UniSIMS服务器安全管理系统

业界首款服务器自适应安全产品

UniSIMS 服务器安全管理系统是业界最早采用自适应安全理念的服务器安全管理产品，是能够根据服务器的资产和状态提供评估和整改指引的安全基线检测工具，为大型机构解决服务器安全管理问题提供直接支撑。

UniSIMS 以信息资产为基础驱动安全基线管理流程，对成千上万的服务器进行集中安全管理。提倡资产驱动自适应安全检查，可发现、识别和跟踪生产服务器上的操作系统、数据库、Web 应用软件等信息资产的安全参数属性，从而自动检查各项安全基线，达到全面和精准核查的要求；能以天或更短的时间周期进行安全基线检查和监控，实现安全的实时检测，最终达到检查精准性、全面性、实时性、高效性的整体目标。

主要功能

资产管理

- 自动发现网络中的服务器设备
- 自动清点服务器上的操作系统、数据库、中间件
- 自动清点服务器上的 web 站点、web 应用
- 自动清点服务器上的大数据组件

基线检查

- 对资产进行安全基线检查并提供检查报告
- 对资产进行安全基线检查并提供整改指引
- 对安全基线的检查结果进行分析统计

异常告警

检查用户、进程等的状态，进行比对，发现异常的安全状态变化并进行告警

主要优势

功能

- 资产清点：自动对服务器上的操作系统、数据库、中间件、web 应用进行自动采集和分析
- 自适应安全基线检查：精准全面获取资产和系统脆弱性，避免出现检查不到位；免手动

搜集资产，免操作系统口令完成每一次的基线检查任务

- 安全基线实时检查：每个服务器被实时监控，任意时刻执行安全基线检查，提供安全趋势图帮助判断当前的安全基线合规趋势
- 安全状态实时监控： 实时呈现，报告用户、进程等变化并根据风险性进行相应的告警，提供全局搜索和统计表格帮助判断当前主机面临的风险
- 基线裁剪、变量自定义：提供弹性的基线检查标准，帮助组织在建立安全基线标准时更灵活的配置和检查方式
- 支持大数据组件：提供大数据组件的检查标准和基线的检查能力，实现对业务系统的大数据平台的安全保障

扩展

支持快速扩展安全基线库：遵循 SCAP 标准，提供必要的扩展性，支持将来的各类安全基线的更新

主要价值

- 主动发现服务器潜在的安全异常
- 减少攻击面，降低业务系统被入侵的风险
- 轻松满足合规性要求

典型应用场景

私有云下的服务器安全基线检查

满足资产快速变化下私有云平台上的服务器安全管理规范检查

服务器等级保护安全管理规范检查

适合银行、证券、电信运营商、电网、大型企事业单位的服务器等级保护监管要求

行业协会、监管机构、公司（单位）服务器安全管理规范检查

- 适合中国人民银行服务器安全规范检查
- 适合电信运营商内部服务器安全规范检查
- 适合电网内部安全管理规范检查
- 适合证券公司内部服务器安全规范检查

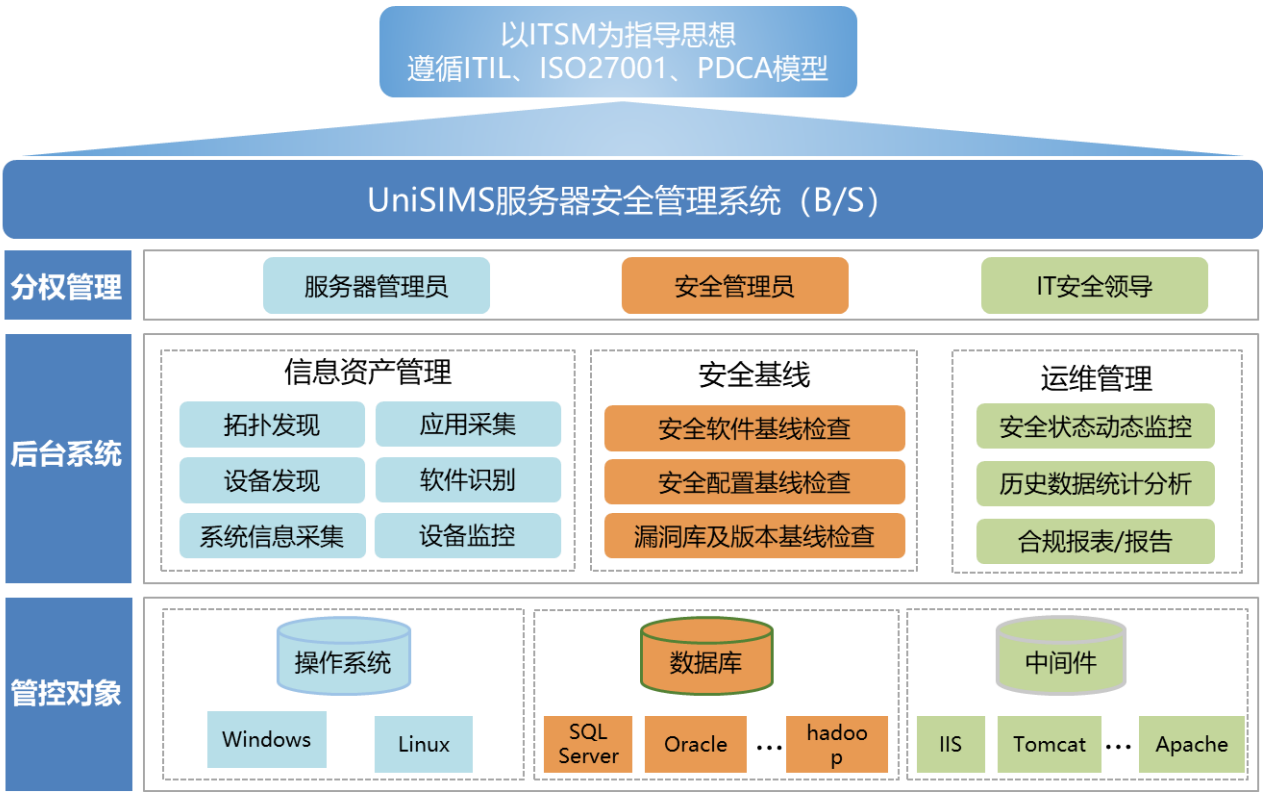

图　UniSIMS服务器安全管理系统结构图