统信软件
UNIONTECH

打造操作系统创新生态

统信UOS & 安恒信息

明御综合日志审计分析平台联合解决方案

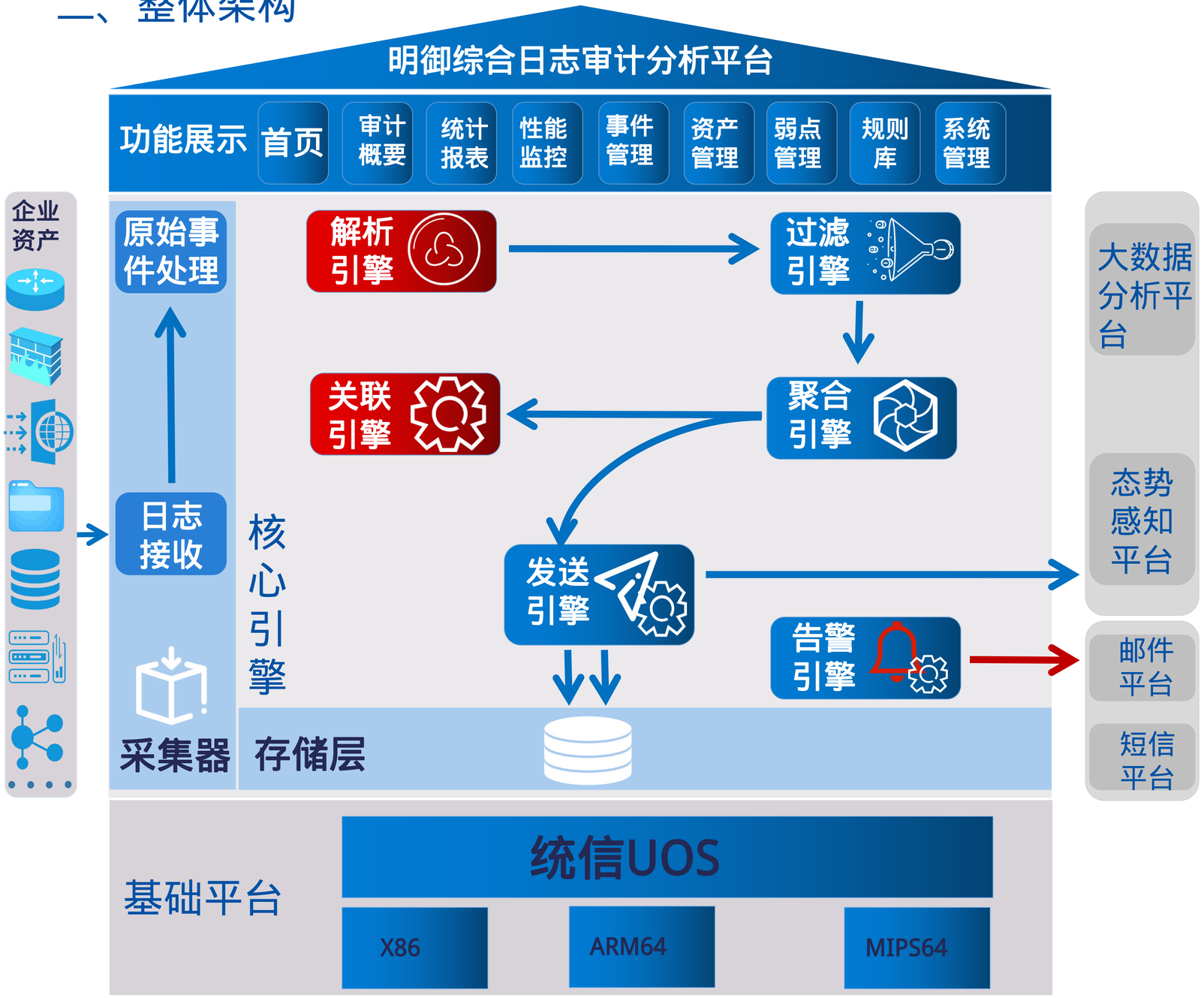
一、方案概述

- 在信创时代下，安恒明御综合日志审计分析平台紧跟步伐，在统信UOS基础平台支撑系统上，完成了产品所有的功能适配
- 明御综合日志审计分析平台是一站式的日志数据综合性管理平台，主要致力于提供**事前预警、事后审计**的安全能力，符合相关法律法规。通过对日志数据的**全面采集、解析和深度的关联分析**，及时发现各种**安全威胁和异常行为**事件。

方案特色

- ✓ 操作系统采用中国自主研发的操作系统，具备强大的抗攻击能力，杜绝自身进程及文件被非法篡改和破坏
- ✓ 多维解析，为进一步分析场景提供丰富维度
- ✓ 提供全维度、跨设备、细粒度的关联分析，深度发现潜在安全事件
- ✓ 提供包含攻击威胁、等保合规及多种审计等丰富报表，为客户提供全面的审计视角
- ✓ 拥有强大而灵活的对接能力，可为上层多种应用提供丰富的数据

二、整体架构



明御综合日志审计分析平台在统信UOS上稳定运行，平台主要由采集器、核心引擎、存储层、系统功能四部分组成：

- ✓ 采集器：主要通过Syslog、snmp、agent、sftp、kafka等多种协议方式接收或采集日志数据，并对原始事件进行资产地理信息识别、内网IP映射、日志来源目的IP区分等特殊处理
- ✓ 核心引擎：由解析引擎、过滤引擎、聚合引擎、关联引擎、发送引擎和告警引擎所组成，用以实现接收到的日志数据进行标准化处理、过滤、聚合、关联分析以及对接第三方平台功能
- ✓ 存储层：由非关系型数据库和关系型数据库组成，用以存储日志数据、索引数据、统计数据以及配置信息
- ✓ 系统功能：系统功能展示由首页、审计概要、统计报表、性能监控、事件管理、资产管理、弱点管理、规则库和系统管理组成，用以实现日志接入、规则配置、资产配置、事件查询、报表展示及系统配置等功能

三、核心价值

- ✓ 统一采集，集中管理：基于多种协议进行日志采集，帮助用户实现日志统一采集，集中管理。
- ✓ 智能标准化：实现日志格式统一标准化，细粒度解析，实现安全事件日志、行为事件日志、状态监控事件日志、弱点扫描日志等各种安全视角事件的全面性描述。
- ✓ 关联分析：基于国际标准化的关联分析引擎，帮助用户实现日志的全维度、跨设备、细粒度关联分析，找出各资产间事件的关联共性，挖掘出潜在的安全风险事件，快速定位外部威胁、黑客攻击、内部违规操作、设备异常等安全事件的根源
- ✓ 监控预警：采集设备的性能数据，实现 CPU、内存、磁盘、吞吐量、执行效率、命中率等诸多系统重要性能参数的曲线监控，帮助用户实时监控主机、数据库、网站等系统的可用性。
- ✓ 监管合规：通过芯片级的加密(国密算法SM4)、签名(国密算法SM3)存储或转发传输，满足密评、等保等合规性要求。
- ✓ 取证分析：通过深入分析原始事件，帮助用户快速定位问题的根本原因，并生成攻击威胁报表、Windows/Linux系统审计报表以及合规性审计报表。

四、方案优势

自主创新

采用中国自主知识产权的处理器、从根本上杜绝了芯片设计上存在的安全隐患；操作系统采用中国自主研发的操作系统，该系统具备强大的抗攻击能力，杜绝自身进程及文件被非法篡改和破坏；应用模块采用安恒信息自主研发的应用模块；真正实现硬件到软件、系统到芯片的完全自主可控。

芯片级加密存储

支持芯片级的加密(国密算法SM4)、签名(国密算法SM3)存储或转发传输，满足密评、等保等合规性要求。

全面解析

内置5000+解析规则，可对不同设备不同格式的日志进行细粒度解析，解析维度多达200+，确保所接收的所有日志统一标准化处理，解析规则可根据现场情况进行定制，且拥有易用美观的自定义解析规则界面，让用户灵活使用。

关联分析

内置设备异常、漏洞利用、横向渗透、权限提升、命令执行、可疑行为6大类50+子类的安全分析场景，基于设备故障、认证登陆、攻击威胁、可用性、系统脆弱性等维度建立安全评估模型，提供全维度、跨设备、细粒度的关联分析，深度发现潜在安全事件。

五、企业简介

杭州安恒信息技术股份有限公司（简称：安恒信息）成立于2007年，2019年于科创板上市（股票代码：688023）。

安恒信息一直专注于网络信息安全领域，公司主营业务为网络信息安全产品的研发、生产及销售，并为客户提供专业的网络信息安全服务。

公司的产品及服务涉及应用安全、大数据安全、云安全、物联网安全、工业控制安全及工业互联网安全等领域。

公司秉承“助力安全中国、助推数字经济”的企业使命，以“诚信正直、成就客户，责任至上，开放创新，以人为本，共同成长”作为企业的价值观，不断提高核心技术创新能力，致力于成为一家具有优秀企业文化和社会责任感的新时代网络信息安全产品和服务提供商。

总部地址：浙江省杭州市滨江区西兴街道联慧街188号安恒大厦

公司网址：https://www.dbappsecurity.com.cn

联系电话：400-6059-110

安恒信息官方服务号

全球网络安全创新500强之一

牵头起草多项国家及行业标准

国家重大活动网络安全保卫技术支持单位