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响应

沙箱　多引擎　多层响应　威胁可见性

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)。

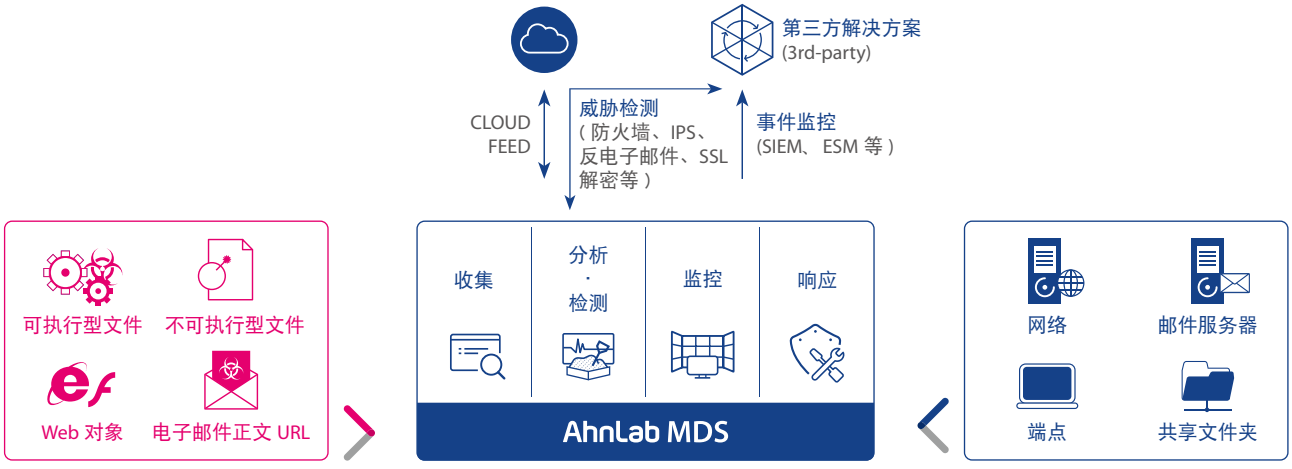
基于沙箱的高级持续性威胁响应解决方案“**AhnLab MDS** (Malware Defense System, 恶意软件防御系统)”使用专用的多引擎技术精确检测来自各种途径的最新高级威胁。它还通过直观的威胁可见性和“收集 - 检测和分析 - 监控 - 响应”流程提供网络层和端点层的连接响应，有效地应对渗透内部的高级威胁。

通过基于多引擎的混合分析技术检测新的和变种威胁
· 基于特征码和机器学习的静态分析，基于信誉的分析
· 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

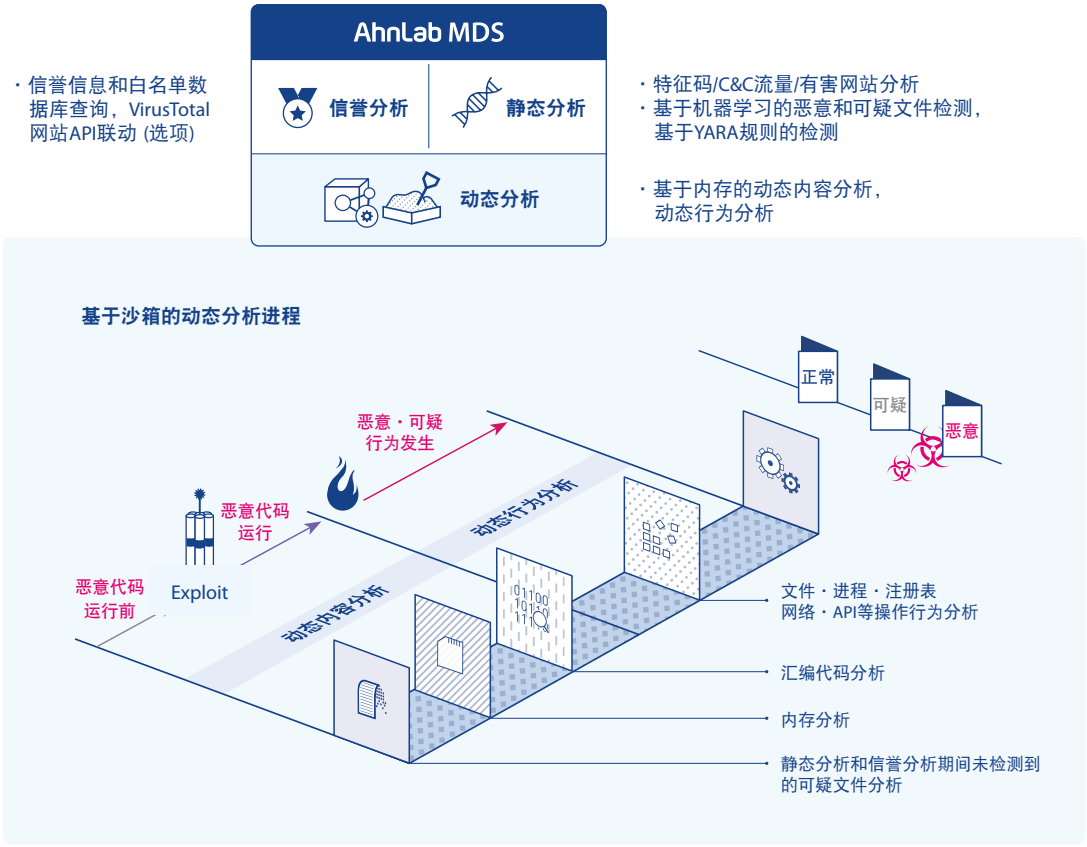
基于威胁可见性的按攻击阶段的优化的响应
· 对威胁类型、渗透途径、相关关系和整个攻击流程的可见性
· 按攻击阶段的优化响应



基于多引擎的精确的威胁检测

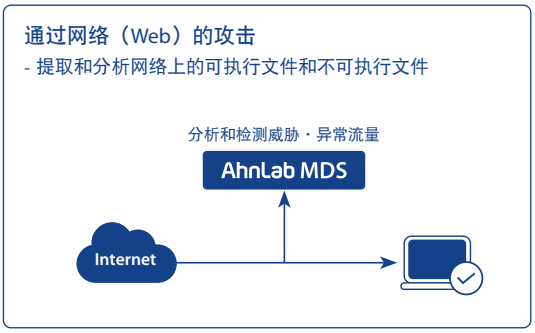
AhnLab MDS 配备了多引擎，通过基于特征码的静态 (Static) 分析和信誉分析，非特征码 (Signature-less) 方式的基于沙箱的动态 (Dynamic) 分析，有效检测已知的威胁和新 · 变种威胁。应用于 AhnLab MDS 的独特的“基于内存分析的漏洞利用检测技术”还可以精确检测使用隐匿技术绕过沙箱分析的高级攻击。

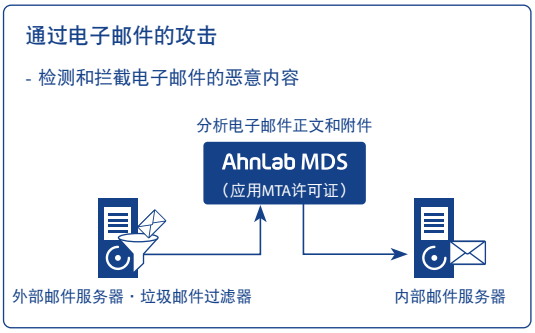
漏洞利用 (Exploit)：利用系统或应用程序错误或安全漏洞，执行恶意行为的攻击方式。

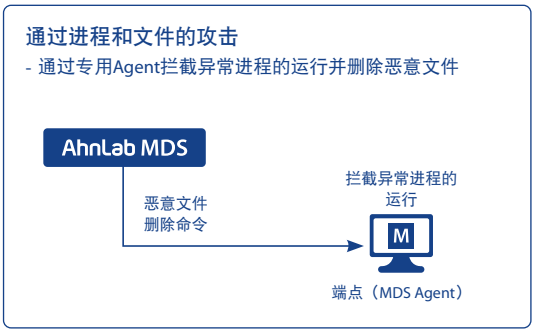


按攻击类型优化的响应

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。

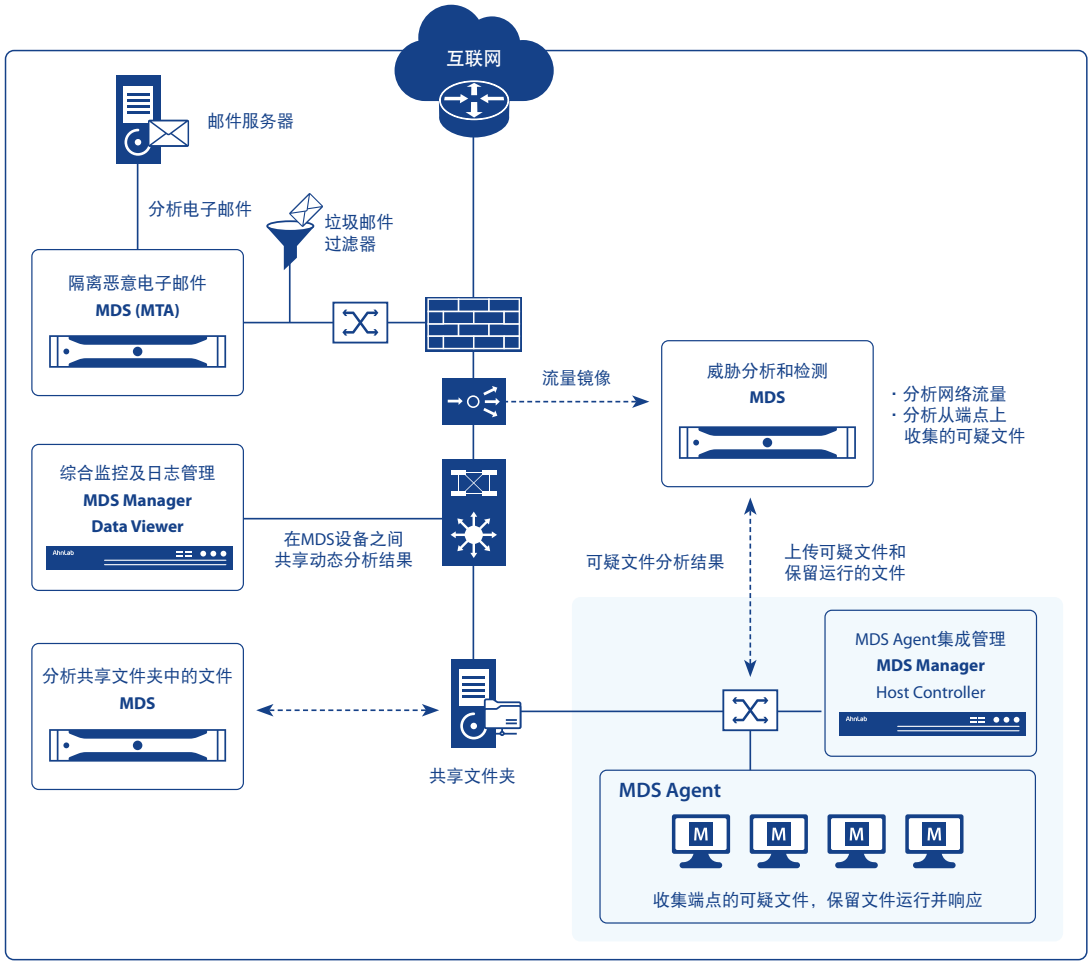






产品概念图及构建方案

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，以及用于端点威胁响应的专用 Agent (MDS Agent) 。可以根据企业的环境和目的，通过基本或扩展部署有效响应通过各种途径 (如网络、电子邮件、共享文件夹和端点) 渗透的最新威胁。



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
- 配备检测不可执行型（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 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

产品配置

▶ AhnLab MDS

类别	MDS 4000A	MDS 8000A	MDS 10000A	
动态分析性能	35,000件/1天	90,000件/1天	200,000件/1天	
管理Agent数（推荐）	700个	2,000个	5,000个	
Throughout	800Mbps	1.5Gbps	4Gbps	
HDD	1TB x 2ea.	1TB x 4ea.	1TB x 8ea.	
RAID	RAID 1	RAID 10	RAID 10	
网络接口	1GbE 4 Ports (Copper) 1/10G SFP+ 4 Ports (Optical)	1GbE 4 Ports (Copper) 1/10G SFP+ 4 Ports (Optical)	默认 (Default)	1GbE 2 Ports (Copper) 1/10G Base-T 2 Ports (Copper) 1/10G SFP+ 4 Ports (Optical)
			选项 (Optional)	1GbE 2 Ports (Copper) 1/10G Base-T 4 Ports (Copper) 1/10G SFP+ 6 Ports (Optical)
电源	750W Redundant			
Rack Mount	1U, 19 inch	1U, 19 inch	2U, 19 inch	
尺寸（W x D x H）	482 x 721.91 x 42.8mm	482 x 721.91 x 42.8mm	482.4 x 715.5 x 86.8mm	

※ 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 5000AR		MDS Manager 10000AR	
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
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	500W Redundant		740W Redundant	
Rack Mount	1U, 19 inch		2U, 19 inch	
尺寸 (WxDxH)	437 x 650 x 43mm		440 x 650 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 Agent 使用环境

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

※ 上述操作系统均支持32/64 bit

AhnLab
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）