AhnLab

安全月刊

2023.03 Vol.124

AhnLab 产品之间的链接

AhnLab 产品之间的链接以及如何使用

AhnLab是韩国唯一一家能够整合并提供包括端点、网络和安全托管服务在内的各种专业服务的综合安全企业。一直以来，我们通过AhnLab安全月刊探讨了有关综合安全的内容。

通过此文章，我们将介绍端点与网络产品之间有哪些链接功能，以及如何使用这些链接功能构建高效的业务系统和安全。

向 ChatGPT 提问集成产品

今年，AhnLab将解决客户各种安全需求作为首要课题，加强客户整合覆盖，增强综合安全能力。为此，集成产品比什么都重要，我们先了解一下什么是集成产品。

最近，一款新的聊天工具ChatGPT爆火。它与网络搜索引擎不同，无论我问什么问题，它都会挑选并显示我需要的信息，这太神奇了。因此，在ChatGPT的帮助下，笔者总结了集成产品的概念。

集成产品可以定义为“为客户提供完整的集成解决方案，以高效且有效的方式满足客户需求。”集成产品的优势包括通过用于监控和管理的单一界面简化了多种安全产品和服务的管理，以及通过将产品和服务集成到单一产品中来减少管理安全基础设施所需的时间和精力。简而言之，可以说集成产品提供了简化的管理、提升的效率、更好的业务环境、改善安全状况和成本节约。

AhnLab 提供的集成产品

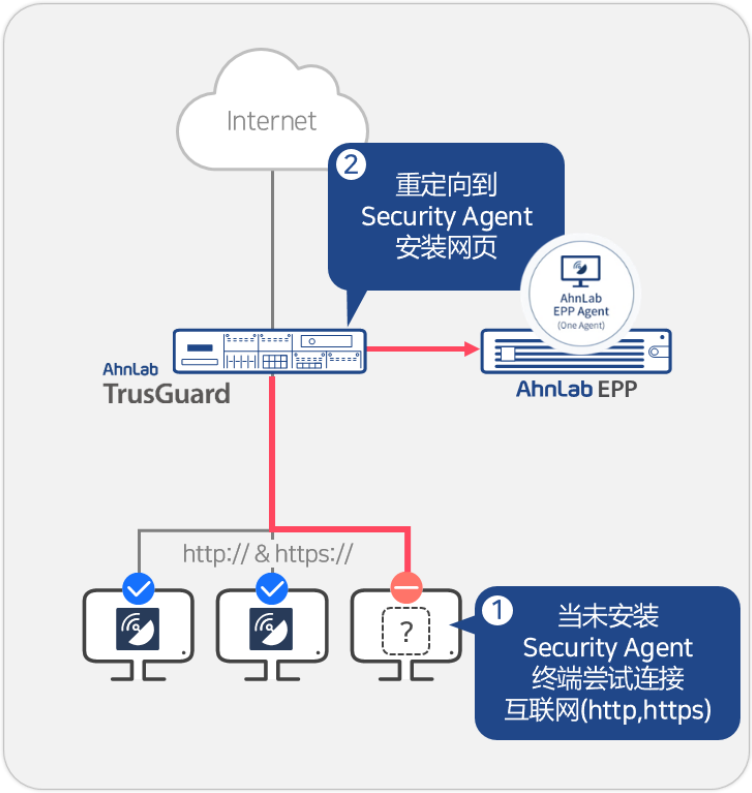
那么，AhnLab是如何提供集成产品的呢？可以分为三大类：第一类是集成平台，第二类是产品与服务的链接，第三类是产品与产品之间的链接和联动。

首先，集成平台中有EPP平台，可以通过一个平台管理叫做“AhnLab EPP Family”的V3（防病毒软件）、EPM（补丁管理）、ESA（计算机安全漏洞管理）、EPrM（个人信息泄漏防护）、EDR（威胁检测和防御）等5种独立产品，并可利用各种连接规则。此外，AhnLab CPP平台可在混合云环境中集成管理各种安全模块，如防病毒软件、基于主机的IPS/防火墙和应用程序控制。还有AhnLab TMS平台，这是一个威胁管理系统，可以对AhnLab TrusGuard（防火墙）、AhnLab AIPS（IPS）和AhnLab DPX（防DDoS攻击）等网络设备进行集中分发策略和集成管理。

其次，在产品与服务链接方面，有EDR和MDR服务，AhnLab的专业分析师远程分析和响应AhnLab EDR产生的各种威胁事件，这是AhnLab最大的优势。另外，还有MDS服务，它基于SECaaS（SECurity-as-a-Service），无需引入APT响应设备AhnLab MDS，只需为终端安装Agent即可获得同等的安全加强效果。此外，还提供与产品相关的数据分析服务和恶意代码分析服务等各种专业服务。

第三是产品之间的链接和联动，本文将详细阐述。链接案例可以分为八种情况。

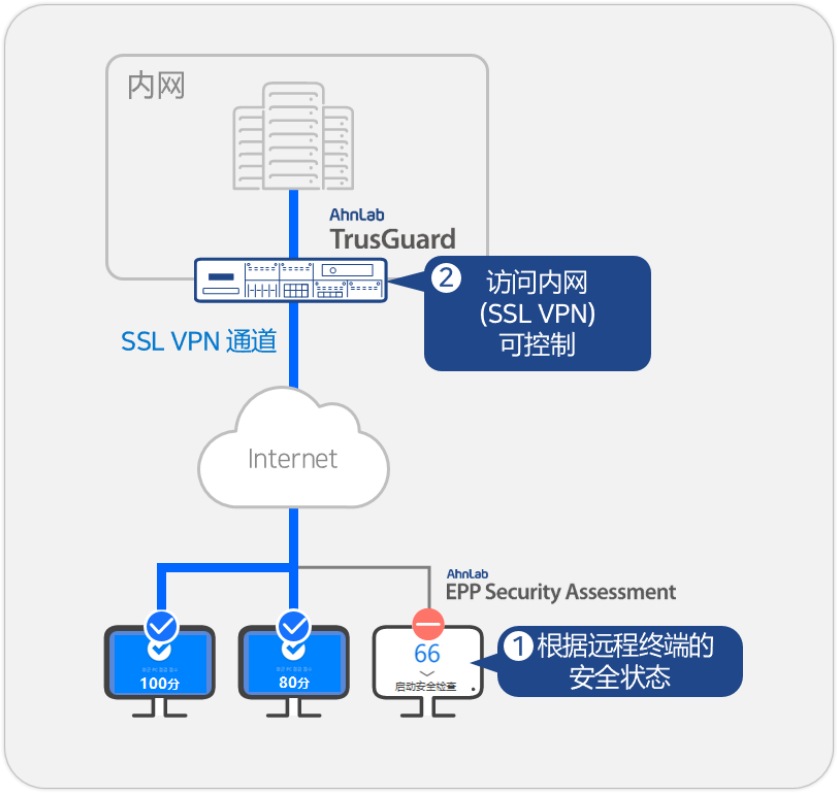
1. 通过EPP + TrusGuard链接强制安装Agent



【图1】EPP & TrusGuard Agent强制安装结构

该链接功能提供Security Agent安装重定向功能，可在用户未安装防病毒产品访问Web时，将用户重定向至可安装Agent的网页。如果新引进或已在使用EPP ，但EPP服务器底层的网络环境配置了NAT（Network Access Translation），则可以使用TrusGuard设备作为NAT设备并配置Security Agent来重定向环境。该功能同时支持HTTP和HTTPS，还可作为TrusGuard的子模型提供功能，无需成本负担即可使用强大链接功能。

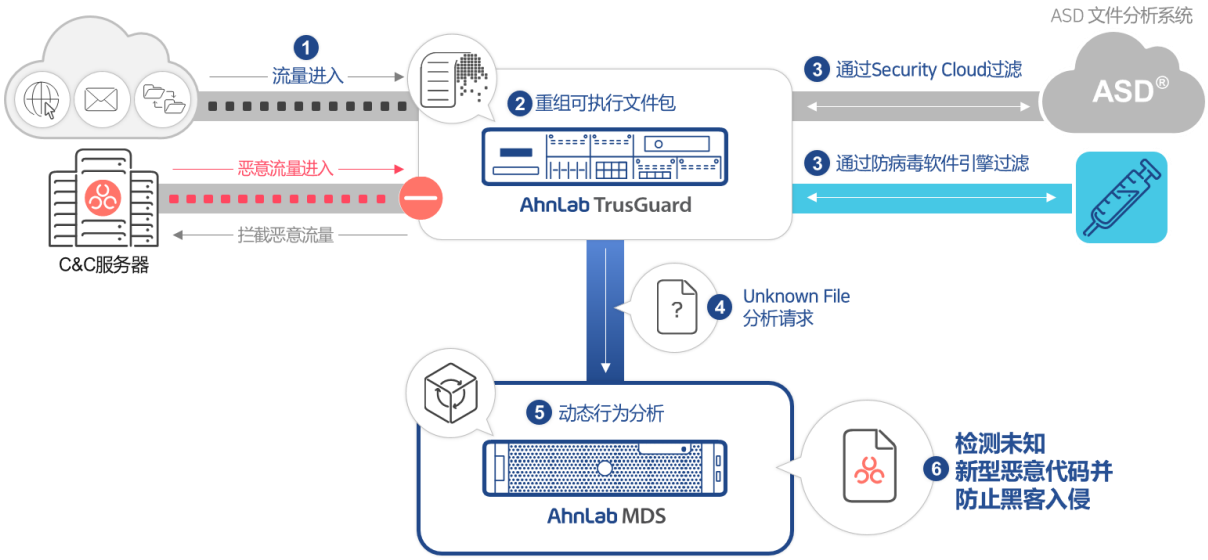
2. 通过ESA + VPN链接且基于安全评分的VPN访问



【图2】ESA + VPN链接结构

当组织需要加强用于远程办公的终端等远程终端安全时，可以使用该链接功能。通过利用ESA产品的安全检查功能，当远程终端的安全评分状态低于标准值时，可限制访问公司内部网络的VPN访问权限，且在只有高于标准值时才被允许访问。由于大多数远程办公人员的终端都是个人计算机，因此它可以用作一种加强安全的实用方案。

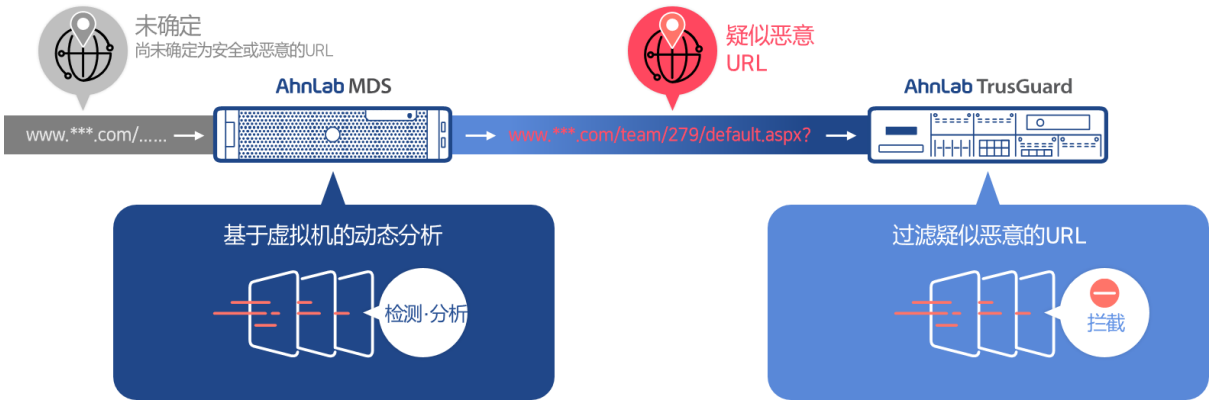
3. TrusGuard + MDS链接可疑流量动态分析



【图3】通过TrusGuard + MDS链接的可疑流量动态分析

对于通过TrusGuard设备引入的流量中的可执行文件，通过与MDS的联动，将引入的可执行文件的数据包重新组合，请求通过MDS进行动态分析，并提供根据分析结果做出响应的功能。作为初级过滤功能，它不会对通过ASD引擎已知的恶意代码进行分析，仅在引入未知恶意代码时才执行分析并查看相应结果。在有多个网络区间的环境中，当单独使用MDS而未配置为镜像（Mirroring）环境时，会非常实用。

4. 通过TrusGuard + MDS链接拦截恶意URL

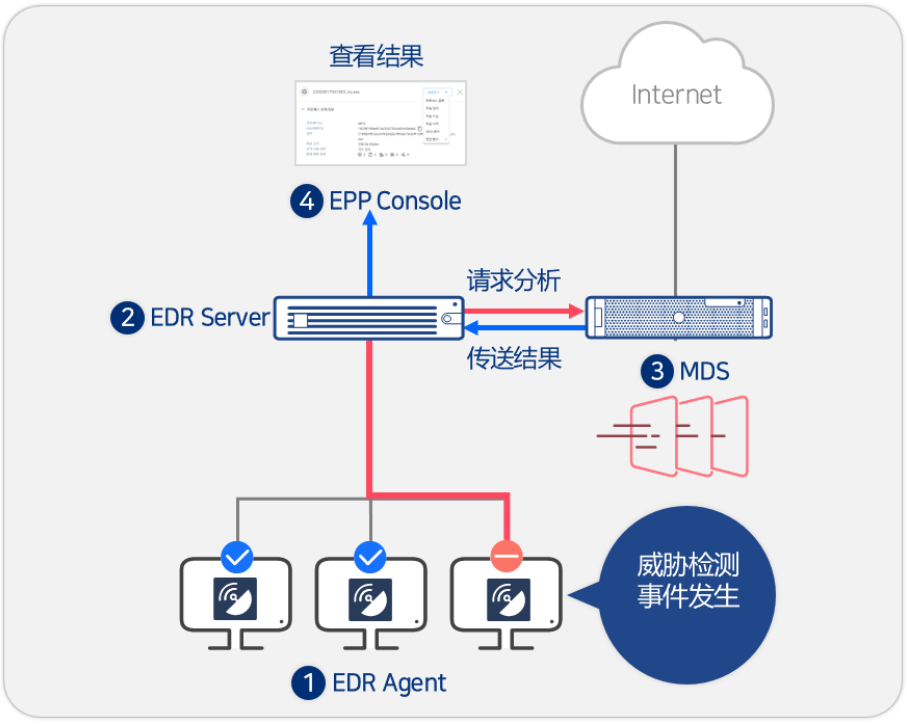


【图 4】通过 TrusGuard + MDS 链接拦截恶意 URL

与第三示例一样，它提供可以通过设备组合应用的功能。对于在MDS检测到的可疑恶意URL，支持通过与TrusGuard设备的链接实现自动拦截恶意URL。TrusGuard中可共享的最大URL数量为1,000，并在发现新URL时，

会删除旧项目后应用新项目。此外，还可以对通过TrusGuard注册的URL进行修改或单项选择删除。当使用能够对TrusGuard进行集成管理的TMS设备时，可以将从MDS接收的恶意URL通过TMS转发给TrusGuard。之后，还可通过物理分布的TrusGuard将需要拦截的URL信息列入黑名单。

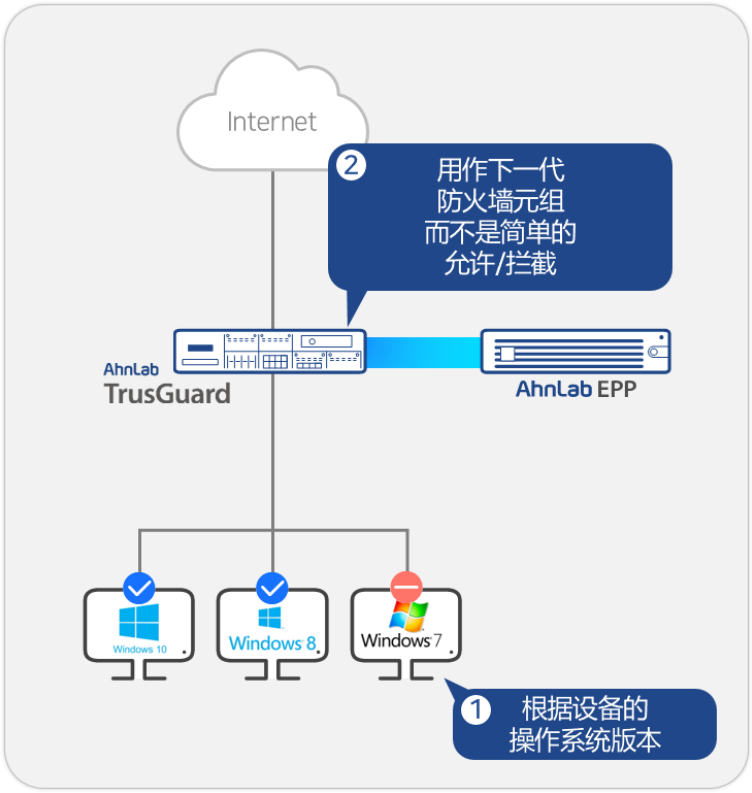
5. 通过EDR + MDS链接交叉分析威胁事件



【图5】通过EDR + MDS链接交叉分析威胁事件

提供通过MDS联动交叉分析EDR产生的威胁事件的功能。如果从EDR接收到的威胁事件中存在难以将其判断为正常或恶意的，相应功能则可以通过MDS请求追加分析可执行文件后，在管理员控制台确认分析结果值。当用户想通过对具有潜在威胁的可疑文件对象进行追加分析来快速做出决策时，该功能会非常实用。

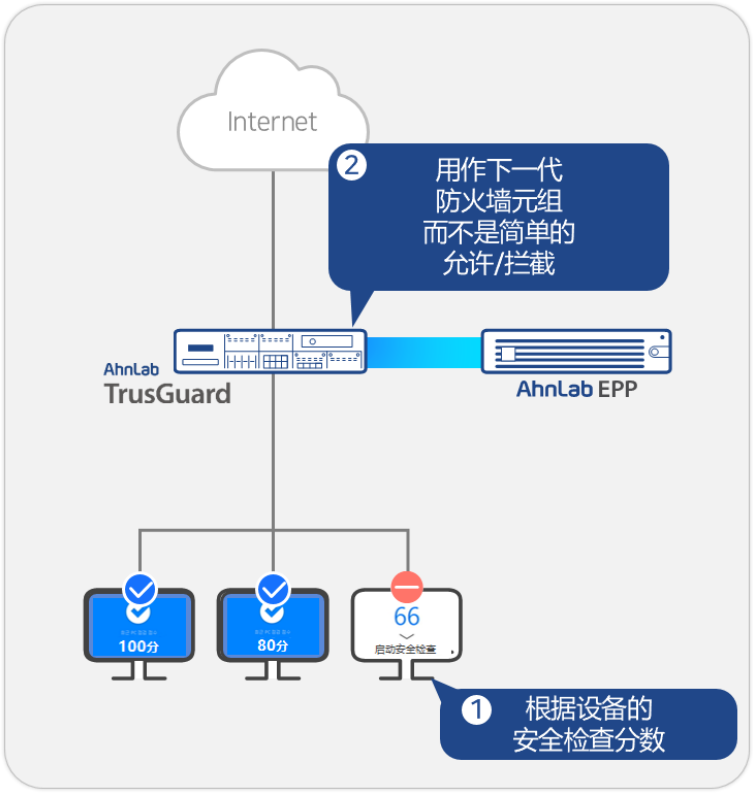
6. 控制EPP + TrusGuard链接设备（基于操作系统的控制）



【图6】基于EPP+TrusGuard操作系统链接控制设备

作为可以利用新一代防火墙特点的链接功能，它根据终端操作系统版本提供各种控制能力。例如，可以对正在使用已停止官方服务支持的Windows 7终端允许访问内部网络，并同时应用阻止互联网访问的规则集。而对正在使用Windows 10或更低版本的计算机根据操作系统版本应用各种安全策略，例如阻止RDP和TeamViewer等远程访问应用程序，或仅阻止KakaoTalk即时通讯工具的文件上传/下载功能。

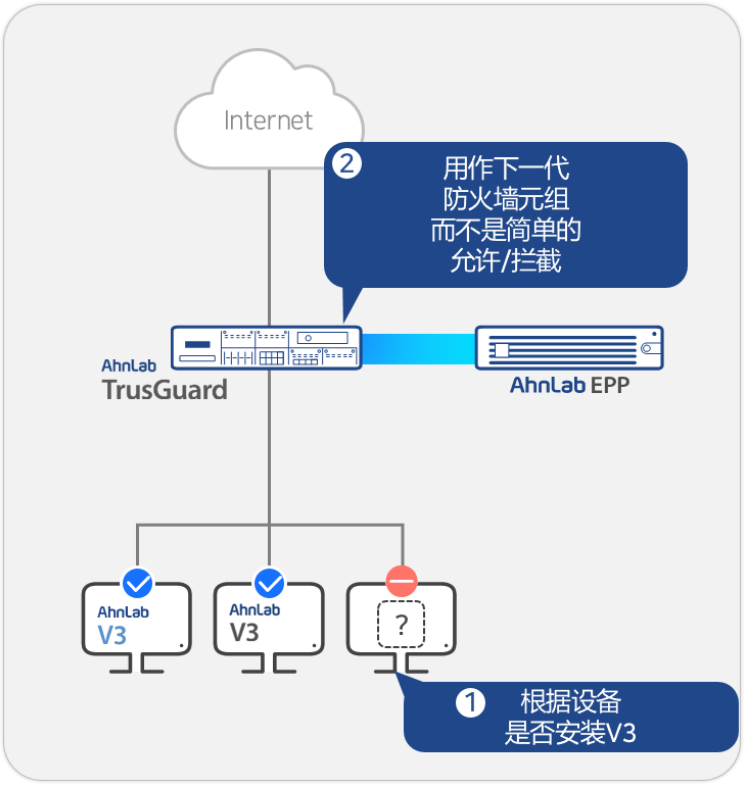
7. 控制EPP（ESA）+ TrusGuard链接设备（安全检查评分标准控制）



【图7】控制EPP + TrusGuard安全检查评分标准链接设备

在使用ESA的情况下，可以根据终端的安全检查评分使用各种控制功能。例如，可以对安全评分低于80分的计算机阻止访问基于全球类别URL的安全威胁类别和未分类类别，或者可以对安全评分低于60分的计算机阻止访问除公司内部系统以外的所有网络。对于安全评分低于80分的计算机，可以应用诸如阻止访问主要公共云（AWS、Azure、GCP）等功能。

8. 控制EPP + TrusGuard链接设备（V3安装标准控制）



【图8】控制EPP + TrusGuard V3安装标准的设备

作为最后一项功能，也可以按V3安装标准控制设备。例如，可以通过对未安装V3的计算机仅允许访问特定站点，或仅允许安装V3的计算机在指定工作时间内访问公司内部系统等利用各种控制功能来加强组织安全策略。

结论

在本文中， AhnLab分8种案例介绍了产品之间的链接和联动。如果根据组织的基础设施环境和特点， 合理运用这些功能，便可加强组织的安全管理能力和基于跨产品链接的监控，充分发挥提高安全可视性等效果。

AhnLab

安全月刊

https:// cn. AhnLab .com

https://global. AhnLab .com

https://www. AhnLab .com

关于AhnLab

Ahnlab的尖端技术和服务不断满足当今世界日新月异的安全需求，
确保我们客户的业务连续性，并致力于为所有客户打造一个安全的计算环境。
我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、
移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。
AhnLab已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

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