AhnLab

安全月刊

2022.08 Vol.117

如何构建云安全

构建云安全，从哪里开始

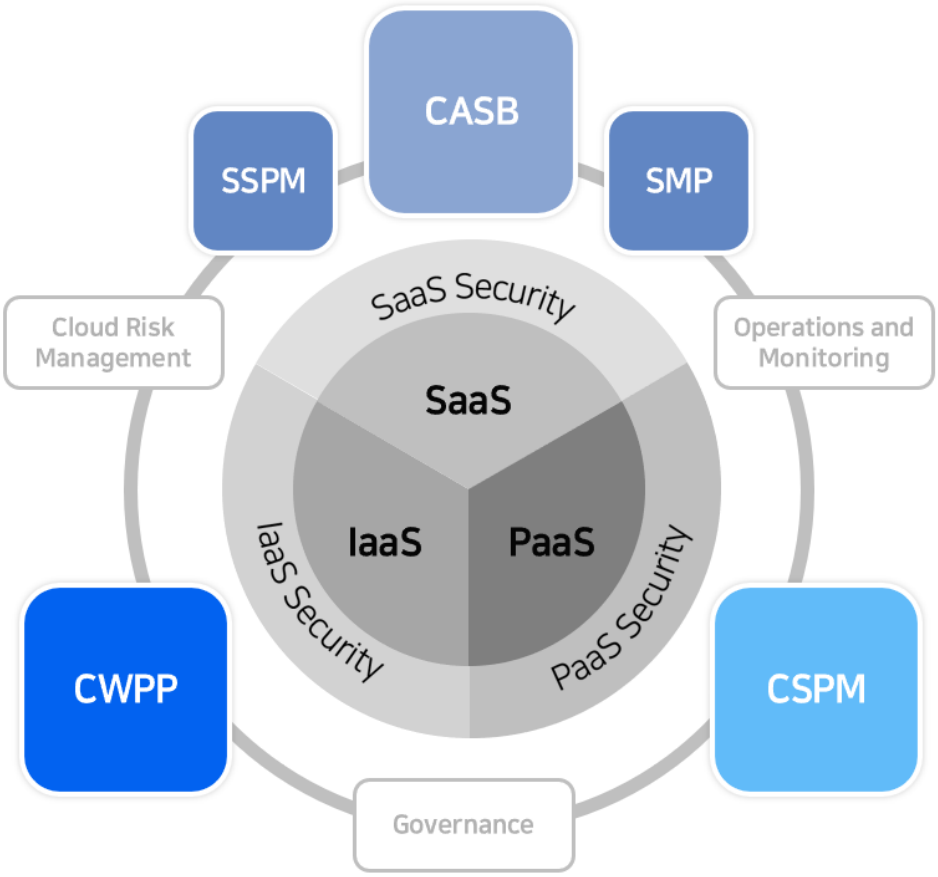
对于AhnLab安全月刊的读者来说，云安全这一概念不会感到陌生。然而，有些读者会意识到，对云安全了解得越多，就越感到比想象的要复杂。如果您正在面对像云安全这样困难但必须完成的任务，需要一种方法来设置优先级并应用可以先做的事情。

在本文中，我们将介绍云和本地部署之间的区别，然后介绍构建云安全应该从哪里开始。

构建云安全并非易事。这主要是因为构成的要素繁多且需要保护的对象并非固定。为了正确了解云安全，首先需要了解本地和云的本质区别。这里的了解指的不仅是本地和云的结构，还包括现有安全防护中被分离的端点和网络的相互理解。

云安全的组成

首先，让我们来看一下云安全的基本组成。根据全球市场调查机构Gartner发布的云安全模型及各安全工具的作用，总结如下。



【图1】云安全工具应用范围（来源：Gartner）

云安全工具正式名称及其作用

▲CWPP：Cloud Workload Protection Platform（云工作负载安全平台）

▲CSPM：Cloud Security Posture Management（云安全态势管理）

▲CASB：Cloud Access Security Broker（云访问安全代理）

▲SMP：SaaS Management Platform（SaaS管理平台）

▲SSPM：SaaS Security Posture Management（SaaS安全态势管理）

安全工具	作用	保护领域
CWPP	云工作负载保护	IaaS & PaaS
CSPM	防止IaaS和PaaS中错误的安全配置	IaaS & PaaS
CASB	控制访问云资源并应用安全策略	SaaS
SMP	在单一平台管理多个SaaS工具	SaaS
SSPM	SaaS应用程序安全态势管理及其风险评估	SaaS

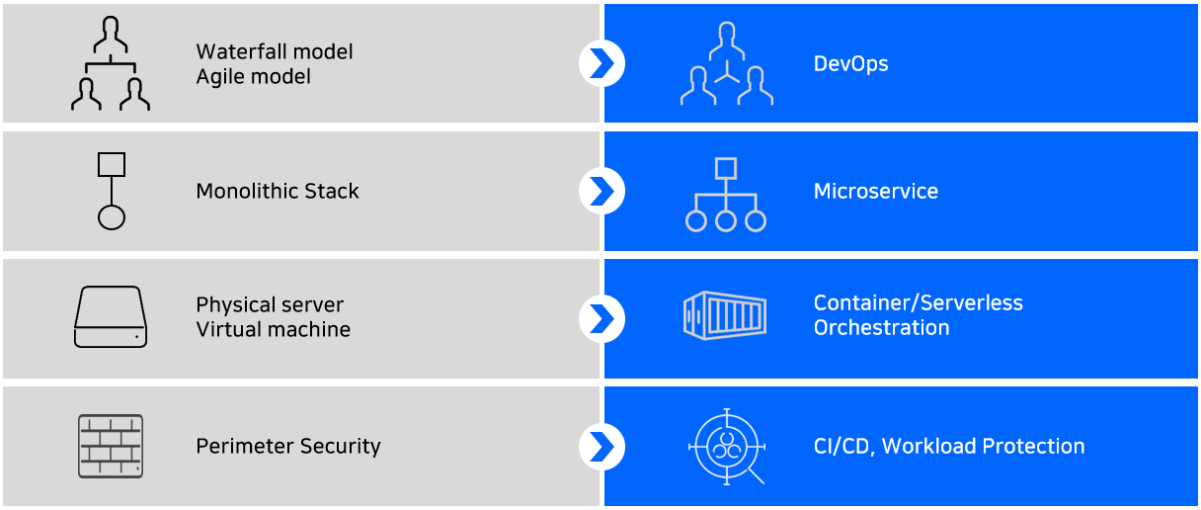
【表1】云安全工具的作用及保护领域

上面的云安全模型是最基本的，实际的云安全分类更加细化。保护IaaS和PaaS的CWPP和CSPM在细分领域时保护点略有不同。因此，可以理解为【图1】和【表1】是在宏观框架下对云安全组成的定义。

重要的是，云安全无法用一个解决方案完全覆盖一个领域。此外，随着云原生服务的生命周期越来越短，还需要快速地响应变化。因此，各解决方案都在朝向构建互补体系的方向进行重组。

本地部署和云：概念上的差异

如果您理解了云安全组成的概念，就会知道它与传统的本地部署安全存在本质上的不同。下面，让我们从概念的角度来看看这两个体系之间的差异。



【图2】“本地部署”和“云”概念上的差异

从开发流程来看，传统的本地环境一般都采用了围绕特定计划分阶段进行的“瀑布（Waterfall）”方式。之后，通过定期不断开发后转换为敏捷（Agile）方式，可以灵活响应变化。随着过渡到云环境，对迅速性和可扩展性的要求不断增加，从开发到分发和运营的集成方法论“DevOps”开始受到瞩目。

对于架构，在本地使用了在一个空间中密集连接组件（Component）和数据的“一体化架构（Monolithic Architecture）”。一体化架构虽然相对简单，但细微的改动都将影响到整个应用程序，导致无法灵活地响应变化。在云环境中，它已更改为将组件细分，并通过API将每个组件连接的“微服务架构（Microservice Architecture：MSA）”。

这些差异也带来了运营环境的变化。传统的本地部署环境中使用了物理服务器和虚拟化技术，而在云中，需要一个运行组件的小规模环境以适应微服务架构。这将导致容器、无服务器和编排的需求增加。

总而言之，云、DevOps和微服务架构的核心是对应用程序开发和运营的迅速性，以及对变化的及时响应。在最近的IT环境中，对这一概念的需求正在增加，越来越多的企业正在从本地迁移到云。

本地部署和云：迁移（Migration）

当使用本地部署的企业采用云时，需要执行各种操作以进行“迁移（Migration）”。根据要迁移的组件在云环境的优化程度，云迁移大致分为四个阶段。

云迁移的四个阶段

▲第1阶段：Rehost - Lift and Shift

▲第2阶段：Replatform - 基于云环境迁移开发逻辑

▲第3阶段：Refactor - 基于云模型更改代码

▲第4阶段：Rewrite - 用云原生（Cloud Native）重新设计

在韩国，有很多企业使用“Lift and Shift”的方式构建云环境以快速转型。当然，新创建的服务并非如此，但大部分的服务器应用程序都是以“Lift and Shift”方式进行迁移。

“Lift and Shift”方式在从本地服务器迁移到虚拟服务器时没有任何严重问题。但是，在对于现有环境完全改变的网络或云基础设施服务，可能会导致运营出现差错。安全也是如此。如果将本地的安全逻辑原封不动地迁移到云中，从长远来看，很可能难以配置。

为了顺畅地运营云并享受最大的收益，需要根据云环境来设计架构的云原生迁移。当然，与Lift and Shift相比，需要更多的时间和费用，但考虑到长期的业务生产力和可持续性，可以说云原生是正确的选择。

云安全与本地部署有何不同?

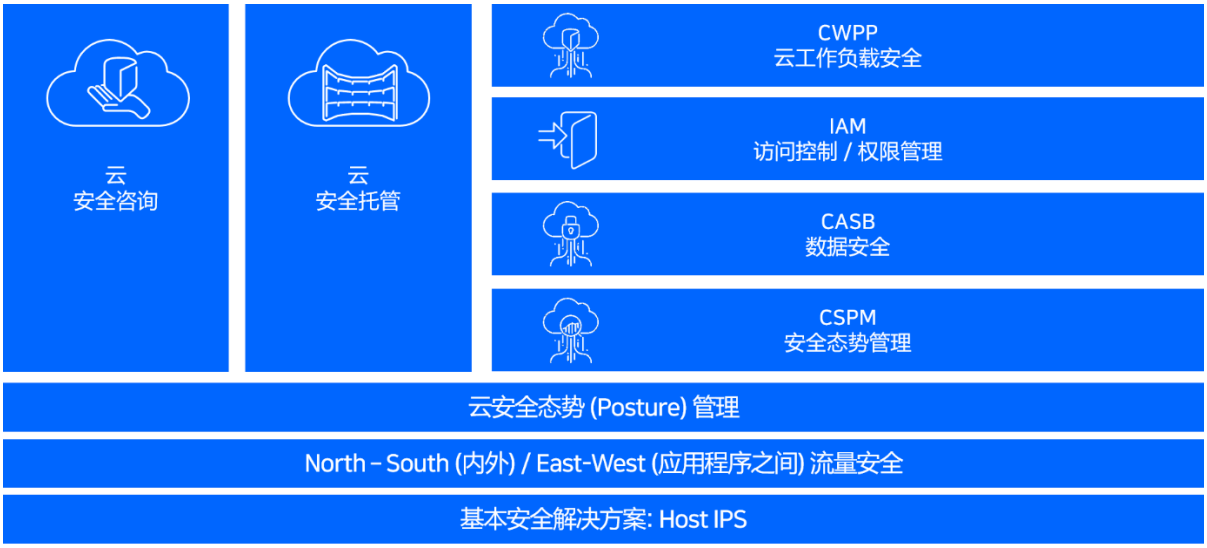
如上所述，与本地存在结构差异的云，在安全方面也有不同的组成。

如果首先查看本地部署安全框架，会发现安全是围绕“边界（Perimeter）”运行的。如果将边界视为内部和外部或端点和网络之间的边界，则很容易理解。本地部署的边界安全要求定义保护对象和资源。它以严格控制对已定义资源的外部访问和加强内部重要资源或与外部连接的资源的安全的形式进行。例如，通过网络安全应用强大的访问控制和威胁拦截，以及控制对系统的访问。

【图3】本地安全框架

本地部署安全管理和应用基于策略（Policy），基本的安全解决方案当属反恶意软件（Anti-Malware）。可以理解为安装防病毒软件后基于策略连接端点安全平台的组件。

然而，在云安全框架中，安全以“工作负载（Workload）”为中心运，这是因为共享资源的云的特性使边界不明确。工作负载是指创造业务价值的资源的集合，例如操作系统和应用程序。可以说，为构建坚固的云安全系统，作为在云环境中运营的资源的工作负载的集成安全，比保护边界更有效。



【图4】云安全框架

与本地部署不同，在云安全中安全态势管理（Posture）尤为重要。安全态势管理是指正确设置云组件。例如，管理配置错误的网络连接或设置为过于容易访问的帐户。根据Gartner的调查，云安全事故中约80%是由配置错误而引起的。因此，可以说安全态势管理是构建云安全环境的核心。

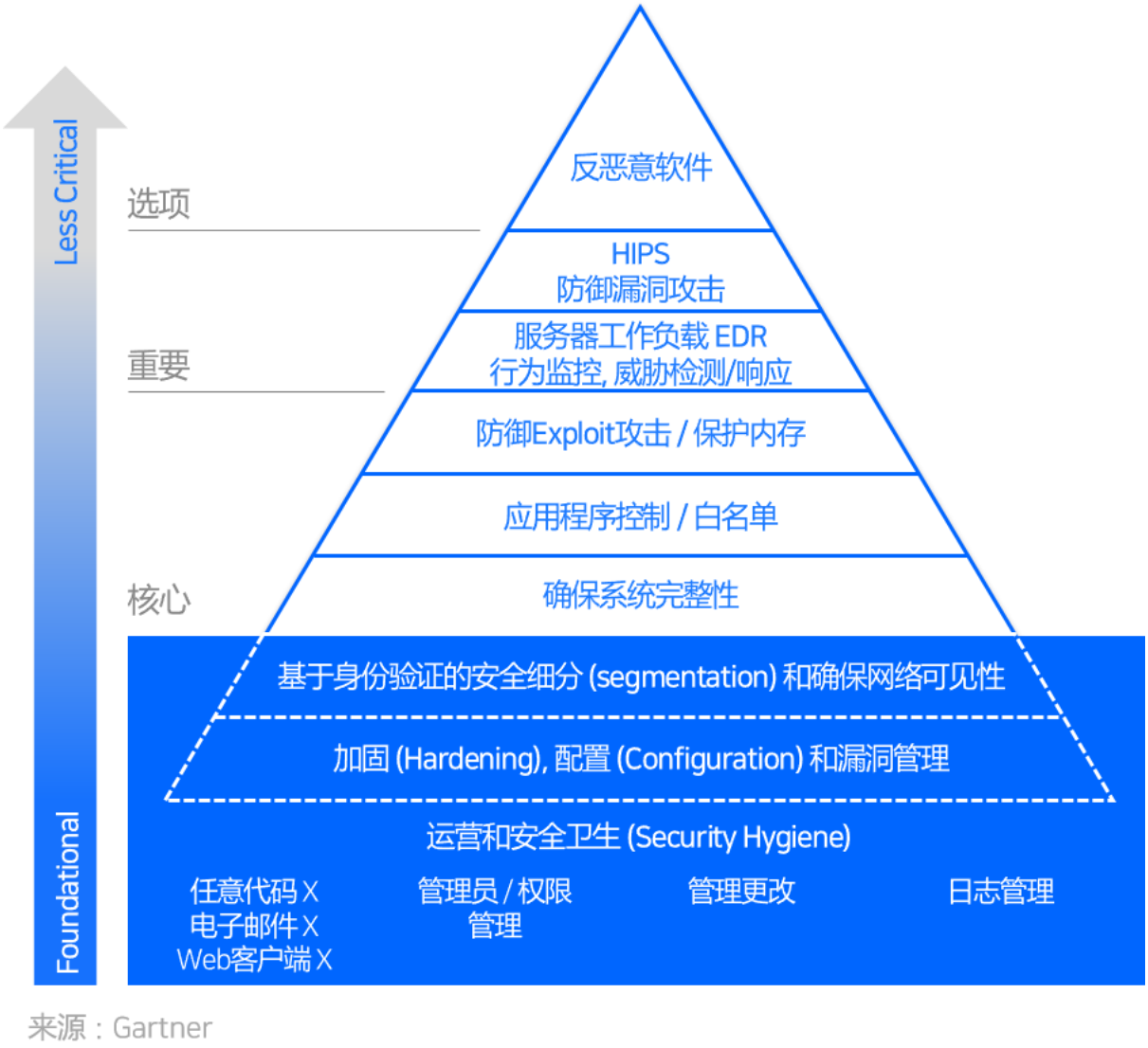
从解决方案的方面来看，与本地部署的反恶意软件不同，在云环境中，主机IPS是基本的解决方案。虽然拦截和修复恶意代码的反恶意软件在云环境中也是一个重要的安全要素，但采用与边界安全不同的方法的云环境中，反恶意软件对安全的重要性不如本地部署安全。

主机IPS在云环境中成为基本的原因在于不仅要保护内部和外部通信（North-South），还要保护服务器到服务器和应用程序到应用程序的通信（East-West）流量。尤其是在云环境中East-West流量频繁发生，攻击者也利用它将破坏扩散到内部，因此需要通过主机IPS来管理流量和漏洞，并拦截威胁。

云安全，从 CWPP 和主机 IPS 开始

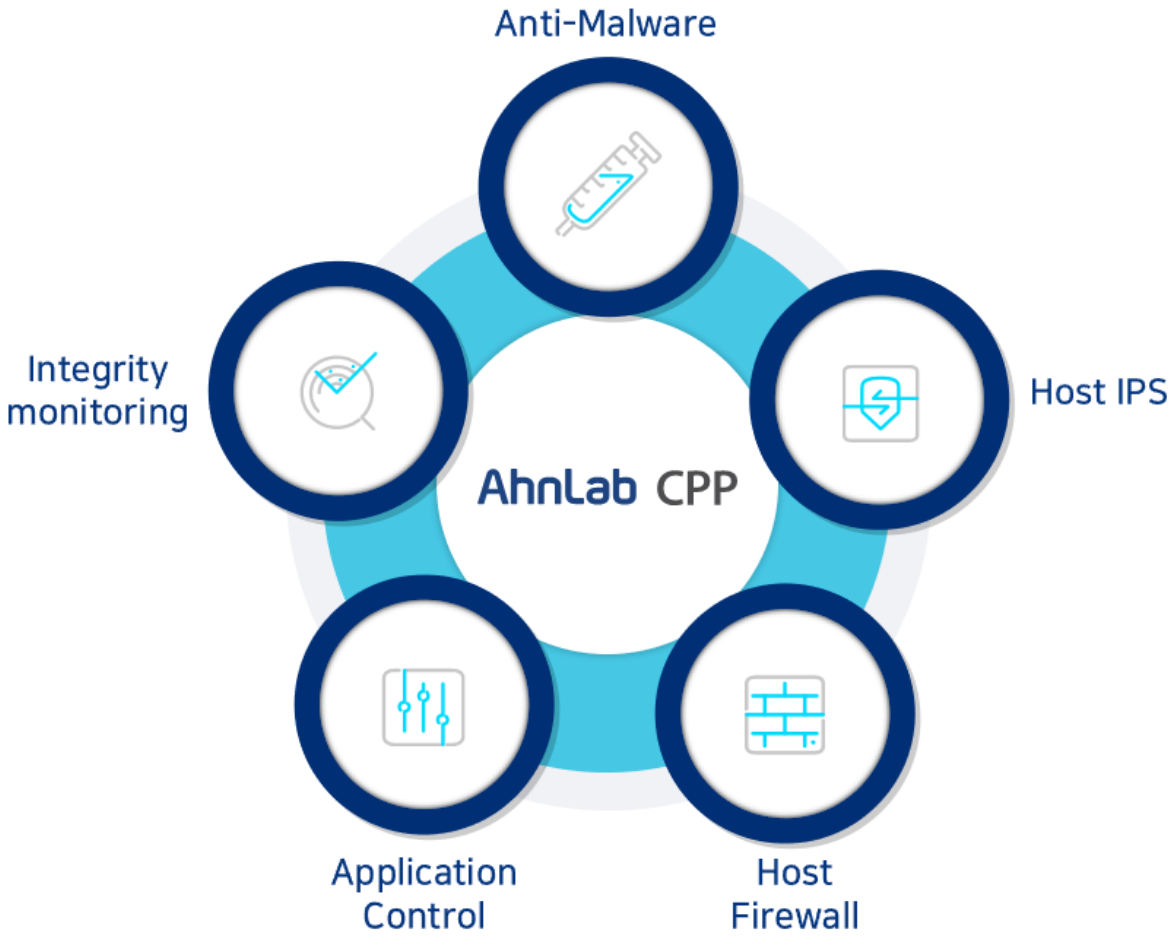
如上所述，云安全框架中的核心是工作负载的集成安全。因此，在云安全解决方案的优先级中，云工作负载安全平台（Cloud Workload Protection Platform: CWPP）一定是排在首位的。

CWPP是一种可以保护混合和多云架构中的服务器工作负载的安全解决方案。从应用程序的开发到分发的全过程中，提供各种功能来检查安全状态并确保一致的工作负载可视性和控制能力。CWPP的核心，即存在的原因是快速检测和响应服务器、虚拟机、容器等多种环境中的工作负载威胁。



【图5】Gartner发布的CWPP优先级模型

根据Gartner发布的CWPP优先级模型，云工作负载安全始于被称为运营和基本安全的各个方面的“安全卫生”，并基于加固、配置和漏洞管理、基于身份的安全细分化和网络可视性。像这样，在要求各种功能的情况下，重要的是通过配备具有高实用性的功能的安全解决方案来提高可用性。



【图6】AhnLab CPP结构图

AhnLab深入分析客户对云安全的要求后推出了CWPP解决方案——“AhnLab CPP”。AhnLab CPP配备了CWPP核心——Host IPS、应用程序控制、完整性监控、防火墙和基于AhnLab独家领先技术和经验的反恶意软件。

接下来，我们将介绍作为CWPP核心的Host IPS。

AhnLab CPP的Host IPS和主机防火墙功能可以防御针对主机和容器环境利用服务器和应用程序漏洞的网络攻击。不仅支持在边界的集中保护，还支持基于内部资源即主机的网络入侵防御。监控传入和传出服务器的流量，并根据防火墙设置允许或拦截，或根据应用的IPS特征码检测/拦截攻击。

AhnLab Host IPS通过其下一代入侵防御系统AIPS提供在韩国验证的数千个特征码，并支持定期更新。另外，管理员还可以直接设置组织所需的特征码。此时，还支持现有的Snort和PCRE等各种形式的注册。

与网络IPS不同，主机IPS以服务服务器作为应用对象，因此如果应用所有特征码，则在提供服务时可能会出现

性能问题。因此，主机IPS旨在仅将必要的特征码应用于相应的服务器，从而减少服务器的负载并提高安全效率。此时，基于各服务器的环境信息进行分析，推荐适合终端的特征码并自动分配。

AhnLab 提供的实用的云安全

AhnLab通过积极投资以AhnLab CPP为中心的云安全平台和收购合并，具备了云Web应用程序防火墙（WAF）、数据集成安全、合规检查自动化等广范围的安全能力。此外，它还具有云安全产品组合，包括安全专业的下一代MSP服务“AhnLab Cloud”、实时检测和响应云威胁的云安全托管以及提供安全要求事项和合规遵守方案的云信息保护咨询服务。

AhnLab在云安全方面指向的关键词是“可操作性（Actionable）”。这是因为，为了让客户在当前复杂的环境中有效确保安全，必须设置正确的优先级并提供实际可应用的安全能力。事实上，AhnLab的产品组合中体现了“可操作性（Actionable）”方向，已经包含了客户绝对需要的产品和服务。

AhnLab的集成安全能力还为客户提供了各种沟通渠道。客户可以通过利用安全解决方案和服务或通过咨询获得云安全情报。未来，AhnLab计划通过优先考虑客户的实际需求，继续发展成为最佳的云安全合作伙伴。

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