产品配置

AhnLab MDS

类别	MDS 5000B	MDS 10000B	MDS 20000B
吞吐量	2G	5G	10G
管理Agent数	1,000个	3,000个	6,000个
SSD	SSD 1.92TB * 1ea.	SSD 1.92TB * 2ea.	SSD 1.92TB * 4ea.
RAID	不支持	默认：不支持 选项：RAID 1	默认：不支持 选项：RAID 10
接口	可以安装下面四个NIC中的两个 ·1GC 8ports ·1GF 4ports ·1GF 8ports ·10GF 4ports		
电源	550W, Redundant		
Rack Mount	1U		

※ 根据客户环境和设置，设备的性能数据可能会有所不同。（添加Agent时需要额外的MDS Manager）

AhnLab MDS Manager

* DV(Data Viewer)：MDS设备的集成监控和日志管理
* HC(Host Controller)：MDS Agent集成管理（添加Agent时需要额外的MDS Manager）

类别	MDS Manager 5000BR		MDS Manager 10000BR	
管理Agent数	HC+DV 综合型	HC 单独型	HC+DV 综合型	HC 单独型
	2,000个	5,000个	5,000个	10,000个
CPU	1 * 3.30GHZ, 6Core		1 * 3.40GHz, 8Core	
RAM	32GB		64GB	
HDD	1TB x 2ea., 2TB x 2ea.		2TB x 2ea., 4TB x 2ea.	
RAID	RAID 1		RAID 1	
网络接口	1GbE 2 Ports (Copper)		1GbE 2 Ports (Copper)	
电源	400W Redundant		800W Redundant	
Rack Mount	1U, 19 inch		2U, 19 inch	
尺寸(WxDxH)	437 x 650 x 43mm		437 x 647 x 89mm	

※ 根据客户环境和设置，设备的性能数据可能会有所不同。

AhnLab MDS Analysis Manager

类别	MDS Analysis Manager
类型	软件
操作系统（OS）	CentOS 7.9
最低配置	CPU: 8Core, 3.0GHz, MEM: 24GB, HDD: 2TB, SSD: 1TB
推荐配置	CPU: 16Core, 2.4GHz, MEM: 64GB, HDD: 4TB, SSD: 2TB
特点	支持多租户功能，为支持Agent & MTA管理（待日后更新）
多租户配置	支持最多管理100个网站

AhnLab MDS Agent使用环境

类别	操作系统（OS）
客户端PC	Windows 7 SP1 (KB4490628, KB4474419 补丁) / Windows 8(8.1) / 10 / 11
服务器	Windows Server 2008 SP2 (KB4493730, KB4474419 补丁) Windows Server 2008 R2 SP1 (KB4490628, KB4474419 补丁) Windows Server 2012 / 2016 / 2022

※ 上述操作系统均支持32/64 bit

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室
http://cn.ahnlab.com | cn.sales@ahnlab.com
电话：+86 10 8260 0932（北京）| +86 21 6095 6780（上海）

AhnLab

KOREA WORLD CLASS 下一代世界级产品

AhnLab MDS

基于沙箱的高级持续性威胁响应解决方案

检测和响应网络、电子邮件和端点威胁
基于威胁可见性的按攻击阶段的优化的响应

产品介绍

无论行业和组织规模，目前大多数的企业和组织暴露于结合各种隐匿手法的新 • 变种恶意代码和勒索软件，还有使用复杂的社会工程技术的鱼叉式网络钓鱼、针对性攻击等高级持续性威胁(Advanced Persistent Threat, APT)。

基于沙箱的高级持续性威胁响应解决方案“AhnLab MDS (Malware Defense System, 恶意软件防御系统）”使用专用的多引擎技术精确检测来自各种途径的最新高级威胁。它还通过直观的威胁可见性和“收集 - 检测和分析 - 监控 - 响应”流程提供网络层和端点层的连接响应，有效地应对渗透内部的高级威胁。

通过基于多引擎的混合分析技术检测新的和变体威胁

· 基于特征码和机器学习的静态检测，基于信誉的检测
· 基于沙箱的动态分析

收集和分析通过各种途径渗透的威胁

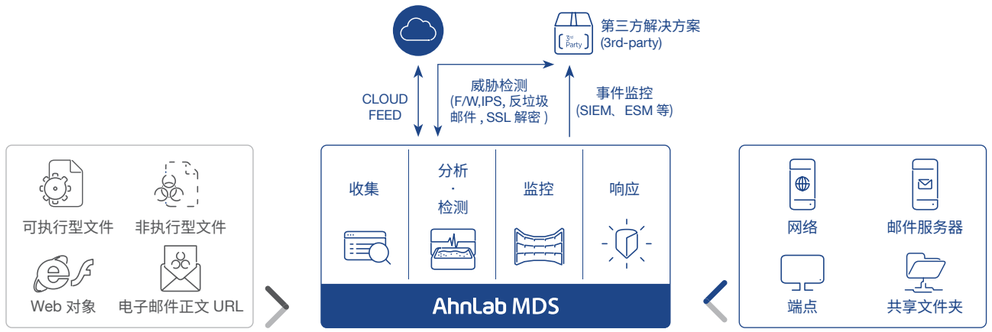
· 实时收集和分析网络流量，分析电子邮件正文和附件
· 从端点收集可疑文件，分析可疑进程

通过网络 - 端点及解决方案联动的多层响应

· 网络层和端点层的连接响应
· 现有安全解决方案和第三方解决方案的联动

基于威胁可见性的按攻击阶段的优化的响应

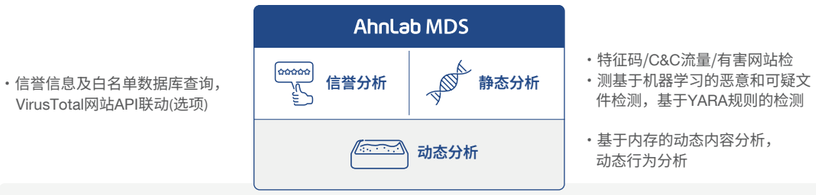
· 对威胁类型、进入途径、相关关系和攻击流程的可见性
· 提供按攻击阶段的优化的响应措施

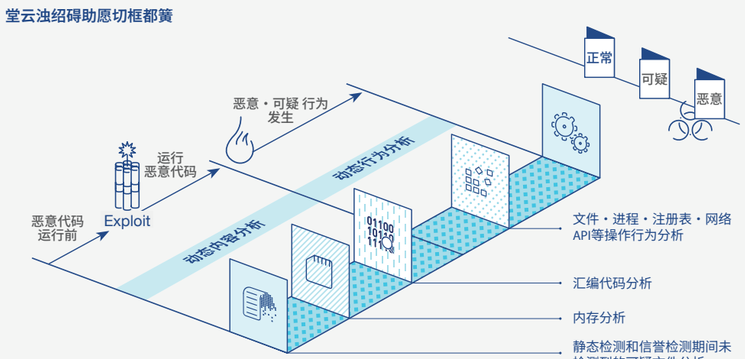


基于多引擎的精确的检测

AhnLab MDS 配备了多引擎，通过基于特征码的静态 (Static) 检测和信誉检测，非特征码 (Signature-less) 方式的基于沙箱的动态 (Dynamic) 分析，有效检测已知的威胁和新 • 变种威胁。基于内存分析的漏洞利用检测技术还可以精确检测和响应使用隐匿技术绕过沙箱分析的高级攻击。

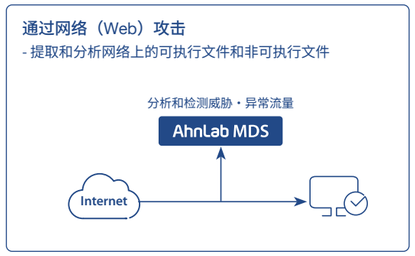
* 漏洞利用 (Exploit)：利用系统或营业程序错误或安全漏洞，执行恶意行为的攻击方式。

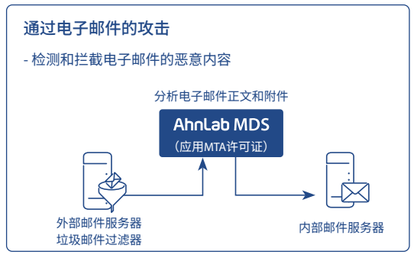


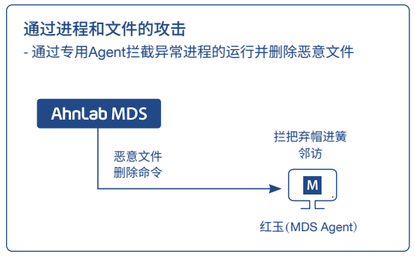


按攻击类型的优化的响应

AhnLab MDS 收集、检测和分析来自各种途径（网络、电子邮件和端点等）渗透的威胁，并根据威胁类型在网络和端点级别进行有效响应。特别是，通过专用 Agent 保留端点上的可疑文件的运行并收集可疑文件，可以主动防御潜在的威胁。

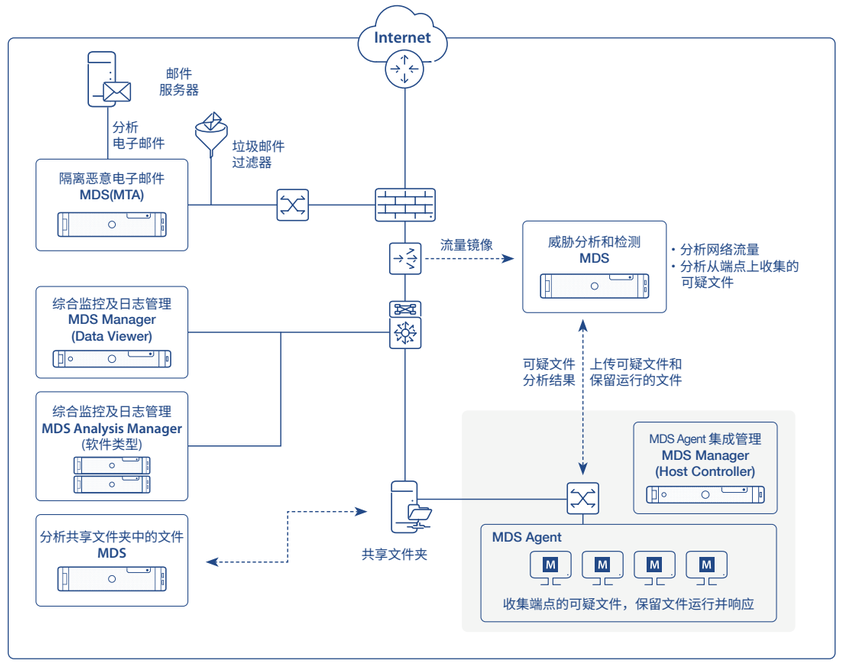






产品概念图及构建方案

AhnLab MDS 包括用于威胁检测和分析的 MDS，用于综合监控和管理的 MDS Manager，MDS Analysis Manager（软件类型), 以及用于端点威胁响应的专用 Agent（MDS Agent) 。



MDS : 基于多引擎的威胁检测和分析

- 收集和分析主要互联网服务协议（HTTP, SMTP, SMB/CIFS, FTP等）
- 电子邮件正文和附件的威胁检测和隔离（应用MTA许可证）
- 通过特征码、机器学习的静态分析和基于沙箱的动态分析检测新的威胁
- 配备检测非可执行型（non-PE）文件（如MDS Office和Hangul）的专用引擎
- 对VM分析过程和C&C检测历史记录的基于PCAP的数据包捕获和PCAP文件下载
- 通过MDS Manager共享行为分析结果和基于云的行为分析信息

MDS Manager : 集成监控及管理

- Data Viewer: MDS设备的集成监控和日志管理
  - 通过直观的仪表板提供主要检测情况和事件信息
  - 事件类型、IP地址、行为历史记录（文件/进程/注册表/网络）的详细日志
  - MDS检测事件和日志的集成管理部署在多个途径中，例如网络区间、电子邮件区间和共享文件夹
  - 共享MDS设备的行为分析结果（配置多个MDS设备时，最小化重复分析和检测）
  - YARA规则管理和分发系统互操作，Syslog传输功能（CEF，LEEF格式）
- Host Controller: MDS Agent集成管理和响应
  - MDS Agent安装、补丁管理、组和策略管理
  - MDS Agent响应命令和发送通知

MDS Analysis Manager : MDS设备集成监控和日志管理，软件类型

- 提供与MDS Manager的数据查看器（Data Viewer）相同的功能
- 支持多租户(IP单位、多个网站的管理员可以访问和运营）

MDS Agent : 收集并响应端点可疑文件

- 应用专有机器学习技术的端点可疑文件收集功能
- 针对感染恶意代码的可疑主机进行网络隔离等措施
- 检测异常进程的运行并保留可疑文件的运行
- 通过V3统一Agent修复端点区域的恶意代码并加强防御系统