AhnLab

安全月刊

2018.04 Vol. 65

Endpoint Detection & Response

采用下一代端点安全技术的建议

EDR 会成为安全的未来吗？

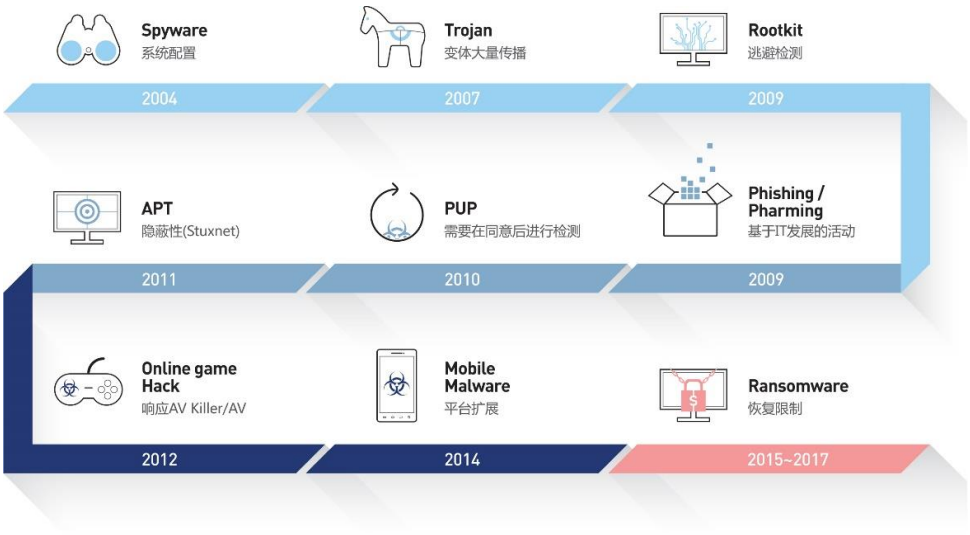
EDR（Endpoint Detection & Response，端点检测和响应）是安全领域最受关注的解决方案之一。EDR市场非常期待能够提高现有安全解决方案缺乏的可见性（Visibility）和响应（Response）能力的解决方案。EDR是否会成为满足这些期望的新解决方案？或者只是出现片刻即消失的时尚东西？

本文将介绍EDR的背景，客户需求以及将于2018年4月底发布的AhnLab EDR和AhnLab EPP。

持续的安全威胁和恶意代码威胁

2017年也发生了大规模的安全事件。Equifax，Uber和Verizone等公司遭受了大量的个人信息泄露。还有很多企业遭受了Ransomware的损害，包括让世界陷入恐慌的WannaCry和Petya以及导致韩国互联网服务公司破产的Erebus等。

这些攻击大部分从端点开始，并使用恶意代码进行的。自从被称为最初病毒的Brain问世以来，这种模式持续了30年。



[图 1] 主要的恶意代码变化

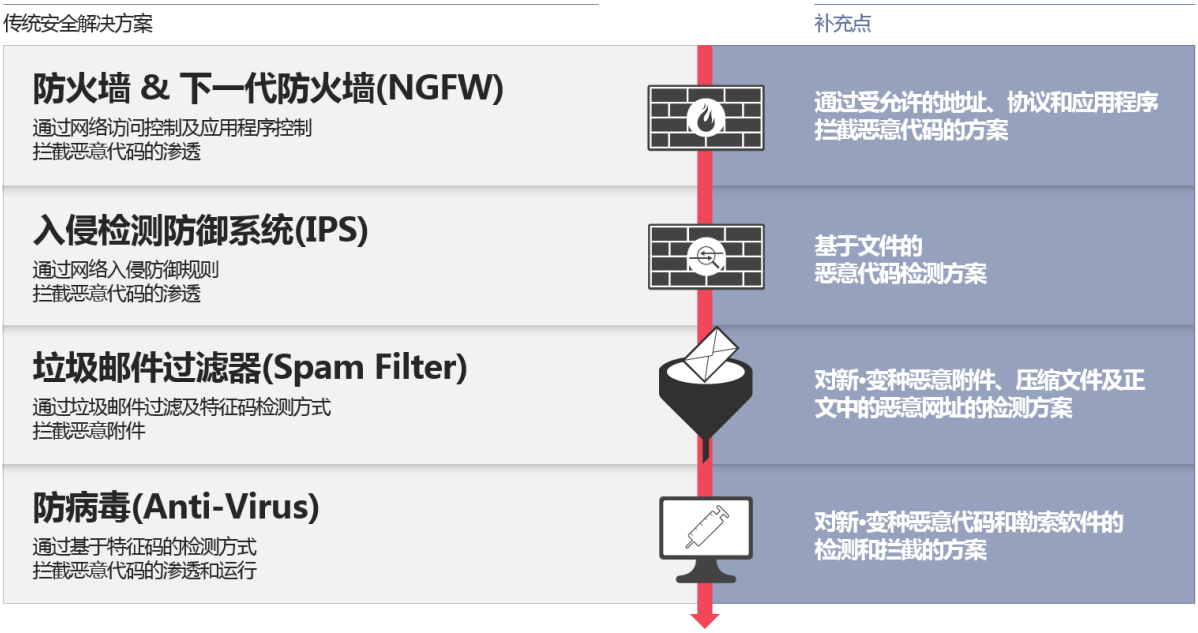
如果安全解决方案有变化，这表示逃避检测的技术也在发展。而不变的是攻击者将继续利用恶意代码并取得成功。因此，需要采取战略和解决方案，以统一管理和响应端点的安全威胁。

传统安全解决方案的限制和客户需求

改变这种看法的需求不仅出现在安全行业，而且也出现在使用安全解决方案的一般企业中。企业通常在其端点领域部署防病毒、补丁管理、媒体控制和网络访问控制等安全产品，而在网络领域部署防火墙（Firewall）、入侵防御系统（IPS），DDoS防御系统和Web防火墙（WAF）等安全产品。尽管如此，仍然出现被恶意代码感染，并导致系统瘫痪和数据泄露的损害。

攻击者绕过防病毒产品和高级持续威胁（Advanced Persistent Threat, APT）防御产品正在展开复杂的攻击，通过没有应用补丁的程序和访问易受攻击的网站频繁出现感染事件。此外，网络安全产品在阻止通过授权地址、协议和应用程序的恶意代码渗透方面也存在限制。

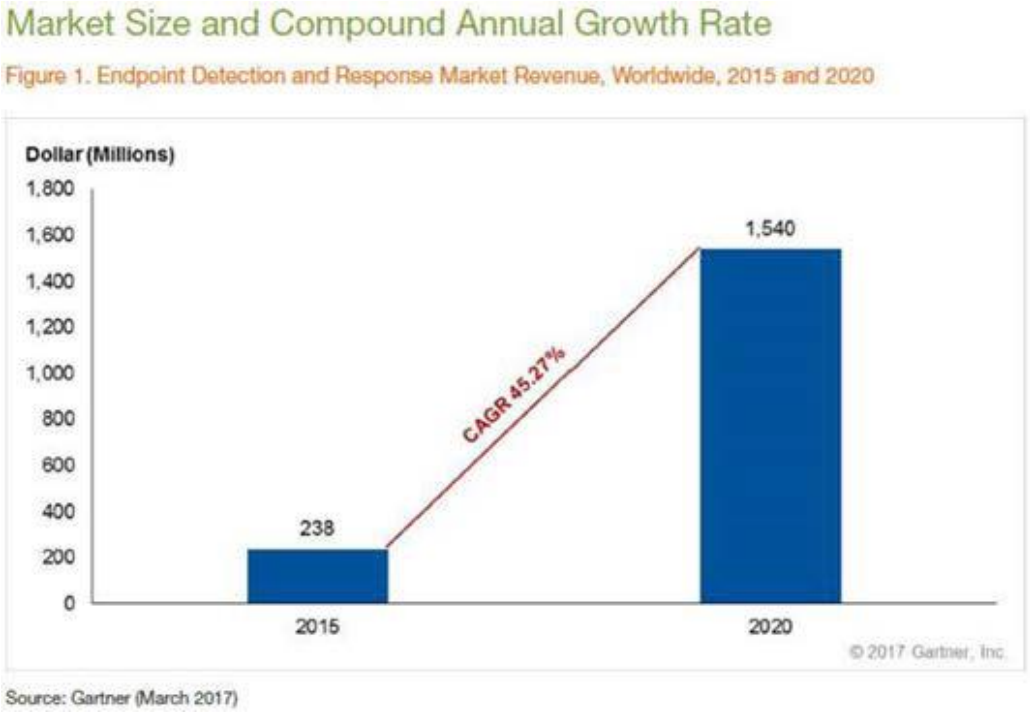
用户和实体行为分析（User and Entity Behavior Analytics, UEBA）和安全信息和事件管理（Security Information and Event Management, SIEM）这些相对较新的产品也不能完全阻止安全威胁。由于UEBA是基于行为的，因此需要一个单独的数据收集服务器，如SIEM。如果链接的单元安全产品不传输日志，则SIEM无法执行分析，因此它依赖于单元安全产品。



[图 2] 传统安全解决方案的限制

现在，企业开始意识到，迄今为止他们采用的安全解决方案不足以抵御安全威胁。也知道，他们必须响应利用新的恶意软件或零日漏洞的“未知威胁”，以及包含在内但发生时不可预测的“隐形威胁”。企业现在意识到在发生过多的损害之前需要一种解决方案来实现快速检测和响应。

从这个角度来看，EDR（端点检测和响应）是大多数企业安全人员最感兴趣的解决方案。EDR的需求和兴趣在全世界都很高。全球研究公司Gartner预测，全球EDR市场将以2015年的2.38亿美元增长至2020年的15亿美元，复合年增长率高达45.27%。到2020年，超过65%的大型企业和不到一半的中型企业将投资具备全功能的EDR。



[图 3] EDR市场规模及发展趋势

什么是EDR（端点检测和响应）？

让我们来看看目前安全领域最大话题的EDR。EDR的出现可以追溯到2013年。Gartner在2013年首次在其博客中介绍了端点威胁检测和响应（Endpoint Threat Detection and Response, ETDR）。自那时起，每年都会发布一份“EDR解决方案市场指南(Market Guide for EDR Solutions)”报告，其中介绍市场、技术趋势和主要供应商的动向。

正如Gartner所定义的，EDR代表了一种安全解决方案，可在端点级别提供持续监控和响应。此外，EDR还要提供“检测安全事故(Detect security incident)”、“调查安全事故（Investigate security incident）”、“在端点控制安全事故（Contain the incident at the endpoint）”以及“将端点修复为预感染前期状态（Remediate endpoint to a preinfection state）”等功能。

重要的是EDR对于在端点发生的多样的行为检测有多快且有多少，并且还应提供端点级别的可见性（Visibility）以追踪除了检测到的终端机之外的其他终端机上发生的入侵行为。

为了防止进一步的破坏，要提供“隔离受感染的终端”、“阻止网络”和“检测漏洞并应用修补程序”等响应（Response）。所有这些行为的目的都是为了尽量减少安全威胁造成的损失。

世界各地的许多安全公司现在正在推出EDR解决方案。 EPP（端点保护平台）供应商，如AhnLab，赛门铁克和趋势科技正在将EDR模块添加到现有产品的方式推出新产品。下一代防病毒（Next Generation Anti-Virus）厂商和新兴EDR厂商也在竞相推出产品并引领市场。

为什么AhnLab谈论EDR时,也谈论EPP?

AhnLab将在4月底发布AhnLab EDR产品。同时展示AhnLab的下一代端点安全平台AhnLab EPP。

最近,作为安全起点和终点的端点再次受到关注。对此,一些人表现为端点的返还。但是，从成立到现在，AhnLab一直强调着端点安全的重要性。

特别是，在2017年发表了AhnLab端点安全平台战略AhnLab SECURITY LADDERS（http://cn.ahnlab.com/global/upload/download/asecreport/ahnlab_zh_201705_vol.54.pdf），指出了端点安全方面的创新需求。

AhnLab SECURITY LADDERS是代表“遗产（Legacy）”、“自适应（Adaptive）”、“检测（Detection）”、“客户驱动（Driven）”、“端点（Endpoint）”、“响应（Response）”和“服务（Service）”，意味着由客户推动的“易于使用的安全和可实现的安全”。

在这一战略下，AhnLab已将关注点从恶意代码检测转向威胁管理，并建立“检测-分析-响应”循环结构，不仅可以实现阻断，还可以实现检测和快速响应。

通常的EPP是防止基于文件的恶意软件，检测和拦截程序的恶意行为，进行调查和修复以响应安全事故的端点安全解决方案。而AhnLab EPP(Endpoint Protection Platform)是下一代平台，有机整合并连接AhnLab的各种端点安全解决方案，以检测•监控•响应不断出现的安全威胁。该平台的最大优势之一是能够通过单一Agent和单一管理（One Agent, Single Agent）控制台统一运营。

例如，使用V3的客户可以通过添加AhnLab EDR许可证后通过AhnLab EPP来统一管理、监控和响应，无需安装额外的Agent程序。不仅如此，通过该管理控制台，客户可以选择适合自己的产品，如补丁管理解决方案（AhnLab Patch Management），漏洞检查解决方案（AhnLab My PC Inspection），隐私管理解决方案（AhnLab Privacy Management）。

[图 4] 基于AhnLab EPP的AhnLab EDR概念图

EDR解决方案基本上需要有效地收集、存储和分析大量数据并与各种安全解决方案联动，因此需要一个可以作为后盾的新的平台。这就是为什么AhnLab EPP是下一代端点保护平台的原因，这也是同时推出EDR和EPP的原因。

EDR市场正与EPP市场迅速融合，EDR、EPP和下一代端点安全产品将在未来三到五年内转变为单一管理控制台和单一Agent（Single integrated agent with single management consoles）。现有的EPP供应商正在迅速采用EDR功能来更好地监控攻击者，而EDR供应商正在增加更好的检测和响应能力来与EPP供应商竞争并取代EPP供应商。

由于许多安全厂商正在发布EDR产品，越来越多的客户正在推出EDR产品，EDR被视为“安全终结者”。但有一点很清楚：EDR非常重要，但它也不过是解决安全威胁的另一种工具。 必须清楚地认识到：如果没有人员和流程可以利用它，EDR无法存在。

AhnLab EDR和AhnLab EPP将在5月份的“AhnLab安全月刊”中详细介绍，以了解各自的特点和功能，以及它们如何一起取得效果。

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