



# 面向未来，有效保护

## 网络安全面临的挑战与对策

第十六届民航信息化发展论坛

- 1** 网络安全面临的挑战
- 2** 面向未来，有效保护
- 3** 持续进化的安全能力

# 网络安全面临的挑战



# 安全威胁快速进化，不断升级



# 基于业务发展的安全保护思考



# 面向未来，有效保护



# 面向未来、有效保护的安全架构

## 智力进化

基于全球情报智能学习的智力进化

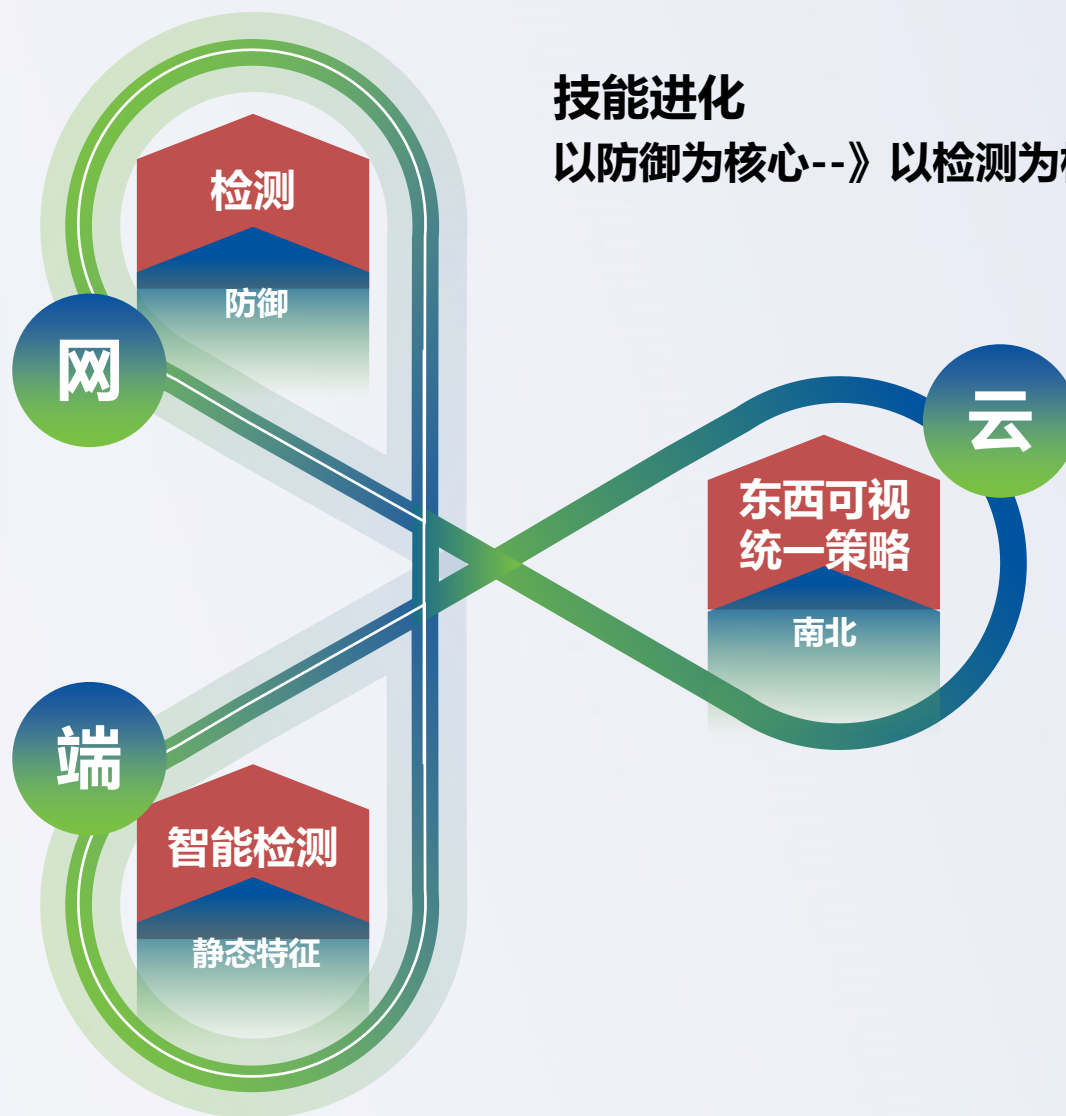


安全云脑



安全云守

订阅服务



## 技能进化

以防御为核心--》以检测为核心

# 持续进化的安全能力





# 本地智能化引擎

## SAVE安全智能检测引擎 Sangfor AI-Based Vanguard Engine



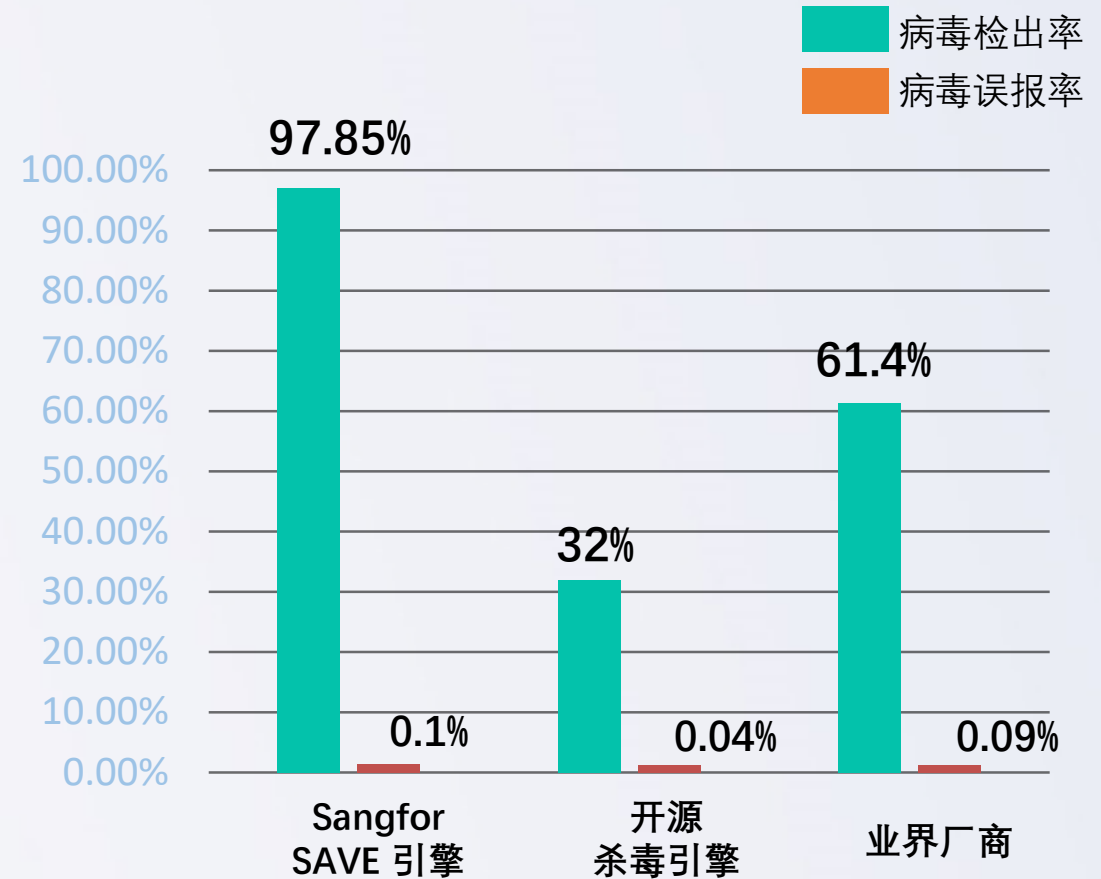
创新人工智能无特征技术  
准确检测未知病毒/勒索病毒



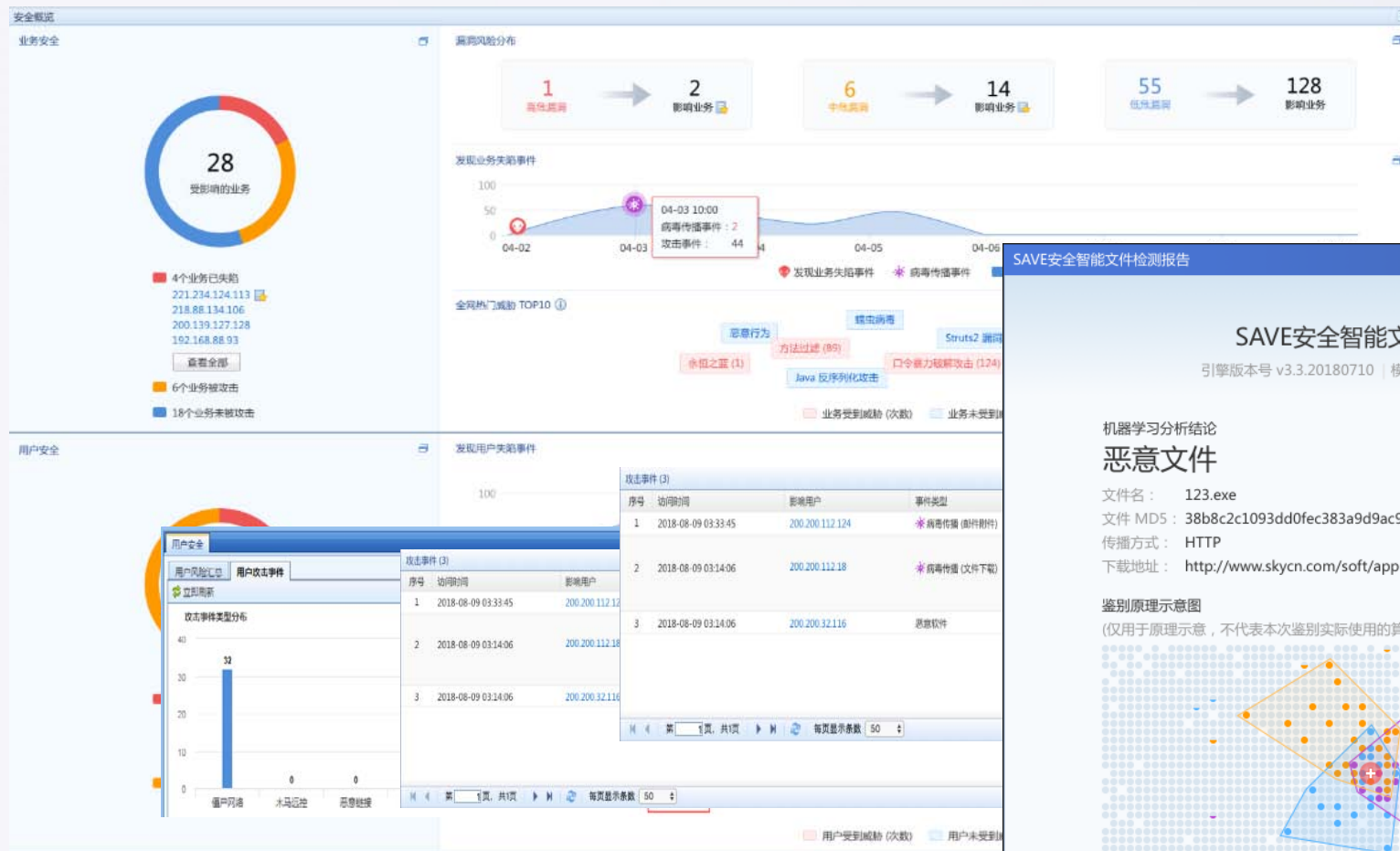
### Bad Rabbit

(17年底出现的最新勒索病毒)

查杀成功率**100%**



# 本地智能化引擎



### SAVE安全智能文件检测报告

引擎版本号 v3.3.20180710 | 模型版本号 v3.3.20180804

#### 机器学习分析结论

## 恶意文件

文件名: 123.exe  
文件 MD5: 38b8c2c1093dd0fec383a9d9ac940515  
传播方式: HTTP  
下载地址: http://www.skycn.com/soft/appid/3572/1246433583.exe

#### 鉴别原理示意图

(仅用于原理示意, 不代表本次鉴别实际使用的算法与结果) [查看原理说明](#)

检测原理说明:  
SAVE安全智能检测引擎通过结合多种机器学习算法对文件进行鉴别, 识别恶意文件。

图中元素说明:

- 圆点: 样本文件 (实际数量巨大);
- 多边形区域: 检测算法将样本文件进行黑白分类然后绘制区域 (内: 黑文件, 外: 白文件);
- 十字星点: 正在被检测的文件。

分析方法说明:  
图中采用了三种检测算法, 当检测的文件被判别位于检测算法绘制的区域内时, 则该文件被认定为恶意文件, 反之则为非恶意文件; 当同时被多种算法认定为恶意文件时, 则该文件为恶意文件的可能性就越大。

文件样本 SVM 算法匹配 XGBoost 算法匹配 CNN 算法匹配

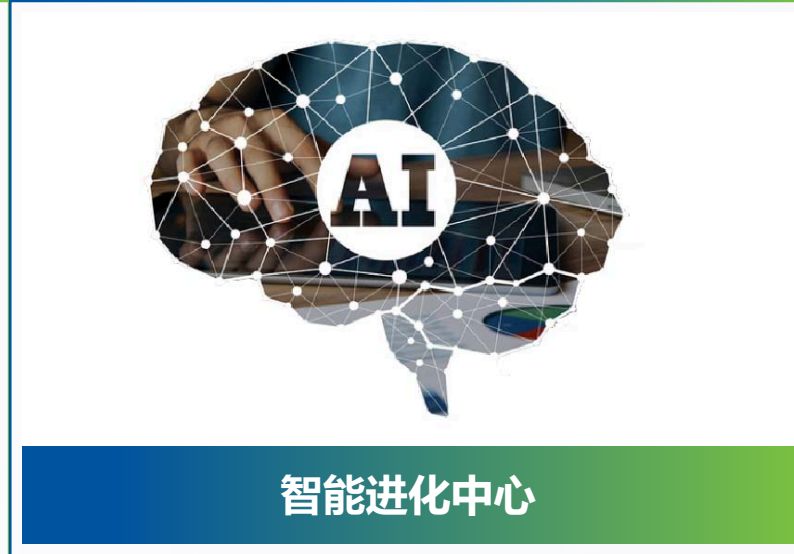
SAVE安全智能检测引擎  
Sangfor AI-based Vanguard Engine

关闭

# 订阅服务-安全云脑



全球情报中心



智能进化中心



安全赋能中心

# 订阅服务-安全云脑



情报生态



资深数据分析与  
攻防团队



安全云脑

前瞻的数据架构

情报  
信誉

云端  
查杀

云端安全能力赋能

安全  
规则

云端  
沙箱



热门威胁10分钟响应



全球热点事件1小时响应



安全能力高频更新

响应速度变快



下一代防火墙



安全能力增强



安全威胁情报



安全分析能力



IOC事件库



安全规则更新



未知威胁防护



热门威胁事件库

规则

算法

事件

## 订阅服务-安全云脑



优质  
样本  
来源

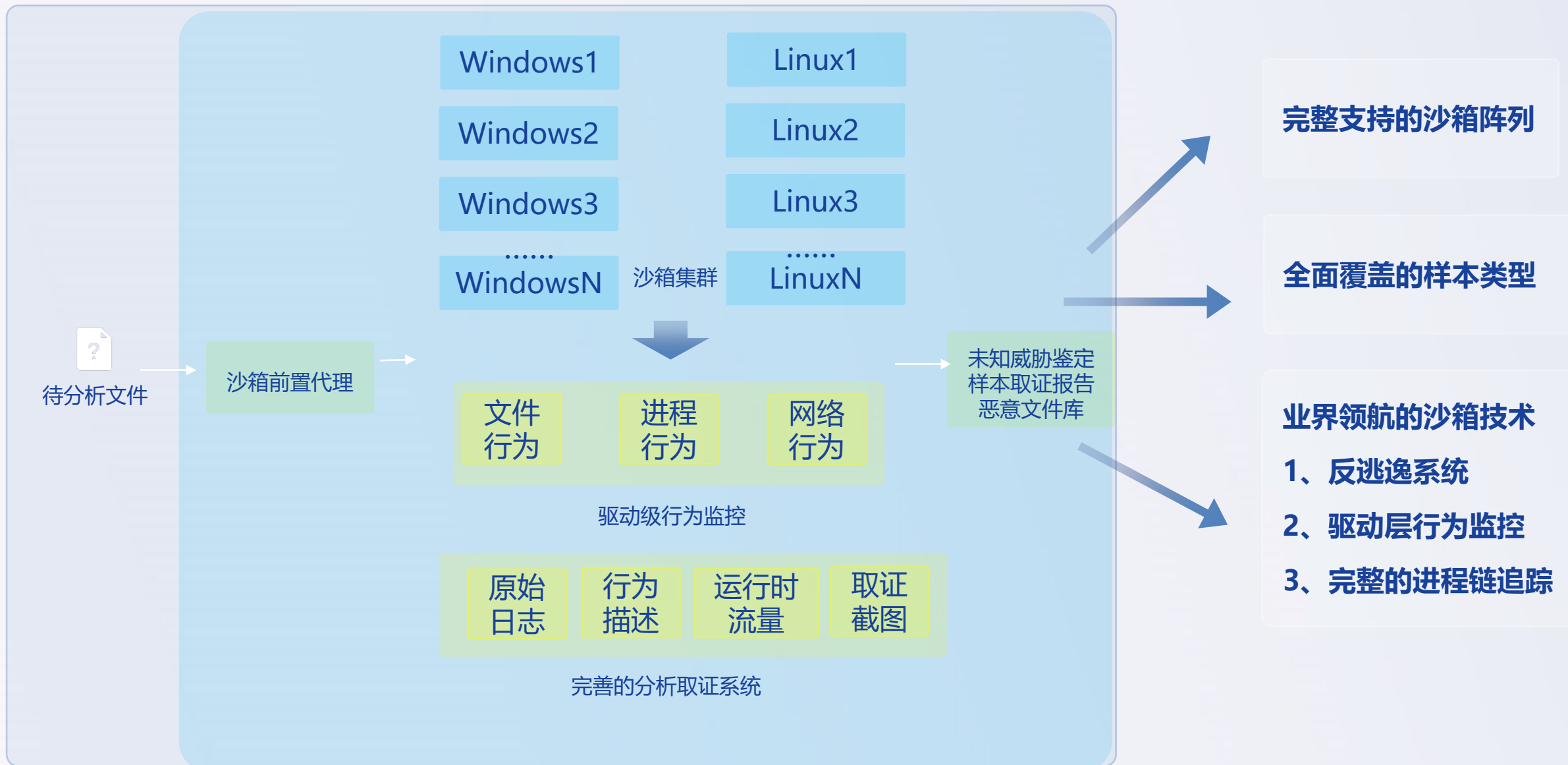
广泛来源

快速采集

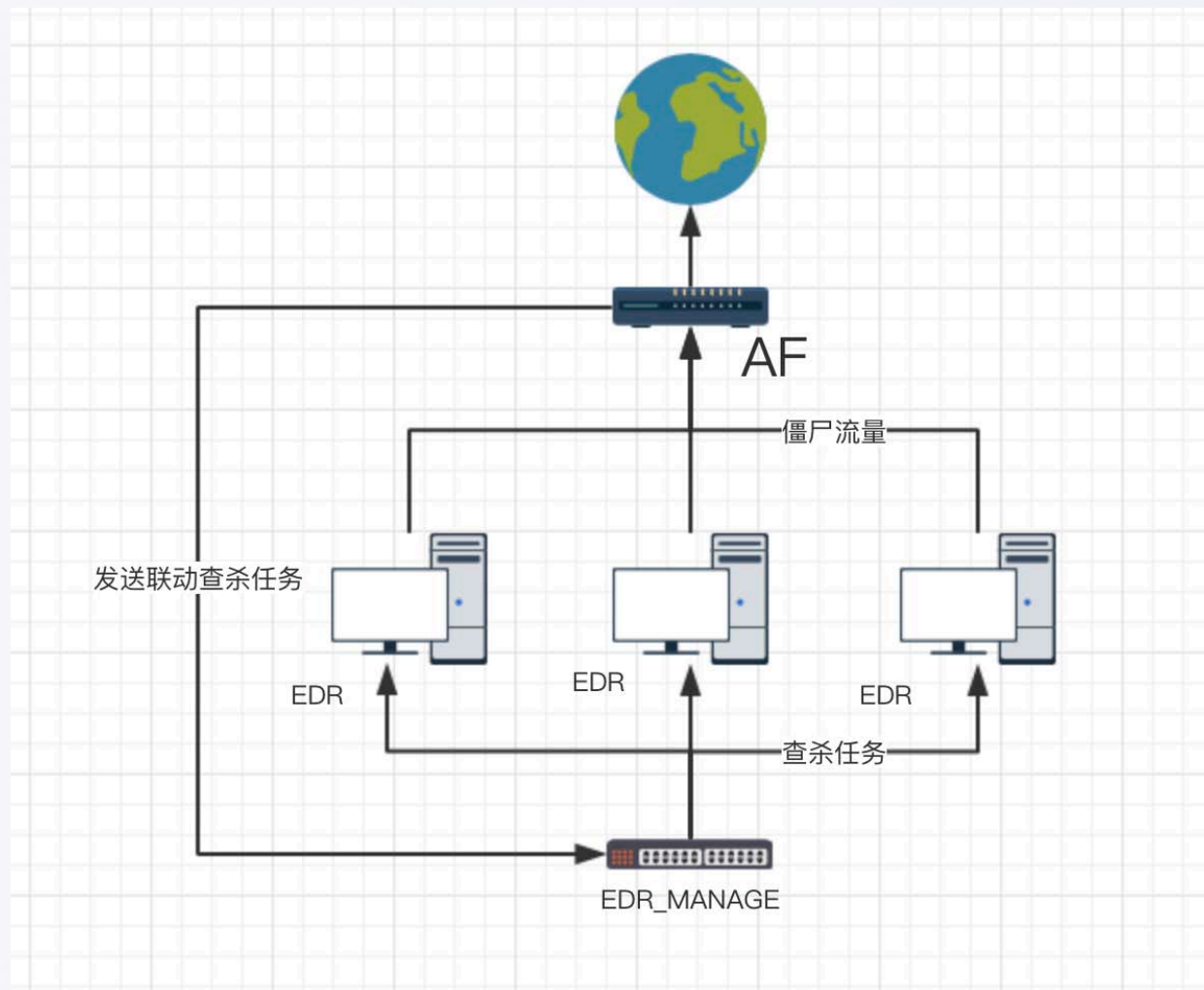
准确识别

攻击预测

# 订阅服务-云端沙箱



# 联动



通过网、端、云的方式来提升整体安全能力，通过在企业的不同位置做好安全应对措施来降低来自于不同介入点的风险；

当内网系统中感染了病毒、木马等恶意软件的终端，其病毒、木马试图与外部通信的时候，AF可以基于流量进行行为深度分析，定位失陷主机，同时联动EDR对问题端点进行扫描、取证、查杀。

## 云端增值服务

通过防火墙 AF 叠加云端增值服务，构建设备和云端深度融合的一体化安全方案；  
提供应对外部不断变化的威胁应对方案 and 用户场景化的需求方案。

[如何购买或续费](#)



### 云端威胁对抗

防火墙联动安全云脑，对未知的威胁进行鉴别，挖掘潜伏的高级威胁，构建应对未知和高级威胁对抗方案。

- 未知威胁鉴别 ⓘ
- 高级威胁分析 ⓘ

[进入](#)



### 门户网站保护

立体化的网站保护方案：联合终端防篡改保护、边界防火墙篡改检测、云端篡改监测构建网站全方位的立体保护。

- 网站安全状况监测 ⓘ
- 网站风险监测 ⓘ

[进入](#)



# 联动



**威胁对抗总览 (演示)**

- 高级威胁对抗 (已开启)
- 未知威胁防御 (已开启)

高级威胁分析 (次) 22,317  
未知威胁分析 (次) 80,227

**攻击事件趋势 (演示)**

次数

06-25 06-30 07-05 07-10

高级威胁入侵 未知威胁攻击

**高级威胁和未知威胁分析 (演示)**

DGA 通信 影响了3个业务, 2个用户 8,872

隐秘隧道通信 影响了17个业务, 资产风险监控 (演示) 9,282

外发 DDos 影响了1个业务, 1 4,163

可疑 URL 影响了17个业务

可疑文件 影响了17个业务 1

序号	资产名称	风险状态
1	OA系统	已关闭
2	BBS系统	已关闭
3	邮件服务器	已关闭
4	数据备份服务器	警告攻击
5	采购部门	警告攻击
6	测试部门	警告攻击
7	开发部门	警告攻击
8	ERP系统	警告攻击

**云信服务**

综合风险等级: 已输入

服务器: 192.168.212.136 已输入 192.168.212.136 警告攻击

**风险评估**

- 病毒传播风险
- 高管通信风险
- 恶意访问风险
- 主机失陷风险
- 数据篡改风险

**威胁事件单证(4)**

序号	事件类型	事件特征	事件标签	检测方式	影响资产	检测次数	检测时间	操作
1	DGA通信	通信域名: xx.com.yy.com.cc.com	恶意病毒	行为关联分析	200.200.88.46	3	最新检测 2018-03-05 17:11:34 最早检测 2018-03-05 17:11:34	查看单证详情
2	可疑URL	URL: www.baidu.com	勒索病毒	沙箱查杀	200.200.88.48	12	最新检测 2018-03-05 17:11:34 最早检测 2018-03-05 17:11:34	查看单证详情
3	可疑文件	MDS: aldaofdsiohdoffdsafds	勒索病毒	沙箱查杀	200.200.88.46	15	最新检测 2018-03-05 17:11:34 最早检测 2018-03-05 17:11:34	查看单证详情
4	隐秘隧道通信	通信域名: xx.com.yy.com.cc.com	勒索病毒	日志关联分析	200.200.88.47	17	最新检测 2018-03-05 17:11:34 最早检测 2018-03-05 17:11:34	查看单证详情

解决建议

- 若已安装EDR终端检测与响应软件, 则使用EDR对受病毒感染的计算机进行病毒查杀与清除。  
若未安装EDR终端检测与响应软件, 建议下载安装NGAF反僵尸网络软件, 对受病毒感染的计算机进行病毒查杀与清除。
- 购买安装EDR终端检测与响应软件, 更好的保护计算机, 避免病毒入侵造成损失。如何购买?

当前显示 1 - 28条, 共 28条

# 联动



The screenshot displays the Sangfor NGAF 7.4 website monitoring interface. The main window is titled "网站监测详情" (Website Monitoring Details) and shows the monitoring status for "内部论坛" (Internal Forum) at "bbs.sdfang.com.cn", which is marked as "已被篡改" (tampered with). The interface includes a navigation menu on the left, a top navigation bar with search and user information, and a main content area with several panels:

- 网站识别与分析** (Website Identification and Analysis): Shows the current website and its status.
- 篡改监测** (Tampering Monitoring): Provides a detailed analysis and recommendations for the detected tampering. It notes that 2 web pages were tampered with as of 2018-08-02 12:00:00 and suggests actions like disconnecting the website and fixing vulnerabilities.
- 攻击行为统计** (Attack Behavior Statistics): Displays a list of top attacked URLs, including 134.132.23.112, 23.17.14.13, 19.223.44.56, 22.1.22.4.57, and 34.66.45.66.
- 篡改监测分析与建议** (Tampering Monitoring Analysis and Suggestions): Shows a monitoring overview with 127 days and 6 hours of monitoring for 128 pages. It includes a summary of tampering types: 0色情篡改 (Pornography), 2赌博篡改 (Gambling), 1政治敏感篡改 (Politically sensitive), 0私服游戏篡改 (Private server game), 0恶意代码篡改 (Malicious code), and 0其他类篡改 (Other).
- 篡改页面** (Tampered Pages): A table listing the tampered pages, their types, discovery times, and evidence information.

URL 页面	篡改类型	发现时间	举证信息
http://www.icconcont.cn/	赌博篡改、反动黑链	2018-08-24 23:48:22	<a href="#">查看篡改代码</a>
http://www.icconcont.cn/	赌博篡改、反动黑链	2018-08-24 23:48:22	-

# 联动



The image shows a screenshot of the SANGFOR NGAF 7.4 interface, specifically the EDR analysis results page. The interface is divided into several sections:

- Header:** SANGFOR | NGAF 7.4, EDR分析结果, and status indicators for 隔离, 信任, and 忽略.
- Table:** A table with columns for 序号 (Serial Number), 风险主机 (Risk Host), 感染病毒类型 (Infection Virus Type), and 感染文件 (Infection File). The table contains 6 rows of data, all with a risk level of 永恒之蓝 (Forever Blue).
- Browser Window:** A browser window is overlaid on the right side, displaying a warning message: "检测到主机感染病毒!" (Detected host infection virus!). The message states: "防火墙检测到您的计算机已被病毒感染, 存在安全风险, 当前您访问的网页已被重定向。" (The firewall has detected that your computer has been infected with a virus, posing a security risk. The webpage you are currently visiting has been redirected.) It also provides advice: "建议下载反僵尸网络软件, 运行'病毒扫描'功能以彻底清除受感染主机中的僵尸病毒, 并安装EDR终端检测响应软件以免再次中毒。" (It is recommended to download anti-botnet software, run the 'virus scan' function to thoroughly clear botnet viruses from the infected host, and install EDR endpoint detection and response software to prevent re-infection.) Two buttons are visible: "下载反僵尸网络软件" (Download anti-botnet software) and "下载EDR软件" (Download EDR software).

序号	风险主机	感染病毒类型	感染文件
1	200.200.200.142	永恒之蓝	恶意文件: www 文件Hash: sdfa 发现时间: 201
2	200.200.200.142	永恒之蓝	恶意文件: www 文件Hash: sdfa 发现时间: 201
3	200.200.200.142	永恒之蓝	恶意文件: www 文件Hash: sdfa 发现时间: 201
4	200.200.200.142	永恒之蓝	恶意文件: www 文件Hash: sdfa 发现时间: 201
5	200.200.200.142	永恒之蓝	恶意文件: www 文件Hash: sdfa 发现时间: 201
6	200.200.200.142	永恒之蓝	恶意文件: www 文件Hash: sdfa 发现时间: 201



第十六届民航信息化发展论坛