AhnLab MDS

应对未知威胁的最佳选择

基于沙箱的文件分析解决方案
检测勒索软件、恶意代码、恶意 URL、C&C 通信及 APT 攻击
并提供对文件的运行保留与响应机制

产品概要

即使在 2024 年之前或之后，针对勒索软件等恶意代码的响应方案仍然是网络安全战略中最为重要的一个部分。因此，企业必须部署能够在网络、电子邮件与终端各环节中检测与分析恶意代码的解决方案。对于已知的恶意代码，通常可以通过安装在终端上的传统防病毒软件进行防御。但若要有效应对未知恶意代码，则需要部署 **AhnLab MDS**（恶意代码防御系统）。

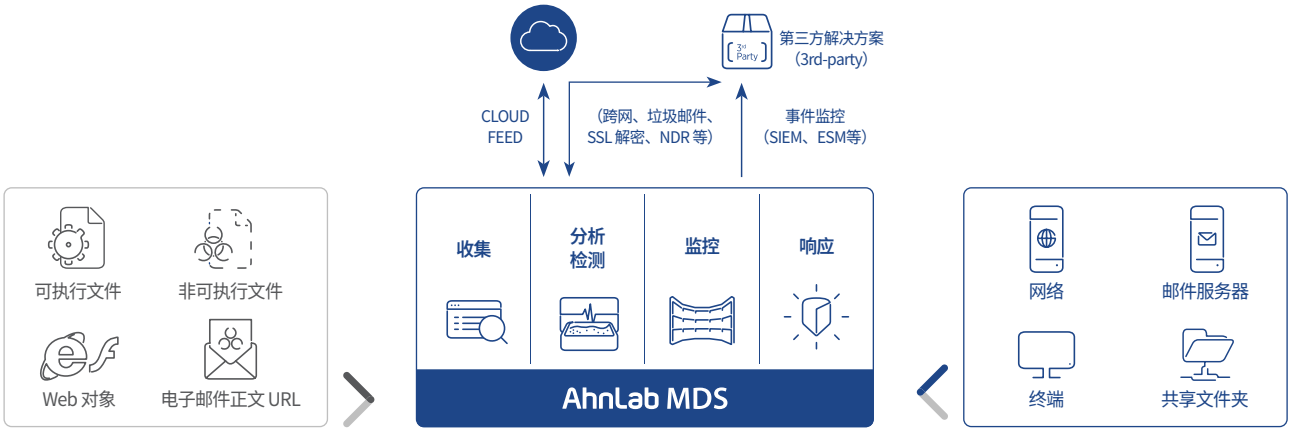
AhnLab MDS（以下简称为 MDS）是一款基于沙箱技术的文件分析解决方案，集成了本公司多年来在恶意代码分析领域的所有技术经验。它可在 Windows 与 Linux 操作系统的虚拟环境中运行可疑文件，并对其行为进行深度分析。即使是新型文件，也往往包含已知的恶意行为特征，因此 MDS 能够有效识别。MDS 搭载了多个分析引擎，可针对文件的行为或文件本身进行分析，从而精准检测高度复杂的安全威胁。

应对未知（Unknown）威胁——沙箱机制
- 基于沙箱技术支持动态分析（支持操作系统：Windows 7/10/11、Ubuntu）
- 规避虚拟机环境的恶意代码检测与分析技术，以及相关文件分析功能

收集和分析通过各种途径流入的威胁
- 支持对 10G 网络流量的实时收集和分析（HTTP、HTTP/2、FTP、SMTP、POP3、IMAP、SMB 等）
- 通过电子邮件传输代理（MTA）许可与终端 Agent，收集与分析文件

支持与多种解决方案联动
- 通过 API 与 MDS 平台联动，对可执行文件、文档文件、邮件等进行深度分析
- 支持与跨网解决方案、垃圾邮件过滤方案、SSL 解密方案、以及 NDR解决方案的联动

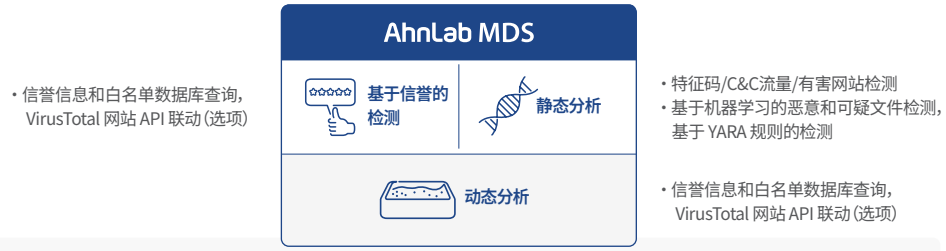
应用 AhnLab 最新的威胁检测技术
- 采用机器学习（ML），识别无法通过规则检测的欺诈性钓鱼邮件
- 提供多样的辅助分析工具，包括 AhnLab TIP 联动、专家分析服务等

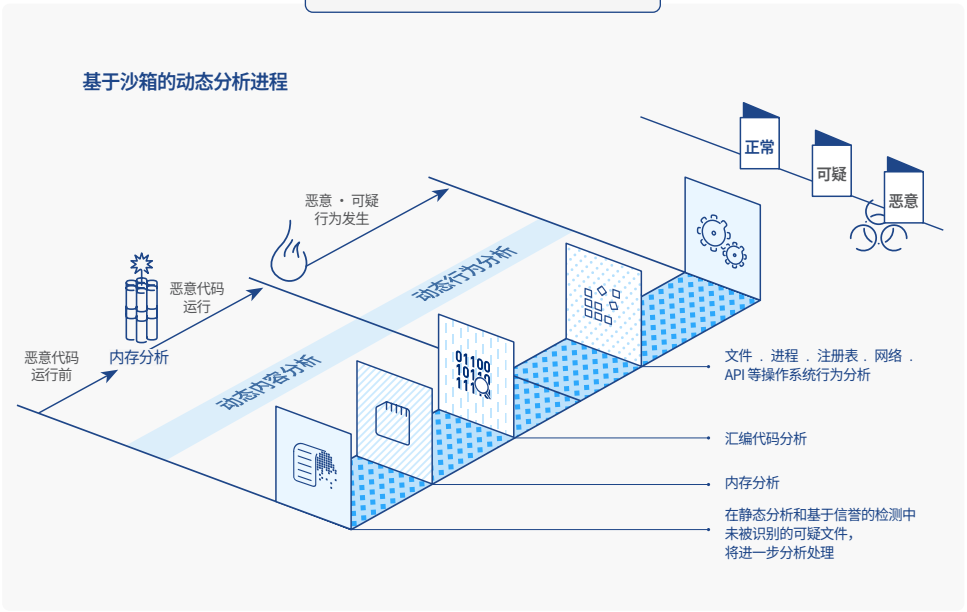


基于多引擎的精确威胁检测

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。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

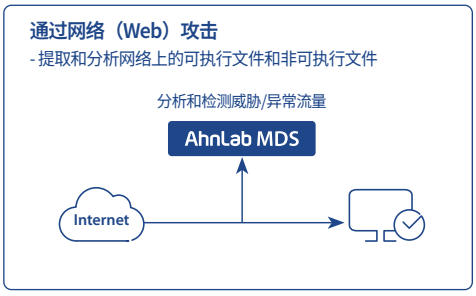
* 漏洞利用（Exploit）：利用系统或营业程序错误或安全漏洞，执行恶意行为的攻击方式。

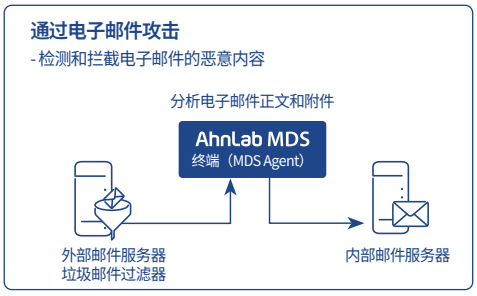


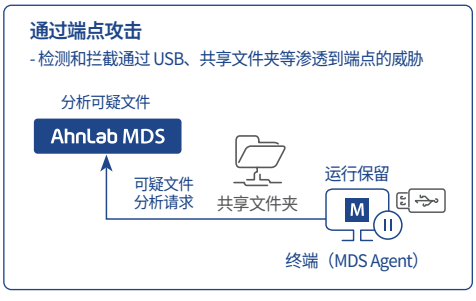


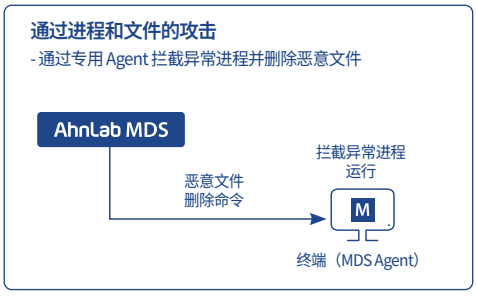
按攻击类型定制的优化响应方案

AhnLab MDS 收集、分析和检测来自各种途径（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层和端点层进行有效响应。此外，通过专用 Agent 对终端中的可疑文件执行“运行保留”和“可疑文件收集”功能，可以主动防御潜在的威胁。



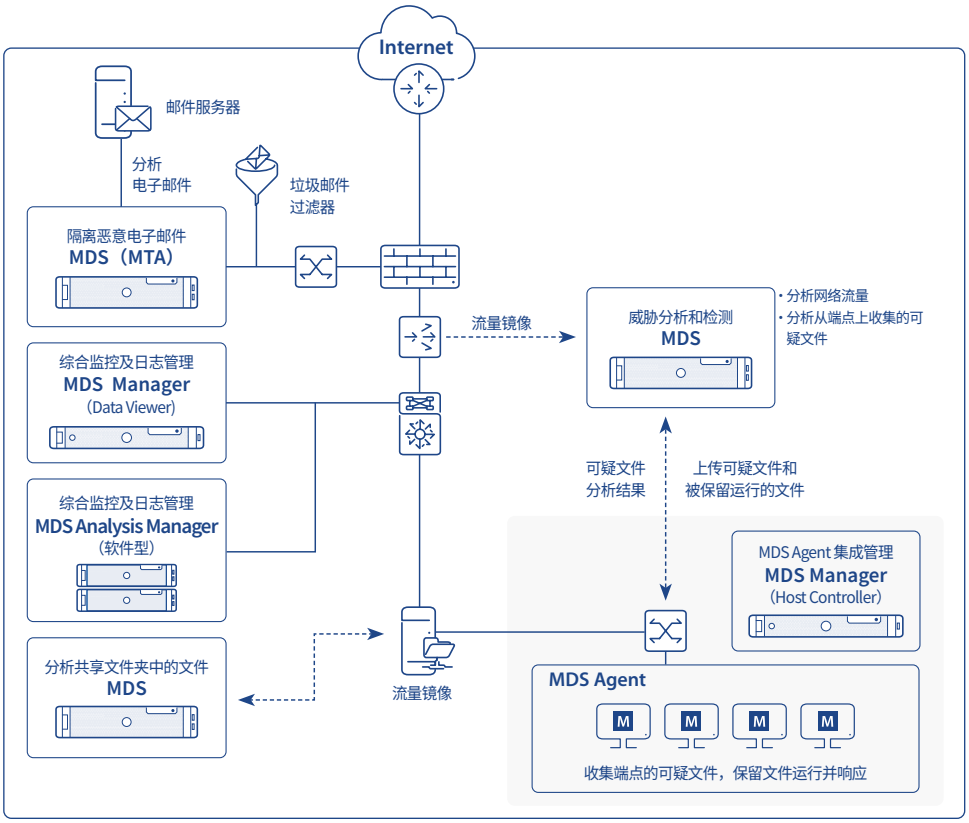






解决方案架构与部署方式

AhnLab MDS 由以下组件构成：用于文件与威胁分析的 MDS，用于邮件区间防护的专用授权 MTA，以及用于终端威胁响应的专用 Agent。



MDS：基于沙箱的文件分析解决方案

· 支持多种操作系统环境虚拟机（VM）运行，包括 Windows 7/10/11 和 Ubuntu
· 提供基于特征码的快速静态分析和基于沙箱的动态分析
· 收集并分析主要协议（如HTTP、HTTP/2、FTP、SMTP、POP3、IMAP、SMB 等）
· 支持基于哈希值（MD5、SHA-256）、IP、URL、邮件、数字签名的黑名单/白名单管理
· 根据文件特性应用不同的分析引擎
· 提供基于正式授权的各种版本 MS Office 和 Hangul Office 的分析环境
· 提供专用邮件区间授权（MTA），用于分析邮件头、正文和附件
· 提供终端 Agent（MDS Agent），用于保留运行和删除/隔离未分析文件
· 可选配 AhnLab TIP（威胁情报平台）集成和专家分析服务作为附加功能

MDS（MTA）：用于邮件区间的MDS

· 支持对邮件头、标题、正文及附件文件的分析
· 提供图像文字识别（OCR）和二维码钓鱼（Qshing）分析功能
· 支持与反垃圾邮件解决方案联动

MDS Agent：安装于终端的专用 Agent

· 保留运行未分析文件，并在分析后决定是否运行该文件
· 对疑似恶意代码感染的主机进行网络隔离并执行恶意代码删除和响应
· 应用自主机器学习（ML）技术收集可疑文件
· 提供可执行文件的证书验证及关联文件同时收集功能
· 支持 V3 统一Agent

MDS Manager：集成管理与监控

· 支持 MDS 多设备的集成管理与监控（数据查看器 Data Viewer）
· 在需要多个 Agent 的情况下，进行 Agent 管理（主机控制器 Host Controller）
· 数据查看器与主机控制器可集成使用或单独使用
· MDS Analysis Manager：MDS Manager 以软件形式提供，并支持多租户（按IP单元管理多个站点）

产品规格

AhnLab MDS

类别	MDS 5000B	MDS 10000B	MDS 20000B	vMDS 5000V
MAX Throughput	2G	5G	10G	1G
管理Agent数	1,000个	3,000个	6,000个	未支持
Log Storage	SSD 1.92TB * 1ea.	SSD 1.92TB * 2ea.	SSD 1.92TB * 4ea.	SSD 1TB
RAID	未支持	可选 （默认：未支持，PAID 1）	可选 （默认：未支持，PAID 10）	NHN CLOUD 专用产品，遵循 NHN CLOUD 设置
网卡(NIC)	可配置两个网卡（管理端口单独分离） • 1GC 8ports • 1GF 4ports • 1GF 8ports • 10GF 4ports			
电源	550W, Redundant			
Rack Mount	1U			
CC 认证	EAL 3（其他）			

※ 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,mm)	437 x 503 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
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，未支持 Agent & MTA 管理（预计后续更新中加入）
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)
桌面	Windows 7 / 10 / 11
服务器	Windows Server 2012 / 2016 / 2019 / 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 | 上海市闵行区新镇路1699弄E栋303室
https://www.ahnlab.com/cn | cn.sales@ahnlab.com
电话： +86 10 8260 0932（北京）| +86 21 6095 6780（上海）