JUMING 聚铭

让安全更简单

# 聚铭 安全服务

EASIER WAY FOR SECURITY

累计服务6500+云端托管客户

# 聚铭云端安全管家
# (iSOC)

聚铭网络

www.juminfo.com

# 聚铭云端安全管家

当前，企业既需要应对不断增长的网络安全威胁，又面临专业人才匮乏、防护经验不足、安全预算有限的现实。聚铭云端安全管家，是聚铭自主研发并率先在国内推出的安全托管运营服务平台，旨在保障企业网络持续安全、可用。平台以传统安全建设为基础，依托“大数据 +AI”全息安全感知技术，通过云 - 地专家协同方式，为企业提供 7x24 小时全网安全监控及响应服务，打造智慧安全运营体系，让客户一键获得常态化的网络安全防护服务。


服务体系概览

## 行业现状

**数字化带来的全新安全挑战**

随着云网端融合、移动互联、万物互联等数字化转型，网络环境日益复杂，网络暴露面和攻击面不断扩大，为企业网络安全运维带来了新的挑战。

**网络攻防战趋白热化**

随着黑色产业链日趋成熟，并逐步向规模化、产业化和专业化的方向发展，企业亟需提升常态化安全防护建设能力。

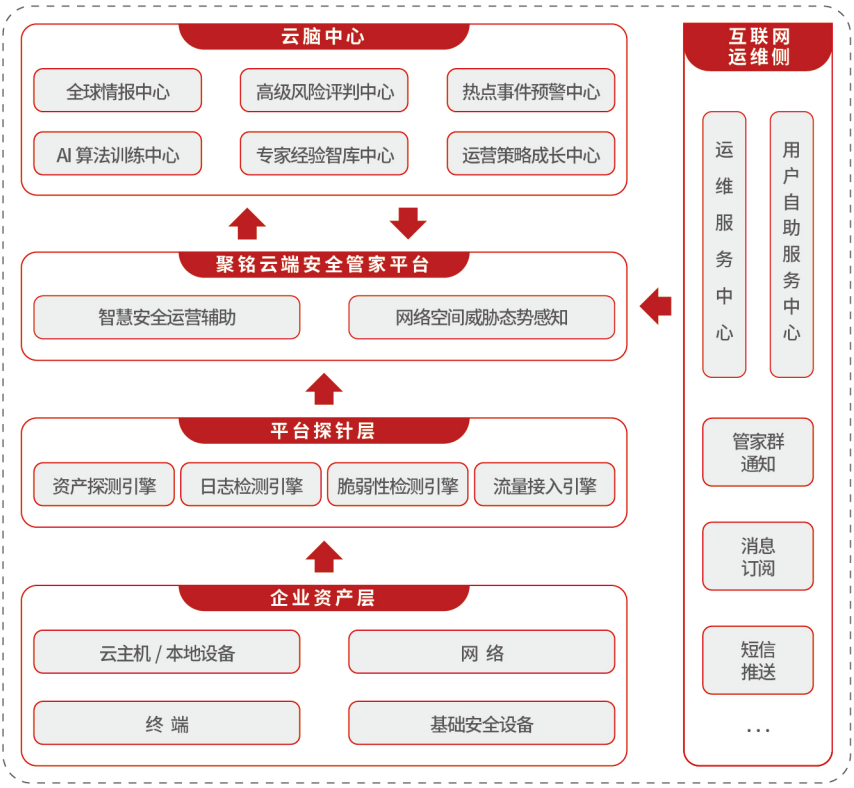

**网络安全运营转向第三方托管模式**

网络安全人才少、成本高，网络安全运维工作量大，企业难以组建专业的安全运营团队，第三方安全托管服务需求日益增加。

企业网络安全服务采用本地化安全托管方式，成本高，且受限于区域、人才等因素难以快速响应，随着共享经济的发展，云端安全托管以 7x24 小时响应快、成本低的优势逐渐受到市场的青睐。

**本地化运营成本高催生云端安全托管**

## 2 服务平台架构




## 3 服务内容

### 资产测绘及管控服务

对全网资产进行探查、梳理及风险治理，协同一线或客户，针对影子资产、资产服务存在的弱点等安全隐患进行防护。

### 脆弱性管控服务

脆弱性处置完成后，平台专家复验脆弱性，确认是否已修复，完成脆弱性生命周期闭环管控。

### 威胁及风险管控服务

平台整合流量日志、脆弱性等多元数据，依托八大研判模型，实现全息动态威胁感知。云端专家 7x24 小时风险监控告警，持续挖掘威胁，跟踪闭环。

## 配置保障服务

每次风险进行处置完成后，自动巡检跟踪加固后的系统配置，包括注册表、服务、文件等，及时发现变更带来的隐患，自动完成风险的闭环跟踪。

## 智慧安全运营辅助服务

提供线上安全技术培训、行业运营策略定制、专家智库沉淀、5x8 小时研判、风险处置全生命周期管控、风险通知推送、运营报告推送、安全成果汇报等全方位运营服务，打造周密的智慧安全运营体系，辅助用户日常运营工作。

## 本地增值服务

针对用户在网络安全业务中的实际需求，提供安全处置、安全加固支撑、渗透测试、红蓝对抗演练、重要保障、等级保护咨询等其他增值服务项，动态适应企业个性化的安全建设场景。帮助用户灵活选择、安全能力叠加升级。

# 服务流程

**S1 威胁感知**

- 自动巡检
- 智能安全分析

**S2 专家 7x24 小时在线监控**

- 云端专家监控到威胁
- 云端专家在线初步分析，确定威胁的性质

**S3 威胁生命周期管理**

- 生成威胁生命周期管理或工单
- 云端专家深度分析、挖掘威胁及相关隐患
- 如无法研判，升级专家组参与分析并提供解决方案
- 推送威胁处置方案给一线支撑人员，配合完成威胁闭环处置
- 自动化配置保障完成，保护加固成果
- 工单、威胁生命周期闭环

**S4 持续跟踪及经验沉淀**

- 云端专家跟踪监控，归档处置经验
- 云端专家输出威胁处置报告并推送客户

# 5 服务优势

## 领先的安全运营技术

- **规范的安全运维管流程**，依托SOC团队对众多企业服务的运营经验，融合了风险管理模型ISO13335、风险分析模型、PDCERF风险闭环响应模型、SOP处置流程，规范化安全服务团队在监测、分析、响应、跟踪、沉淀的全流程。
- **全息网络空间威胁感知无死角**，覆盖动态安全+静态安全。将资产、日志、流量、脆弱性作为核心，融合众多研判模型，全面检测无死角。

## 专业的安全运营团队

- **中国安全运营中心（SOC）的首创团队**，已广泛应用于电信、教育、能源、金融、政府、医疗等众多行业。
- **中国最早的日志审计研发团队**，专注多源日志分析超20年，支持800多种设备、超过2万种日志格式，全面支持主流厂家网络设备、安全设备的信息接入。
- **团队服务6500+家云端托管客户、10000+家政企客户**，积累了大量的行业安全运营策略、专家经验、安全检测分析能力。

## 全方位的管家式服务

- **专家保障**，三级专家团队，7x24小时在线防护，100%闭环，0容忍。
- **专属安全保障持续生长**，企业专属运维知识库、预案、方案持续沉淀，企业专属运营策略持续调整动态适应企业个性化场景。

# 6 服务价值

### 安全运营 高性价比

将安全体系方案、基础设备建设、安全专家协助、运营协作与监管，整个安全体系云化共享。用以租代购、云化共享的创新方式将安全建设投入成本降低到原有的10%，以极高的性价比提供专业化安全运营服务。

### 安全保障 常态化

以“重大保障活动”为标准，以全面为基础、精准为目标，为客户打造常态化安全运营，满足企业安全建设“零事故、零通报、零问责”的整体要求。

### 安全服务 分钟级

大数据赋能AI，AI辅助专家。通过风险威胁预测、风险评估自动化、风险感知智能化等AI技术，辅助专家加速安全闭环流程，7x24小时实时在线，将安全服务响应缩短到分钟级。

### 安全运维 轻松监管

将安全感知、安全运维成果相结合，通过大屏监控技术使安全运营监管可视化、指标化，并将预警、风险、报告等实时同步公众号及管家群，实现安全运维监管化繁为简。

# 服务套餐

| 服务特权 \ 服务套餐 | | SLA1 智能运营支撑套餐 | SLA2 云端专家守护套餐 |
|---|---|---|---|
| | | 在平台、专家的辅助下开展安全运维工作 | 专注于自身业务，安全运维工作全部交由服务商主导 |
| | | 套餐以租赁形式提供微信管家群、iSOC 安全管家账号一套、探针一套、NFA 一套；按年收费 | |
| 脆弱性管控服务 | 脆弱性巡检服务 | ✓ | ✓ |
| | 脆弱性评估服务 | | ✓ |
| | 脆弱性治理协同服务 | | ✓ |
| | 互联网暴露面巡检服务 | ✓ | ✓ |
| | 互联网暴露面收敛及防护协同服务 | | ✓ |
| 威胁及风险管控服务 | 威胁检测服务 | ✓ | ✓ |
| | 7x24 小时风险监控服务 | | ✓ |
| | 风险挖掘及研判服务 | | ✓ |
| | 风险处置协同服务 | | ✓ |
| 配置保障服务 | 配置巡检服务 | ✓ | ✓ |
| | 配置变更监控服务 | | ✓ |
| 资产测绘及管控服务 | 智能资产测绘服务 | ✓ | ✓ |
| | 资产梳理服务 | | ✓ |
| | 资产治理协同服务 | | ✓ |
| 智慧安全运营辅助服务 | 线上安全技术培训服务 | ✓ | ✓ |
| | 5x8 小时研判服务 | ✓ | ✓ |
| | 行业运营策略定制服务 | ✓ | ✓ |
| | 风险处置全生命周期管控服务 | | ✓ |
| | 热点事件、风险预警及预防服务 | ✓ | ✓ |
| | 风险通知推送服务 | | ✓ |
| | 威胁情报更新服务 | ✓ | ✓ |
| | 脆弱性插件库更新服务 | ✓ | ✓ |
| | 专家智库沉淀服务 | | ✓ |
| | 运营报告及推送服务 | | ✓ |
| | 安全成果汇报服务 | | ✓ |

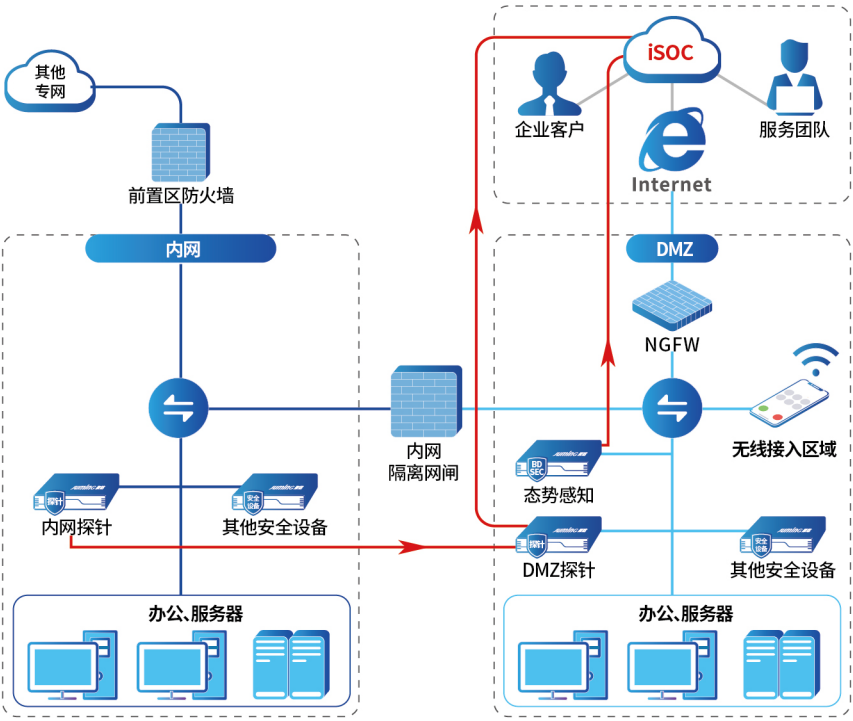
本地增值服务（按需购买）

- 安全处置服务
- 安全加固支撑服务
- 安全培训服务
- 应急响应服务
- 渗透测试服务
- 红蓝对抗演练服务
- 重要保障服务
- 等级保护咨询服务
- 安全体系咨询服务

交付方式：公有云 / 私有云部署

## 8 部署方式

支持轻量级探针及聚铭态势感知接入，部署快捷灵活。用户一键绑定 iSOC 平台，即可开启云端安全管家服务。




## 9 服务案例

### 聚铭云端安全管家监控大屏


累计服务

电信、教育、能源、金融、政府、医疗等行业

**6500+** 家云端托管客户

聚铭 juminc

聚铭订阅号

荣获国家发明专利20余项
通过【ISO9001质量管理体系认证】【ISO27001信息安全管理体系认证】
【ISO20000信息技术服务管理体系认证】【CCRC信息安全风险评估服务资质认证】
【CCRC信息安全应急处理服务资质认证】

北京总部:北京市海淀区丹棱街18号创富大厦9层
南京总部:江苏省南京市雨花台区软件大道180号南京大数据产业基地7栋4层
电话:010-82666399 / 025-52205520　　传真:010-82669679 / 025-52205565
全国统一服务热线:400-1158-400　　公司官网: www.juminfo.com