医院防通报解决方案

1 需求背景

1）医院业务变化趋势

近年来随着医院业务的发展，医院门户网站、互联网医院业务、OA、微信公众号、小程序等对外业务越来越多，对外风险暴露面也越来越多，如“三高一弱”的问题。同时，卫健委/网信办利用多种专业工具进行扫描，结合技术人员的人工渗透和检查，医院网络中部署探针进行监测，医院被发现各种问题，通报的频率也越来越高，医院如何做好暴露面的管理和脆弱性的预防，从而降低被通报的频率，变成了一个备受关注的问题。

2）通报工作的挑战

通报工作的主要以查促建的方式提升医院的安全建设水平和安全效果，近两年通报逐渐规范，政策要求进一步明确，如《网络安全法》、《关键信息基础设施安全保护条例》、《党委（党组）网络安全工作责任制实施办法》以及一些行业政策文件均对通报做了明确要求。而随着网信网安单位监管职能愈加明确，各单位均在积极履行安全监督管理职责，权威性得到加强，经过大量客户调研得出常见被通报的常见问题类型如下：

类别	细分	详细内容
脆弱性	web 漏洞	web 漏洞，如任意文件上传、SQL 注入、xss 跨站、WebShell 等
	弱口令	如 web 管理员弱口令、主机弱口令、数据库弱口令等
	业务逻辑漏洞	如未授权访问、越权访问
	系统漏洞	如中间件、操作系统相关的漏洞，log4j、strust2
安全事件	非法外联	如挖矿病毒、蠕虫病毒、勒索病毒主动访问恶意域名、Cobalt Strike 远控外连 C2 服务器

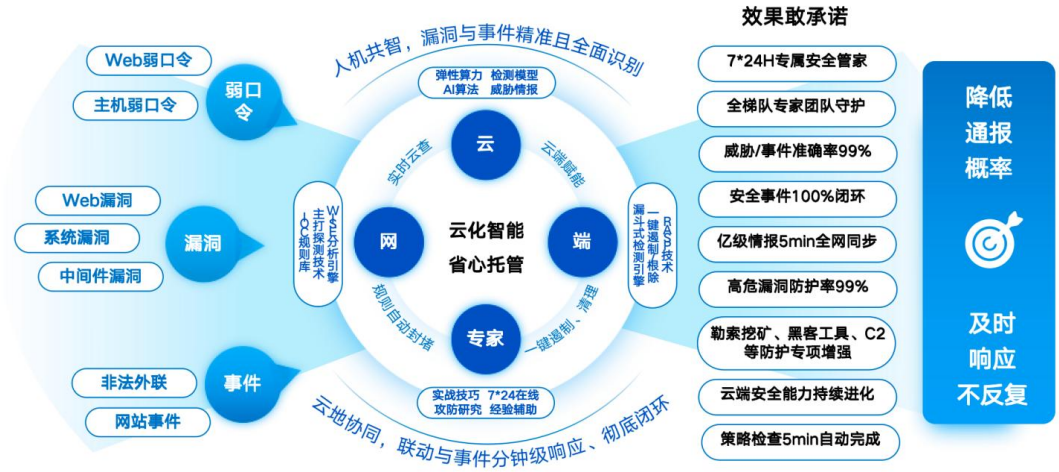
	网站安全事件	网站被篡改、挂马、暗链等安全事件

3）通报工作的挑战

- **通报方式多样化：**主管监管单位往往会使用多种专业的扫描工具做自动扫描，不同的工具在检测能力上各有所长，不好应对
- **风险识别不及时：**业务发展下，资产边界逐渐模糊，外网暴露面增多，像微信小程序、公众号也在被通报的范围内；安全事件的告警看得不够及时，事件发现得十分滞后
- **本地设备有限制：**由于本地安全检测和防护设备规则库不全、情报滞后，导致恶意外联会漏掉了前几个威胁包，无法完全封堵掉，最终还是被通报
- **处置响应难闭环：**失陷主机的恶意程序、僵木蠕杀不死，容易复发，造成反复通报；漏洞补丁难获取，有些服务器又不敢打补丁，导致漏洞修复效果差，尤其 web 漏洞很容易被扫描到导致通报
- **缺少人员和精力：**单位人员编制少但是业务繁忙，日常 IT 运维已经筋疲力尽，想要通过自身的安全团队去全面的做好漏洞和事件的通报预防工作，是较难实现的；

2 深信服解决方案

针对医院常见的通报问题类型，深信服通过化被动应付为主动应对，确保日常安全运营工作做到位、做扎实，时刻领先一步；被通报也能快速响应、按期完成整改并提交反馈报告，充分降低通报的负面影响。



深信服以安全效果为核心的“云网端”的安全架构为用户提供更加简单、有效的解决方案，为用户提供 7*24H 的通报预防与响应方案。

方案配置：

方案配置		标准版 (MSS+网站监测+AF+云威胁情报网关+SaaS aES)	基础版 (AF+云威胁情报网关)
漏洞	web 漏洞	☑	✗
	操作系统漏洞	☑	✗
	中间件漏洞	☑	✗
	业务逻辑漏洞	✗	✗
弱口令	web 弱口令	☑	✗
	主机弱口令	☑	✗
非法外联事件	勒索外联	☑	☑
	挖矿外联	☑	☑
	黑客工具外联	☑	☑
网站安全事件	网页篡改	☑	✗
	网页挂马	☑	✗

	黑链暗链	☑	✕
	敏感词	☑	✕
可选增值	EASM	☑互联网暴露面检测（如数字资产、高危端口） ☑暴露的攻击路径和资产风险(如 APP、小程序、公众号等) ☑防敏感数据泄露如敏感文件、代码泄露、暗网情报等	
	渗透测试	☑可挖掘业务逻辑漏洞	

3 方案优势

降低通报概率 | 7*24H 立体守护、有效预防、实时处置

- **脆弱性：**基于庞大漏洞库有效防护各类常见 web 漏洞和系统漏洞，并提供可落地的修复建议
- **非法外联：**云威胁情报网关创新搭配 SASE 架构赋能 AF 实时拦截百亿级非法外联类威胁，独创未知威胁 AI 检测技术实现未知威胁 5min 内识别并在深信服设备全球情报同步
- **网站安全事件：**组件的优势能力与网站监测服务结合，实现网站事件的精准监测和分钟级阻断

及时响应不反复 | 极致响应、精准溯源、联动防御

- **秒级联动一键处置：**MSS 秒级联动 AF 实现一键封堵 ip 域名，联动 aES 实现一键遏制、清除痕迹
- **高效调查溯源：**AF、aES 详细举证，加上 MSS 专家丰富经验，调查溯源更高效，及时反馈报告
- **彻底闭环不复发：**服务专家专门沉淀出最佳处置方案和工具，联动 AF、aES 精准配置防护规则

7*24H 服务机制 | 覆盖非工作时间，防止攻击趁虚而入

- **全年轮班制：**白班专属服务经理（9：00-18：00）+ 夜班轮值服务经理（18：00-9：00）
- **威胁/事件管理：**云端算力对网端遥测数据进行关联聚合分析，服务专家二次研判，检测准确率超过 99%；专家协助进行威胁/事件处置闭环，闭环率 100%

- **漏洞管理：**扫描频率更高，防护更及时，对高危可利用漏洞的防护率达到 99%

4 典型案例

山东省第二人民医院	复旦大学附属中山医院	深圳大学总医院	四川大学华西天府医院
湖南省人民医院	东莞市第八人民医院	淄博市中医院	白银市第一人民医院