AhnLab

安全月刊

2021.07 Vol.104

统一安全平台的核心价值和应用事例

统一安全平台的核心价值和应用事例

安全解决方案走向何方?

AhnLab始终专注于“强化（Hardening）”现有解决方案和服务，在新领域推进安全技术，并加强云安全能力。而且，其核心是通过联动各解决方案，根据客户的环境，以平台的形式提供安全服务。

一直以来，AhnLab始终在强调统一安全平台的必要性。本文将通过安全平台具有的真正价值和实际应用事例，讲述让读者更有切身体会的统一安全“故事”。

过去，当本地（on-premise）占主导地位时，各产业的安全要求事项非常相似，安全领域也划分明确。

因此也有人认为 ， 安全市场长期停滞不前 ， 没有太大发展。然而 ， 在过去几年 ， 随着高级持续性威胁（Advanced Persistent Threat: APT）、电子邮件攻击、端点检测和响应（Endpoint Detection & Response: EDR ）等新概念攻击和解决方案的出现， 重新定义了安全市场的格局。随着威胁的高度化和安全环境的复杂性日益加深，预计统一安全平台将变得比单一领域中的个别解决方案更加重要。

为什么统一安全很重要？其核心概念是什么？

由于新冠疫情的大流行， 云端系统的引入和远程办公的趋势在不断增长， 进一步突出了统一安全的重要性。随着越来越多的客户迁移到称为 “云” 的一个全新的环境中， 要求能够有效保护云端的安全能力。此外， 云技术虽然已成为主流， 但这并不意味着本地就不再重要。本地仍然占据韩国市场的很大一部分。因此， 本地和云结合起来的 “混合（hybrid）” 概念备受关注，安全供应商需要能够有机地保护这种混合环境。

此外， 由于要保持社交距离， 导致远程工作迅速增加， 这要求客户在分散的工作环境中全面关注安全的网络连接、用户身份验证和终端安全。最终， 从安全供应商的角度来看， 我们得出了一个结论， 那就是包括端点、网络、安全服务和云领域的 “统一安全” 非常重要。

统一安全的核心大致有两个方面。首先是提高客户的使用性。无论一个特定的解决方案在技术上有多出色 ， 如果实际客户无法使用或不需要， 它的价值必然会降低。因此， 应该基于对客户的需求和状况的基本了解， 进化安全平台，以促进与客户的共同成长。

二是加强联动。对于安全整合， 重要的不是将解决方案和服务原封不动地集成（Integrated）在一起， 而是要充分利用它们的特点并将他们联动 （ Unified ） 在一起。换句话说， 应该要实现一个 “ 联动型统一安全平台（Unified Security Platform）” ，将端点、网络、安全服务、云等各领域的安全能力连接起来，形成协同效应，提高管理便利性。

AhnLab 统一安全的支柱——AhnLab EPP

AhnLab的端点安全平台AhnLab EPP(Endpoint Protection Platform)实现了各种安全解决方案的有机联动和统一运营，始终追求之前强调的 “联动型统一安全” 。其核心是基于不再是简单的安全管理的平台， 提供系统且高效的端点威胁管理和响应。

【图1】AhnLab EPP结构图

AhnLab EPP提供5个端点安全解决方案，包括EPP Privacy Management(EPrM)、EPP Patch Management(EPM)、EPP Security Assessment(ESA)、EDR(Endpoint Detection & Response)，以及最著名的防病毒解决方案“AhnLab V3 Internet Security(V3 IS)”。各解决方案都执行安全所需的功能，例如防病毒、个人信息保护、补丁管理、漏洞检测和响应，并且可以基于单一Agent和单一控制台进行管理，从而提高客户的安全性和效率性。

尤其，在威胁变得越来越复杂的环境中，像AhnLab EPP这样的平台变得更加重要。作为示例，以下从威胁响应的角度，将EPP和EDR联系起来加以说明。仅在几年前，当防病毒解决方案阻止特定攻击时，很少有客户对其背景感到好奇。这是因为，人们认为通过拦截就已经成功地防御了攻击，无需进一步的后续措施。

然而，现在情况发生了变化，越来越多的客户正在寻求了解攻击的背景。只有了解正确的背景，才能防止攻击再次发生，并有助于定义内部合规性。在这里，EDR的作用不仅仅是提供简单的拦截攻击这一“结果”，而是提供攻击的“理由”。

众所周知，EDR是一种对威胁“响应”而不是拦截攻击的解决方案。这里所指的响应并不意味着解决方案会自行检测并修复攻击，而是会随时保留日志和历史记录，并在问题发生时帮助验证（Validation）威胁。也就是说，基于储存在EDR中的信息，例如验证记录，可以建立防止再次发生的对策，并且当这些信息被累积后模式化时，可以利用通过EDR自动发出警告的附加功能。此外，为了让用户能够选择自己需要的信息，还应用了机器学习等技术。

在这方面，EDR与现有的拦截解决方案互相补充，通过在EPP中添加EDR，将完成一个有机地进行威胁检测/响应和攻击拦截/修复的安全系统。当前已知威胁和未知威胁并存的安全环境中，这是一个非常重要的价值。

此外，正如AhnLab在4月刊“探索云安全面临的七大威胁”中强调的那样，AhnLab不仅正在开发端点，也在开发作为统一平台的云安全产品组合。通过以云工作负载安全平台“AhnLab CPP”为首的云安全管制、咨询服务，以及安全专业MSP服务“AhnLab Cloud”，构建了将从安全服务中获得的经验应用于促进安全平台发展的“良性循环系统”。

此外，借助新一代网络防火墙“AhnLab TrusGuard”与端点平台解决方案联动，正在逐渐形成全面的威胁管理能力，其他网络安全产品也正在进行端点安全联动的工作。

统一安全平台的实际应用事例

到目前为止，我们已经探讨了统一安全平台的概念和价值。但是，从客户的角度来看，可能会提出以下的问题。“我完同意安全平台的重要性，但现在我们的组织真的会需要它吗？”

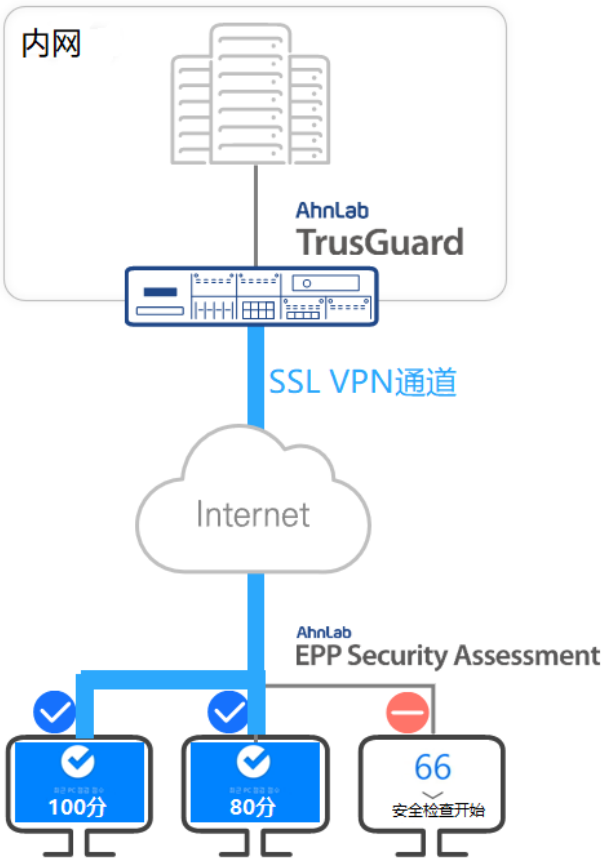
因此，我们介绍两个简单的示例，说明联动型统一安全平台目前在组织面临的问题中所起的作用。

1. 远程办公

远程办公环境是一个复杂多变的环境，其工作方式不是像过去那样在公司内部指定的空间进行，而是员工们分散在多个地点进行工作，从安全角度来看，需要保护的区域和价值被进一步扩大。对此，进行安全的远程办公需要很多安全要求，而其中的基础和核心就是前面提到的“用户身份验证&安全的网络连接”和“端点安全”。

AhnLab的远程办公安全防护服务主要由新一代网络防火墙“AhnLab TrusGuard”和“AhnLab EPP”组成。TrusGuard负责通过OTP联动进行用户验证和安全的VPN连接，EPP中的解决方案对终端进行有机保护。作为参考，有关EPP远程办公安全的更多信息，请查看3月刊“远程办公带来的风险以及解决方案，AhnLab告诉你答案！”。

AhnLab的网络安全和端点安全并没有单独执行各自的任务，而是通过互动创建更安全的远程工作环境。【图2】展示了TrusGuard和ESA在EPP平台上执行终端漏洞检查和采取措施的联动结构。



【图2】TrusGuard & ESA联动概念图

简而言之，当TrusGuard的SSL VPN客户端启动时，会自动检查远程访问终端的ESA检查结果。只有在检查分数符合设定标准时才会允许VPN连接，如果不符合，则限制VPN连接并提供措施方案。此外，以分钟为单位判断ESA的检查分数来保证实时安全。

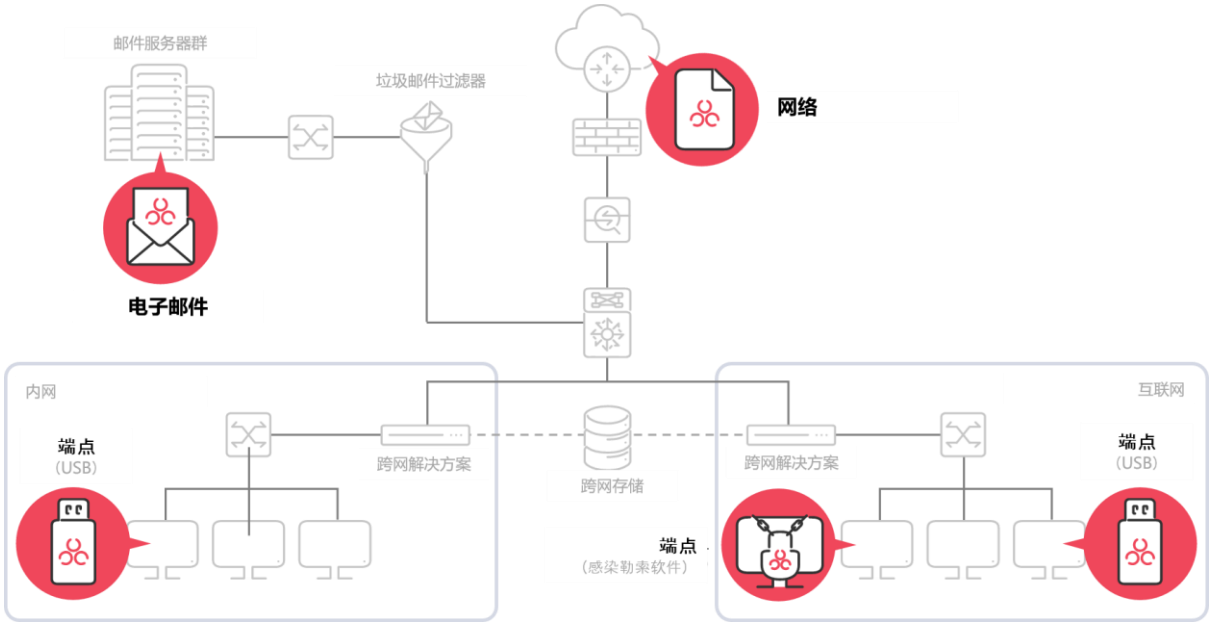
通过这种方式，当客户在远程办公环境中工作时，只有经过安全验证的终端才能访问公司内部网络，从而增强了安全性。并且，对于金融相关组织，可以遵守以下金融安全局的《电子金融监管条例实施细则》：【2.内部网络访问控制 > 远程访问时预检查安全措施】项目。

2. 响应勒索软件

今年5月，美国最大的燃油管道运营商“科洛尼尔管道运输公司（Colonial Pipeline）”遭到勒索软件攻击，导致管道被迫关闭。这一事件意义重大，以至于美国总统约瑟夫·拜登的官方回应消息传遍了世界各地。由于勒索软件攻击在此之后仍持续不断，美国采取了全国性的应对措施。

今年11月，韩国大型流通企业A公司的系统也感染了“CLOP勒索软件（CLOP Ransomware）”，并导致销售中断。为了加强响应对国内外接连发生的勒索软件攻击，韩国科学技术信息通讯部正在主导民官合作。

重要的是，现在勒索软件并不是一个遥远的故事，而是成为了一种随时威胁着我们的存在。而且，【图3】显示了组织可能感染勒索软件的地点结构。



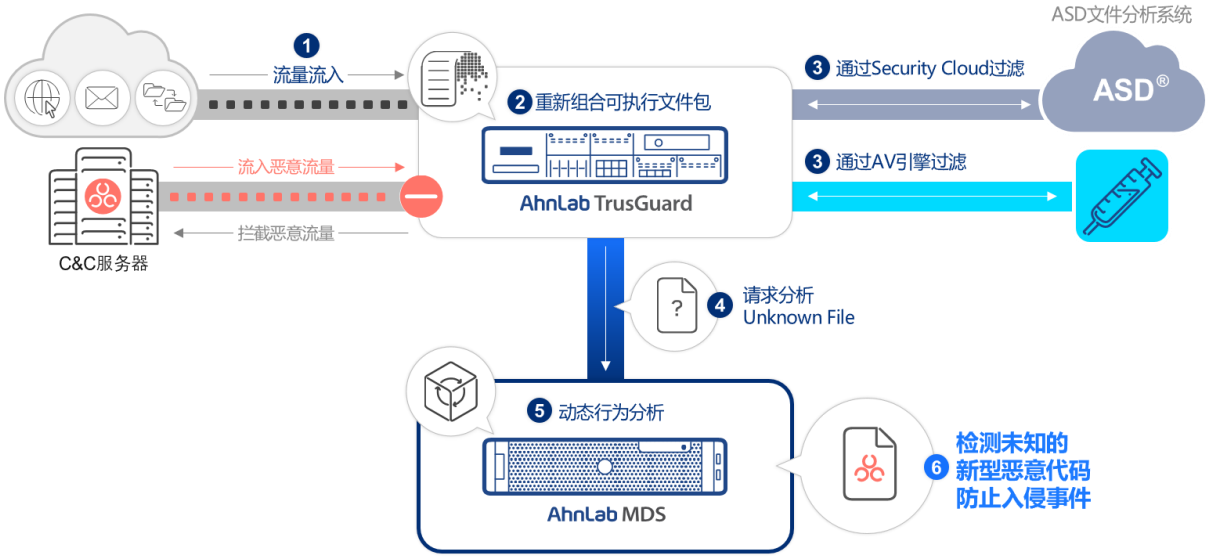
【图3】勒索软件感染地点结构图

从上面的结构图可以看出，要防御勒索软件的攻击，仅仅保护某一地点是不够的，还需要建立一个集体有机的安全体系。AhnLab提供基于安全产品组合的勒索软件全面响应防护服务，该组合涵盖网络、端点和电子邮件以及解决方案之间的有机联动。许多解决方案都和该产品有相关的联系，其中的核心是APT响应解决方案“AhnLab MDS”和AhnLab EPP以及AhnLab TrusGuard。

基本上，MDS针对基于网络、端点和电子邮件的攻击，提供了优化于各流入路径的有效的响应方案。主要功能包括▲异常流量检测与拦截▲恶意代码删除▲运行保留▲可疑文件提取▲系统隔离▲电子邮件隔离▲电子邮件过滤联动等，通过“采集 → 检测 → 分析 → 监控 → 响应”的过程，有效响应勒索软件。在这里，TrusGuard可以拦截勒索软件分发站点的访问和使用未经授权的端口访问内部服务器的行为，而EPP通过上述解决方案之间的有机联动来保护端点。

此外，在各领域为了拦截勒索软件以确保安全的关键功能执行解决方案，通过相互联动最大限度地发挥协同作用。

首先通过MDS和TrusGuard的联动，TrusGuard在流量流入后重新组合可执行文件数据包，通过ASD文件分析系统和AV引擎过滤器，向MDS请求动态分析可疑文件。之后，MDS执行动态分析并检测未知的新型恶意代码，以预防入侵事件的发生。此外，这两种解决方案还通过联动提供了对推断为恶意的URL的拦截功能。



【图4】TrusGuard & MDS联动

此外，MDS可以通过与V3产品一起安装的方式提供Agent，以优化安全流程和性能。由此，可以通过V3提前检测、拦截和响应已知（Known）的恶意代码和恶意行为。未知的（Unknown）新/变种恶意代码可以通过MDS进行检测、拦截和响应。此外，TrusGuard还提供了更强大、更便捷的安全能力，例如无需单独安装TrusGuard Agent，通过与EPP的联动实现基于设备的控制。

结论：坚实的构建是实现联动型统一安全的原动力

考虑到不断发展的威胁形势、混合使用本地和云的混合环境的出现，以及统一安全平台在远程工作和勒索软件事例中的作用，我们得出的结论是“仅单一安全有局限性”。

这里的单一指的是解决方案和公司。安全防护企业利用其解决方案的特点提供安全平台当然很重要，但为了客户创造安全的商业环境，他们需要与竞争对手携手合作。这就是合作（Cooperation）与竞争（Competition）相结合的“合作型竞争（Coopetition）”概念受到关注的原因。

从客户的角度来看，需要认识到不断变化的威胁环境和单一解决方案的局限性，并考虑一个可以长期保护业务的联动型统一安全平台。但是，如果盲目地引入安全平台和解决方案，安全性可能会变得过重，因此需要在不影响可用性的范围内明确定义要保护的对象。

我们通常提到逐步构建某些东西以实现的过程称为“构建（Build-up）”。该术语特别是在足球领域中所常提及到。意思是整个球队系统地进行过去被认为是前锋专属的进攻战略，通过从后方开始的传球到移动来创造空间并组建进攻，让队伍继续前进。最近，即使是处于最后方的守门员也参与到该构建当中。

此构建过程对于成功实现联动型统一安全非常重要。这是因为， 为了让先进的安全平台取得真正的成果， 必须有机地支持个性化的解决方案和服务、客户洞察以及基于它们的改进工作。在构建的过程中， 可以获得 “共同成长”的价值，比如客户的安全防护系统的完善和AhnLab的联动型统一安全的演进。

通过扎实的构建，让我们一起期待接近完成的AhnLab联动型统一安全平台，未来会以怎样的面貌演进。

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