AhnLab

安全月刊

2020.05 Vol.90

2019 新型冠状病毒与安全

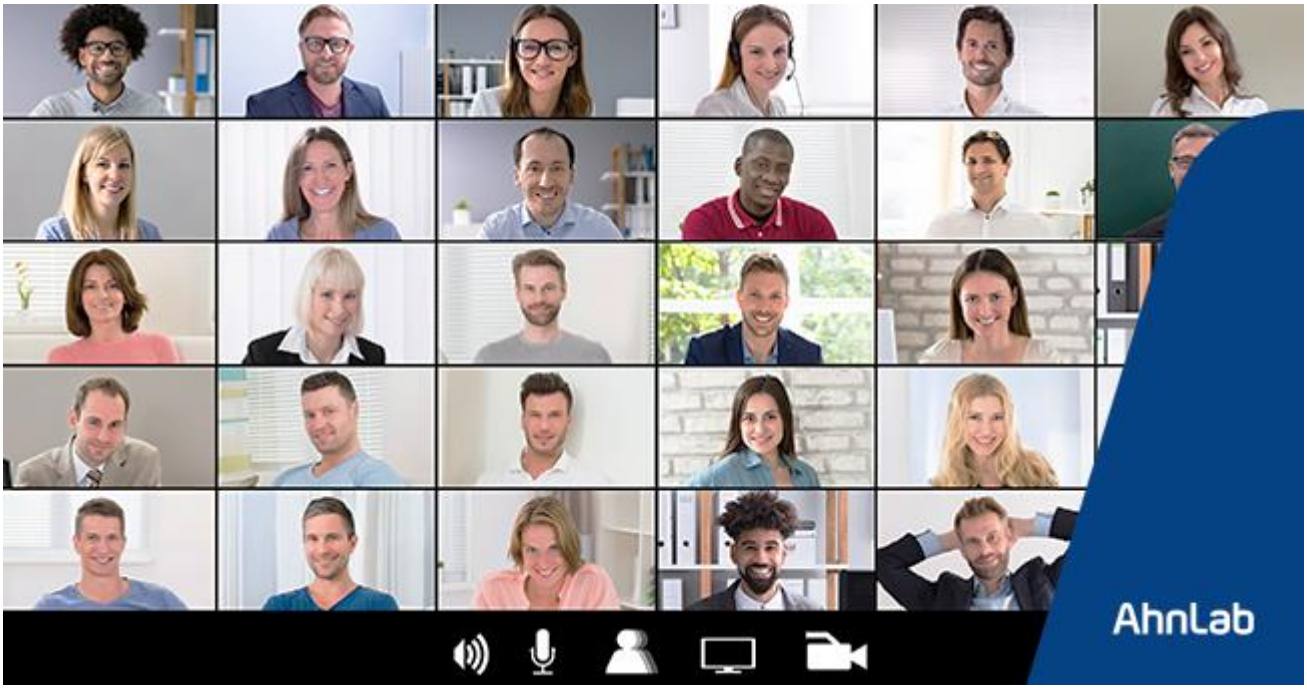
2019新型冠状病毒与安全

大流行后，

非接触时代的安全解决方案

远程办公、远程授课、远程研讨会……

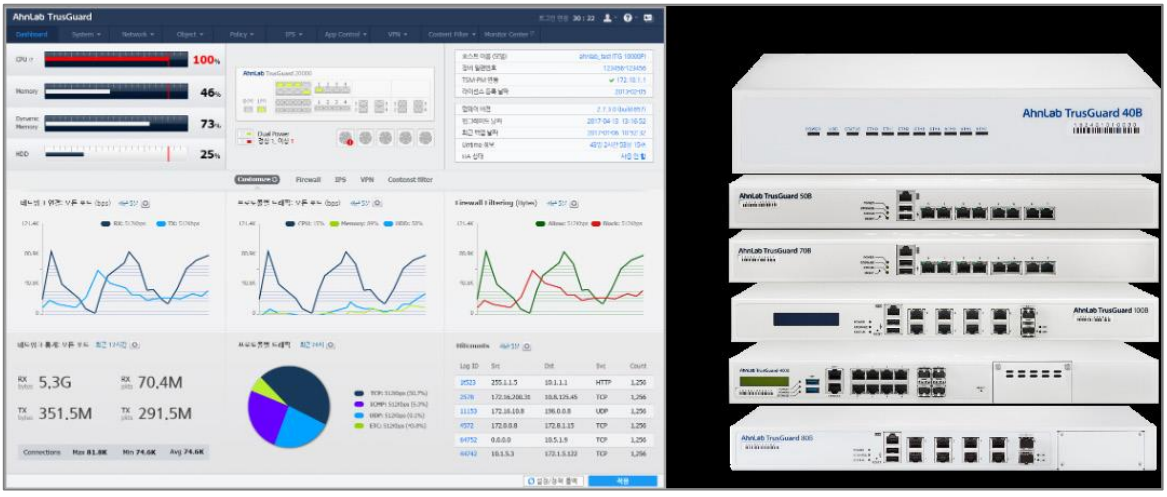
这种非面对面工作环境以前只有少数人在特殊情况下以辅助手段使用，但如今我们发现其实这种方式是可以在更多环境中使用。在 2019 新型冠状病毒肆虐的情况下，很多企业纷纷紧急引入了支持这种非面对面业务环境的各种解决方案和服务，以支持这种非面对面的工作环境来实现业务连续性。在此过程中，一些解决方案露出了安全漏洞，而针对这一漏洞的恶意攻击也有所增加。然而在全球大流行的情况下，不得不将业务连续性放在安全和治理之上。但是，安全确保业务生产效率和业务连续性的基本基础设施，而不受时间和场所的限制。在大流行后的时代，预计企业将加速云转型，以加速数字化转型和非面对面系统的扩展。此时，有必要纠正尚未应用的安全卫生（Security Hygiene）问题，并准备改善方案以提高安全性。在本文中，我们将介绍 AhnLab 有哪些安全解决方案可以在未来不断加速的非接触时代加强安全卫生。



非接触时代的网络安全

随着 2019 新型冠状病毒的长期化，越来越多的企业实施远程办公。随着这种趋势，虚拟专用网络（VPN）已成为必备的安全解决方案。由于 VPN 可以从外部访问企业的内部网或数据库，因此已构筑 VPN 的企业很容易转换为远程办公。

目前，AhnLab 在下一代防火墙 TrusGuard 中提供 VPN 功能。 在需要突然进行远程办公的情况下（例如 2019 新型冠状病毒），扩展现有 VPN 或新建 VPN 是最实用和现实的方案。通过使用 TrusGuard，在远程办公环境中，安全水平也可以达到企业内部网的水准。

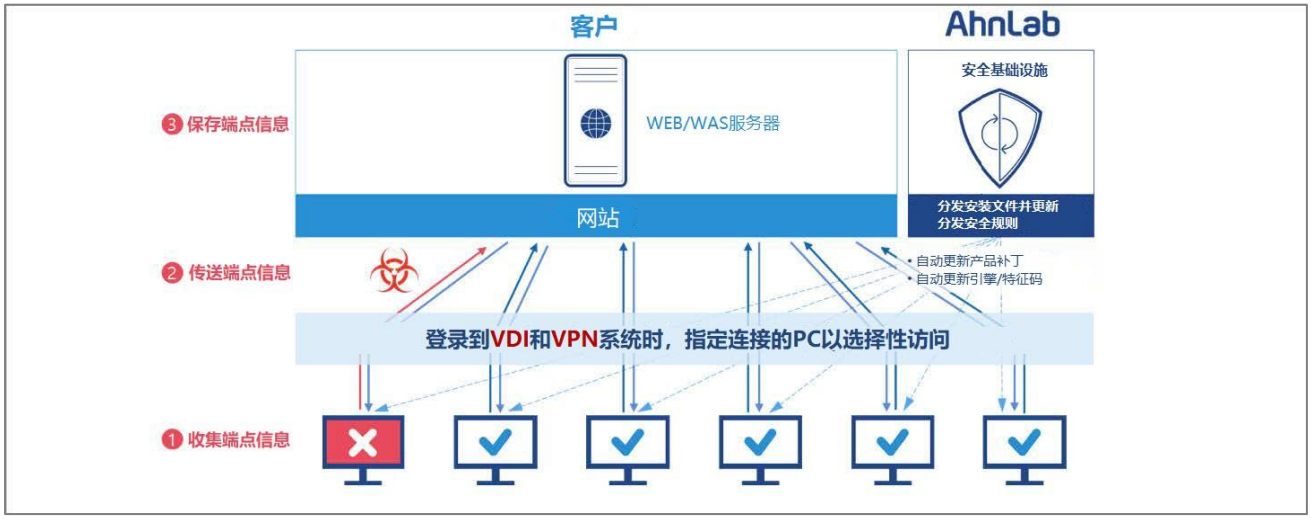


【图1】AhnLab TursGrad

AhnLab TrusGuard 是下一代网络集成安全系统，提供各种安全功能，例如防火墙、IPS、应用程序控制、VPN、防病毒/反垃圾邮件、C&C 检测和拦截 。尤其是，它搭载了应用程序控制，可对 P2P、网络硬盘、即时通讯工具、SNS 等数百种的应用程序数据提供实时分析和行为控制功能，而这些数据经常被利用于高级安全威胁（例如 APT）。

非接触时代的端点安全

虽然 SSL VPN 广泛用于远程办公，但是加密通信才是核心。外部终端、家用电脑等其他无法识别的终端可能容易受到攻击。



【图2】 AhnLab Safe Transaction端点信息收集功能

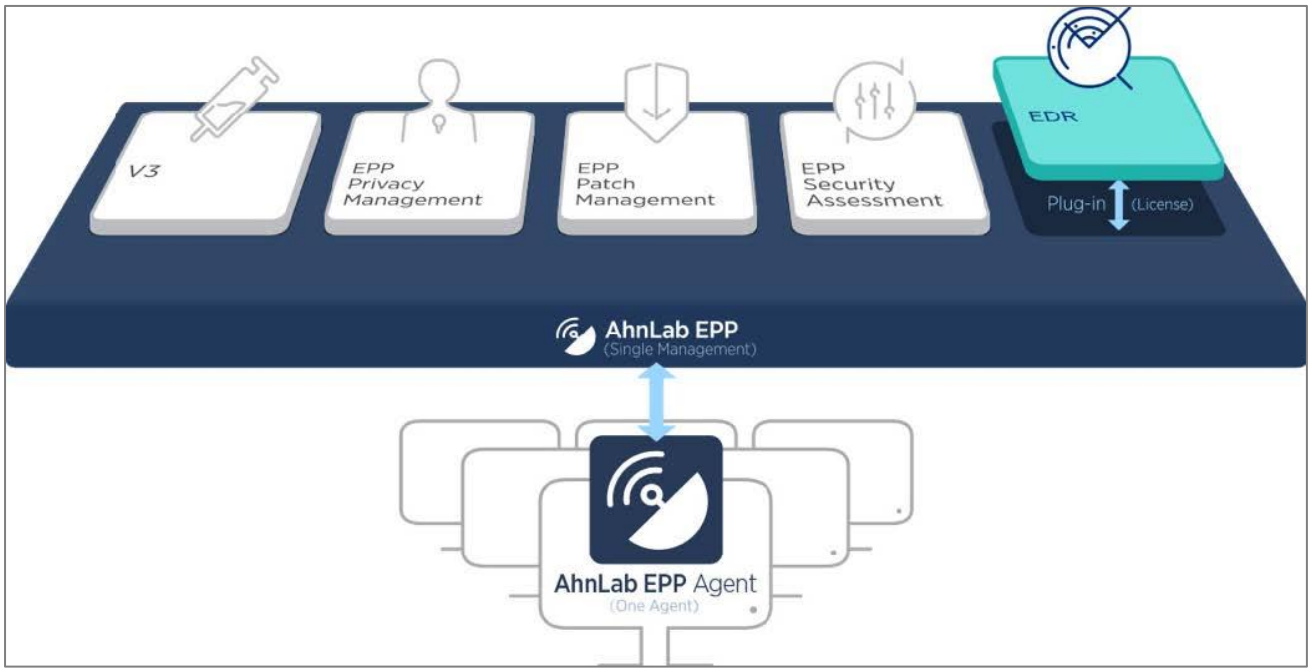
AhnLab Safe Transaction（ASTx）通过终端信息收集功能仅允许访问外部可识别的终端。这为使用 Web 服务时可能发生的各种威胁和黑客攻击因素提供了强大的安全功能。此外，通过加密保证收集到的信息的机密性和完整性。除此之外，通过键盘安全不仅可以防止泄漏和篡改用户的交易信息和个人信息等主要内容，并提供检测恶意代码、拦截网络、拦截漏洞、拦截网络钓鱼或域欺骗等综合安全功能。

如果企业正在对访问公司内部的外部终端加强安全而发愁，可以考虑引进 AhnLab MDS。

【图3】通过AhnLab MDS增强端点的安全

MDS Agent 安装在通过虚拟专用网络（Virtual Private Network, VPN）和虚拟桌面基础架构（Virtual Desktop Infrastructure, VDI）访问内部资产的外部终端上，以提供三个重要的终端安全功能。这三个功能分别是：▲通过实时监控终端 PC 来提前防止感染新种和变种恶意代码；▲搜索和收集疑似感染终端的隐藏的恶意代码；▲自动拦截通过操作系统和应用程序漏洞发生的恶意行为。

根据全球市场调查机构 IDC 的调查，70%的安全入侵事件发生在端点上，这突显了端点监控和安全的重要性。因此，端点安全平台（EPP）和端点威胁检测与响应解决方案（EDR）正在成为端点上的备选方案。



【图4】AhnLab EPP & AhnLab EDR 构筑概念图

下一代端点安全平台 AhnLab EPP，基于单一 Agent 和单一控制台，提供各种端点安全解决方案的有机链接。通过有机的端点安全管理和运营，提供强有力而有效的威胁响应。另外，端点威胁检测和响应解决方案 AhnLab EDR，通过对端点区域的持续监控提供威胁可见性，从而提前预防潜在威胁，并通过与各种安全解决方案的有机链接来实现更强大的安全。

当企业内的电脑感染了恶意代码，可能会通过网络将其传播给整个公司，从而造成巨大的破坏，例如网络瘫痪和主要信息泄露。为了最大程度地减少企业有形和无形资产的损失，使用企业版综合电脑安全解决方案 AhnLab V3 Internet Security 9.0 是理想的解决方案。V3 IS 9.0 保护企业用户的系统安全，使计算环境能够安全地使用客户端电脑，并保护企业的信息资产。

POS/自助服务机等非面对面系统的安全

全球大流行之后，使用 POS 设备或自助服务机下单和付款与日俱增，无人值守和自动化的扩散已成为了不可阻挡的趋势。然而，在非面对面系统中，通过勒索软件从 POS 设备或自助服务机窃取信用卡信息的攻击也很常见。在暗网（Dark Web）上交易的信用卡信息包括银行识别号、有效期和信用卡认证号等，经常通过 POS 设备、自助服务机或 ATM 机之类的支付系统的安全漏洞泄露。这是因为 POS 设备或自助服务机通常采用与现有电脑环境此案共同的安全系统，尽管它们在与典型电脑完全不同的运营环境中运行，因此很容易受到高级威胁的攻击。

【图5】通过AhnLab EPS增强自动服务系统的安全

AhnLab EPS 是一种超轻型安全解决方案，优化于工控系统和 POS 机、自助服务机、重要服务器等专用系统。基于 AhnLab 独有的白名单和恶意代码拦截技术，通过仅允许运行系统所需的程序和网络连接，拦截不必要的程序或非业务程序的运行，从而防止恶意代码入侵和利用恶意代码的信息泄露。

目前，该产品已在大型超市、百货、咖啡馆等大型流通企业的结算系统，以及铁路、机场、公交车站的交通流量显示屏等自助服务终端上使用，并得到了验证。

无接触时代的安全管制服务

当企业在推广远程办公解决方案时会考虑使用 SSL VPN，但是紧急构建的远程办公系统反而更有可能成为黑客的攻击对象。另外，即使通过引入 SSL VPN 来构建远程办公系统，也必须监视 24 小时以查看是否发生了异常事件，而且对日志文件管理和应用程序更新等管理和维护至关重要。由于没有足够的人力来构建和管理安全基础设施而犹豫进行远程办公的企业，值得考虑引入安全管制服务，该服务提供安全咨询、24 小时监控、技术支持服务。

AhnLab 的远程安全管制服务提供 24 小时监控、策略设置、入侵尝试检测、分析和响应等必须在企业中持续执行的一系列安全系统运营。作为基本提供防火墙、IDS/IPS、UTM、WAF 管制服务和 DDoS 防御服务，另外提供反垃圾邮件、信息安全、漏洞管理、系统强化、入侵事件分析、模拟黑客服务等。

尤其是，AhnLab 通过与 AWS、Azure、IBM 云等主要云服务供应商的合作关系提供云安全管制服务，并已确保了各个行业的云安全管制客户，其稳定的运营能力得到了认可。另外，AhnLab 将为本地（On-premise）环境提供的信息保护咨询服务以最优化的方式提供给云端环境，还提供为遵守云服务安全认证等规定的咨询服务。

远程或在家办公时应遵守的安全守则

受 2019 新型冠状病毒的影响，远程或在家办公的企业在不断增加。以此为契机，人们越来越期待远程或在家办公能够被更广泛利用，因此，为了成功开展远程或在家办公，有必要制定出针对性的信息保护方案。以下是韩国科学技术信息通信部发布的《2019 远程办公时应遵守的六大信息保护守则》。

用户守则	安全管理员守则
1.个人电脑保持最新安全更新 -在家中使用个人PC工作时，请保持操作系统和应用程序为最新	**1.建议使用远程工作系统（VPN）** -建议根据公司的安全策略使用VPN -对于没有VPN的公司，建议保持访问内部网络的PC的防病毒软件为最新版本并执行强制检查
2.防病毒程序的更新和检查 -防病毒程序的安全补丁程序的最新更新和定期病毒扫描（在远程访问之前和之后，每天执行一次或多次） -禁用防病毒自动更新设置和实时扫描功能	**2.制定安全准则并提高远程办公者的安全意识** -提供安全准则和进行安全教育，使远程办公者使用的PC的操作系统、软件和防病毒程序更新为最新版本，路由器要设置密码，最好不要访问网站
3.家用路由器的安全设置（密码），避免使用私有Wi-Fi / 公用PC -将您的家庭互联网路由器更新为最新的软件并设置路由器密码 ※ 密码包括特殊字符 -不要在咖啡厅和餐厅等使用私人Wi-Fi /公用PC进行远程办公	**3.管理远程办公者的用户帐户和访问权限** -强化远程办公者的密码设置，并建立方案限制远程办公时访问权限 -访问远程工作系统时，除了密码以外，还必须应用OTP等辅助身份验证方法
4.建议使用公司电子邮件，使用个人邮件时要注意 -建议使用公司提供的电子邮件服务 -使用商用电子邮件服务时，不要打开来源不明的邮件的附件并不要点击邮件内容中的链接 ※在公用 PC 上阅读邮件后，必须终止连接。	**4.闲置一段时间时断开网络** -当远程办公者连接公司网络后闲置一段时间时，网络连接将被断开 ※建议闲置时间设置为10到30分钟
5.避免使用不必要的网站 -除了出于商业目的使用网站以外，请勿出于个人目的访问网站	**5.强化远程访问的监视** -监控远程办公者的访问公司内部网络情况，集中远程办公者的旁路访问网络状态
6.文件下载时要注意 （注意勒索软件感染） -通过邮件或Web浏览器下载文件时，可能会感染勒索软件。因此，禁止下载来源可疑的文件。 -定期将工作文件备份到另外的存储设备	**6.个人信息和公司信息等数据安全** （注意勒索软件感染） -建立数据泄漏防止措施，例如重要文档的DRM设置 ※如果发生数据泄漏，管理员的批准程序等 -当远程办公者引入工作文件到内部时，必须对文件进行扫描。 -建议备份重要的数据

【表1】2019远程办公时应遵守的六大信息保护守则

该安全守则包含了目前韩国一般企业环境下必须遵守的基本内容，各企业应该重新检查一下是否具备对此提供支持的安全解决方案。同时，随着企业的数字化转型，需要树立为引入“SASE（Secure Access Service Edge，安全访问服务边缘）”、“CARTA（Continuous Adaptive Risk & Trust Assessment，持续自适应风险与信任评估）”等解决方案框架的相关战略。

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