安天智甲防勒索病毒解决方案

安天产品事业部

長纓待展

CONTENTS

目 录

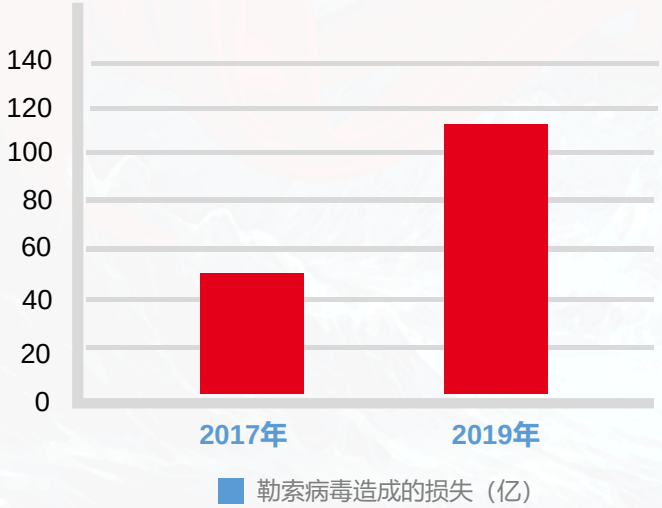
智者安天下

01 勒索病毒现状与演变

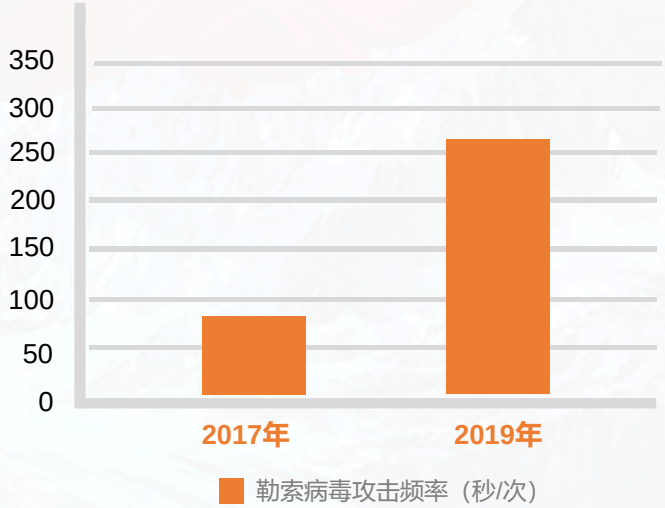
危害、现状、演变

勒索病毒危害不断加剧

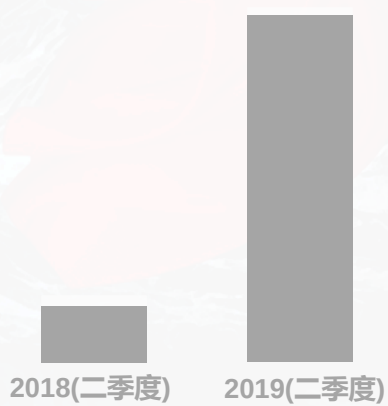
2017年与2019年勒索软件造成的花费对比



2017年与2019年勒索软件攻击频率对比



针对企业的勒索病毒攻击数量比对



根据Cybersecurity Ventures的预测，2015-2017年由勒索病毒造成的损失将达到50亿美元，在2019年会攀升至115亿美元勒索病毒威胁全球，中国、美国、俄罗斯遭受了最多攻击；

飙升的损失主要由愈发频繁的攻击导致，勒索病毒针对业务的攻击频率由每40秒一次提高到2019年的每14秒一次；

勒索病毒攻击将重点从消费者转移至企业，针对企业的勒索病毒攻击数量首次超过了针对消费者的数量，前者在2019年第二季度比2018年第二季度增长了363%。

数据引自：
https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/
https://www.aqniu.com/industry/29701.html
http://www.199it.com/archives/921445.html

勒索病毒演变

03

开始出现窃取用户敏感数据，以公开数据相威胁逼迫用户支付赎金，形成“勒索+窃密”的新组合

02

病毒制作和传播门槛不断降低

04

从以往的水坑攻击、钓鱼邮件等发展为远程代码执行漏洞利用、暴力破解等方式，入侵和传播能力增强

01

新型病毒家族数量越来越多，变种更新频繁

05

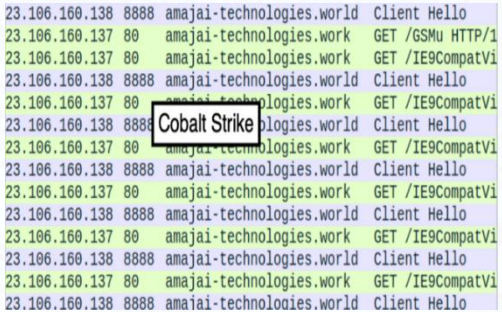
采用内存加密、进程注入方式、盗用签名、系统进程利用等方式增加了防御难度

定向攻击+数据窃取+数据加密，辅以曝光威胁成为套路模式

定向攻击

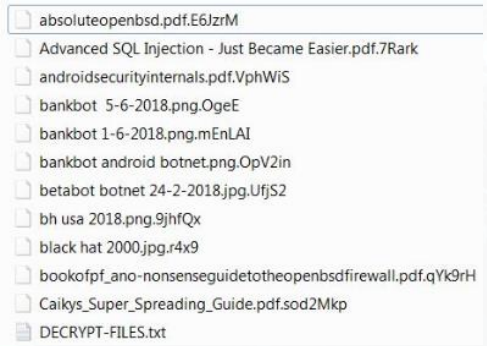
闪存巨头SK Hynix公司遭到了Maze勒索软件定向攻击。

数据窃取



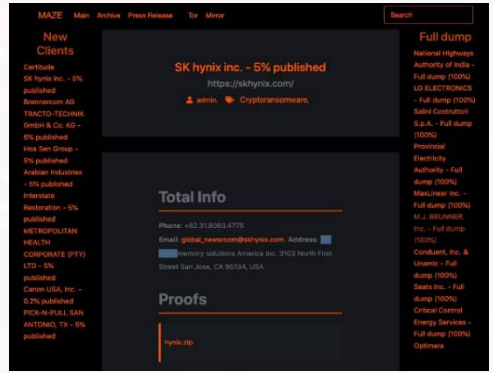
Maze勒索软件攻击者先投放Cobalt Strike进行窃密，然后下发勒索软件进行加密勒索。

数据加密



Maze勒索软件加密计算机上的文件，在文件名结尾追加由字母和数字随机组合形成的后缀。

数据曝光



Maze勒索软件攻击者曝光了从SK Hynix公司的窃取的部分数据文件。

威胁框架：细粒度对抗

02 病毒分析与防护方案

分析对比、防御核心、防护方案

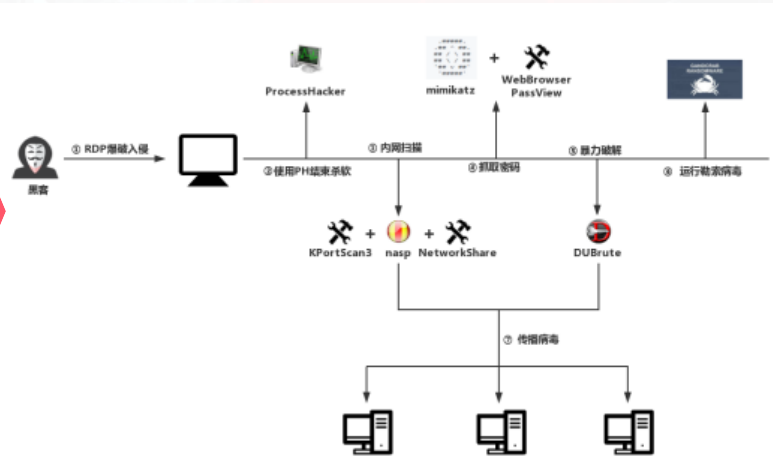
典型勒索病毒分析对比

加密数据，提供赎金解锁文件 ⟶ 蠕虫化传播，攻击网络中其它机器 ⟶ RDP爆破入侵，加密数据

TeslaCrypt勒索病毒

WannaCry勒索病毒

GandCrab勒索病毒



主机可能感染勒索病毒的途径

蠕虫式传播

通过漏洞和口令进行网络空间中的蠕虫式传播
典型案例：WannaCry、Petya变种
主要对象：无定向，自动传播都有可能

Exploit Kit分发

通过黑色产业链中的Exploit Kit漏洞套件来分发勒索软件
典型案例：Cerber
主要对象：有漏洞的业务Server

钓鱼邮件/水坑攻击

恶意代码伪装在邮件附件中，诱使打开附件
典型案例：Locky、Petya变种
主要对象：个人PC

暴力破解

通过暴力破解RDP端口、SSH端口，数据库端口
典型案例：.java 、 GlobeImposter变种
主要对象：开放远程管理的Server

勒索病毒防护难点

难点一

传统病毒库检测机制逐渐失效

新型病毒不断出现，导致基于文件静态特征检测的方式无法及时具备对新型病毒的检出能力，这种情况在隔离网络这种病毒库更新滞后的环境中更是凸显。

难点二

入侵技术的提升给传统主动防御机制造成极大挑战

现阶段勒索病毒的加密技术在快速迭代与提升，由简单粗暴到精细化作业，通过进程注入、系统服务利用、签名伪造等方式躲避杀软防御，给防护带来了极大挑战。

难点三

缺乏完善的端点安全防护机制

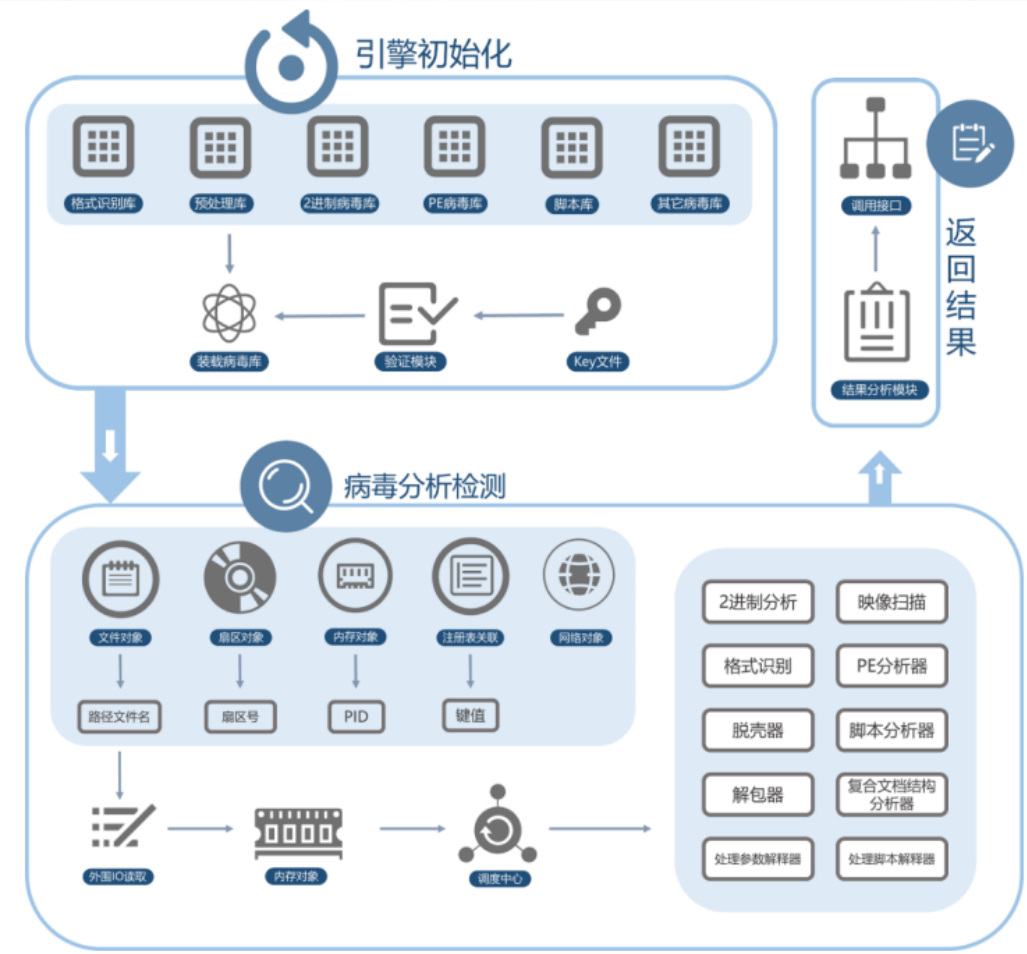
勒索病毒的攻击常常是利用系统漏洞、弱口令等主机脆弱点，单纯依靠病毒防御，而不从根本上加固主机，缩小受攻击面，则依然会给主机带来极大安全风险。

智甲防勒索核心能力

防勒索关键——在端点建立有效的安全防护能力

防火墙、流量检测、备份系统能够一定程度上防御勒索软件，但很多方式**治标不治本**

依托下一代反病毒引擎实现文件多元向量检测



实现原理

基于私有云架构，在云端存储海量病毒特征，当文件进入系统时，通过云查杀功能自动检测文件安全属性，判定是否为勒索文件

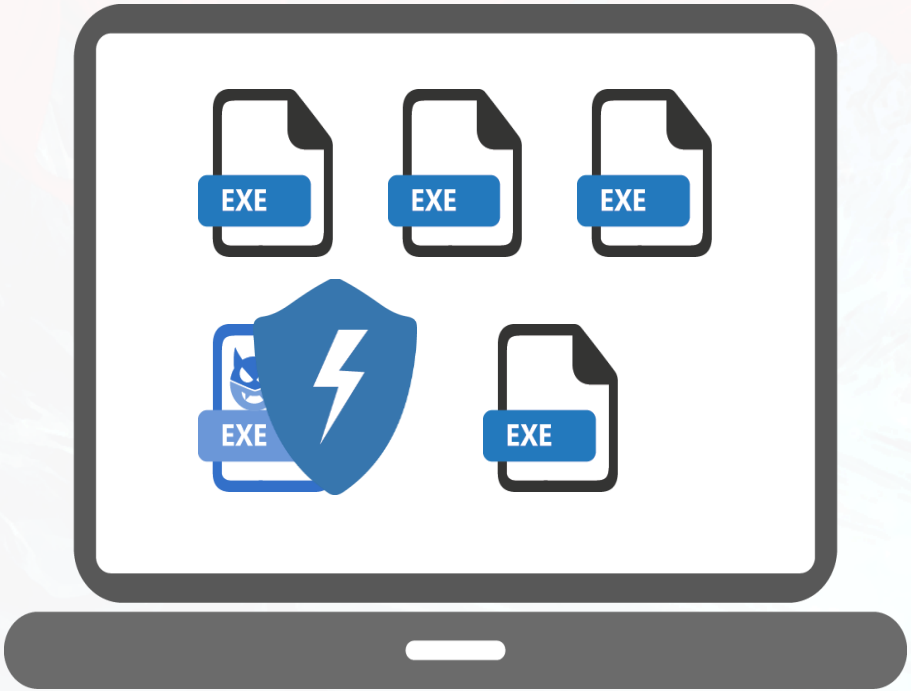
功能价值

可对已知勒索软件即时发现并拦截

防护范围

系统各来源新增文件，包括：浏览器下载、即时通讯传输、邮件附件、下载工具、U盘拷贝.....

针对性、细粒度主动防御能力



实现原理

客户端构建勒索行为特征库，包括写操作文件加密防御、重命名加密防御、删除重建加密防御、注入式加密防御、直接内存加密防御、内存映射加密防御等多种机制，发现具有勒索行为的进程，立即拦截并告警。

功能价值

能够在不依赖病毒库情况下，对未知勒索软件进行检测与防护

防护范围

系统终端非授信进程。

文件可操作进程范围限制

实现原理

可设定受保护文件夹与文件类型，阻止非授信进程的修改，并能对可能被恶意修改的文件进行备份与还原。

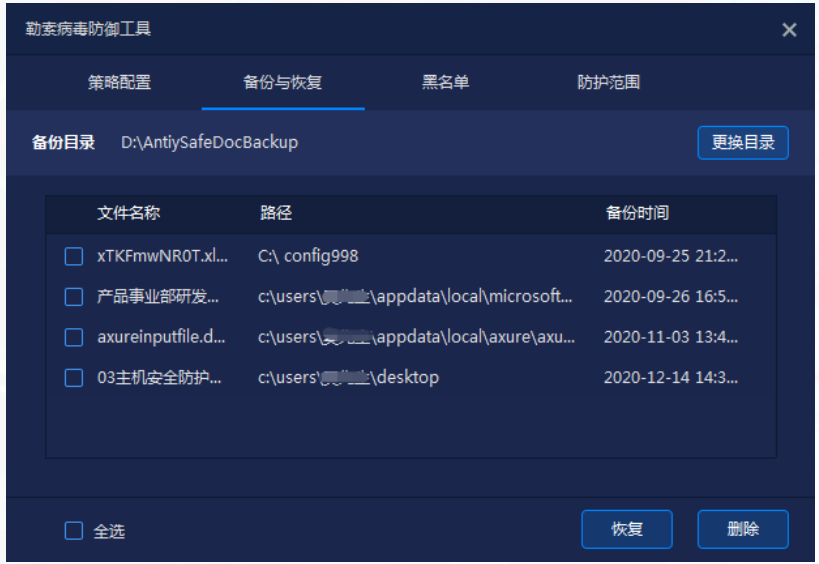
功能价值

保障核心文档的安全

防护范围

核心文件。

文件智能备份，将损失减少到最低



实现原理

当发现文件可能疑似遭受勒索病毒破坏时，智甲支持自动对文件进行本地加密备份，并禁止其他一切进程访问，用户可手动进行文件还原。

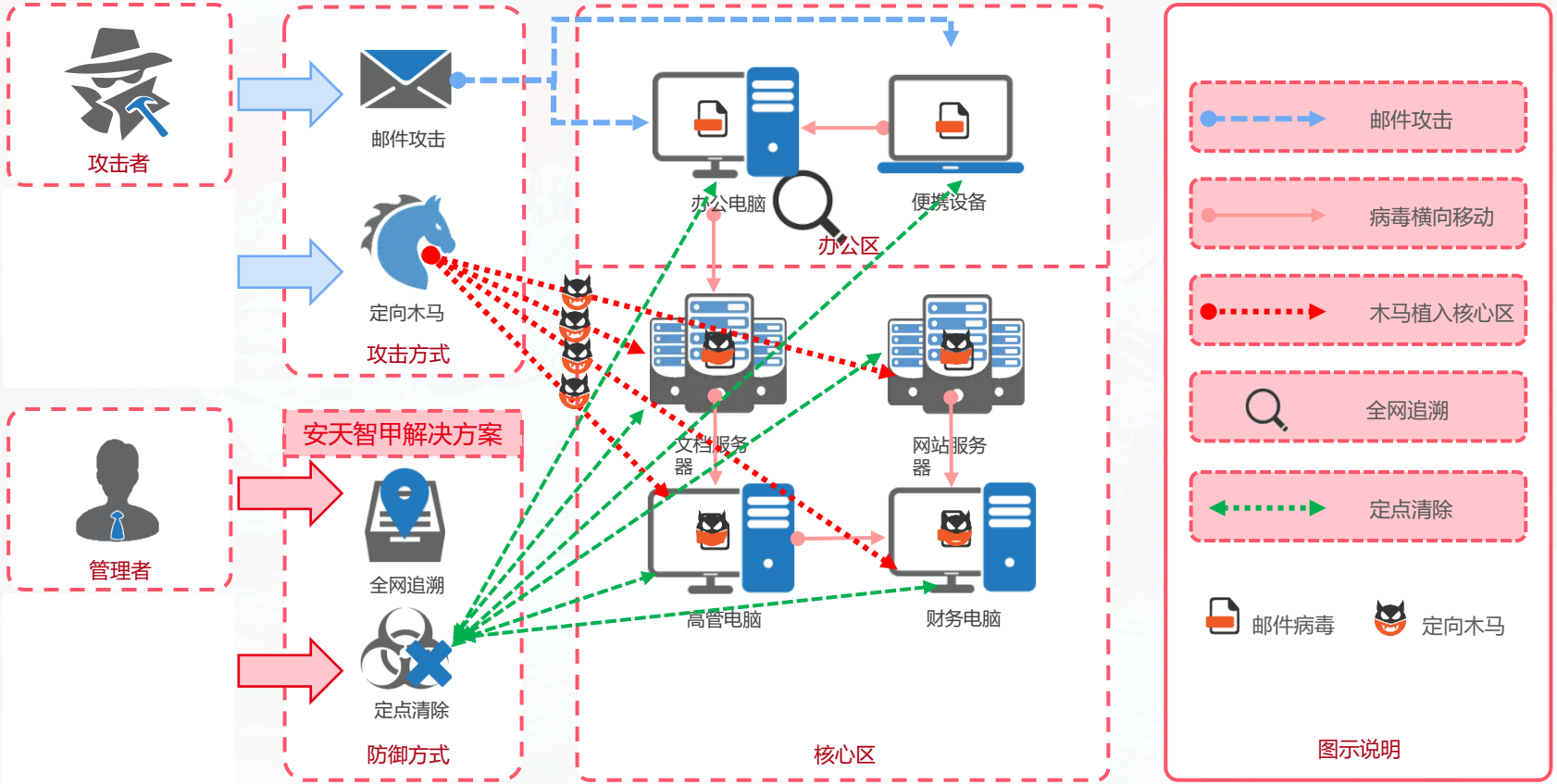
功能价值

传统备份工具资源消耗高，用户使用成本高，智甲可精准识别攻击行为的发生，进行自动化备份，将用户损失降到最低

防护范围

核心文件。

威胁快速响应“全网追溯+定点清除”



一台终端发现威胁 -> 15分钟内全网追溯 -> 远程一键清除

漏洞与补丁管理，提升主机安全性

可检测对象

- 操作系统，包括Windows、Linux、国产化系统
- 应用软件，包括Office、Adobe…
- 数据库，MySQL、SQLServer…
- Web组件：Apaceh、iiS……

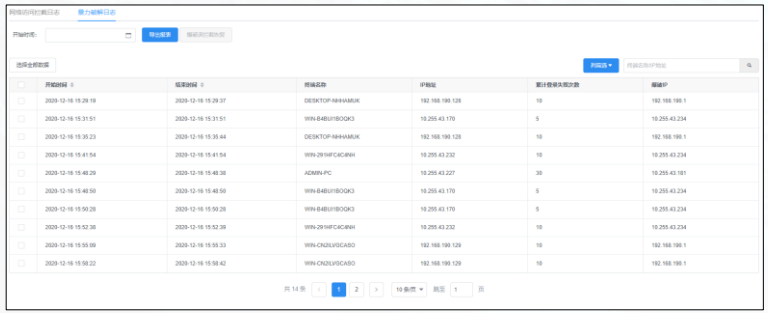
补丁更新流程

- 选取灰度测试终端
- 客户端一键检测漏洞存在情况
- 智能屏蔽不适配、无效补丁
- 漏洞与所需补丁信息上报管理中心
- 从管理中心下载补丁升级文件
- 补丁安装
- 补丁修复效果验证
- 扩大修复范围

补丁获取方式

- 互联网环境，从智甲互联网升级服务器下载
- 隔离网环境，使用专用下载工具下载后上传至管理中心

主机防火墙，拦截针对主机的网络攻击行为



网络连接管控

- 基于IP、端口、协议等设置放行/阻止等管控规则
- 对违规联网行为阻断和记录

程序联网管控

- 对联网程序以及基础网络连接信息进行记录
- 支持设置是否允许特定程序连接网络

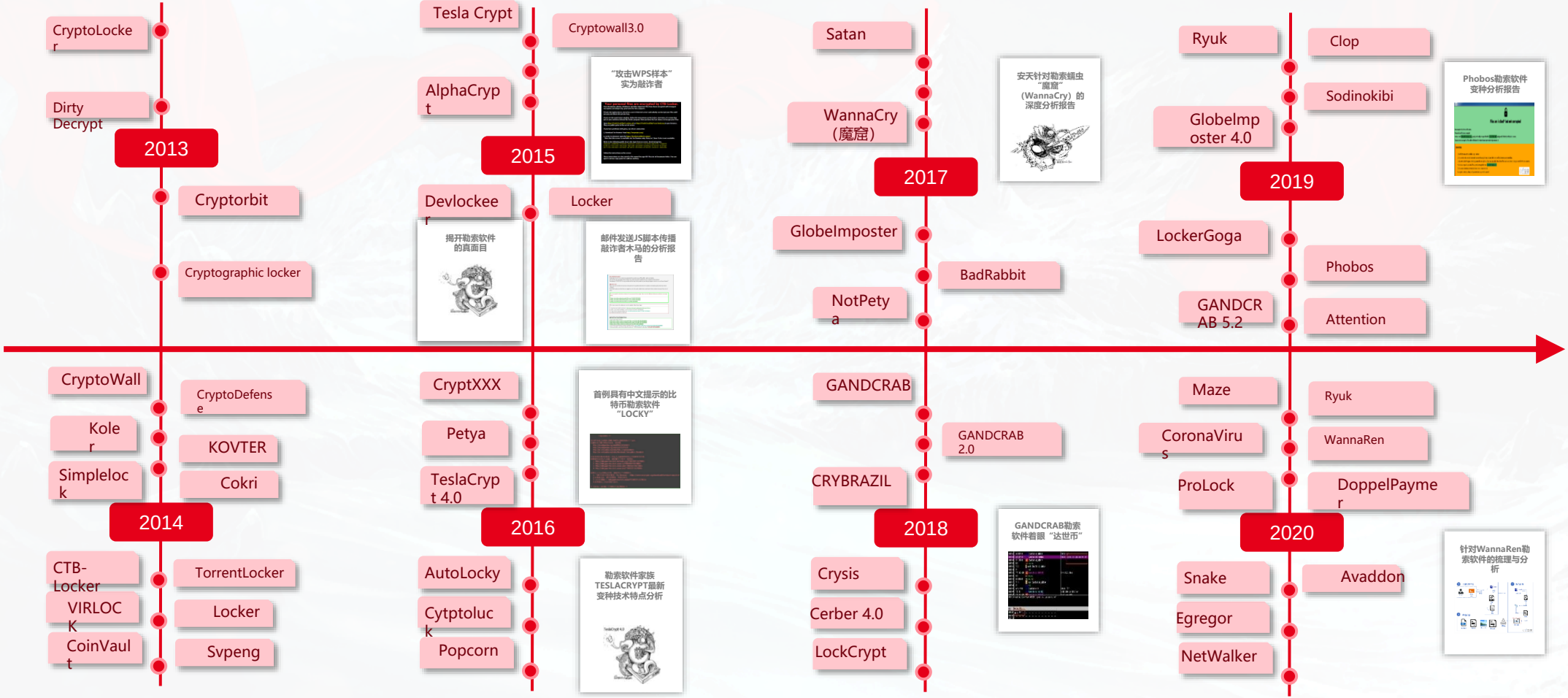
流量管控

- 程序网络流量统计
- 程序网络访问限速

网络攻击防护

- 暴力破解防护
- SMB漏洞攻击防护

对勒索病毒进行持续分析和产品研发投入



勒索病毒防护优势——产品&能力

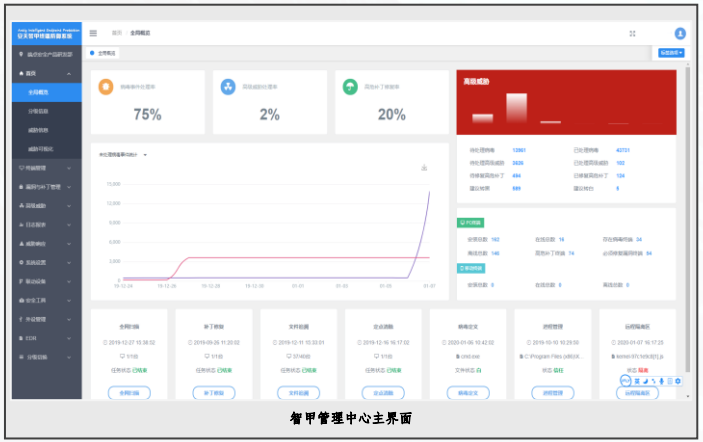
01 较早就开始了针对防勒索持续投入，具有深厚的实战经验；

02 依托自研反病毒引擎，可对勒索病毒进行精准查杀；

03 多种防护机制融合，层层阻隔，有效拦截，为端点提供强大的防御能力

智甲产品简介

智甲客户端主界面



智甲管理中心主界面

——产品定位——

智甲终端防御系统是安天研发的面向政企客户的**端点类综合安全防护软件**，其内置**安天下一代威胁检测引擎**，为办公机、服务器、虚拟化节点、移动设备、国产专用计算机、各类自助终端、工控上位机等各类端点场景提供**多层次、全周期的动态防护能力**。

——功能、优势与价值——

核心功能

- 反病毒，包括病毒查杀、主动防御、威胁分析、威胁追溯与清除等；
- 终端管控，包括外设管控、运行管控、网络管控、白名单等。

产品优势

- 主动防御能力，尤其是针对勒索者、挖矿病毒等新型威胁；
- 国产化防护方面具有领先优势，投入早、适配全，与全部主流国产化操作系统厂商完成兼容性互认证。

用户价值

- 支持多种平台和不同类型终端的统一管理；
- 为威胁情报和态势感知提供重要的数据支撑。

可适配平台——具有良好的兼容与适配能力

客户端可适配环境

适配操作系统

平台	版本
Windows	支持Windows XP/Win 7/Win 8/Win 10/Win 10政府版等桌面操作系统 支持Win 2003/Win 2008/Win 2012/Win 2016等服务器操作系统
Linux	支持CentOS、Redhat、Ubuntu、Debian、SUSE等
国产化操作系统	支持UOS、中标麒麟、银河麒麟、中科方德、凝思、深度和中标普华等
Android	支持Android 5.0以上所有操作系统

适配硬件平台

支持**x86（Intel、AMD）**、**MIPS（龙芯）**、**ARM（飞腾）**、**鲲鹏**等硬件平台

适配虚拟化平台

支持**VMware**、**KVM**、**H3C**、**华为**、**Xen**、**深信服**、**阿里云**等虚拟化平台

管理中心可适配环境

硬件平台	操作系统
x86	CentOS 7.0-7.5
x86	Redhat7.0-7.5
x86	中标麒麟V7U4
x86	中科方德
鲲鹏	ubuntu18.04.1
鲲鹏	UOS

03 防御成果展示

防护视频、防御能力

实战化的终端防御能力建设

安天在国内较早专门针对“勒索软件”发布分析报告并持续跟进。

- 智甲在不依赖病毒检测，不升级软件的情况下，可有效防御多数勒索软件。

- **Win7 64**

  共测试样本121个，首次防御成功比率98.4%

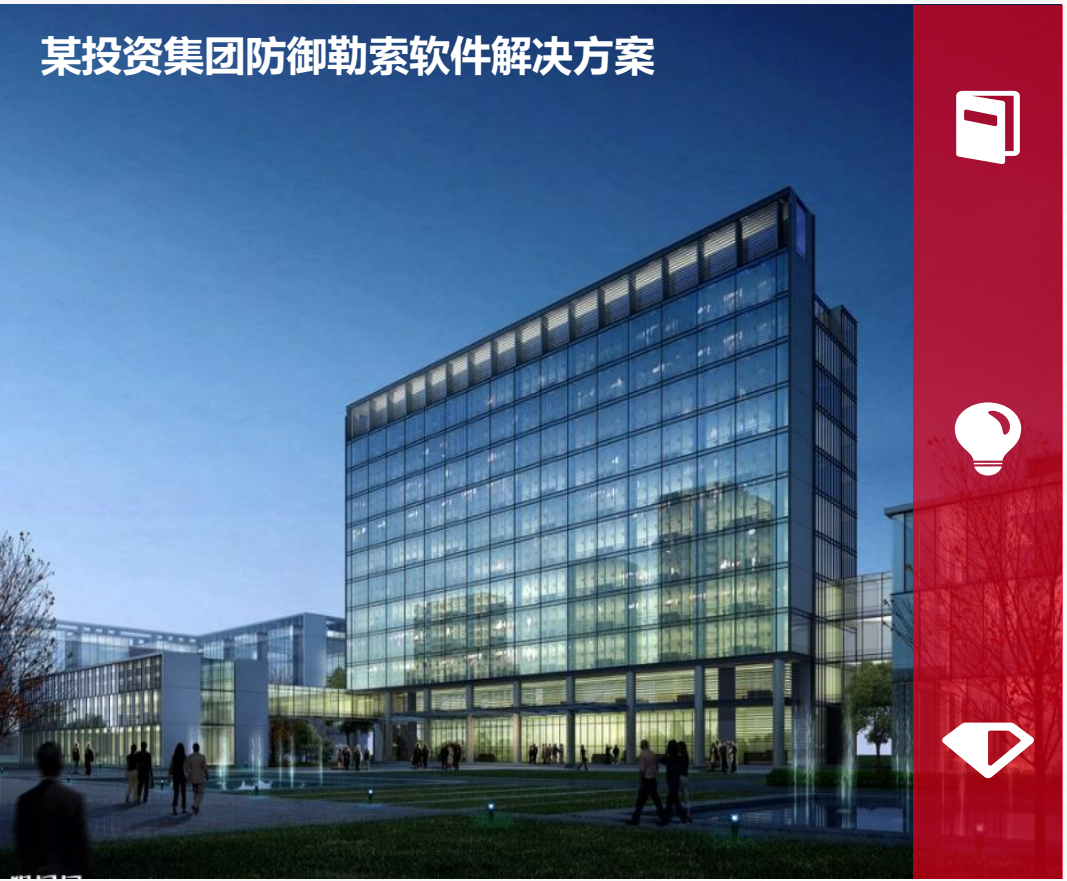
- **Win10 64**

  共测试样本119个，首次防御成功比率97.5%

数据来源：*安天自测

04 典型案例分享

实战案例——某投资集团案例



项目背景

某投资集团，其核心数据的安全性关乎全省经济发展大局。其集团OA系统和财务系统受到勒索软件攻击，约20万个关键文件被加密，断网8日，对工作运行产生严重影响并造成一定经济损失。

安天方案

安天智甲终端防御系统拥有专门的针对勒索软件的文档保护功能。该功能通过勒索行为感知、传输文件深度检测与管控、文档访问控制的方式，对勒索软件进行层层阻断，让勒索软件无机可乘。

客户价值

帮助用户加固系统，防御恶意代码入侵，实时保护用户核心资产安全，持续保障用户业务顺畅，为用户构建相对安全的办公环境，降低用户风险，增强用户的安全自信。

谢谢大家