

方案价值

- 防止数据和文件泄露
- 阻止服务器被恶意攻击
- 阻断非法终端接入服务
- 简化安全运维，降低运维成本

方案亮点

- 分布式感知对异常进行精确定位和阻断
- 大数据分析对行为进行持续审计和追溯
- 利用桌面虚拟化，防止数据被直接下载
- 严格且可灵活配置的数据文件审批流程
- 实现云端旁路部署，毫不影响现有业务

公有云服务安全解决方案通过将系统安全、数据安全、应用安全和网络安全有机结合，实时防护与拦截来自非法终端和互联网的恶意攻击、木马病毒和风险请求。

在业务系统部署在公有云的情况下，充分考虑数据信息安全要求，以至明®安全策略平台和至安盾®智能安全平台为核心，采用准入控制、网络隔离、信息管控、日志分析审计和行为追溯等手段，在公有云中，构建区域安全“内网”，并实现安全可视化。

在保证安全的同时，使用者完全无感，将对工作效率的影响降到了最低。同时，以大数据分析技术和数据可视化技术持续、精准地发现数据资产安全异常情况，提供全方位的数据信息安全保护。

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

业务痛点

公有云安全基础薄弱

公有云主要目标是面向所有用户提供开放服务，尚无成熟的安全解决方案使得公有云服务达到私有云的安全级别；且服务和数据托管在公有云上，企业对其掌控力度较弱。

非法接入云端服务

基于公有云提供服务，使得非法人员与非法应用接入云端服务，造成数据泄露、系统破坏、木马种植和传播等风险发生的概率将极大增加。

云服务器被攻击与劫持

公有云的服务器容易遭受来自互联网的各类攻击，造成服务瘫痪、数据泄露甚至服务器被完全劫持；另外，来自公有云内部的攻击，更容易造成数据泄露。

运维与管理成本高

运维、办公与研发人员从不同的设备与端口接入云端，导致网络架构复杂，管理成本高企，而且存在安全隐患。

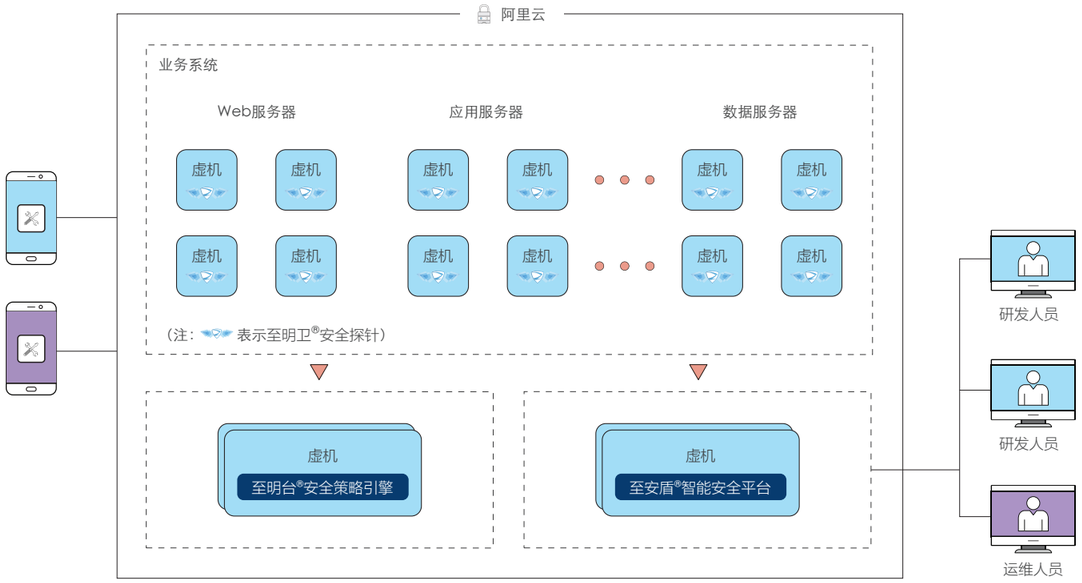
解决方案

至明安全策略平台包括至明卫®和至明台®两部分：

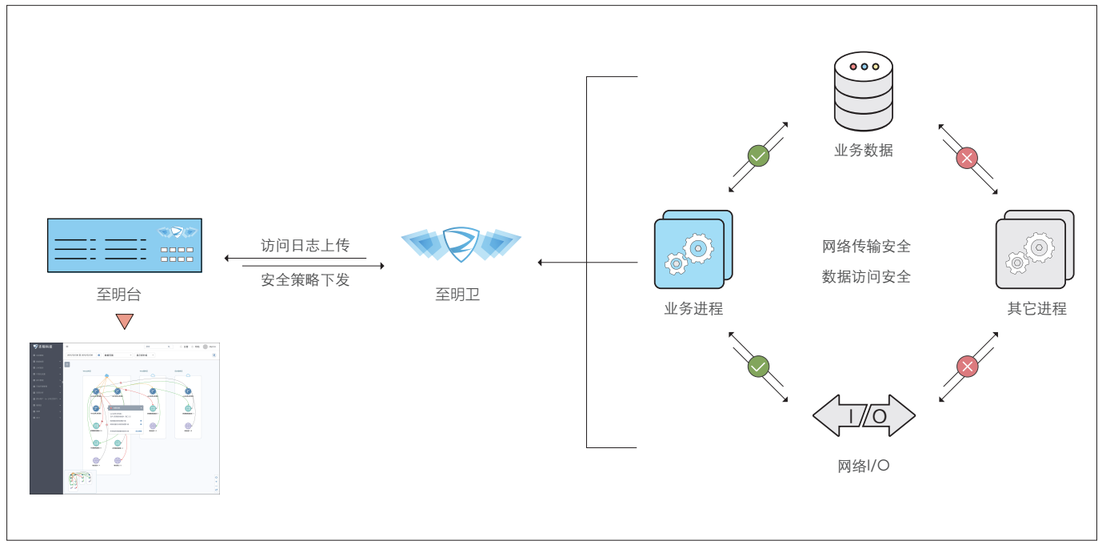
至明卫是轻量级安全探针，支持域内一键静默安装，自动升级；至明台旁路部署于公有云上，负责配置和管理至明卫的安全策略，是智能可视化数据和网络安全策略引擎。

至安盾智能安全平台基于“零信任”实现数据不落地的操作，防止研发、运维等特权人员对服务进行篡改与对数据进行窃取。

针对企业在公有云（例如阿里云）上的虚拟机服务器，在所有支持业务系统的虚拟机服务器上安装至明卫安全探针，在其它虚拟机服务器上并行部署至明台安全策略引擎，用以管控全部至明卫安全探针；在另外的虚拟机服务器上旁路部署至安盾智能安全平台，将业务系统和人员隔离，实现对业务系统虚拟机服务器上数据的管控。



解决方案部署示意图



云服务端安全策略示意图

功能优势

数据安全

通过安全探针建立云可信基础环境，防止数据被窃取和滥用；建立业务数据的云端全局资产地图；对系统异常运行、数据异常流动自动报警。

网络安全

通过安全探针建立云端的分布式隔离网络，防止服务器被恶意攻击；建立云端业务数据流向关系图；对异常的网络访问进行阻断和报警。

行为监控

至明卫安全探针将日志发送给至明台安全策略引擎；通过大数据安全分析自动发现异常行为；所有行为留痕，所有安全事件都可以被定位和追溯。

研发人员和业务系统升级管控

安全虚拟桌面隔离用户和核心数据；智能高效的数据和文件流转管控；系统升级包的分发和安装管控。

安全运维管理

建立云端运维的统一安全入口，数据不落地；建立面向云端的特权凭证、超级凭证管理体系；对云端操作进行全息安全审计。

可视化和高效的安全审计

文件存取和系统接入的日志分析与审计；可视化展示审计内容；安全事件自动推送报警。

场景及案例

业务系统放在公有云上时，该方案可基于开放的公有云，建立安全可靠的区域安全“内网”，保证服务稳定运行且数据不泄密、不丢失，既能为系统的安全运行和用户访问提供保证，又能确保数据安全；政府、科技、教育、电力等对安全要求较高的行业，在公有云中运行的系统，非常适合使用该方案进行安全加固。该方案已在国家电网某省电力公司输电通道看护移动互联网作业系统中应用。