AhnLab

安全月刊

2017.05 Vol. 54

AhnLab SECURITY LADDERS

AhnLab发表“SECURITY LADDERS”战略

端点安全为何需要创新？

在“数字化转型（Digital Transformation）的时代，网络安全应该如何变化？

这是目前很多公司正苦恼的一部分。因为几乎所有的公司和组织的业务都基于IT。事实上，网络攻击或安全威胁并不是今天和昨天才有的事情。从1986年世界上首个计算机病毒-布雷恩病毒（Brian Virus）出现到2017年当前给个人和企业造成严重损失的勒索软件（Ransomware）的暴增，我们不断面临着各种安全威胁。但是，即使安全威胁一直都存在，它们并不总是以相同的形式存在。此外，在数字化转型的时代，诸如云、物联网（IoT）、人工智能（AI）和机器学习（Machine Learning）等新技术在各个领域得到扩展和发展，为了安全的业务运营，我们该如何做好准备？

为了寻找对这个问题的解决方案，剖析一下数字转型时代的安全范式，并讲述为什么AhnLab强调端点安全平台。

IT技术正在以比我们预期更快的速度来实现着我们曾经想象的东西。一个典型的例子就是智能手机。第一款iPhone发布于2007年。之后，不过几年的时间，智能手机对全世界人们的日常生活到主要工业景观，都带来了革命性的变化。另外，被贴在“手机”的修饰语“智能”，已经扩展到“智能家居”、“智能工厂”和“智能电网”。包括智能时代、数字化转型、数字业务和第四次工业革命等穿透当前潮流的大话题的核心将物理世界与创新的IT技术融为一体，创造出新的价值。这些变化导致了我们过去没有想过的各种产品的出现，并需要比以往任何时候更多的连接（Connectivity）。事物和人、事物和事物、事物和技术等各种连接不可避免地会面临安全威胁。

	Gartner Security Summit	RSA Conference
2014	Security Intelligence	Share, Learn, Secure Capitalizing on collective intelligence Digital Business
2015	Threat Intelligence Alliance & Share	CHANGE: Challenge today's security thinking Digital Transformation
2016	Automation, Visibility	Connect to Protect The Speed of Digital Transformation
2017	Business Driven Security	Power of Opportunity

【图 1】 网络安全关键词的变化

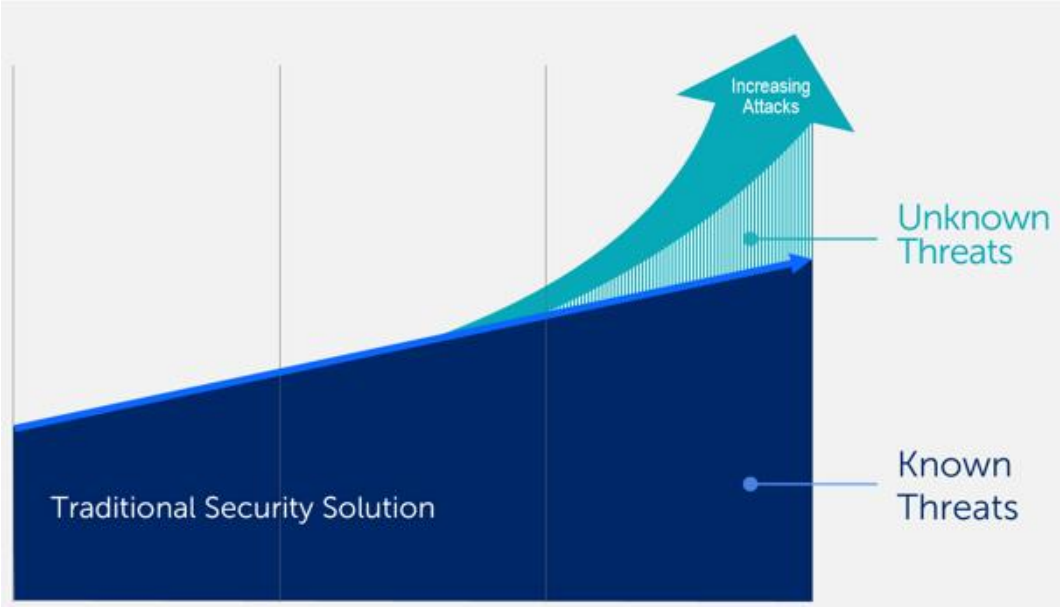
变化、创新和转型

IT（Information Technology，信息技术）或ICT（Information & Communication Technology，信息和通信技术）带来的环境变化也对安全威胁带来了变化。应对不断变化的威胁的安全技术也必然会需要变化。网络安全行业已经在几年前就对这种必然的变化开始意识。

那么什么是变化？人文学或词典上的“变化（Change）”意味着“事物的性质、形状和状态发生变化”。然而，从业务角度的“变化”与实现或发展面向目标部分的一般的概念相冲突。许多研究机构已经开始使用“转型（Transformation）”一词。“trans-”的词源是拉丁语，意思是“跨（across）”，包含着方向性。转型意味着“变化到更好的方向或状态”。在某些情况下，“Change”被解释为“简单的变化”，“Transformation”被解释为“变革”，意味着变化与创新 。

未知的威胁，只是我们看不到而已

传统的安全供应商都有一个对已知（Known）威胁迅速响应和服务的结构。AhnLab也是如此。



【图 2】 需要观点变化的理由

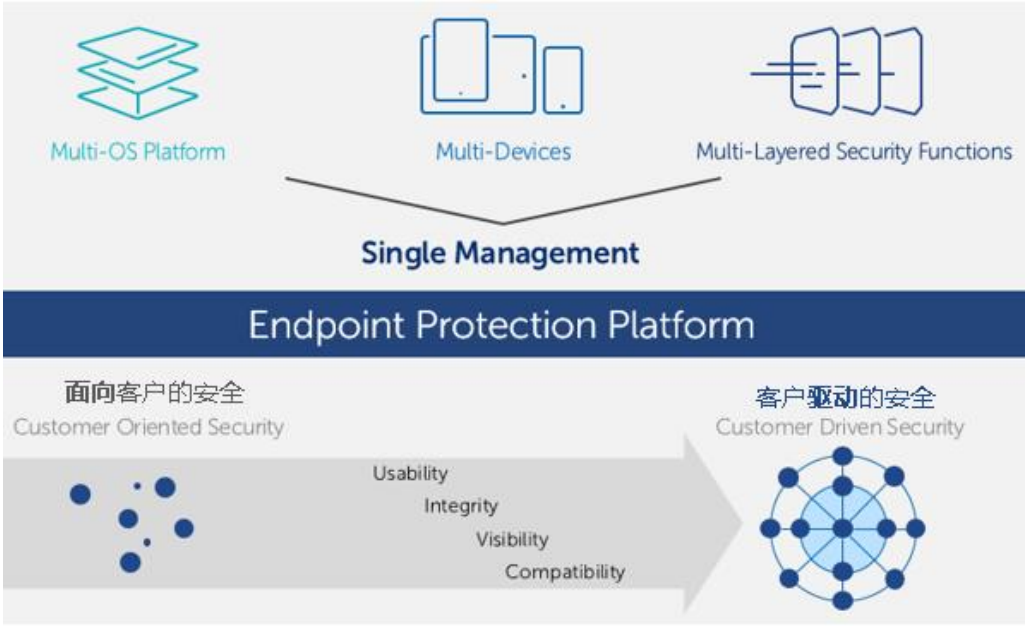
但从几年前，安全厂商开始关注未知（Unknown）的威胁。从安全角度来看，“Unknown”即是一个未知的威胁。有些人说，由于1%的未知威胁，才处于危险之中。但是，如果我们将这个“未知”已具体说道1%，那么我们还可以说我们不知道这个“未知”吗？ 此外，当分析实际发生安全入侵事故时利用的攻击方法和恶意代码，结果，大多数情况下利用了大部分已知的攻击方法和恶意代码。这还可以说是不知道的、未知的威胁吗？ 最后，网络安全中提及的“未知”威胁应该理解为“看不见”的威胁。换句话说，这是一个已知的安全威胁，但并没有显露出来，而看不到和感觉不到而已。

安全观点的变化和平台安全战略

为了应对数字化转型时代不断变化的安全威胁，需要从接近安全的观点开始创新。AhnLab为这个“创新”，专注于提供一种使“看不见”的可以“看见”的解决方案（Resolution）。

安全威胁和响应通常比喻成“攻击和防御”。传统的防御观点是围绕要保护的对象（信息，系统等）寻找“潜在的漏洞”，并提供适当的对策（安全解决方案）。然而，攻击者使用各种手段来整体地探索攻击目标，并找到他们可以渗透的所有路径。因此，安全需要了解“攻击与防御”之间的观点差异，并改变范式本身，以最大限度地减少这种差异导致的危险因素。从总体防御的观点，通过“检测（Detection）-分析（Analysis）-响应（Response）”的循环结构来应对这一问题，从而可以通过“阻止”来防御威胁，还可以实现检测和快速响应。

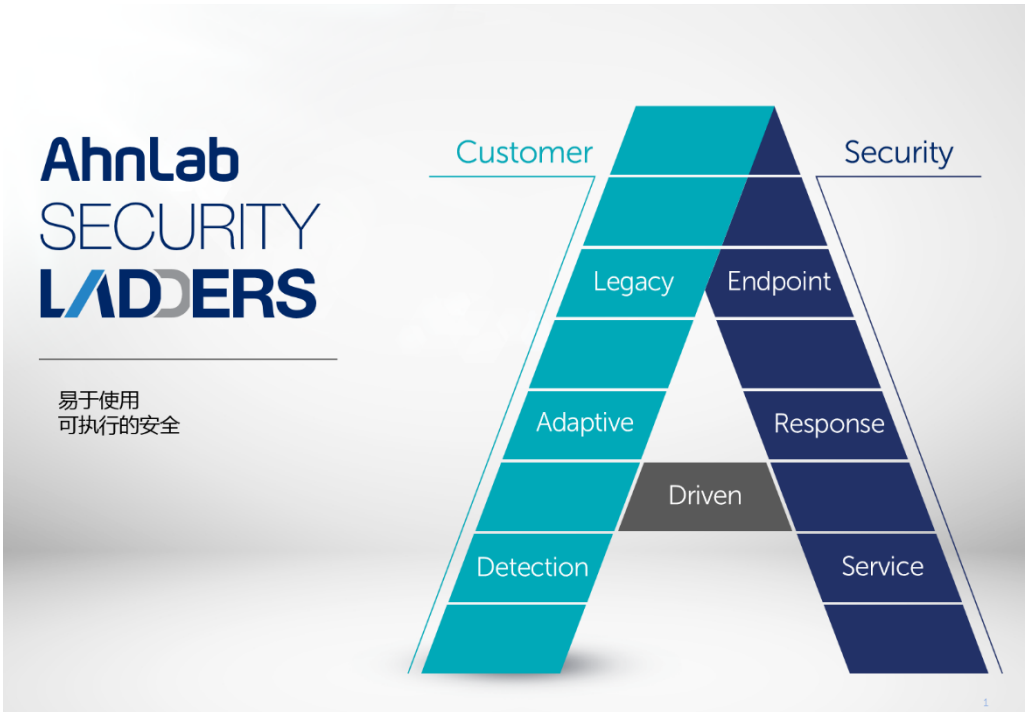
也应该伴随着对端点环境的理解，这个环境已经变得非常错综复杂，不能与过去相比较。今天，端点环境与各种操作系统（OS）以及以不同语言（language）设计或提供的各种设备（device）共存。这也在说明存在着多样且看不见的威胁因素。这就是为什么端点是下一代安全核心的理由。在将来，端点安全必须支持各种操作系统、设备和语言，以及在单个系统中可以管理和监控这些。进而需要“端点保护平台（Endpoint Protection Platform, EPP）”来统一管理和响应在各种环境和层中实现的端点的安全。



【图 3】AhnLab端点安全平台

AhnLab端点安全平台战略， SECURITY LADDERS

当前，安全已进入平台时代。客户和安全厂商为实现EPP而一起苦恼，并在此过程中寻找什么是客户实际需要的，以及他们现在可以做的是什么，这是下一代安全的起点，也是解决安全威胁最重要的一步。这就是为什么AhnLab强调客户驱动安全（Customer-driven Security）的理由，为实现这一点，AhnLabb提出了“AhnLab SECURITY LADDERS” 。

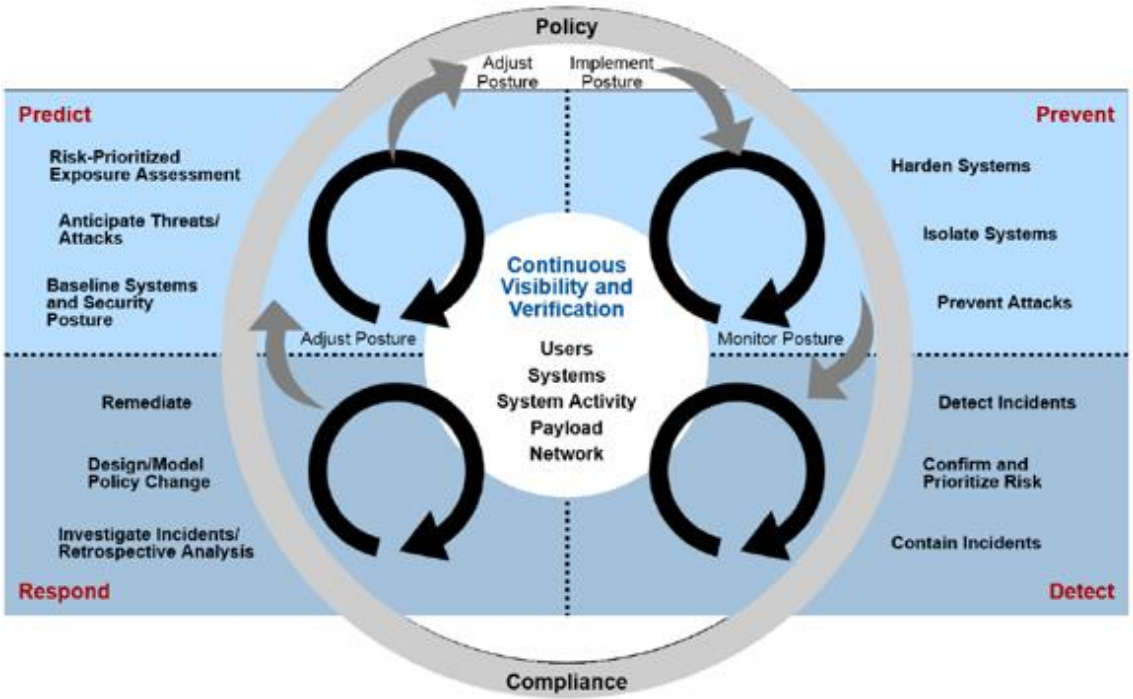


【图 4】AhnLab端点安全平台战略“SECURITY LADDERS”

英文单词“LADDERS”的词典含义是“梯子”。众所周知，梯子是爬上高处时使用的工具。在火灾等危险情况下为抢救人员起着非常重要的作用。AhnLab所说的梯子，LADDERS的作用也与此相同。LADDERS所包含的意思是Legacy、Adaptive、Detection、Driven、Endpoint、Response和Service，蕴含着客户驱动的安全战略。它是一个可以实现安全业务环境的工具，象征着“易于使用的安全，可执行的安全”。每个关键词的详细含义如下。

Legacy：Legacy的词典含义是“遗产”，但在计算机行业中的含义是“使用时间过长而难以维护的”，被用于过去的技术或旧系统。然而，AhnLab认为这种Legacy是“当前”客户在内部运营的基础架构，例如“应用程序（Application）”，“中间件（Middleware）”和“平台（Platform）”。需要准确了解客户的实际环境和基础设施，才可以通过技术、解决方案和流程检测、分析和响应安全威胁。因此，Legacy作为AhnLaLADDERS的第一步，起着垫脚石的作用。

Adaptive：为保护客户的业务安全，需要各种安全解决方案。但是，由于成本和管理方面的原因，实际上无法引进所有的安全解决方案。面对这种现实，AhnLab建议将“自适应（Adaptive）”安全框架作为在客户引进安全解决方案时判断适用性和有效性的指南。自适应安全是由预防、检测、响应和预测四个阶段组成的安全框架。它建议考虑客户的实际和危险的优先级和未来的发展蓝图。



【图 5】自适应安全框架（Adaptive Security Architecture）

Detection：基于自适应安全的基准，“Detection”也有必要改变原有方式。除了传统的通过阻止的防御（Prevention），还要着重于检测和响应（Response）信息的量和速度。最近，由于可穿戴设备（Wearable Devices）等物联网（IoT）技术正在变得越来越商业化，除了传统的标准数据之外，非标准数据的安全威胁也越来越成为了现实。最终，检测将成为决定响应威胁的优先级的范式转变的基础。

Driven：AhnLab曾在2014年的AhnLab综合安全展览会（AhnLab Integrated Security Fair，AISF）上提出安全厂商面向客户情报的“客户驱动的安全（Customer-driven Security）。这不是以安全提供商基准的面向客户，而是要提供客户希望并实际可适用的安全。AhnLab的这一基本理念将在2017年持续下去。

Endpoint：端点是安全的起点，是在安全方面创建所有信息并移动的起始点，也是接近网络的关口。传统上，端点是指终端用户访问企业网络的地点，即如PC，笔记本电脑和智能手机等终端用户的设备。但现在，它已不再是简单的设备的概念，包含了各种操作系统（OS）、虚拟化、IoT、云、大数据和分析等，已经变成巨大的端点。而且，这些端点必须能够在一个系统上统一管理。

Response：在端点安全平台中，应通过考虑检测和及时响应来实现每个安全解决方案和功能之间的有机联系。为了使每个解决方案和功能在平台上有机地工作，流程需要顺畅。AhnLab将其定义为“响应（Response）”。AhnLab提供各种端点安全

解决方案，如PC安全解决方案-V3为首的各种PC安全解决方案，如AhnLab补丁管理（AhnLab Patch Management）、漏洞管理和解决方案（AhnLab MY PC Inspection）和AhnLab隐私管理套件（AhnLab Privacy Management Suite）等。这些产品通过被称为EMS的单一管理解决方案统一管理。在提升端点安全的角度来看，AhnLab集成了APT响应解决方案-AhnLab MDS，端点检测和响应（Endpoint Detection and Response，EDR）和机器学习(Machine Learning)技术，进行着连接AhnLab威胁情报（Threat Intelligence）的工作。为了在将来实施有效的应对，AhnLab计划发展为不仅是一个特定的起始点，而且还要看到整个流程的平台，即起始点和流程结合的平台。

Service：最后是服务。在这里指的服务意味着优化和升级现有产品和解决方案的服务，而不是传统的简单维护。AhnLab力求通过优化客户所拥有的解决方案并附加服务来最小化端点攻击面（EPP Hardening）。作为其第一步，最近新设了一个AhnLab专业服务。该服务包括7个方面，▲ 安全解决方案优化服务 ▲ 专家随选服务 ▲ 安全审核预检服务 ▲ 可疑系统诊断服务 ▲ 恶意代码专家分析服务 ▲ A-FIRST取证服务 ▲ 信息安全教育。

目的在于全球水平的易于使用的安全和可实现的安全

全球研究公司Gartner将端点安全平台（EPP）定义为在端点级（如工作站，智能手机和平板电脑）提供安全的解决方案。此外，EPP的组件包括防恶意软件（Anti-Malware）、个人防火墙、端口和设备控制（Port and device control）、漏洞评估（Vulnerability Assessment）、应用程序控制（Application Control）等。要包括应用程序沙箱（Application Sandboxing），企业移动管理（Enterprise Mobile Management, EMM），内存保护（Memory Protection），EDR，数据保护（Data Protection）和数据丢失防护（Data Loss Prevention, DLP）等技术，还需要云计算、APT响应、机器学习、威胁情报和人工智能（AI）等技术。

Gartner每年根据这些基准来评估EPP解决方案提供商，并发布在EPP魔力象限（Magic Quadrant for EPP），而AhnLab是刊登在EPP魔力象限的今年唯一的韩国安全供应商 。这表明，AhnLab的技术不仅已跟上全球水平，而且AhnLab所追求的“安全梯子（SECURITY LADDERS）”战略已经为迅速变化的IT环境做好了准备。通过与客户的沟通，AhnLab将继续致力于实现数字化转型时代顾客忧虑和需求优化的易于使用和可执行的安全。

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