



# OfficeScan 12 亮点功能介绍

# OfficeScan 12 亚信版

## 亮点功能:

- 机器学习预测功能
- 勒索软件防护增强功能
- 可疑文件样本提交
- CVE弱点攻击扫描



## 卖点：

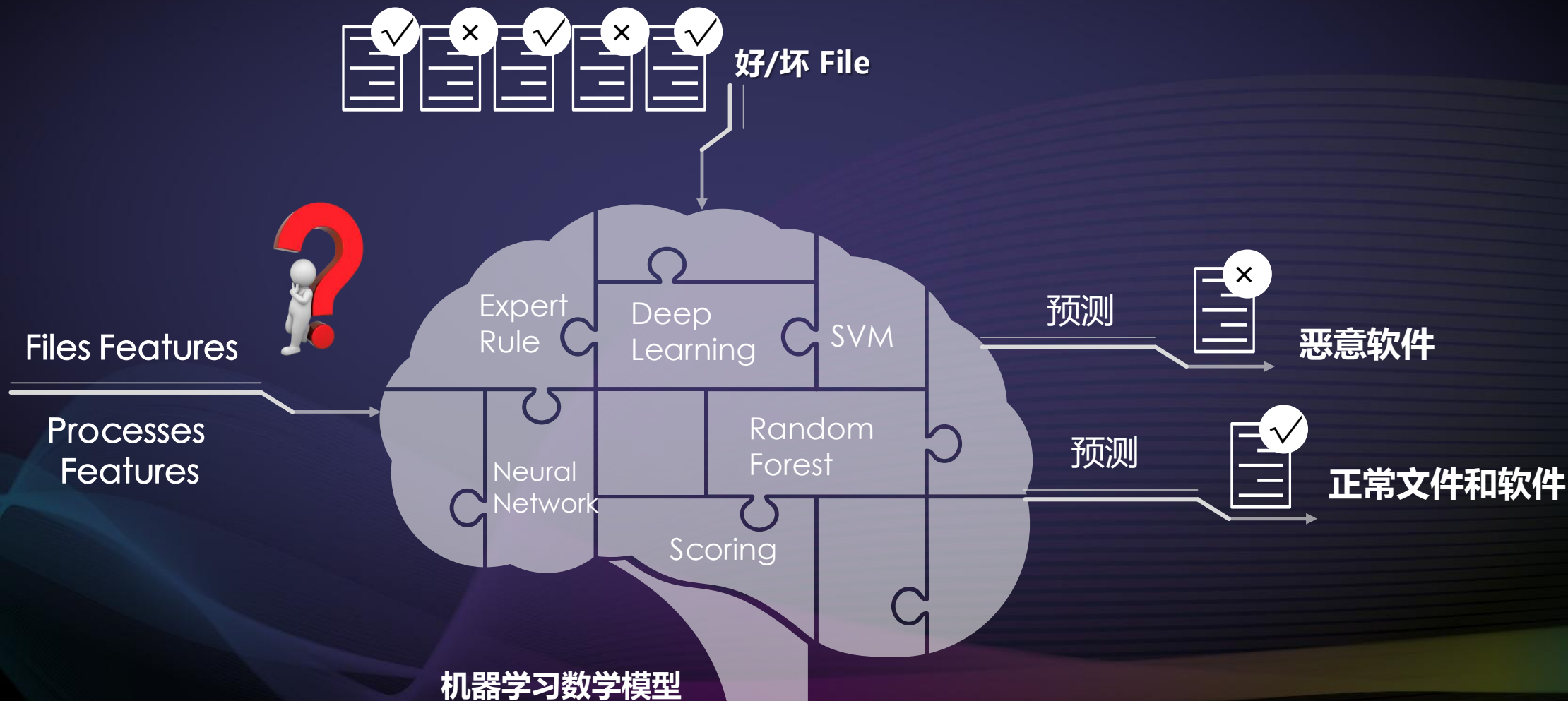
- 机器学习拦截未知病毒 — 拦未知
- 有效阻止勒索软件 — 防勒索
- 智能联动的安全防护体系 — 智能联动
- 杜绝文档型漏洞攻击 — 阻止恶意文档

# OfficeScan 12 机器学习介绍



# OfficeScan 12 机器学习介绍

「亚信安全使用被训练过的机器学习模型可以预测未知的文件是否是恶意软件还是正常文件」



# OfficeScan 12 机器学习介绍



## 训练机器学习的数据量和文件特征处理的能力最重要

100TB/天  
50万新恶意软件/天  
10亿白名单

海量

数据

全球数据，交给机器学习的恶意软件和正常文件的样本数量最多，种类最全

精准

特征

25年以上恶意软件鉴别知识和技术的积累，更精准的定义和优化恶意软件的特征

算法

算法

10年以上机器学习算法技术积累

轻简

模型

高精度,低功耗双重机器学习威胁检测模型



# 机器学习引擎截获未知恶意程序日志-WannaCry

预测机器学习日志详细信息

Ransom.W



2017/5

已隔离

什么时

## RANSOM\_HPCRYPTESLA.SM2

September 05, 2016

Analysis by: Michael Jay

**ALIASES:** Win32/Filecoder.TeslaCrypt.K (ESET), Trojan.Cryptolocker.N (Symantec), Trojan.Win32.Filecoder (Ikarus)

**PLATFORM:** Windows

**OVERALL RISK RATING:**

**DAMAGE POTENTIAL:**

**DISTRIBUTION POTENTIAL:**

**REPORTED INFECTION:**

**INFORMATION EXPOSURE:**

相似的恶意软件在2016年9月就已经出现，使用学习过这些样本的机器学习引擎可以有效拦截

威胁指示器

威胁概率

100%

亚信安全预测



文件DNA

- CreateProcessA
- CreateServiceA
- DeleteCriticalSection

WannaCry存在可疑行为的系统接口调用列表



Web

C:\Users\aaa\Downloads\

什么位置 Where

文件功能检测新兴未知安全风险。

类似已知威胁  
Ransom\_HPCRYPTESLA.SM2

相似已知恶意  
程序列表

## 亚信安全成功抵御全球第一只勒索蠕虫WannaCry

上海某电站启用OfficeScan 11行为监控功能后，成功防御了WannaCry勒索加密行为

	F	G	H	I	J	K	L
1	日志类型	策略	主题	事件类型	目标	处理措施	操作
2	事件监控	未经授权的文件加密	c:\programdata\oagynumukqlbox081\tasksche.exe	文件系统	C:\Users\41710195\Desktop\201	终止	关闭
3	事件监控	未经授权的文件加密	c:\windows\tasksche.exe	文件系统	C:\Users\41710195\Desktop\201	终止	关闭
4	事件监控	未经授权的文件加密	c:\programdata\oagynumukqlbox081\tasksche.exe	文件系统	C:\Users\41710195\Desktop\201	终止	关闭
5	事件监控	未经授权的文件加密	c:\programdata\oagynumukqlbox081\tasksche.exe	文件系统	C:\Users\41710195\Desktop\201	终止	关闭
6	事件监控	未经授权的文件加密	c:\programdata\oagynumukqlbox081\tasksche.exe	文件系统	C:\Users\41710195\Desktop\201	终止	关闭
7	事件监控	未经授权的文件加密	c:\programdata\oagynumukqlbox081\tasksche.exe	文件系统	C:\Users\41710195\Desktop\201	终止	关闭
8	事件监控	未经授权的文件加密	c:\programdata\oagynumukqlbox081\tasksche.exe	文件系统	C:\Users\41710195\Desktop\201	终止	关闭
9	事件监控	未经授权的文件加密	c:\windows\tasksche.exe	文件系统	C:\Users\41710195\Desktop\201	终止	关闭
10	事件监控	未经授权的文件加密	c:\programdata\oagynumukqlbox081\tasksche.exe	文件系统	C:\Users\41710195\Desktop\201	终止	关闭
11	事件监控	未经授权的文件加密	c:\programdata\oagynumukqlbox081\tasksche.exe	文件系统	C:\Users\41710195\Desktop\201	终止	关闭
12	事件监控	未经授权的文件加密	c:\programdata\oagynumukqlbox081\tasksche.exe	文件系统	C:\Users\41710195\Desktop\201	终止	关闭
13	事件监控	未经授权的文件加密	c:\programdata\oagynumukqlbox081\tasksche.exe	文件系统	C:\Users\41710195\Desktop\201	终止	关闭
14	事件监控	未经授权的文件加密	c:\programdata\oagynumukqlbox081\tasksche.exe	文件系统	C:\Users\41710195\Desktop\201	终止	关闭
15	事件监控	未经授权的文件加密	c:\programdata\oagynumukqlbox081\tasksche.exe	文件系统	C:\Users\41710195\Desktop\201	终止	关闭



### 勒索软件加密的文件恢复

#### 自动备份被可疑程序更改的文件功能：

启用后，可以为终端上正加密的文件创建副本。加密过程完成且防毒墙网络版检测到勒索软件威胁之后，防毒墙网络版将提示最终用户恢复受影响的文件，且不会丢失任何数据。

# OfficeScan 12 联动功能介绍

1. 勒索软件感染了一个终端
2. 网络的威胁发现设备(TDA/DDEI)发现了这个感染事件
3. 透过威胁防御管控中心TMCM,实时的将勒索软件的SO (IP, SHA-1, URL) 推送到该终端设备并进行清除或隔离,同时根据预先设定的规则给所有其它终端
4. 通过TMCM调查该勒索病毒感染的区域和是否已经扩散



# OfficeScan 12 联动功能介绍

1. 勒索软件试图感染终端或通过邮件进入企业网
2. 提交给沙盒(DDAN)检测评估

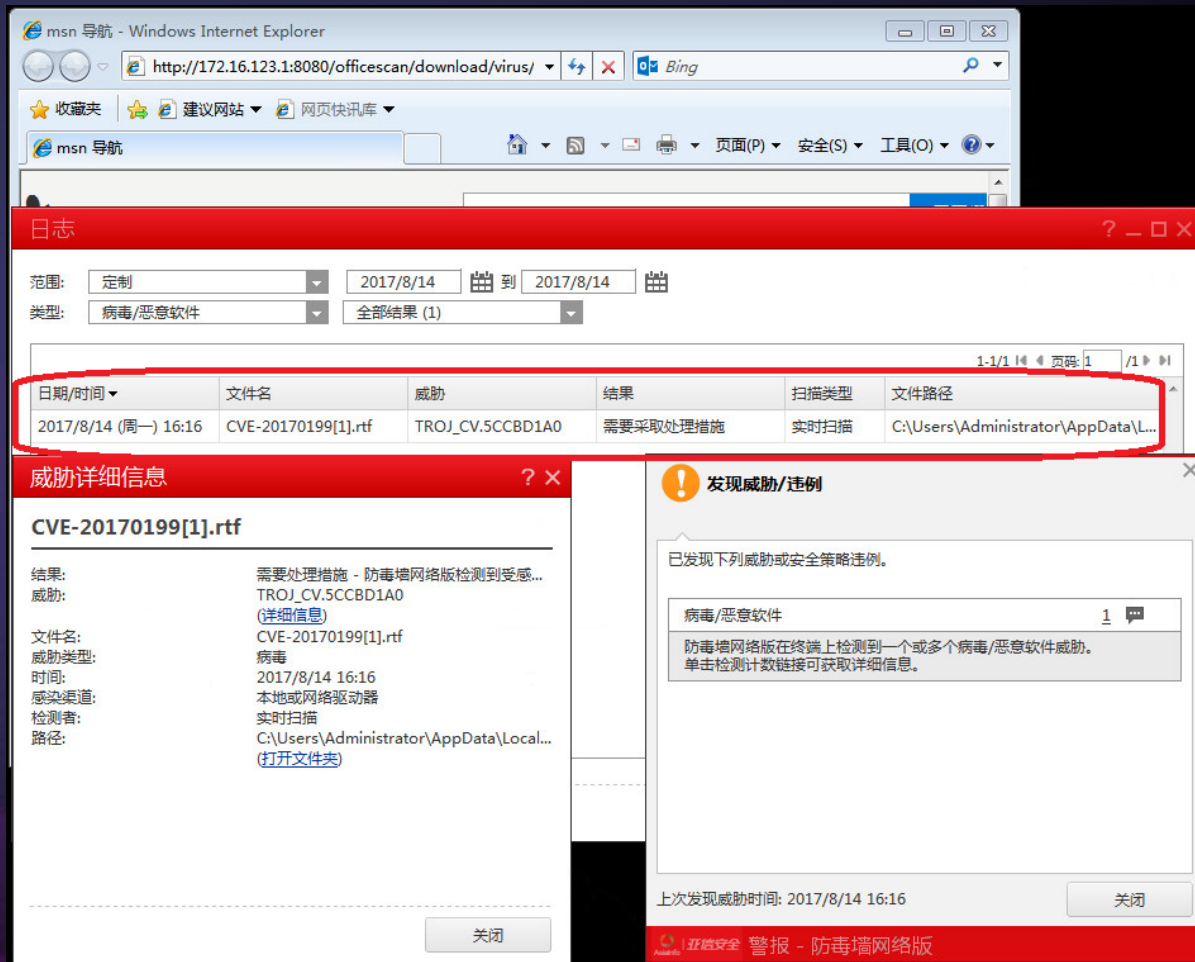
3. 沙盒发送勒索软件的SO(Sha-1,IP,URL)信息给TMCM, 提交沙盒的OSCE终端将从TMCM哪里获得给对应的SO并和操作策略
4. 同时TMCM管理中心通过**情报分享, 自动发送该SO**给组织内部所有的其他终端。



威胁防御控管中心(TMCM)

# Office Scan 12 CVE弱点攻击扫描-防止文档型漏洞攻击

- 通过ATSE（高级威胁扫描引擎）及时防护经由网页/电子邮件下载的文档漏洞利用(CVE)
- 例如 Petya勒索病毒变种Petwrap 使用 office 远程执行代码漏洞 [CVE-2017-0199](#)

The screenshot shows a Windows Internet Explorer browser window displaying a log entry for a detected threat. The log entry is highlighted with a red box and contains the following information:

日期/时间	文件名	威胁	结果	扫描类型	文件路径
2017/8/14 (周一) 16:16	CVE-20170199[1].rtf	TROJ_CV.5CCBD1A0	需要采取处理措施	实时扫描	C:\Users\Administrator\AppData\L...

Below the log entry, a "威胁详细信息" (Threat Details) window is open, showing the following information:

**CVE-20170199[1].rtf**

结果: 需要处理措施 - 防毒墙网络版检测到受感...  
 威胁: TROJ\_CV.5CCBD1A0  
 (详细信息)  
 文件名: CVE-20170199[1].rtf  
 威胁类型: 病毒  
 时间: 2017/8/14 16:16  
 感染渠道: 本地或网络驱动器  
 检测者: 实时扫描  
 路径: C:\Users\Administrator\AppData\Local...  
 (打开文件夹)

On the right, a "发现威胁/违例" (Detected Threat/Violation) window shows a notification: "已发现下列威胁或安全策略违例。" (The following threats or security policy violations have been discovered.)

病毒/恶意软件 1

防毒墙网络版在终端上检测到一个或多个病毒/恶意软件威胁。单击检测计数链接可获取详细信息。

上次发现威胁时间: 2017/8/14 16:16

关闭

非信安全 警报 - 防毒墙网络版



# Office Scan 12 CVE弱点攻击扫描-防止文档型漏洞攻击

## 支持的文档扩展名

扩展名	名目
Word	DOC, DOCX, DOCM, DOT, DOTX, DOTM
Excel	XLS, XLSX, XLSM, XLSB, XLT, XLTX, XLTM, XLA, XLAM
PowerPoint	PPT, PPTX, PPTM, POT, POTX, POTM, PPS, PPSX, PPSM, PPA, PPAM
Outlook	MSG
Office	XPS, MHT, MHTML
Other	PDF, RTF, SWF, XLR, WPS, WPD, ODT

## 支持的应用

渠道	进程名
电子邮件	- outlook.exe - wlmmail.exe
浏览器	- iexplore.exe - chrome.exe - firefox.exe - microsoftedge.exe - microsoftedgecp.exe - browser_broker.exe - opera.exe - safari.exe - sleipnir.exe



# 最新评测，依然领先

## 2017 Gartner 终端安全魔力象限



2017最新报告被推荐,  
获得误报率为0的好成绩



2016 获得所有的Award,  
误报率评测获Gold Award



持续3年累积评测得分最高

### Magic Quadrant

Figure 1. Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (January 2017)