医院防勒索解决方案

1 需求背景

近年来勒索病毒肆虐，且在持续快速地迭代、变种。医疗行业作为受病毒攻击的重灾区，令医院防不胜防。受攻击严重的用户，甚至服务器关键数据被勒索加密，导致业务系统无法对外提供服务，严重影响用户的正常营业。面对如此严峻的安全形势，传统的安全防护体系对勒索病毒的防御效果并不理想。深信服基于自身在安全行业十余年的技术积累，以及近年来多次处置勒索病毒事件所积累的经验，提出了深信服勒索病毒防护解决方案

2 深信服解决方案

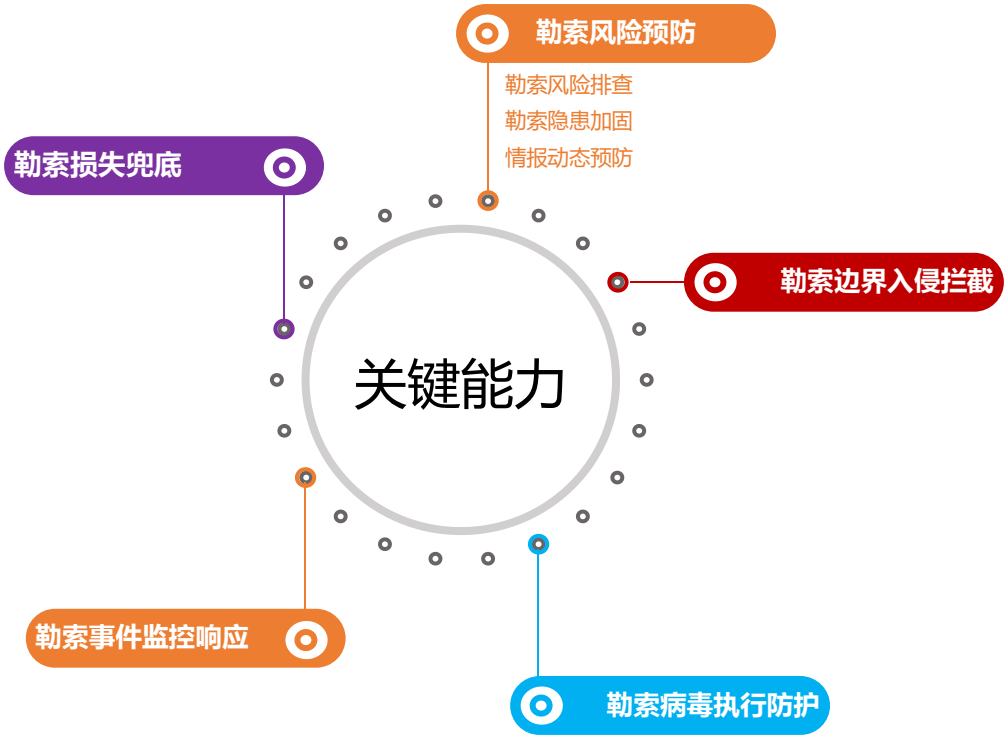
深信服以“安全 AI+人机共智+纵深防御”的理念革新传统勒索病毒防御方案

方案配置：

方案配置		**标准版（主推）** MSS、SaaS aES、保险、AF（含云情报）	基础版 MSS-Lite、SaaS aES、保险、AF（含云情报）
勒索风险预防	勒索风险排查	✓	✗
	勒索隐患加固	✓	✗
	情报动态预防	✓	✗

勒索边界入侵拦截	勒索漏洞攻击即时防御	✓	✓
	勒索弱口令爆破封堵	✓	✓
	勒索远控勒索远控外联拦截外联拦截	✓	✓
	钓鱼式勒索流量过滤	✓	✓
勒索病毒执行防护	变种勒索精准查杀	✓	✓
	勒索行为秒级阻断	✓	✓
	勒索防退出、防卸载	✓	✓
勒索事件监测响应	专家团队值守分析	✓	✓
	勒索事件 7*24H 快速响应	✓	✓
	勒索事件闭环溯源	✓	✓
	安全加固	✓	✓
勒索损失兜底	安全托管理赔服务	✓ 20-600w（额度可选）	✓ 20w（额度不可选）
可选增值	SaaS XDR/SIP	以 UEBA、AI 检测引擎为核心，对网络流量进行深度解包分析，基于业务模型流量进行异常检测，发现未知威胁以及高级可持续攻击，同时结合 SOAR 技术对安全告警及事件进行流程化响应，实现快速闭环及溯源分析取证展示	
	云备份	安全、高可靠、低成本的一体化整机云备份，用户无需关注主机内部的业务应用、数据库、配置文件等，只需简单几个步骤实现整机备份恢复，可有效避免勒索病毒感染导致业务长时间停机 根据用量选型，支持动态扩容 ✓ 云备份订阅-资源包（5TB） ✓ 云备份订阅-资源包（10TB）	

3 方案优势



方案核心组件：MSS+aES+AF +保险

4 典型案例

客户名称	级别	客户名称	级别
上海市仁济医院	三甲医院	山东省立医院	三甲医院
河北省肿瘤医院	三甲医院	复旦大学附属肿瘤医院	三甲医院
中山大学附属第五医院	三甲医院	成都市第五人民医院	三甲医院
云南省第三人民医院	三甲医院	深圳市第六人民医院（南山医院）	三甲医院
重庆渝北区人民医院	三甲医院	……	……