志翔科技
ZSHIELD INC

大数据平台安全解决方案

方案价值

- 防止数据窃取和泄露
- 确保数据合规使用
- 避免数据孤岛产生

方案亮点

- 提供数据不落地的访问方式以及完善的文档审批和流转功能
- 提供五种安全策略和四道安全防线
- 提供严格的用户权限管理和强大的用户行为审计和追溯功能
- 提供高性能、高可靠稳定运行的大数据使用环境

大数据平台安全解决方案为大数据平台提供完善的数据安全防护体系，保护核心数据资产不受侵害，同时保障平台的大数据能被安全合规的共享和使用。

数据安全防护体系以至安盾®智能安全平台为核心进行建设。智能安全平台支持三权分立、安全分区、数据流转、报警预警和审计追溯等五种安全策略，以及嵌入式防火墙、访问控制、桌面水印等四道安全防线，保证安全体系在系统安全接入、安全运维、数据流转、数据使用、数据导出脱敏、用户管理、用户行为审计追溯等方面的建设，保障大数据平台安全高效运行。

智能安全平台提供安全桌面云，保证数据不落地的访问方式，并可根据需求提供高性能计算资源和图形处理资源，并支持“N+M”高可靠性架构，保证桌面云的稳定运行，为平台用户提供安全高效的数据使用环境。

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，2020年数世咨询评选的中国网络安全百强企业，并获中国网络安全产业联盟（CCIA）“2020年中国网络安全成长之星”（CCIA成长之星），以及赛博英杰《2020年中国网络安全十大创新方向》代表厂商。2019-2020年，志翔科技的至明产品连续两年入选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：contact@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

数据泄露的风险增大

大数据平台将业务系统产生的各类数据汇集在一起，数据量巨大；同时，大数据平台用户类型和数量多。这些因素增大了大数据平台被攻击造成的数据泄露的风险，也增大了因内部管理疏忽造成的数据窃取和泄露风险。

有形成新数据孤岛的风险

目前大数据平台的安全措施，主要是通过账号对数据访问权限进行控制，不同类型或不同渠道汇集来的数据需要不同权限才能访问，往往造成大数据分析得不到足够有效的数据支持，即使在数据集中的情况下，也有形成新数据孤岛的风险。

数据被滥用的风险增加

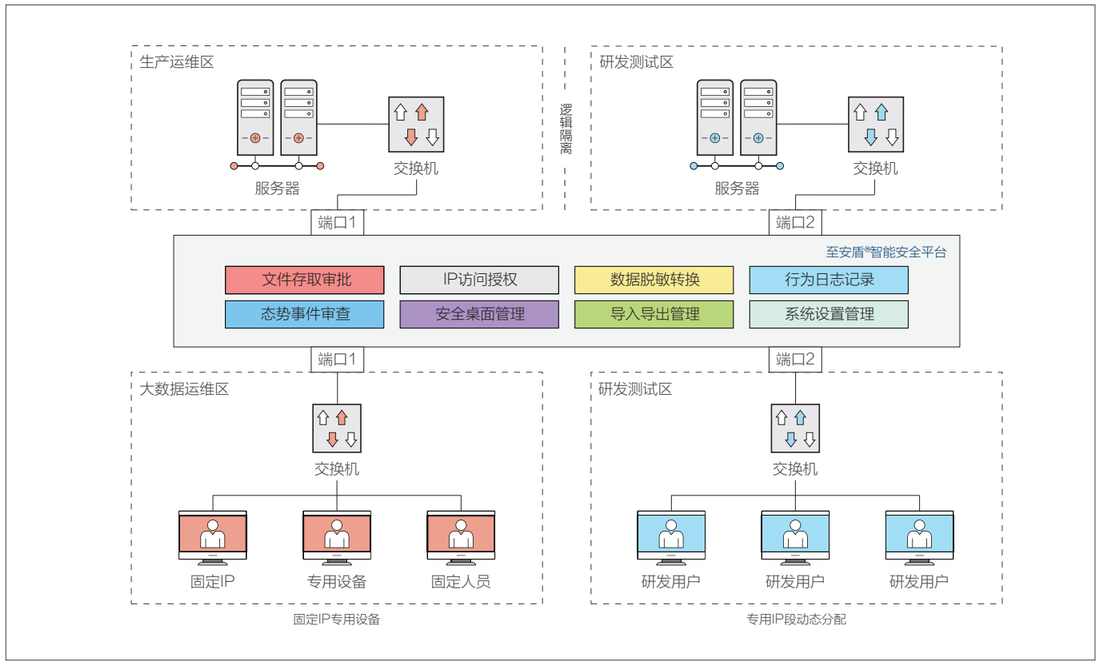
大数据平台一旦建成后，若没有科学合理且安全稳固的数据使用管理，很容易造成数据被滥用，导致普通用户的隐私泄露和公司的经济损失等伤害。

安全运维成本增高

大数据平台建成后，集中了大量有价值的数据。使用一般的网络和数据防护手段，在安全运维方面的人员和设备投入都比较大，增加了整体安全运维成本。

解决方案

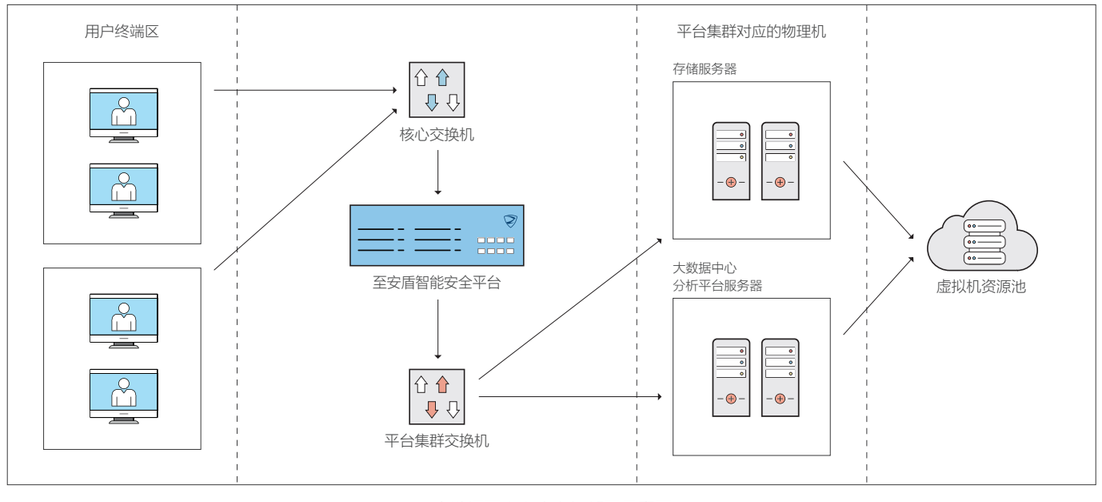
基于至安盾部署，基于至安盾支持的三权分立、安全分区、数据流转、报警预警和审计追溯等五种安全策略以及嵌入式防火墙、访问控制、桌面水印等四道安全防线，在安全平台中实现安全桌面云管理、文件存取审批、IP访问授权、数据脱敏转换、行为日志记录、态势事件审计、导入导出管理以及系统设置管理等安全功能。安全桌面云将人与分析环境和数据隔离，保证数据不落地的访问方式；利用安全分区将数据使用分为生产运维区和研发测试区，生产运维区的数据需经过脱敏并经审批后流转到研发测试区，研发人员在研发测试区进行开发、测试等研发工作，进一步保证了数据使用的安全性。



大数据平台安全架构图

部署方式

大数据安全解决方案部署简单，配置快捷，采用旁路部署的方式将用户和大数据平台隔离，形成安全防护系统，不影响大数据平台原有的IT架构和网络拓扑。



大数据平台安全实施部署示意图

功能优势

网络安全防护

基于嵌入式防火墙、访问控制、系统水印等四道安全防线，有效减少来自内外网的网络攻击威胁，尽可能降低大数据平台被攻破的风险。

数据安全防护

通过桌面云将人和数据隔离，实现数据不落地的访问方式，有效减少数据泄露风险；同时辅以安全分区和桌面云接入权限，进一步对数据安全进行加固。

用户行为审计追溯和安全可视化

对网络和数据进行安全防护，并对用户使用数据的行为进行监控和日志记录，所有行为留痕，进行审计并确保所有安全事件可被定位和追溯。与此同时，基于大数据技术进行安全分析发现异常行为并进行预警或报警，实现安全可视化。

实现真正的数据共享

基于严密的网络安全防护、审计追溯和安全可视化措施，使得大数据平台的访问和数据使用得到严格的安全保障，从而让平台用户真正获得数据共享带来的便利，推动大数据业务的健康发展。

场景及案例

可满足中各类大数据平台的安全保障需求，如统一大数据中心的安全保障、不同业务大数据平台的安全保障、不同业务大数据平台间的数据交换和流转安全保障等。目前已应用于国网计量中心营销大数据分析平台，保证数据安全及合规使用。