网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

亂雲飛渡

资源代价与安全算力

危城智甲

——端点安全防护的资源代价与优化

安天 | 端点安全部

CONTENTS

目 录

01 端点安全防护资源分配现状

02 端点安全防护资源占用优化方案

03 安天智甲对资源占用优化的工程实践

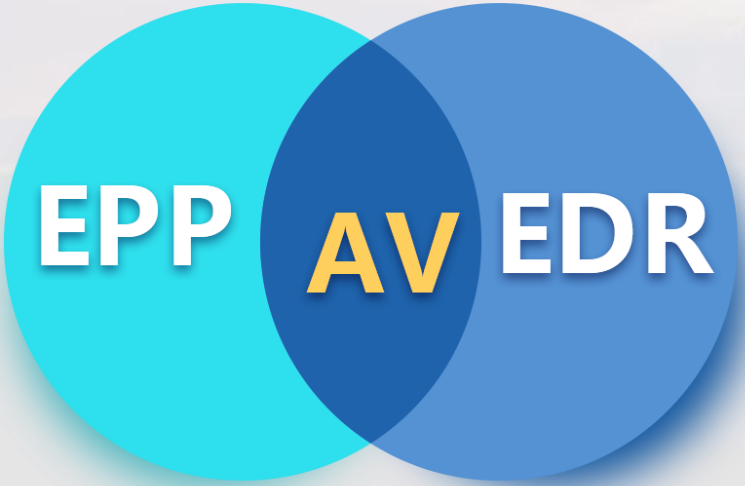
04 未来展望

01 端点安全防护资源分配现状

端点防护产品能力提升同时资源消耗增加

代码片段	独立文件	场景化	高级持续过程
感染式病毒 宏病毒	蠕虫 木马	主机：Rootkit、KillAV 服务器：钓鱼勒索	工业控制 认证体系

EPP+EDR



AV产品

防护方式：

- 实时检测
- 病毒查杀

反病毒引擎

算力需求特性：

病毒查杀时，资源占用相对较高，具有间歇性资源占用的特点

EPP产品

防护方式：

- 多种管控能力
- 其他能力
- 统一管理

AV

算力需求特性：

持续性进行监控，以及不断扩充的管控规则，整体资源消耗情况高于AV产品。

EPP+EDR产品

防护方式：

- 采集数据
- 其他能力
- 情报分析
- 快速响应

EPP

算力需求特性：

持续性进行监控和采集，日常运行消耗资高于传统EPP产品，进行威胁分析时，服务器资源消耗也高于传统EPP产品。

资源消耗伴随增加

资源共享性与同步运行导致资源争抢矛盾加剧

系统资源共享并且运行周期相同，随着业务系统和安全防护能力的资源需求增加，必然会出现资源抢占，影响用户业务和安全防护的效果，所以安全防护能力和资源消耗的平衡将成为关键。

国产化硬件算力阶段性受限让安全防护受到影响

国产CPU性能盘点 SPEC2006

公司	CPU	主频	核心数	单核性能	工艺	时间
申威	SW3232	2.4G	32	25+	14/16nm	2020
	SW432	2.4G	4	25+	14/16nm	2021
龙芯	3A5000	2.5G	4	25+	12nm	2020
	3C5000	2.5G	16	25+	12nm	2021
飞腾	FT-2000/4	2.6G	4	16.5	16nm	2019
	D2000	2.3G	4	18.6	14nm	2020
	S2500	2.0~2.2GHz	64	25+	16nm	2021
兆芯	KH-40000	3G	32	25+	16nm	2021
	KX-7000	3G	?	25+	16nm	2021
海光	HYGON C86	3.5G	8、32	35+	14nm	2020
英特尔	1165G7	3.6	4	45+	14nm	2021

随着国产处理器和操作系统自主研发技术的飞速发展，国产终端逐渐成为端点防护的重要战场，但国产硬件依然阶段性受限，这些限制也为国产端点的安全防护带来了挑战。不仅在硬件方面，一些信创特殊业务环境也让端点防护受到限制。

02 端点安全防护资源占用优化方案

从端点防护产品工作机理看资源消耗情况

类型	必要能力	资源消耗度
数据识别	文件识别、文件脱壳、特征提取、特征比对	高
行为体识别	进程启动监控、进程源文件识别，行为监控	高
网络流量识别	五元组采集、流量识别、网络攻击判定	高
数据采集的汇聚	资产数据采集、运行数据采集、威胁分析	高

检测 塑造 防护 响应

端点安全资源占用优化整体方案

病毒查杀

- 病毒库从HASH库到云代码特征库，降低服务器资源消耗
- 扫描策略化，优化病毒扫描策略，提高资源利用率

主动防御

- 识别主机特性，建立有针对性的防御策略，减少不必要资源消耗
- 防御能力可根据主机业务进行调整，保证防御连续性
- 基于安全威胁框架进行指导，使防控更加精准

数据采集

- 采集能力可配置，基于业务需要定制化采集点，减少不必要浪费
- 数据上报优化，减少带宽资源占用
- 通过端点防护一体化方式，减少数据重复采集，提高数据利用率

病毒查杀能力资源消耗优化

HASH病毒库到代码特征库

病毒库从单纯依赖HASH特征库升级到以**代码特征库为主**，HASH库为辅模式

代码特征可实现一条特征检测多个样本

可以达到5000万条特征可以覆盖100亿hash的能力

通过缓存机制减少重复扫描

建立主机和**服务器双缓存机制**，对相同文件再次检测时，可不用重新检查，直接通过缓存记录快速判定

缓存采用**路径hash+文件关键特征形式**，缓存匹配时无需计算文件hash值

扫描场景优化减少资源占用

闲时扫描机制，可以在主机资源相对充裕时进行病毒扫描工作，结合双缓存机制

配置扫描模式，可进行高/中/低占用模式切换，有效控制资源占用

特殊文件检测后置减少消耗

可以调整策略，过滤深层、较大的特殊文件，采用**完整性监控机制**，对特殊文件进行触发式检测，有效的避免因为扫描类似深层压缩包，产生的解包资源消耗等问题

发挥安天引擎内建安全机制

除了业务上的优化，还需要充分发挥**安天引擎内建的安全机制**，例如：跳过无毒格式文件等，也可以减少病毒查杀的资源消耗

针对端点属性合理建立主动防御策略

- 主动防御是对端点的系统环境、进程行为、运行状态等进行实时监控，发现异常行为时进行拦截，实现对多种入侵和破坏行为的防护；
- 监控范围越大虽然防护效果越强，但是同时对资源消耗也会加大，并且部分监控并不一定适用端点环境，造成资源浪费；
- 针对端点特性、业务场景，建立有针对性主防策略，减少资源浪费。

ATT&CK中技术点T1055.003防御策略对比

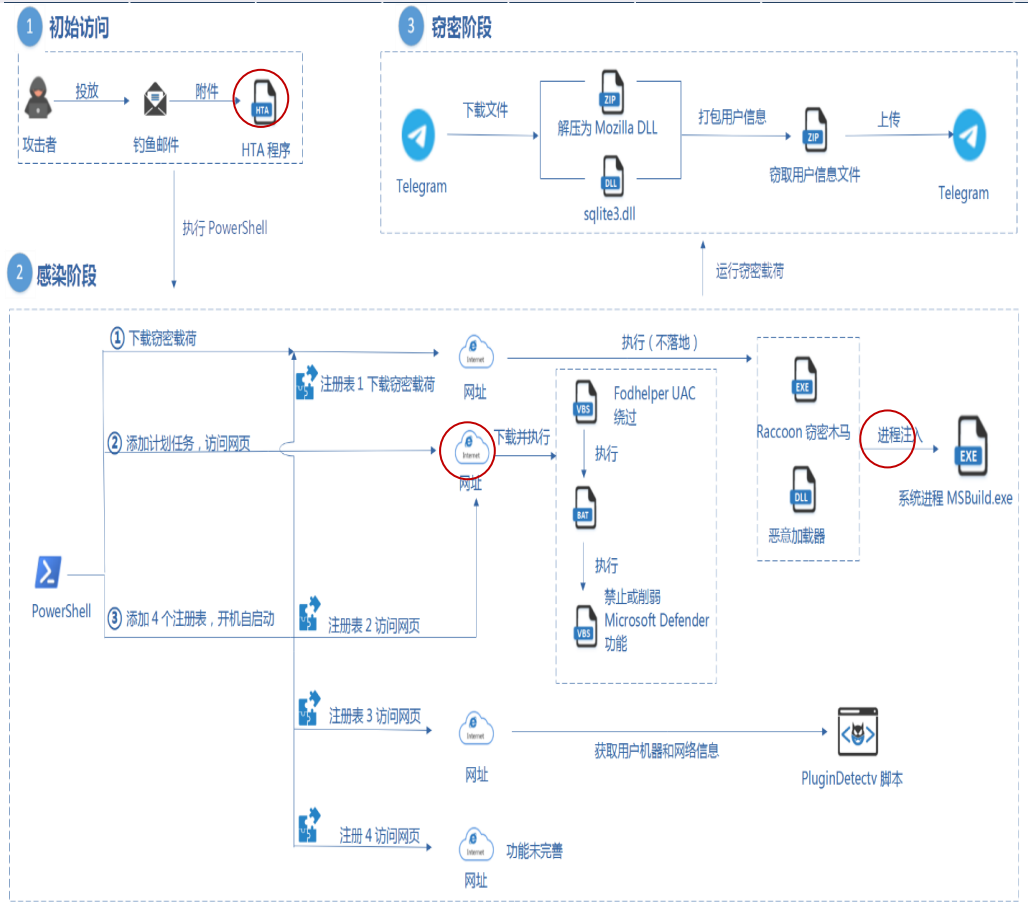
办公机

应用程序申请内存进行相应的实时检测，确定是否进行线程注入，通过对其他进程内存的写入数据的分析，从而确定是否有相应shellcode或恶意代码

服务器

为了保证服务器的业务程序的正常运行，会主动针对业务程序加强防御特征，直接拦截注入行为，以及对应用程序的改写行为。

以威胁框架为指导构建精准的防御策略



ATT&CK阶段/类别	具体行为	注释	防御手段
初始访问	网络钓鱼	攻击者发送带有恶意附件的电子邮件	网络流量监控->邮件协议解析->附件HTA程序检测
执行	利用命令和脚本解释器	用PowerShell命令和VB脚本执行恶意命令	PowerShell调用者检测，进程启动检测
	利用计划任务/工作	设置计划任务重复下载恶意文件	计划任务创建防护
	诱导用户执行	诱导用户解压恶意附件并双击运行	进程启动防护
持久化	利用自动启动执行引导或登录	攻击者设置开机启动项下载恶意文件	启动项防护
	利用计划任务/工作	设置计划任务重复下载恶意文件	任务计划防护、网络防护
提权	操纵访问令牌	攻击者使用重复的令牌创建新进程	令牌验证、进程启动防护
防御规避	执行签名的二进制文件代理	利用Mozilla DLL从Mozilla产品中收集数据	伪造、盗用、过期签名验证
	操纵访问令牌	攻击者使用重复的令牌创建新进程	令牌验证、进程启动防护
	反混淆解码文件或信息	载荷中多次使用到混淆代码和字符串	异常文件检测
	间接执行命令	调用VB脚本执行PowerShell命令	进程调用链检测
	修改注册表	添加注册表项实现开机自启动	注册表篡改防护
	进程注入	注入到合法的MSBuild.exe进程中	进程注入防护
凭证访问	从存储密码的位置获取凭证	搜寻密码管理器1Password和bitwarden	关键位置防护
	窃取Web会话Cookie	搜寻浏览器cookie值	浏览器防护

基于ATT&CK安全威胁框架使防护更加精准

安天中译版V10.0

数据采集实现可配置化并数据上报策略

力度可配置 采集项细

```
{
    "collect": "process_behavior",
    "desc": "进程监控",
    "switch": "1",
    "supplement":"1",    //是否补充上报 0：否 1：是
    "supplement_num":"1",    //补充次数
    "frequency":"second|0",//频率-类型|数值--类型：day-天-minute-分钟-second-秒钟
    "detail": [
        {
            "collect": "F_ProcBaseInfo",
            "desc": "父进程基础信息开关",
            "switch": "1",
        },
```

采集频率差异化

采集项	采集频率
系统资源信息	5 MIN
漏洞补丁信息	1 DAY

采集方式差异

采集项	采集策略
网卡信息采集	插拔事件触发时进行采集
软件信息采集	差量采集上报

数据上报策略 — 延时上报

数据上报处理 — 数据压缩

数据上报大小 — 流量阈值设置

基于威胁框架建立有价值的数据采集能力

文件实体
病毒文件、未知程序

网络五元组
源IP地址、源端口、目的IP地址、目的端口和传输层协议

网络访问行为信息
域名访问行为、网络下载信息等

文件信息
文件版本、文件创建时间、文件特征、文件MD5

资产信息
终端硬件与操作系统信息、软件名称、软件安装目录、文件详细信息

漏洞信息
采集系统、应用得漏洞信息

外设信息
USB存储设备文件信息、接入日志

进程监控信息
进程信息

配置信息
采集系统弱口令等配置信息

初始访问

执行

防御规避

发现

网络流量信息
采集网络事件、解析网络数据包、提取邮件

邮件信息
采集邮件发送者、邮件正文、邮件附件

任务计划信息
采集系统任务计划信息

进程事件信息
采集进程信息

配置信息
采集系统弱口令等配置信息

边界防御监控信息
采集邮件附件、网络下载行为

主动防御信息
RootKit BootKit检测信息、系统关键点信息采集

重要数据信息
采集重要数据信息

文件向量信息
静态检测

关键位置监测信息
启动项、注册表、系统服务、计划任务等

系统信息
采集系统敏感数据

病毒检查日志
扫描、清除日志

操作系统日志
应用程序、安全、setup

外设信息
USB存储设备文件信息、接入日志

进程事件信息
文件事件信息
注册表事件信息
采集系统账户、电子邮件账户信息
采集操作系统、软件、浏览器、网

构建端点一体化防护架构提升数据利用率

随着端点安全产品类型增加，用户可能需要在端点环境中安装多个Agent才能实现各类防护与管控效果，但这也同时极大消耗了端点资源，而且由于需要部署多个管理服务器，也让部署和使用成本增加。

服务器环境	杀毒软件 服务器	终端管控 服务器	安全审计 服务器	网络准入 服务器	DLP 服务器	……
端点环境	杀毒软件 AGENT	终端管控 AGENT	安全审计 AGENT	网络准入 AGENT	DLP AGENT	……

构建端点一体化防护架构提升数据利用率

一体化管理平台

数据分析与管理

- 态势引擎
- SIME引擎
- 元数据存储

统一管理

- 资产监控中心
- 威胁检测中心
- 日志报表中心
- 告警处置中心
- 告警处置中心
- 系统防护与加固中心
- 终端管理中心
- 系统运行支撑中心
- 风险检测中心
- 运维中心

数据分析

策略下发与响应处置

终端管控与审计

主机审计	桌面管控
进程事件审计	进程操作管控
文件事件审计	文件操作管控
软件服务审计	违规外联管控
用户登录审计	打印刻录管控

终端检测与响应

威胁识别	检测与防护	事件分析	威胁响应
资产管理	病毒检测	主机行为异常分析	线索调查
安全基线	入侵检测	进程行为异常分析	可编排剧本
风险检测	威胁事件检测	账号异常行为分析	快速响应
身份认证	异常行为检测	横向关联分析	威胁追溯

数据安全

- 屏幕水印
- 打印水印
- 水印追溯
- 数据加密
- 安全数据管理

身份鉴别

- UKEY PIN码登录
- 系统账户登录
- 紧急登录
- 远程设备绑定
- 异常登录处置

执行体约束

当 | 主体对象：进程、文件、驱动、内核模块 | 触发 | 执行体动作 | 且 | 关联单元（父、子）的属性 | 满足 | 条件匹配规则 | 执行 | 约束动作：阻止、放行、审计

元数据采集

- 资产信息采集
- 文件事件采集
- 进程事件采集
- 网络事件采集
- 外设事件采集
- 服务事件采集
- 注册表事件

03 安天智甲对资源占用优化的工程实践

国产专用强管控环境下的安全工程实践

恶意代码检测系统　终端数据防泄漏系统
端点安全管理系统　主机监控与审计系统


配置管理


三合一


强防策略


安全卡





NFS-CHINA


统信UOS





环境特点

大量的强管控软件和策略占用较多的资源，安全防护软件可用资源受到限制

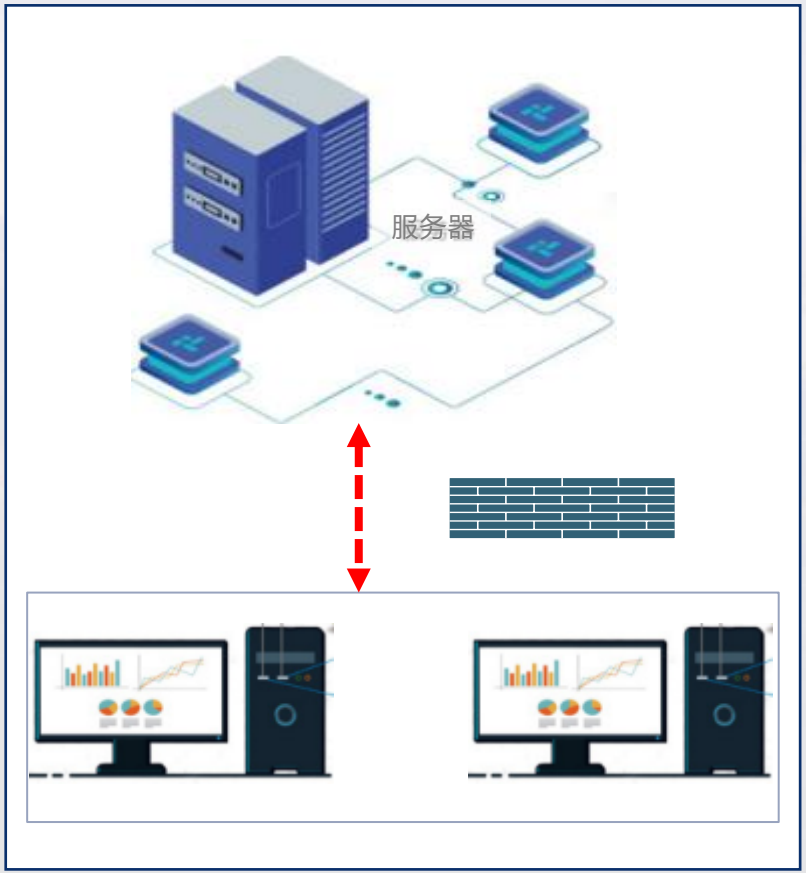
操作系统和硬件的安全定制，包括：硬件的bios、安全卡、单导等定制，和操作系统Selinux，Audit定制，类似于使安全防护软件可应用资源更加受限

基于权限划分和资源损耗情况，将服务进行拆分重组，达到资源占用平衡，例如防御服务和扫描业务进行剥离，减少了防御业务的资源消耗

可信与主防内核模块关联，获取可信软件白名单列表，收缩检测和防护范围，降低防御成本

与系统安全机制高度融合，通过检测HOOK自适应防御能力，识别并自动关闭与其他强管控软件重叠的能力点，减少不必要的浪费，提高稳定性

网络资源受限环境的安全工程实践



某电网环境下，存在大量网络带宽受限，网络访问权限受限终端，影响安全产品运行和维护，例如云查杀、数据上报、病毒库升级等。

- 压缩通信数据，降低数据包传输成本
- 细粒度拆分数据包，数据包大小可根据带宽进行配置
- 部分环境更改网络通信形式，改为长连接，避免频繁建连带来的数据包消耗
- 实现数据补报机制，可以根据数据类型，配置是否补报，补报频次

04 未来展望

从终端场景谈资源的有效利用

端点云化场景

终端类型云化是一个趋势，云化终端解决了资源难扩充的问题，安全能力必然占用相对较多的资源，解决资源瓶颈，才是解决因资源问题导致安全能力受限的彻底方法。

网内横向联动场景

在保证网内横向连通安全的前提下，通过网内横向联动，构建部分数据的全局化，例如：可信白名单、防护策略等。

通过终端分布式感知，构建在安全策略上的强弱搭配。

强化系统配置管理

加强对操作系统和业务软件本身的安全性利用，可以对冲掉一部分，由高算力需求的安全机制所带来的资源消耗。

深度业务融合场景

深度与受保护对象环境业务的融合，提高兼容性和稳定性，从根本上解决用户业务与终端安全产品资源分配问题。

谢谢大家

安天冬训营 wtc.antiy.cn