Case Study

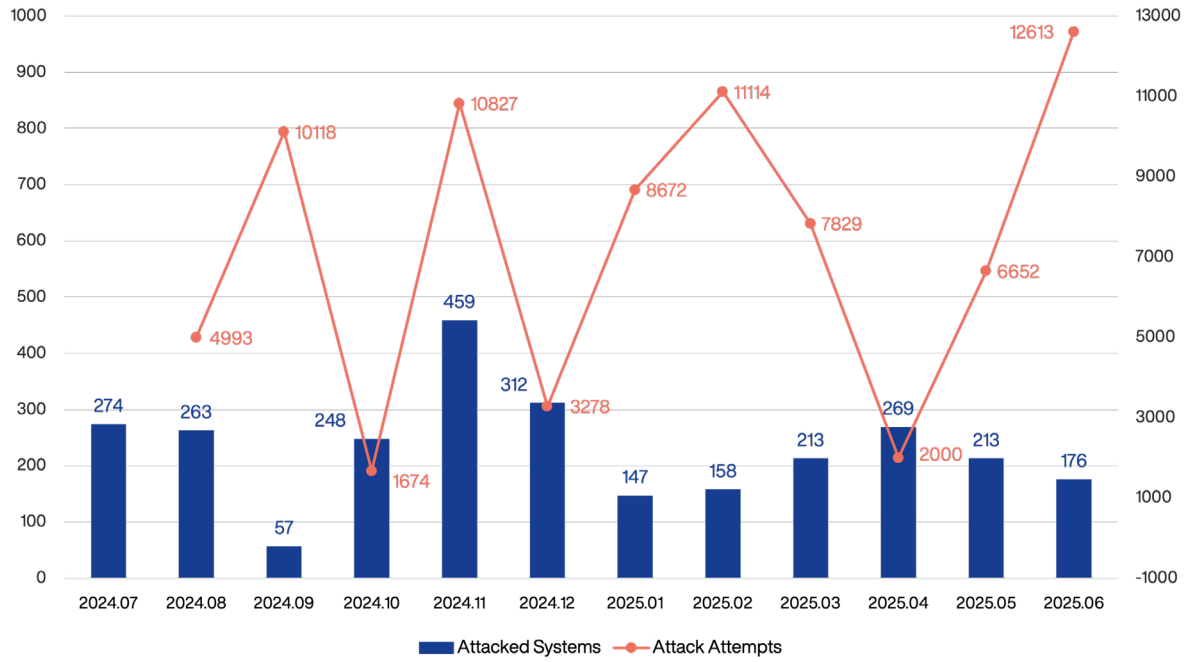
从 Linux 攻击案例看企业应该如何应对?

近期，针对Linux 服务器的攻击日益猖獗，造成的损失也正在不断扩大。攻击者之所以盯上 Linux 服务器，是因为它们连接着大量客户端计算机，并存储着各种关键的业务数据。随着针对 Linux 系统的恶意代码（包括勒索软件）数量持续增长，导致了严重的损害，例如业务中断。现在，企业必须将处理其重要资产和客户信息的 Linux 服务器作为优先防护对象，全面强化其安全防御。

AhnLab通过将防病毒（V3 Net for Linux）、沙箱（AhnLab MDS）、EDR（AhnLab EDR）解决方案联动的安全架构，提供包括 Linux 在内的终端全域的强大安全。该架构已在众多客户环境中实际部署，为提升安全水平发挥了积极作用，其所集成的解决方案也在全球安全评估中取得了优异的成绩，充分展现了其卓越的技术实力。

1. 通过统计数据看 Linux 服务器攻击

AhnLab的威胁情报组织ASEC（AhnLab Security Intelligence Center）利用蜜罐技术，检测和分类对管理不当的 Linux SSH（Secure Shell）服务器的暴力破解（Brute Forcing）、字典攻击（Dictionary Attack）等行为，并提供相关统计数据。这里所说的“管理不当”是指设置了易受攻击的账户信息的环境。



【图1】截至2025年6月过去一年 Linux 服务器攻击统计

【图1】展示了截至2025年6月，过去一年中针对 Linux 服务器的攻击统计数据。

各项指标说明如下：

- **被攻击系统**（Attacked Systems）：指的是实际被恶意代码或攻击者利用的系统数量，这些系统确认了执行恶意代码安装命令的历史。如果攻击者以管理员账户成功登录到管理不当的系统，就可以控制该系统。
- **攻击次数**（Attack Attempts）：指的是攻击者针对目标系统执行攻击的次数。Linux SSH服务器攻击通常从扫描（scanning）开始，随后进行暴力破解或字典攻击，以获取账户信息或收集基本信息。“攻击次数”是指在执行这些步骤后，确认有实际安装恶意代码的日志记录的案例。

用于 Linux 服务器攻击的恶意代码类型有多种多样，包括 DDoS 僵尸（DDoS Bot）、挖矿程序（CoinMiner）、后门（Backdoor）、勒索软件（Ransomware）等。

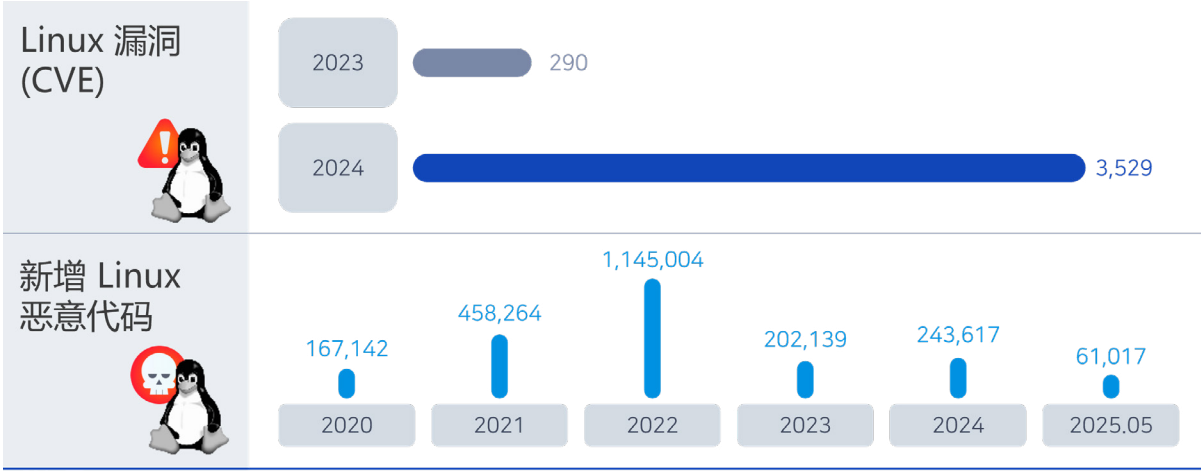
以下是对这些恶意代码类型的简要说明：

- **DDoS 僵尸：**根据攻击者的指令控制感染的系统并执行DDoS攻击，通常还具备安装额外有效载荷或执行其他命令的功能。

· **挖矿程序：**利用受感染系统的资源挖掘虚拟货币。
· **后门：**允许攻击者隐秘访问系统并执行进一步恶意行为。
· **勒索软件：**对受感染系统中的文件等进行加密，并以各种方式向受害者索要赎金。

从【图1】的统计数据来看，最近的6月中，共有176个系统遭受了超过12,000次攻击。从过去一年的趋势来看，虽然每月有所不同，但大致上每月都有超过100个系统遭受数千次甚至超过10,000次的攻击。尽管由于大型黑客事件，Linux 服务器攻击最近备受关注，但实际上此类攻击早已持续活跃多年。

从 AhnLab 提供的另一项统计数据【图2】中可以更清楚地看到这一趋势。2023年时的 Linux 漏洞数量为290个，到了2024年则暴增到3,529个，增长了10倍以上。而到2025年5月为止，也就是近半年的时间，就已经发现了超过60,000个针对 Linux 环境的新型恶意代码。



【图2】Linux 漏洞与新增恶意代码数量

Linux 服务器攻击增加的原因很简单：它们连接着大量客户端计算机，并存储各种关键业务数据。随着针对 Linux 系统的恶意代码（包括勒索软件）的增加，企业不仅面临数据泄露风险，还可能导致业务中断等严重的损失。

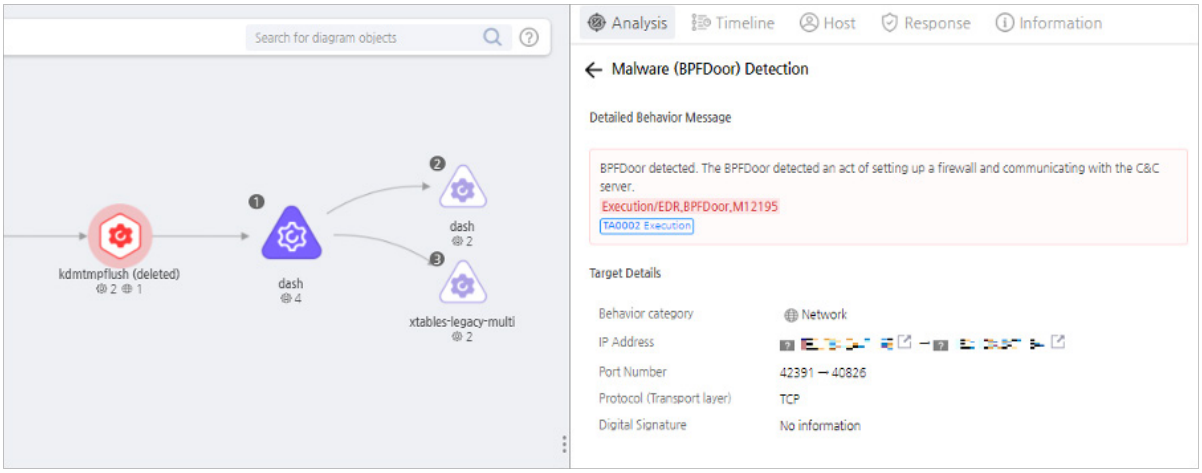
2. Linux 服务器攻击案例

接下来，我们通过两个实际案例分析，深入了解针对 Linux 服务器的攻击行为。

案例一：通过BPFDoor（后门）窃取信息

BPF（Berkeley Packet Filter，伯克利数据包过滤器）是一种用于网络数据包过滤的机制，部署在内核区域，可以决定是将接收到的数据包传递到用户区域。BPFDoor 是一种利用 BPF 的数据包过滤功能的 Linux 后门恶意代码。它通过添加数据包过滤规则，检查是否接收到特定的“魔法数据包（Magic Packet），进而执行恶意行为。

AhnLab 于去年10月借助其端点检测与响应解决方案 AhnLab EDR 成功检测并分析了 BPFDoor 恶意代码，并将相关内容发布于 ASEC 博客。



【图3】 2024年10月 AhnLab EDR 的检测到的 BPFDoor 部分内容

根据分析结果，BPFDoor 在首次执行时，会通过特定命令将自身复制到 /dev/shm 路径下，并命名为“kdmtmpflush”，随后删除原文件以隐藏踪迹。/dev/shm 是 Linux 的基于内存的文件系统，应用程序常用于临时数据的存储与处理。由于该路径中的内容不会写入磁盘，仅存在于内存中，因此经常被攻击者滥用。

之后，该恶意程序会从【图4】中的字符串中随机选择一个名称，并进行重命名以伪装成正常进程。此过程中，使用了 prctl() 函数。

```
char *self[] = {
        "/sbin/udevd -d",
        "/sbin/mingetty /dev/tty7",
        "/usr/sbin/console-kit-daemon --no-daemon",
        "hald-addon-acpi: listening on acpi kernel interface /proc/acpi/event",
        "dbus-daemon --system",
        "hald-runner",
        "pickup -l -t fifo -u",
        "avahi-daemon: chroot helper",
        "/sbin/auditd -n",
        "/usr/lib/systemd/systemd-journald"
};
```

【图4】用于伪装成正常进程的字符串示例

接下来，BPFDoor 会注册 BPF 过滤器并进入等待状态。当攻击者发送包含魔术数据包（Magic Packet）的命令时，BPFDoor会通过 BPF 过滤器接收该数据包，并执行相应的恶意命令。

根据魔术数据包的源代码逻辑：

- 若密码为 justforfun，则连接到魔法数据包中的IP/端口，并提供反向Shell（Reverse Shell）；
- 若密码为 socket，则提供绑定Shell（Bind Shell），开放新端口并配置防火墙以建立攻击者的内部连接；
- 若密码不匹配，则响应字符“1”，用于告知攻击者恶意代码是否成功植入。

通过这一流程，攻击者与内部环境建立连接，，并进一步实施信息窃取等恶意行为。

值得注意的是，近期针对通信公司攻击事件及 SIM 卡信息泄露事件中，也被发现使用了变种的 BPFDoor 恶意代码。尽管该变种在功能上与上述 BPFDoor 稍有差异，但核心机制基本一致。相关详细内容可参考 AhnLab 发布的《BPFDoor案例研究》。

案例二：通过部署代理实现系统非法访问

在2025年第二季度，出现了多起攻击 Linux 服务器并部署代理程序的案例。根据分析结果，攻击者安装了 TinyProxy 或 Sing-box 等代理工具。从日志来看，由于没有发现其他攻击行为，推测攻击者的主要目的是将受感染的系统作为代理节点进行利用。

攻击者在成功登录目标 Linux 服务器后，下载并执行了恶意 Bash 脚本以安装代理工具 TinyProxy。接着，攻击者修改了 TinyProxy 的配置文件 /etc/tinyproxy/tinyproxy.conf 或 /etc/tinyproxy.conf，删除了以 Allow 和 Deny 开头的访问控制规则，并添加了 Allow 0.0.0.0/0 规则。此规则一旦生效，意味着任何外部 IP 都可以不受限制地访问该代理服务。最终，攻击者通过 TinyProxy 所监听的 8888 端口连接并滥用该系统作为代理跳板。

```
200 #Allow 127.0.0.1
201 #Allow ::1
202 #Allow 192.168.0.0/16
203 #Allow 172.16.0.0/12
204 #Allow 10.0.0.0/8
205
325 #
326 #ReverseBaseURL "http://localhost:8888/"
327
328
329
330
331 # Added by script - WARNING: Allows all connections!
332 Allow 0.0.0.0/0
```

【图5】被注释及插入的 TinyProxy 配置内容

另一起案例中，攻击者在受害系统中安装了名为 Sing-box 的代理工具。Sing-box 是一个多功能代理工具，支持 vmess-argo、vless-reality、Hysteria2、TUICv5 等协议。根据 GitHub 的介绍，该工具可用于解除对 ChatGPT 和 Netflix 的访问限制。在本案例中，攻击者非法访问Linux系统并安装了Sing-box，可能意图通过该代理平台进行更多的非法活动或谋取经济利益。

从近期的Linux服务器攻击案例来看，攻击者越来越倾向于利用 TinyProxy 和 Sing-box 等合法工具，而非传统的恶意代理程序。通过将受感染系统作为代理节点，攻击者不仅可以隐藏自身身份，还可能通过出售代理访问权限获取非法收益。

3. 实现 Linux 服务器安全的必备解决方案有哪些?

面对当前日益复杂的网络威胁，仅依赖单一安全解决方案已难以有效应对。攻击可能从终端、电子邮件等多个入口发起，且新型与变种恶意代码频繁出现。此外，攻击往往不是一次性的，随时可能再次发生。因此，为实现有效的安全防护，企业需要具备以下能力：

- 覆盖威胁检测、分析与响应的完整安全体系
- 支持产品间联动与整合，保护多个安全区域的架构
- 不仅实现检测与拦截，还能持续追踪威胁、防止复发的安全策略

当然，如果企业有能力有效运维多种安全解决方案，自然是最佳选择。但现实中，很多企业往往资源有限，难以全面部署。在这种情况下，若要实现对 Linux 服务器的成功防护， 以下三种解决方案是不可或缺的：

#1. 杀毒软件（Antivirus, AV）

杀毒软件基于特征码（Signature）与行为分析技术，能够在恶意代码进入系统前进行检测与拦截。它是终端安全中最基础且最必要的解决方案。AV 产品可适用于 PC 与服务器，并支持 Windows、macOS、Linux 等多种环境。对于 Linux 服务器，应选择专为该环境优化的专用防病毒解决方案 。

#2. 沙箱（Sandbox）

沙箱解决方案会在多个安全区域收集文件，并在虚拟环境（VM）中进行动态分析。
例如，可以在虚拟环境中运行文档文件，通过模拟操作来发现隐藏的恶意行为或未知威胁。
此外，还能检测绕过杀毒软件（AV）解决方案的勒索软件。
与基于特征码快速识别已知恶意代码的杀毒软件相比，沙箱技术是一种互补的安全手段。

#3. EDR（终端检测与响应）

EDR（Endpoint Detection & Response）是一种检测和记录终端上发生的所有行为和事件的解决方案，能持续收集调查安全事件所需的数据。通过分析这些行为数据，EDR 能够主动追踪与识别威胁，帮助企业建立长期的威胁响应机制。简单来说，它的作用就像一个随时监控一切的监控摄像头（CCTV）。

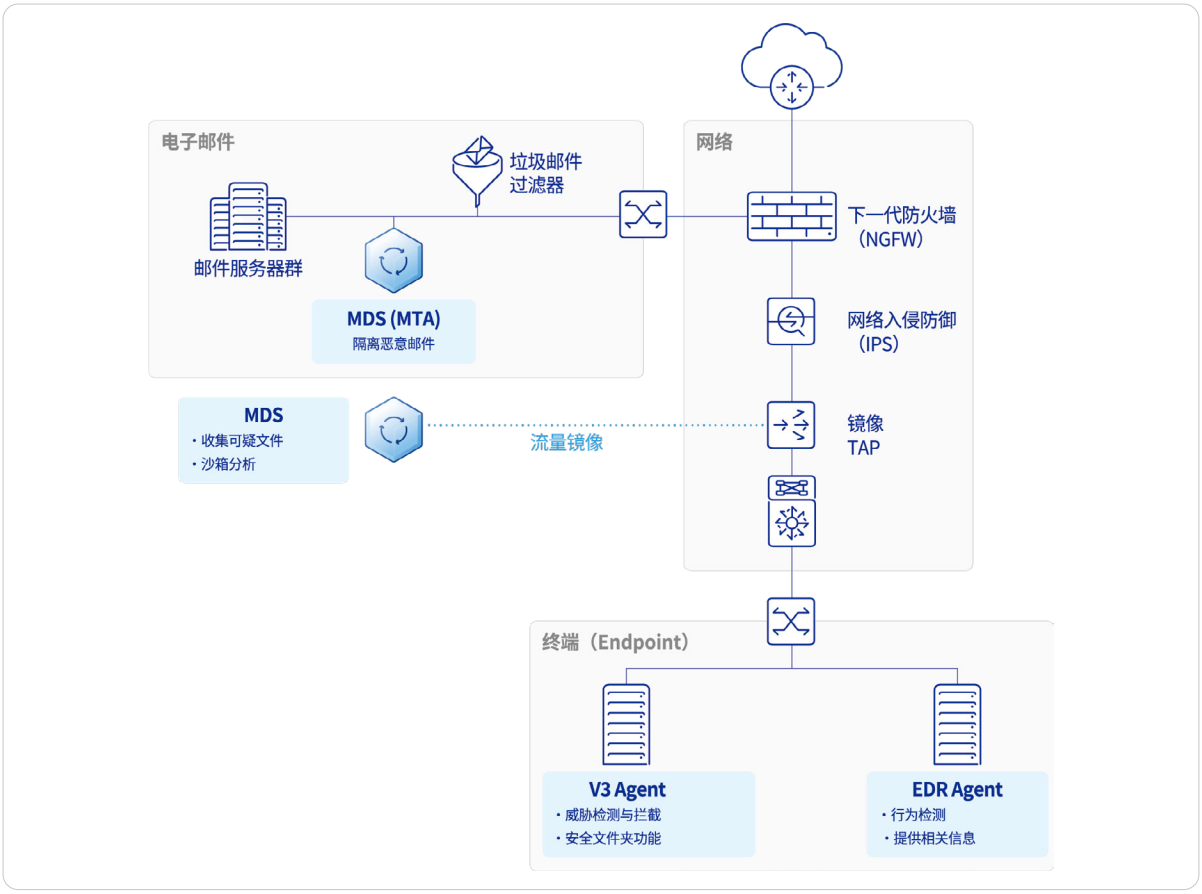
#4. MDR服务（托管检测与响应）

MDR（Managed Detection & Response）是由安全专家利用 EDR 提供的威胁检测、分析与定制化响应服务。通过该服务，可以减轻企业在安全运营方面的压力，并增强检测与响应能力。随着网络威胁的不断升级，以及基于 EDR 的检测与分析要求也日益专业化，对 MDR 服务的需求和关注也持续上升。

因此，若能正确运用杀毒软件（AV）、沙箱技术和EDR，并结合使用MDR服务，可建立针对各种威胁的高级响应体系，从而在Linux服务器安全方面取得显著成效。

4. AhnLab的系统化的安全架构

AhnLab 针对终端、电子邮件等可能成为网络攻击入口的区域，提供最优的安全解决方案，帮助客户构建强大的威胁应对体系。从攻击者频繁使用的恶意邮件隔离，到终端的多种安全功能与威胁追踪，实现威胁的复发防止与预防，AhnLab 提供了近乎完美的整体安全防护体系。



【图6】 AhnLab 的 Linux 服务器安全架构

【图6】展示了 AhnLab 的 Linux 服务器安全架构，以应对勒索软件等主要网络攻击。该架构中的各个解决方案相互灵活联动，形成协同效应。架构中的解决方案基于静态（Static）、信誉（Reputation）、动态（Dynamic）、行为（Behavior）等多种分析技术，构建全面的威胁检测与防御体系。

AhnLab 安全架构中各解决方案的作用总结如下：

【图7】 AhnLab 的 Linux 服务器安全架构 - 各安全方案的作用

#1. AhnLab V3：已知恶意代码的检测与拦截

拥有30年历史与技术积累的 AhnLab 防病毒解决方案 AhnLab V3，基于自家数据库中数十亿条恶意代码特征码，能够快速、准确地检测并拦截已知恶意代码。它利用数千种恶意行为模式，也对未知恶意代码也具备一定的检测与响应能力。

此外，还提供以下针对勒索软件的专用功能：

- 诱饵文件检测（Decoy File）
- 应用隔离扫描
- 勒索软件安全文件夹
- 进程内存检测
- AMSI（Anti Malware Scan Interface）检测

这些功能使其也能识别以无文件形式传播的恶意代码。

AhnLab V3 根据终端类型和操作系统提供不同产品版本。对于 Linux 服务器，V3 Net for Linux 提供了专门针对 BPFDoor 等 Linux 恶意代码的优化检测与防护。同时考虑到 Linux 服务器在云环境中的广泛使用，支持容器（Docker）扫描等云端安全功能，帮助客户实现真正的混合云安全。

#2. AhnLab MDS：恶意邮件阻断与未知恶意代码分析

AhnLab MDS 是一款沙箱解决方案，可在网络、终端、邮件服务器前端、网络隔离区域等所有文件存在的路径上进行文件检测。

从 Linux 安全的角度来看，AhnLab MDS 在网络、邮件服务器前端、内网与外网连接区域等多个领域执行基于沙箱的文件检测。

在邮件区域，MDS 的 MTA（邮件传输代理）功能会综合检查邮件头、正文、URL 与附件。正文中的URL 会被实际访问以验证其安全性，附件则在沙箱环境中进行分析。恶意邮件会被隔离，防止其进入系统。

此外，AhnLab MDS 通过网络流量镜像收集可疑文件，并在虚拟机环境中执行与分析，以判断其是否为恶意文件。从 Linux 安全的角度来看，一般的 Linux 文件常常会与特定参数一起运行，而 AhnLab MDS 的优势在于用户可以手动输入文件及参数，以确认是否会触发恶意行为。此外，还可将多个文件集中于虚拟环境中统一分析，有利于检测与分析 Linux 相关威胁。

#3. AhnLab EDR：终端所有事件与行为的检测与响应

AhnLab EDR 监控服务器、计算机等各种设备上的所有行为，检测并响应终端威胁。其主要功能包括：

- 收集所有终端行为信息
- 分析事件关联关系
- 与 AhnLab V3、MDS 等解决方案联动的威胁响应

其目标是全面管理终端威胁，最小化未知威胁的潜伏期，并防止潜在损害与复发。

AhnLab EDR 还提供基于 MITRE ATT&CK 框架的威胁情报，包括入侵路径、主要行为、关联信息、风险级别和威胁情报链接等详细分析内容。分析信息以图表、时间线、进程树等直观形式展示，帮助用户全面理解攻击流程。

同时配套的专用控制台 EDR Analyzer 可帮助用户准确识别威胁并制定最适合自身组织的防护策略。

#4. MDR 服务：最大化 EDR 效能

由于 EDR 相比其他方案运维难度较高，为提升客户使用效率，AhnLab 为 AhnLab EDR 提供默认配套的 MDR（托管检测与响应）服务。EDR 客户可享受以下服务：

- 安全专家的实时监控
- 高优先级威胁分析与响应
- 分析报告与月度统计报告等服务

若客户需要更专业的服务，可选择包含高级 MDR 服务的“EDR Premium”。该服务提供更深入的日志分析、结合组织环境与安全问题的定制化检测规则等深度服务。

5. 选择 AhnLab 的产品的三大理由

尽管市场上已有多种 AV（杀毒软件）、沙箱、EDR 解决方案，但 AhnLab 的产品在以下三方面展现出独特优势，使其成为客户值得信赖的选择：

#1. 解决方案之间的灵活联动和协同效应

自30年前推出 V3 以来，AhnLab 构建了自主研发产品组成的完整的安全架构，具备极高的内部兼容性。各解决方案之间可灵活联动，形成强大的协同效应。客户可以将这些解决方案互为补充地使用，从而获得更强大的安全防护效果。

【图8】AhnLab EDR 与 MDS 联动分析

特别是在分析与响应层面，可以发挥显著效果。例如：

- 当 V3 检测到恶意代码时，EDR 可基于该信息提供详细的入侵路径分析，帮助预防未来可能发生的类似威胁。
- 若需对 EDR 收集的进程或文件信息进行深入分析，可请求 MDS 进行沙箱分析，从而获取更全面的威胁情报。

#2. 通过客户参考验证的卓越实力

AhnLab 的Linux 安全架构经过长期广泛的客户部署与使用，已充分验证了其有效性。客户在使用时，既有分别部署 V3 Net for Linux、AhnLab MDS 与 AhnLab EDR 的情况，但更多情况下会组合使用其中两款或三款，以实现综合安全效果。这些解决方案各自承担不同的角色，但由于具有互补性，因此联合运行时能够发挥最佳协同效应。

此外，这些解决方案不仅覆盖 Linux 环境，还能覆盖 Windows 环境，提供基于联动的安全防护，帮助客户构建安全的业务环境。

#3. 卓越的全球权威评估成绩

最后，AhnLab 的安全解决方案在全球权威安全评估中屡获佳绩，持续验证其技术实力。

特别是，AhnLab EDR 是韩国唯一连续四次参与全球最具权威的安全产品评估之一 MITRE ATT&CK Evaluation 的安全厂商。该评估通过模拟主要威胁组织的攻击技术，测试产品的威胁检测与响应能力。

在最近进行的第六轮评估中，针对勒索软件组织 CL0P 与 LockBit 在 Windows 与 Linux 环境中的真实攻击技术，AhnLab EDR 检测率达 95%，在全球安全企业中属于顶尖水平。 此外，在检测到的 56个子步骤（Substep） 中，有 49个获得最高等级“Technique”，这意味着用户可以通过检测信息全面理解威胁行为的上下文。

有关 AhnLab 在 MITRE ATT&CK 第六轮评估中的详细结果，可参考官方发布的《结果分析报告》。

6. 结语

希望能够与AhnLab的安全架构一起有效应对日益复杂的 Linux 安全威胁。

AhnLab 凭借过去30年积累的技术实力与经验，构建了覆盖 Linux 服务器在内的所有终端区域的强大安全能力，并以联动为核心构建防御体系。通过众多客户的实际部署案例，AhnLab 已验证了其解决方案的实用性，并在全球权威安全评估中屡获佳绩，持续证明其卓越的技术实力。

希望您能借助 AhnLab 的安全架构，有效应对日益复杂的 Linux 安全威胁。

想了解更多关于AhnLab的Linux安全架构解决方案的内容，请访问AhnLab官方网站。

- V3 Net for Linux Server
- AhnLab MDS
- AhnLab EDR
- MDR 服务

AhnLab China
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
http://cn.ahnlab.com | cn.sales@ahnlab.com
电话： +86 10 8260 0932（北京）| +86 21 6095 6780（上海）