



# 信创安全运维一体机

## 产品概述

上讯信息信创安全运维一体机是由 InforCube 智能运维安全管理平台为基础，全面支持和兼容国产化信创环境而诞生的一款安全运维合规平台化产品。以企业中的人和资产为数据基准，以场景为导向，针对资产实时监控(IMP)、日志安全审计(SIEM)、数据库安全审计(DBA)、运维安全审计(OMA)四大场景，实现了资产风险的闭环管控，构建了安全、运维和合规三位一体的综合性管理平台。

上讯信息信创安全运维一体机可为有需要的客户提供国密套件，以满足客户的国密改造要求。



## 信创支持

- 产品系统：产品自身采用符合信创要求的国产操作系统、国产数据库、国产中间件等，且为全自主研发产品。
- 信创环境兼容与适配：支持国产服务器、数据库、中间件、网络及安全设备等的统一运维管理和安全审计，包括但不限于：
  - ① 基于鲲鹏、飞腾、龙芯、兆芯、海光等国产服务器
  - ② 中标麒麟、银河麒麟、红旗 Linux、EulerOS 等国产操作系统
  - ③ TiDB、OceanBase、达梦、openGauss、PolarDB、人大金仓、TDSQL、南大通用、神州通用、AnalyticDB 等国产数据库
  - ④ 华为、华三、锐捷等网络设备

## 产品功能特性

### ▶ 用户身份统一管理

1. 构建统一组织信息，用户账号集中管理
2. 角色有效划分，并遵循最小权限原则
3. 资源权限细分，并细粒度授权管控
4. 认证方式多样且灵活，账号安全全面保障
5. 高效规范账号审计，全生命周期管控



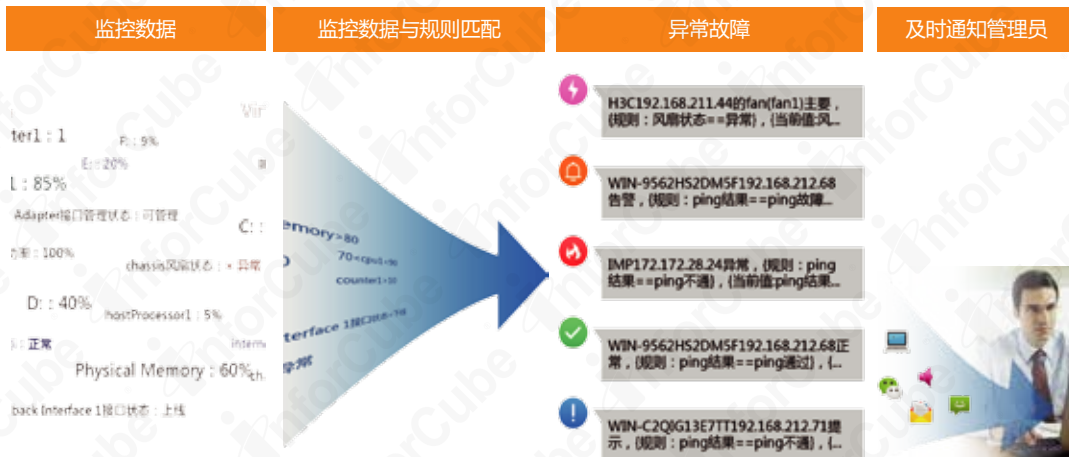
▶ **资产全生命周期管理**

1. 网络资产自动识别,减少人为工作量与失误
2. 资产统一集中管理,灵活检索便捷高效
3. 资产配置自动化管理,定期核查降低风险影响



▶ **7\*24 小时全栈监控**

1. 7\*24 小时全栈监控,构建完整监控体系
2. 资产网络拓扑自动识别,资源运行状况一目了然
3. 指标监控基线灵活设置,风险问题及时告警通知
4. 业务监控视角快速构建,掌握核心资产影响范围



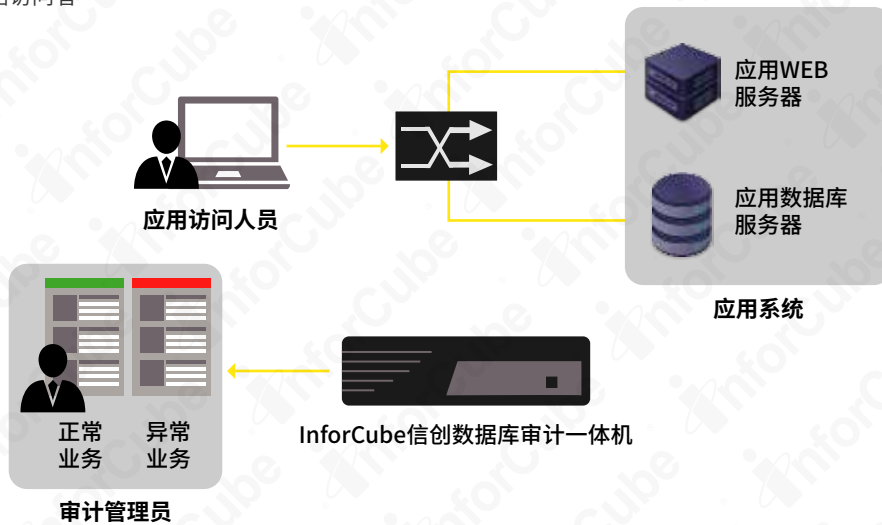
▶ **高性能日志安全审计**

1. 高适应性日志采集,确保全方位数据获取
2. 高性能日志智能汇聚,实现多元数据标准化、归一化
3. 基于大数据的海量日志集中存储,快速灵活检索
4. 灵活的审计策略配置,多视角细粒度监测,及时告警
5. 智能化日志趋势预测与异常分析,帮助风险及时感知与处理
6. 多维度报表与自定义报表统计分析,满足用户个性化统计需求



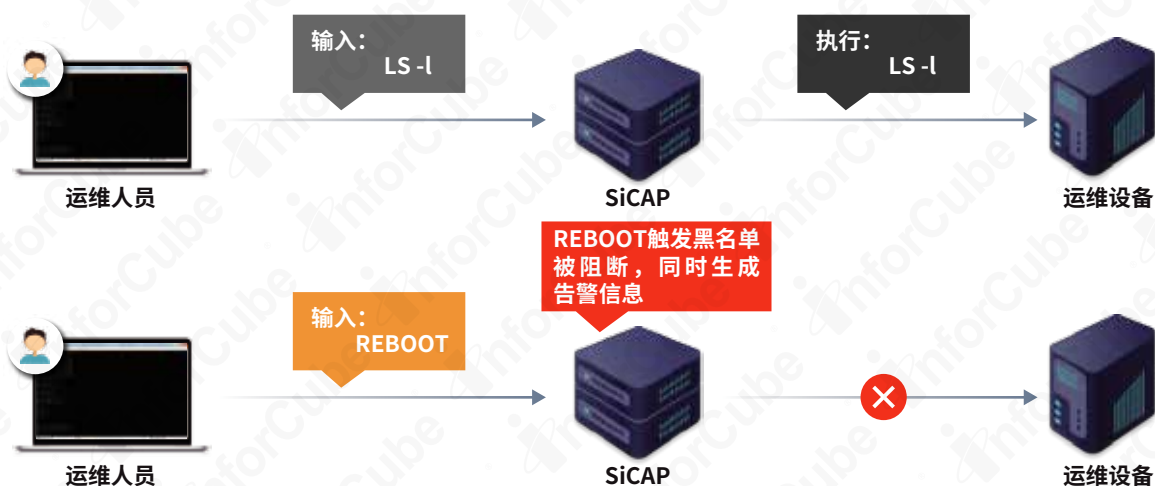
► **全方位数据库安全审计**

1. 支持丰富的数据库类型,涵盖国际主流数据库与国产化数据库
2. 提供“事前规划、事中监控、事后取证”的立体化防御与全过程审计
3. 细粒度、全面性的会话与操作审计,实现对敏感信息的精细监控
4. 关联应用层的访问和数据库层的访问操作请求,追溯应用层原始访问者
5. 分析浏览器与 WEB 服务器之间的通讯协议,识别业务操作行为
6. 灵活定义审计策略,重要事件和风险事件及时告警
7. 建立规则库实现智能免审计,减轻审计工作量
8. 内置丰富的统计报表并提供自定义报表,满足等保、行业规范等合规性要求



► **细粒度运维安全审计**

1. 集中细粒度的授权管控,实现最小权限访问及操作控制
2. 提供客户端、无客户端、直连、op 运维多种运维方式
3. 支持图形化、字符型、文件型、数据库等多种运维协议
4. 灵活的审计策略配置,实时精准的违规告警与阻断
5. 安全高效的双人协作,高安全性的密码会同
6. 方便快捷的离线审批机制,保证排障工作及时进行
7. 全面的操作行为审计,全过程的录像与回放
8. 无引擎式资产自动改密,满足密码安全相关要求
9. 跨系统平台的无缝管理,提供流畅的访问体验



►构建安全运维合规闭环管控体系

平台以人和资产为基准,围绕安全与审计,有效整合监控、日志、运维、审计数据,构建了安全运维合规闭环管控体系,有效缩短风险事件的处理周期,降低风险的影响,强化操作合规性,保障企业数据安全。

软件规格	说明
软件授权	标配100个业务综合监控许可,2000EPS日志审计许可,100个运维审计许可,10个数据库实例审计许可
处理器支持	支持基于鲲鹏、飞腾、龙芯、兆芯、海光等国产信创处理器,以及X86系列、ARM系列处理器
操作系统支持	支持中标麒麟、银河麒麟、红旗Linux、EulerOS等国产操作系统,以及Windows、Linux、Unix等操作系统
网络设备支持	支持华为、华三、锐捷等国产网络设备,以及思科等国际主流网络设备
中间件支持	支持东方通、宝兰德、普元信息等国产中间件, Tomcat、Redis、Kafka、Nginx、RabbitMQ等主流中间件
业务综合监控	支持对主机系统、主机硬件、网络设备、存储、数据库、中间件、终端等进行全面实时的监控管理
日志审计	支持对服务器、交换机、路由器、应用系统、中间件、数据库等系统的日志采集与集中存储及审计
数据库审计	支持对所纳管设备类型中的数据库类设备进行数据库审计 支持Oracle、Informix、DB2、SQL Server、Sybase、MySQL、Cache、PostgreSQL等国际主流数据库及TiDB、OceanBase、达梦、openGauss、PolarDB、金仓、TDSQL、南大通用、神州通用、AnalyticDB等国产数据库审计
运维审计	支持对所纳管设备的运维与审计 支持Telnet、SSH、RDP、VNC、HTTP(s)、X11、FTP、SFTP协议,支持ORACLE、MSSQL、MySQL、达梦、KingBase、OSCAR等数据库协议的远程访问协议审计
*国密套件 (可选模块)	包含符合国密要求的加密卡,数字证书认证,密钥管理,时间戳服务,动态口令牌等
硬件规格	说明
操作系统	内置64位国产操作系统
数据库	内置符合信创要求的国产数据库
机箱规格	2U机架式,标配12个3.5寸硬盘槽位或者24个2.5寸硬盘槽位
处理器	国产信创64核高性能处理器
运行内存	标配64GB,*最大支持512GB
硬盘	标配2块8T SATA企业级硬盘,逻辑存储容量8T(RAID 5),*最大支持192T存储容量
RAID类型	支持RAID 0/1/5/6
网络接口	2个千兆网络,2个万兆网络接口(SFP+)
电源	550W(1+1冗余电源)



上海上讯信息技术股份有限公司

咨询电话:86-21-51905999

传真:86-21-51905959

网址:www.suninfo.com

咨询热线:400 880 5062

邮箱:market@suninfo.com

地址:上海市浦东新区郭守敬路498号20号楼

©上海上讯信息技术股份有限公司。保留所有权利。SUNINFO InforCube 均为上海上讯信息技术股份有限公司在中国的商标或注册商标。Vsuninfo000-023M 印刷日期:2023年3月