应对高级网络威胁：

保护您的数据和品牌

概述

从合作到沟通到数据访问，网络都是任务关键型业务工具。企业的创新与竞争要依靠网络，开展业务同样也离不开网络。但网络会使用户很容易遭受巨大的安全风险，而且这种风险难以检测。

为了有效解决网络安全问题，企业需要使用综合解决方案。思科®网络安全就是这样的解决方案。思科解决方案提供:

- 基于云的智能
- 基于上下文的策略与管理
- 网络执行

挑战

其中一些最复杂的基于 Web 的威胁企图隐藏在合法且流量巨大的网站上。根据思科 Talos 安全情报和研究小组 (Talos) 为*思科 2015 年度安全报告*所做的研究，攻击者使用当今一些主要漏洞利用工具包 (如 Angler 和 Sweet Orange)，依赖于通过恶意广告将用户重定向至植入这些漏洞利用工具包的网站 (包括合法网站)。[1]

虽然各种规模的公司组织都存在遭受网络恶意软件攻击的危险，但 Talos 显示，超大型企业 (员工不少于 2.5 万名) 遭遇网络恶意软件的危险比小公司大 2.5 倍以上。知识产权和这些公司生成、收集并存储的其他高价值信息——比如财务、客户信息和大数据，具有巨大的财富价值，使其成为网络犯罪的主要目标。最近的新闻报道显示，全球的各类实体——包括公司，甚至是国有企业都在雇佣黑客来强化公司的间谍活动或其他类型的“情报收集工作。”

一旦公司的网络遭受入侵，可能需要数周、数月甚至更长时间才能在网络里检测到通过网络恶意软件启用的高级持续威胁 (APT)。同时，被攻击的公司继续丢失数据，并面临遭受重大财务和信誉损失的风险。

由于不断演变的威胁和网络形势以及充满挑战的业务形势，保护企业的网络、数据和员工免受基于 Web 的威胁面临着空前的难度 (请参见图 1)。

图 1. 当今企业面临的网络安全挑战概述

传统网络安全边界正在分解，其趋势包括:

- 员工不受控制地使用基于网络的应用和社交网络应用，这不仅对网络恶意软件敞开了大门，同时也使企业面临合规性和数据安全的风险
- 不安全公共 Wi-Fi 的扩张
- 小型分支机构数量不断增加
- 高度移动的员工
- 自带设备 (BYOD) 政策

[1] *思科 2015 年度安全报告*, 思科, 2015 年 1 月.

企业必须检查的网络流量飙升，虚拟化业务应用数量不断增加，这些也是企业难以识别并阻止基于网络的威胁的其他因素。很多公司需要在严格遵守业务约束条件的前提下，发展更可靠的网络安全，这对公司提出了更大的挑战。例如，这些公司必须使用现有架构，或是依赖有限的资源来扩展网络安全，使通常缺乏现场IT支持的远程位置和分支机构获得保护。

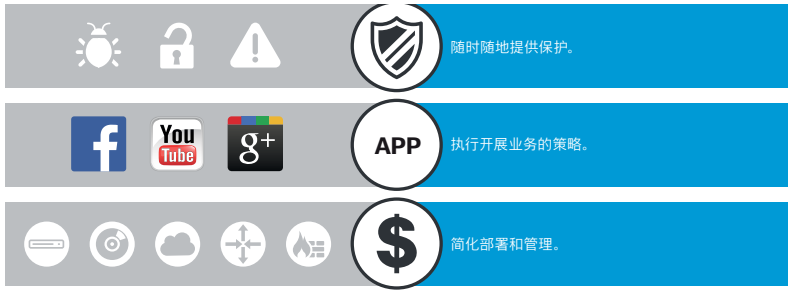
综合解决方案

当今企业需要能够驾驭网络的力量，但又不能损害业务灵活性或网络安全。但是，随着网络使用的不断扩展，企业面临的有形风险也在增加，而这些风险可能会影响企业的品牌、运营、数据以及更多方面。只需了解以下事实就一目了然：目前每秒钟有四个新网络恶意软件出现，即每分钟240个，每小时1.5万个，每天30万个。[2]

为了有效应对网络安全挑战，企业需要高效、无处不在的解决方案（请参见图2），这种解决方案可以：

- 随时随地提供全面保护，包括传统的公司办公室用户、自带设备用户、远程办公室以及公共无线接入点。
- 执行随业务发展（而不是妨碍业务发展）的使用政策。
- 在企业网络以及业务环境限制范围内轻易部署。

图2.综合网络安全的要素



保护每台设备、每个用户以及通过企业网络传输的所有数据，这需要自适应、响应式以及架构型方案。思科基于网络的安全架构就是这类方案。利用其组件（请参见图3）提供的封闭式解决方案，企业可以防御、发现并弥补源自网络的威胁。思科解决方案还能帮助企业更好地管理无边界网络的安全风险，使员工可以通过自己选择的设备在全球范围内访问网络，并使用完成本职工作所需的应用和信息。

图3.思科基于网络的安全架构

[2]资料来源：Cisco Talos。

思科基于网络的安全架构包括:

- **基于云的智能**–在威胁出现前几个月提供自适应和一致的威胁保护，避免出现与纯签名和补丁周期相关的问题
- **基于上下文的策略和管理**–基于用户、设备、位置、形势、应用等丰富上下文，而不是“白名单”和静态设置的智能安全策略
- **网络执行安全**–在整个网络基础设施范围内一致地执行安全策略

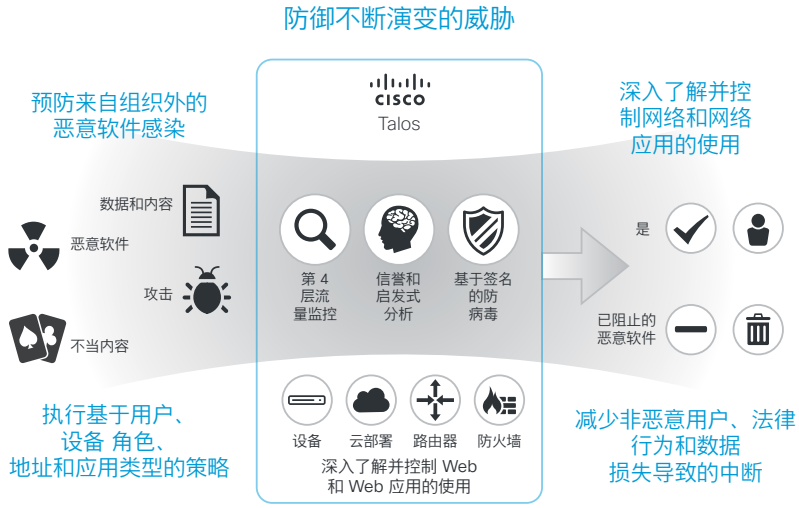
高级恶意软件防护

高级恶意软件防护 (AMP) 增加了思科网络安全的成熟度，有助于在扩展的网络范围内连续监视并分析。AMP 是一种检测系统，它不依赖恶意软件签名，您可能需要数周或数月才能为每个新的恶意软件样本创建此类签名。相反，它结合使用文件信誉、文件沙盒和追溯性文件分析方法 (本文稍后介绍)，在攻击前、攻击中和攻击后的整个攻击过程中识别和拦截威胁。

思科网络安全

思科网络安全支持思科基于网络的安全架构，防范可能扰乱公司运营的威胁 (请参见图 4)。思科网络安全被 Gartner 评为 2014 年领先安全网关，它将恶意软件挡在网络外面，帮助各种规模的公司组织更有效地控制并保护网络使用。思科网络安全提供入站和出站保护，并借助 Cisco AnyConnect® 安全移动客户端，将网络安全扩展至远程和移动用户，包括智能手机和平板电脑的安全；此移动客户端是一种轻质、高度模块化安全客户端，它可以根据业务的具体需要提供轻松自定义的功能。

图 4.思科 Web 安全的工作原理



思科网络安全使用 Talos 提供的信誉和零日威胁情报。Talos 由一流的威胁研究人员组成，是为思科综合安全情报 (CSI) 生态系统提供威胁信息的主要团队，它包括威胁响应、情报和开发 (TRIAD)、托管威胁防御，以及安全情报运营中心。思科 CSI 可在多种安全解决方案中进行共享，并提供行业领先的保护和效力。

Talos可调用由数十亿Web请求和电邮、数百万恶意软件样本和开源数据集、以及数百万网络入侵组成的无可匹敌的遥测数据集，从而创建出可全盘理解威胁的情报。这种能力转换为具有行业领先效果的思科安全解决方案。我们的安全情报云可产生“大情报”并进行信誉分析，从而在各种网络、端点、移动设备、虚拟系统、Web和电邮中跟踪威胁。

Talos可以24小时查看全局流量活动，分析异常，发现新威胁，并监控流量趋势。Talos能持续生成新的规则，以便每3到5分钟将更新馈送到思科网络安全设备(WSA)，从而有助于防御零时攻击。同时，它还能先于同类竞争产品数小时或数天提供威胁防御。

思科网络安全由全球最大的威胁检测网络支持，不仅可视性最高，而且覆盖范围最大，可处理:

- 每天100 TB的安全情报
- 160万个已部署的安全设备，包括防火墙、入侵防御系统(IPS)、网络和电子邮件设备
- 1.5亿个终端
- 每天130亿个的网络请求
- 全球35%的企业电子邮件流量

思科网络安全使用动态信誉分析和基于行为的分析，为企业提供针对零日网络恶意软件的最佳威胁防御。对所有入站和出站网络流量进行实时扫描，防范新出现和已知的网络恶意软件。从HTML到图片到Adobe Flash®文件，每一个被访问的网络内容均会通过安全和上下文感知扫描引擎进行分析。

思科网络安全让企业全面掌控最终用户访问互联网内容的方式。精确控制甚至可应用于动态内容，比如Facebook和Twitter内容，以及来自很多其他流行平台和流媒体的内容。您可以根据业务和用户的需求允许或阻止聊天、消息传送、视频和音频等具体功能，而无需阻止整个网站。

采用AMP技术的增强型恶意软件检测

思科网络安全的AMP插件为思科WSA提供恶意软件检测、阻止、连续分析和追溯性警报。Cisco AMP在整个攻击过程中结合使用文件信誉、文件沙盒和追溯性文件分析方法，来识别和阻止威胁。Cisco AMP的功能说明如下:

- 文件信誉在每个文件通过思科网络安全网关时捕捉文件的指纹，并将指纹发送到AMP基于云的情报网络进行信誉鉴定。获得此类结果后，您可以自动拦截恶意文件，并应用管理员定义的策略。
- 利用文件沙盒，您可以分析通过思科网络安全网关的未知文件。借助高度安全的沙盒环境，AMP可以收集精确详细的文件行为，并将其与详细的人工和机器分析结合，以确定文件的威胁级别。之后，处理结果会被植入AMP的基于云的情报网络，用于动态更新和扩展AMP云数据集，以增强保护性能。除了在第一版AMP中支持的EXE文件以外，客户现在还能对PDF和Microsoft Office文件执行沙盒处理。
- 文件追溯可解决恶意文件在通过边界防御后才被视为威胁的问题。此功能解决了大部分边界防御与生俱来的弱点，即仅在单个时间点有效。即使是最先进的技术也可能会在边界漏识某些恶意软件，因为多态攻击、模糊攻击、休眠定时器和其他手段可以帮助恶意文件穿过防线时有效地躲过检测。恶意文件只需等待进入网络后再进行破坏活动即可。这些包括通过Dropbox和Box等软件即服务(SaaS)应用进出网络的流量文件。
- 文件追溯不是在某个时间点进行操作，而是借助AMP的基于云的情报网络所提供的实时更新，对通过安全网关的文件进行持续分析，以与不断变化的威胁级别保持同步。恶意文件被识别为威胁后，AMP将向管理员发出警报，让管理员一目了然地了解哪些人有可能已被感染以及何时被感染。这样，客户就可以在攻击还没来得及扩散之前，就迅速识别并处理掉它们。

思科网络安全的其他优势

当今基于网络的威胁复杂多变，但是构建更好的安全基础设施并不一定意味着更复杂的基础设施。但是，基础设施和基础设施内的元素必须共同配合，从而利用更多的情报来检测并缓解威胁。思科架构型安全解决方案功能全面，由思科网络安全提供支持。利用思科解决方案，公司可以实现服务再利用，并且根据业务需要的变化快速部署新功能，从而保持公司业务的敏捷性。

思科网络安全提供连续的高性能网络安全和策略，而无需考虑用户在哪里以及如何访问互联网。思科网络安全是针对基于网络的恶意软件的最有效防御方案，它可以提供最佳应用控制和URL过滤功能，使用户可以管理数据丢失风险、员工工作效率和带宽用量。思科网络安全是企业无处不在的网络安全策略的一部分，它可以为用户提供更好的数据和品牌保护，并有助于确保合规性。该解决方案还有助于随时随地保护用户，使用户可以安全、适当地访问网络。

与单点产品相比，无论是通过设备还是通过云部署此解决方案，思科网络安全都能提供更高的投资回报。（有关部署和许可选项，请参见表 1。）思科网络安全与思科网络基础设施，以及其他思科的安全产品紧密集成，使企业可以重新利用现有资产，在以前部署成本或难度过高的领域部署网络安全。

思科网络安全及其简化架构还可以提高运营效率来减轻管理负担，包括减少要管理、支持和维护的设备。此外，该解决方案通过减少硬件、机架空间、电源、散热和维修成本来降低总体拥有成本。

表 1.思科网络安全：产品提供

产品	许可选项
思科 WSA – 现场型网络安全网关，可以保护所有用户，无论位置。由Talos提供综合零日威胁保护的技术支持。网络安全、应用控制、代理缓存和报告功能完全集成至单个设备，并提供三种模型选择。	*高级网络安全*–应用可视性与可控性（AVC）、URL过滤和信誉分析，以及实时防恶意软件保护与防数据丢失(DLP)集成。
思科网络安全虚拟设备(WSAv) – 虚拟 WSA 可以实现简化、多位置部署；提供与WSA相同的功能，但又具有虚拟模式的灵活性。	*高级网络安全*
思科云网络安全(CWS) – 基于云的网络安全由Talos提供技术支持，它通过行业领先的实时保护，以及实施详细的网络使用策略来提供综合网络防御。多连接器选项便于部署。	*CWS Essentials（包括网络过滤、病毒爆发情报、AVC）、CWS Premium（具有AMP和认知威胁分析）*

总结

安全对网络的意义变得空前重要。由于威胁和风险持续存在，再加上对保密性和控制的顾虑，对于提供业务连续性、保护宝贵信息、维护品牌声誉以及采用新技术而言，安全性是必不可少的。高度安全的网络帮助员工拥抱移动性，并安全地获取正确的信息。这种网络还能使客户和合作伙伴与您更轻松地开展业务。

没有其他公司能像思科一样如此深刻理解网络安全。我们不仅占据市场领先地位，具有无可匹敌的威胁防范、预防和创新产品，更能提供长期持续服务，这些优势使我们成为满足您安全需要的最佳供应商。

更多详情

有关思科网络安全解决方案和部署选项的更多信息，请访问www.cisco.com/go/websecurity。