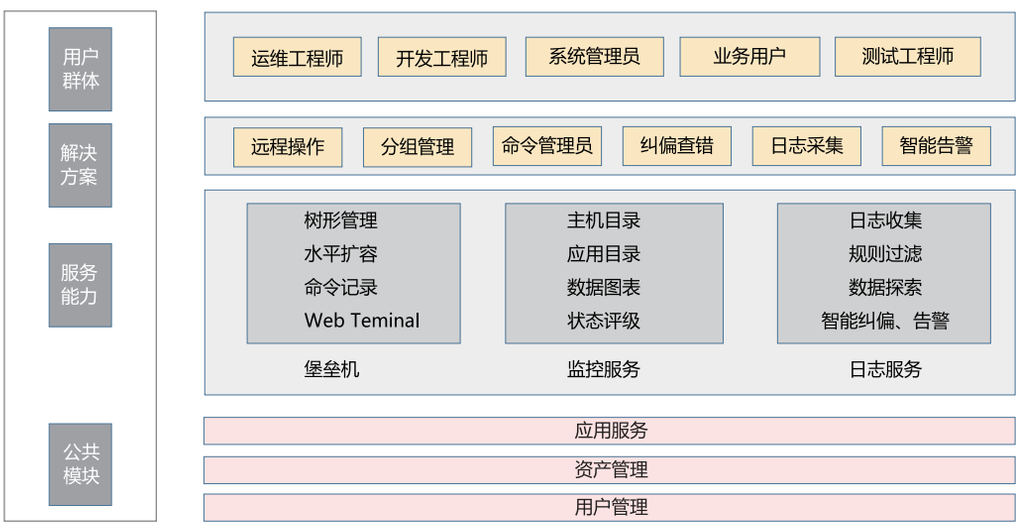
XMonitor 智能管理工具

集堡垒机、日志分析、应用性能监控于一体的智能运维工具，抛弃低效被动运维管理，实现业务稳定运行。

XMonitor简介

XMonitor是逸迅科技研发集堡垒机、日志分析、应用性能监控于一体的智能运维工具。不仅提供服务器安全检测、集中身份认证，集中访问授权，还提供灵活的通知机制，让系统管理员快速定位/解决存在的各种问题，多服务日志汇聚管理，海量运维知识库提供自动化运维脚本推送，服务器出错自动修复等功能。

XMonitor安装配置简单，学习成本低，基于web界面管理，极简的操作体验完胜传统堡垒机。分布式架构设计无限扩展，容器化部署方便快捷。有效提升运维效率，节约企业运维成本。



图一：产品架构图

产品优势

提供六大智能能力

智能感知监控 | 智能检测预警 | 智能分析决策 | 智能场景匹配 | 智能资源调配 | 智能安全保障

五大核心价值

√ 提高系统感知能力

√ 降低故障持续时间

√ 维持系统高可用

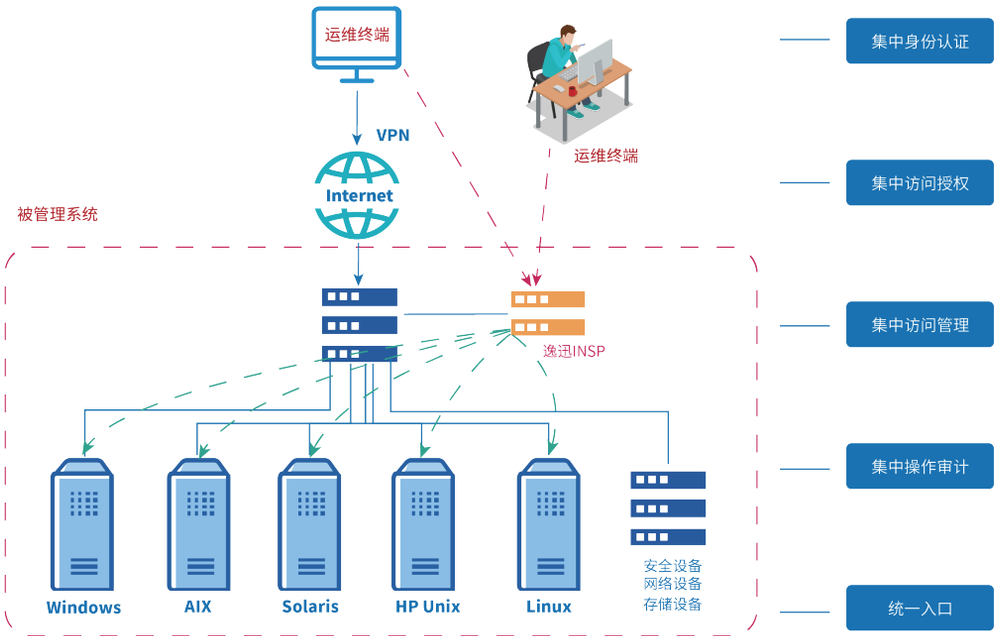
√ 保障系统稳定度

√ 拥有极佳的用户体验

产品功能

1. 服务器集中身份认证、访问授权、访问管理

传统服务器运维存在诸多的安全隐患，XMonitor通过切断终端对计算机网络和服务器资源的直接访问，采用协议代理的方式接管终端计算机对网络和服务器的访问；通过细粒度的安全管控策略，保证企业的服务器、网络设备、数据库、安全设备等安全可靠运行，降低人为安全风险，避免安全损失，保障企业效益。



图二：访问控制管理

√ 健全的用户管理机制和灵活的认证方式

为解决企业IT系统中普遍存在的因交叉运维而产生的无法定责的问题,平台提出了“集中账号管理“的解决办法；集中帐号管理可以完成对帐号整个生命周期的监控和管理，而且还降低了企业管理大量用户帐号的难度和工作量，同时，通过统一的管理还能够发现帐号使用中存在的安全隐患，并且制定统一、标准的用户帐号安全策略。

√ 多种密码保护方式

针对平台中创建的运维用户可以支持静态口令、动态口令、数字证书等多种认证方式；新的认证方式通过证书避免身份伪造，通过动态token避免证书丢失后的身份假冒，能够最大程度保证安全

√ 细粒度、灵活的授权

系统提供基于用户、运维协议、目标主机、运维时间段等组合的授权功能，实现细粒度授权功能，满足用户实际授权的需求。授权可基于：用户到资源、用户组到资源、用户到资源组、用户组到资源组。

2. 提供分布式系统监视、网络监视以及数据收集功能

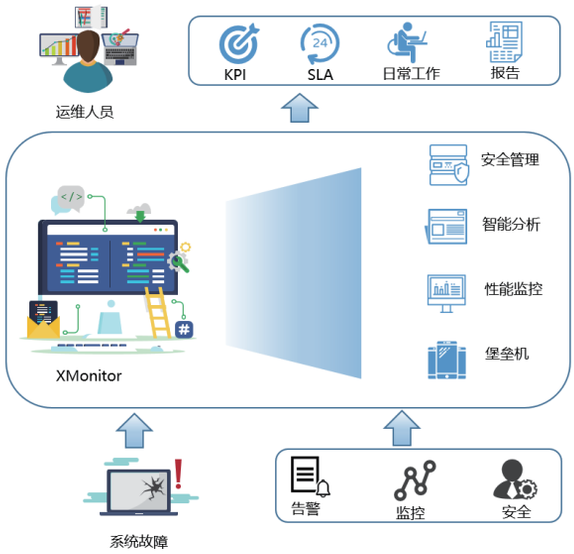
XMonitor通过监视各种网络参数，保证服务器系统的安全运营。可以通过SNMP、ping，端口监视等方法提供对远程服务器/网络状态的监视，数据收集等功能，并提供灵活的通知机制以让系统管理员快速定位/解决存在的各种问题。

√ 全面监控

提供CPU负荷、 内存使用、磁盘使用、 网络状况、 端口监视、日志监视等监控指标，监控正在运维的会话：信息包括运维用户、运维客户端地址、资源地址、协议、开始时间等；监控后台资源被访问情况，提供在线运维操作的实时监控功能。针对命令交互性协议，可以实时监控正在运维的各种操作，其信息与运维客户端所见完全一致。

√ 提供灵活的通知机制以让运维人员快速定位/解决存在的各种问题

用户可以新增自定义触发器，并设置触发规则，当收集的数据指标达到触发条件时，系统提供email或微信方式告警，帮助运维人员快速定位和解决存在的故障。



图三： 多维度运维监控

3. 智能分析与告警、运维自动化

XMonitor将基础监控、特性监控等现网各种日志，通过Logstash收集至日志中心，经过一系列的筛选，提取一些特征，计算一些中间值，形成全连路数据，通过Elasticsearch做搜索和分析，最终给出异常和告警通知。

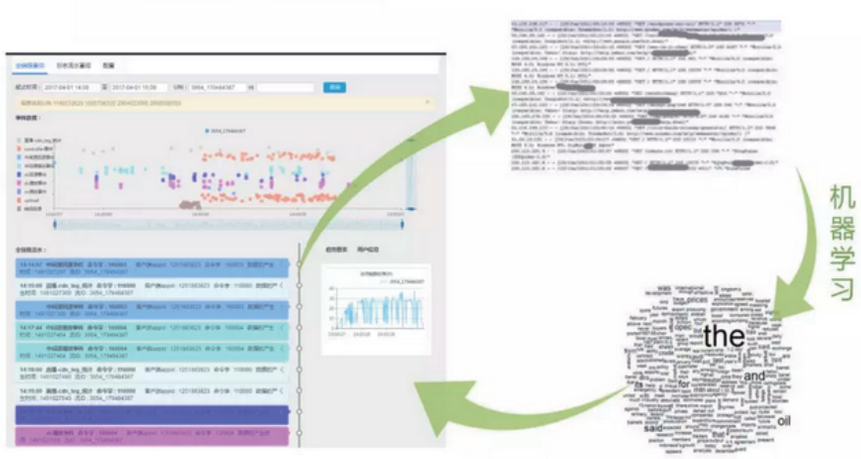
√ 运维自动化

动改密：通过定制任务计划，定期去修改服务器、网络设备的密码。不仅满足等保的密码管理要求，还定期回收下发密码，可有效减少非法登录的可能。

自动运维脚本推送：通过定制任务计划，定期自动登录到服务器、网络设备执行预订的脚本，可实现批量服务器状态检查、网络设备配置备份等任务。

√ 机器学习

通过Logstash收集到的文本日志，通过机器学习中的自然语言处理 (NLP) 方法，找出异常。告诉 AI 规则是什么，让机器首先去做一些粗判，人工去做一些监督，训练机器对错误信息有准确的判断，从而实现故障自愈，实现自动化处理。



图四：机器学习自动处理

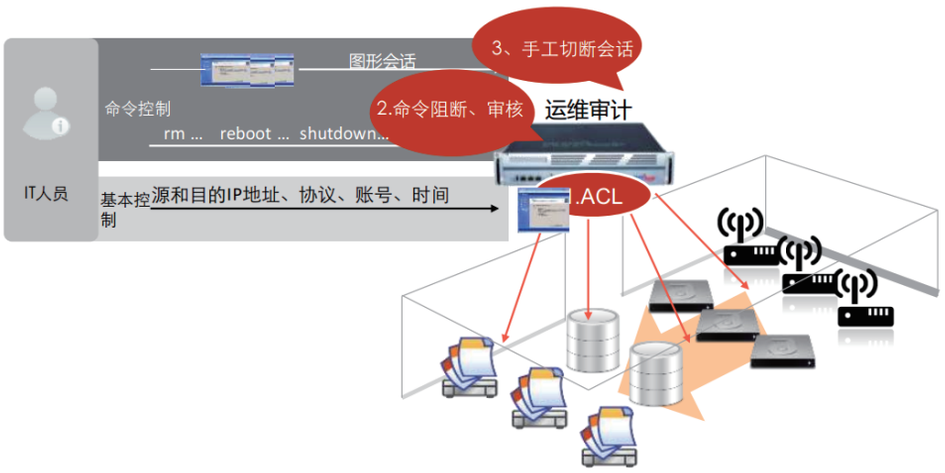
4.操作审计、用户操作内容录像回放

超全的审计协议范围平台采用协议分析、基于数据包还原虚拟化技术，实现操作界面模拟，将所有的操作转换为图形化界面予以展现，实现审计信息不丢失。

√ 全面监控

√ 运维事件事中控制

实时监控正在运维的会话，信息包括运维用户、运维客户端地址、资源地址、协议、开始时间等；监控后台资源被访问情况，提供在线运维操作的实时监控功能。



图五：运维操作实时监控

√ 违规操作实时告警与阻断

针对运维过程中可能存在的潜在操作风险，XMonitor根据用户配置的安全策略实施运维过程中的违规操作检测，对违规操作提供实时告警和阻断，从而达到降低操作风险及提高安全管理与控制的能力。

√ 详尽的会话审计与回放

提供图像形式的回放，真实、直观、可视地重现当时的操作过程；回放提供快放、慢放、拖拉等方式，针对检索的键盘输入的关键字能够直接定位定位回放；

√ 丰富的审计报表功能

XMONITOR平台能够对运维人员的日常操作、会话管理、审计平台进行的操作配置以及报警次数等做各种报表统计分析。

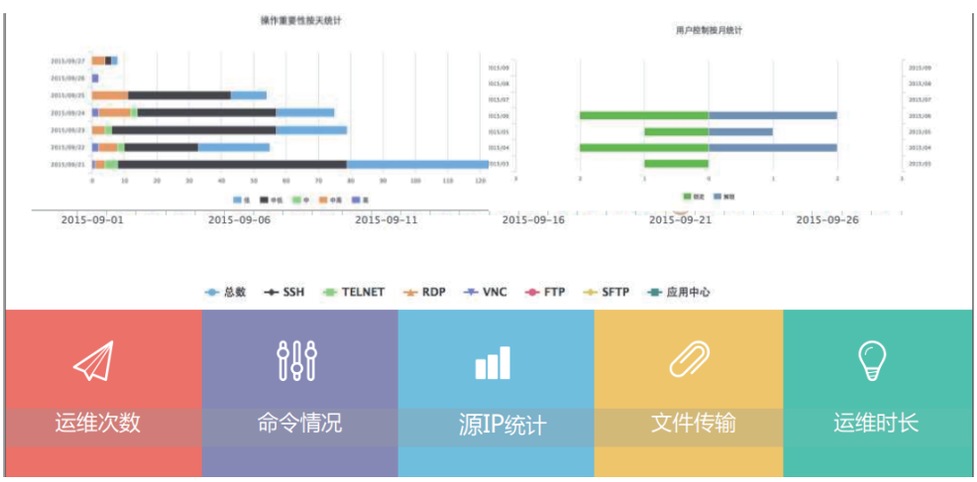


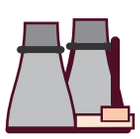
图 六：运维情况统计

典型应用领域：

公安

金融

银行



政企