AhnLab

安全月刊

2018.05 Vol. 66

AhnLab EDR

下一代端点安全解决方案AhnLab EDR上市

AhnLab EDR

力求响应更高级的威胁

最近，端点安全再次受到瞩目。端点是企业和机构生成、存储和移动重要信息的领域，存在着不仅是操作系统和软件漏洞还存在着“用户”漏洞。过去几年中，我们也遇到了各种各样的新的安全威胁，例如高级持续威胁(Advanced Persistent Threat)和勒索软件，从而得出结论：一切都归结为“漏洞”和“恶意代码”。 另外，在整个端点领域，监控、收集威胁信息和响应角度的安全已经引起人们的关注。

应对当前这种局势，AhnLab最近发布了端点威胁检测和响应解决方案AhnLab EDR。

“我公司的员工由于业务需要而经常上网。因此，无论定期进行员工安全教育和应用安全补丁，还是会出现被恶意代码感染的计算机。更大的问题是，即使V3已经修复了恶意代码，但受感染的PC又被另一个恶意代码感染。我担心新的恶意代码会通过这些PC进入，导致个人信息泄漏或成为针对性攻击的牺牲品。我希望能够知道有关恶意代码的渗透路径和时间等信息，而不只是用V3进行检测和修复恶意代码而已。”

-A公司安全主管

“我公司运营各种端点安全解决方案，如V3和媒体控制解决方案等。在安全管理方面，报告每月V3的检测历史记录，还提取媒体控制例外处理请求的审批细节并报告每月例外处理情况。但我们的主管想知道如何进一步加强端点安全。要比现在更积极地运营和管理，我们应该如何做？”

-B金融公司安全官员

上述内容是企业和机构的安全人员对端点安全解决方案的运营和管理所提出的常见问题。许多企业和机构运营各种端点安全解决方案，而这些解决方案在安全的范围和角色上有所不同。例如，V3等防病毒软件g主要针对进入端点并造成危害的恶意代码进行检测并消除。 NAC（网络访问控制）或媒体控制（设备控制）解决方案根据安全策略阻止终端系统的网络连接，或防止诸如USB的介质连接到终端。此外，根据组织业务的性质，各种安全解决方案也被引入和运营，以满足各种合规性要求。

所有这些解决方案通常根据其目的和角色执行功能，并将结果显示给安全管理员。这是一种忠实地执行所需安全功能的解决方案，这意味着它不是一个安全管理员想要的那样积极响应的解决方案。在这种情况下出现的即是端点检测和响应（EDR）解决方案。

什么是EDR解决方案？

与传统的安全解决方案不同，EDR可以查看端点发生的各种事件和威胁，而不是执行特定功能，关键是使安全管理员能够快速做出决策并主动响应。全球IT研究公司Gartner将EDR描述为“是端点安全的另一种工具，可与现有的安全解决方案（如防病毒软件）协同工作。” EDR的作用是通过最大限度地缩小现有安全解决方案之间的差距（gap），提高组织对安全威胁的“威胁响应能力（resilience）”。这也意味着EDR要不负众望，就要了解各种端点环境以及具备相应的安全威胁响应能力和技术。这就是为什么AhnLab EDR的上市受到瞩目的原因。

AhnLab EDR是下一代端点安全解决方案，积累了过去30年AhnLab恶意软件分析技术和端点安全响应经验。基于不间断监控，它收集实际端点区域中出现的所有威胁信息，并提供基于威胁可见性的高级威胁响应。

AhnLab EDR，有什么不同？

我们可以将AhnLab EDR的目的概括为“通过确保端点安全威胁可见性的主动威胁响应”。

“提供端点安全威胁可见性”这个表达可以被广泛解释。AhnLab EDR通过应用于V3的MDP引擎检测、收集、存储和分析基于端点实际操作系统的所有行为信息，这是AhnLab独自研发的韩国最初的基于行为的分析引擎。此外，通过端点威胁事件的时间线分析提供有关威胁渗透路径、类型、目标、行为和内部传播等详细信息。

它还提供了一个关联图，如[图1]所示，可根据检测到的恶意代码或可疑文件和进程执行安全入侵检测和调查。安全管理员可以通过AhnLab EDR提供的关联图一目了然地查看相关文件、注册表、进程和网络连接之间的相关关系以及端点发生的威胁事件。

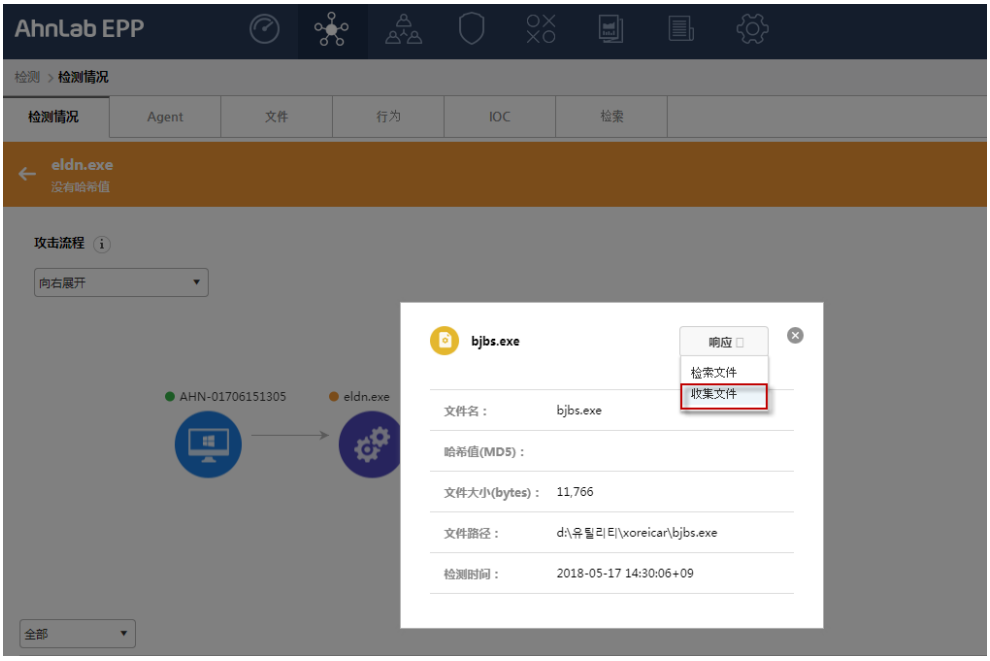
【图1】AhnLab EDR关联图

如【图1】所示，该图显示了端点上的威胁的相关关系，使安全管理员能够知道何时何地引入了威胁。 在传统的端点安全环境中，安全管理员只能看到检测到的恶意软件。但是，通过AhnLab EDR提供端点安全威胁的详细可见性，可以一目了然地查看与威胁相关的内容，并迅速做出响应实现了更积极的响应。

通过基于端点安全平台的EDR运营实现快速的威胁响应

AhnLab EDR基于下一代端点安全平台AhnLab EPP(AhnLab EPP, Endpoint Protection Platform)，易于构筑和运营。

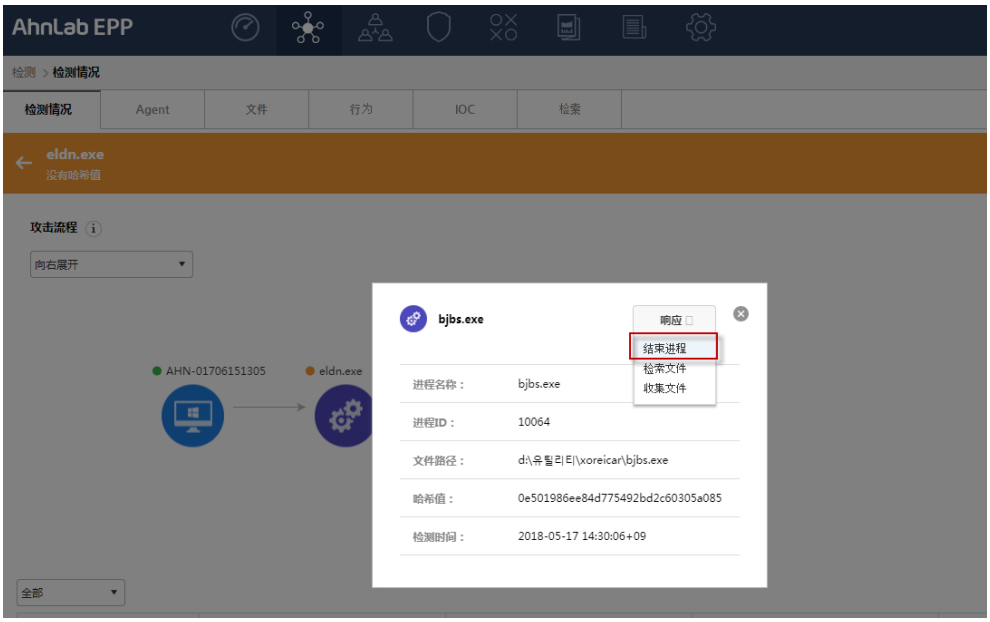
在制定威胁管理决策时，安全管理员将通过EDR收集的威胁相关的文件、注册表、进程和网络信息等转发给AhnLab请求详细分析。如[图2]所示，通过Web浏览器，可以连接到EDR服务器AhnLab EPP，发出文件收集命令来收集需要分析的文件，并将位于端点的目标文件下载到管理员计算机。



【图2】通过EDR管理服务器收集端点的文件

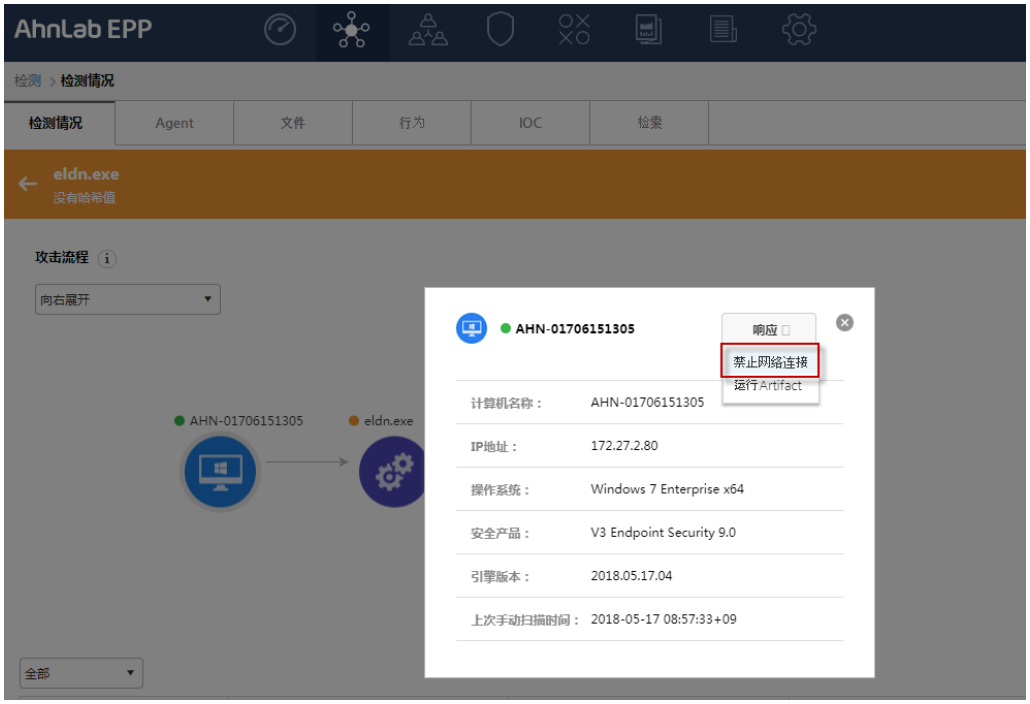
以前，当安全管理员收集端点上的文件时，他们必须远程连接或物理移动到他们所在的位置，并通过USB或电子邮件传输它们。但是，如果安全管理员可以访问基于Web的EPP管理服务器，则可以随时随地轻松快速地收集和分析可疑文件。

AhnLab EDR的管理服务器AhnLab EPP还可以在收集和分析端点文件时终止可疑进程。例如，如果即使确定为正常，由于漏洞而重复下载恶意代码，必须强制终止相应文件的进程，直到应用安全补丁。在这种情况下，可以通过AhnLab EPP管理控制台轻松终止在远程端点的进程。



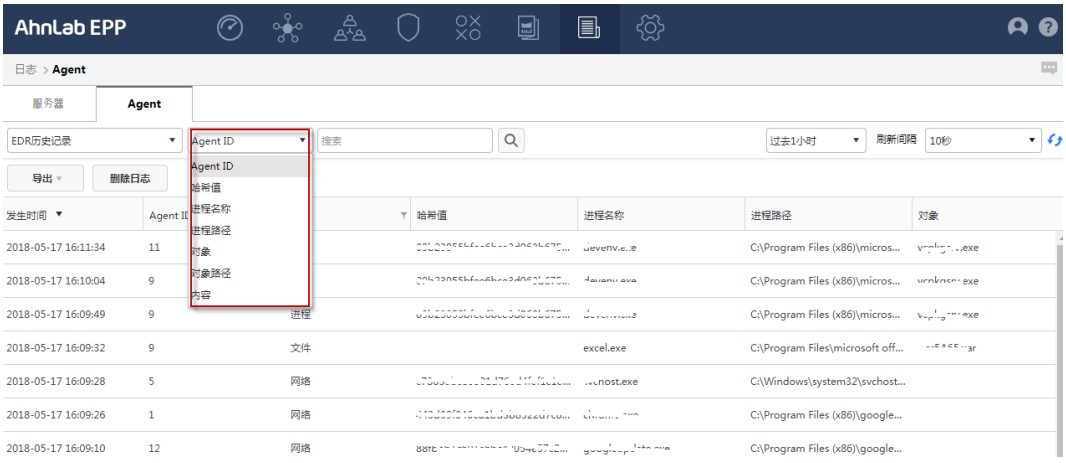
【图3】 通过EDR管理服务器结束端点的文件进程

在端点系统上执行收集可疑文件和终止进程等操作时，同时可能会在后台执行被新的恶意代码感染的危险行为。在这方面，AhnLab EDR提供了禁止网络连接功能，可以完全封锁可疑系统的网络连接。禁止除了与AhnLab EPP服务器的通信以外的所有网络连接，配置安全隔离的环境来执行各种响应。它还提供从系统收集Artifact以调查其他安全事件。



【图4】禁止网络连接功能

另外，AhnLab EDR提供了多样的收集行为信息功能，如[图5]所示，有助于潜在的威胁响应。特别是，在从外部组织共享利用在入侵事故的文件信息（文件名，哈希值等）和网络信息时，可以通过AhnLab EDR搜索组织内部是否存在相同的文件或哪些端点系统访问了相关网络。



【图5】搜索多样的威胁行为信息

V3用作EDR Agent，减轻管理负担并使效率最大化

需要Agent来监视和收集端点上数以千计的威胁行为，这些端点由数十到数百甚至数千个系统组成。但是，如果端点上已安装多个安全解决方案，则安装其他Agent可能会导致端点系统的性能下降或与现有应用程序发生冲突。如果存在多个安全解决方案的运营相关的多个管理控制台，在配置额外的管理控制台对安全管理员来说也是一种负担。事实上，一些外国EDR解决方案已进入韩国国内市场，但由于这个原因，他们难以确保客户。

AhnLab在过去两年收集来自不同客户的反馈，开发了使用现有的V3而不是安装另外的Agent的方式。换句话说，V3成为AhnLab EDR Agent。使用现有V3产品的客户可以轻松构建和运营EDR，而不会影响端点系统的性能或稳定性。

V3被许多全球认证机构认定为具有世界水准的性能，V3提供了一种“实时监控”功能，可在恶意代码进入端点或发生恶意行为时检测并阻止恶意代码。为了执行实时监控，V3已经在监控端点上的各种威胁路径。根据V3监控的数据，AhnLab EDR收集、保存和分析端点的威胁信息。

基于平台的EDR可实现更强大的威胁响应

大多数EDR解决方案监控和收集大量行为信息，例如注册表、进程和网络连接，以及端点上与各种威胁相关的文件，并将它们保存在管理服务器上。为了将这些保存的大量数据作为有意义的“信息”提供，需要执行使用各种技术的分析工作。问题在于，现有的基于关系数据库的管理系统（RDBMS）在存储和分析来自许多端点的大量数据方面存在局限性。即使EDR Agent收集并传输与威胁相关的行为信息，如果传统管理服务器无法接收、保存并及时分析，也没有任何意义。

出于这个原因，AhnLab开发了一个大数据平台，可以平行分布处理数据，以有效保存和分析EDR收集的大量数据，并与AhnLab EDR一起上市。

新的端点安全平台AhnLab EPP不仅仅是EDR的管理解决方案。 AhnLab EPP可以通过单个管理控制台有效地管理各种端点安全解决方案，如V3、AhnLab Patch Management、AhnLab Privacy Management和AhnLab My PC Inspection以及EDR。多个端点安全解决方案的互联提供了灵活的安全管理和更强大的威胁响应。

可以毫不夸张地说，AhnLab EDR和AhnLab EPP是由客户而诞生的。这是因为许多AhnLab客户与AhnLab一起建立和运营端点安全系统，他们的观点和担忧引发了这些解决方案。自引入EDR和EPP以来，建立了持续监控端点并收集和分析威胁信息的环境，我们将继续通过收听和反映客户的需求来提供更高级的威胁响应。

AhnLab

安全月刊

http:// cn.ahnlab.com

http://global.ahnlab.com

http://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