白皮书

Web 安全：保护您在云中的数据

概述

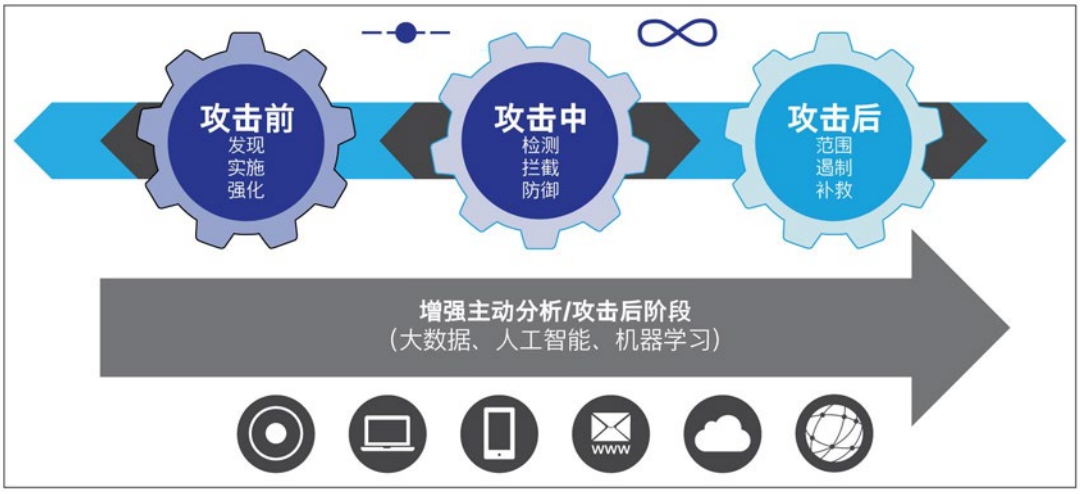
安全团队不能无处不在，但是，当前环境要求组织在威胁可能出现的任何地点保护他们的数据。“任何地点”包括网络、移动设备、虚拟环境以及云或数据中心。

今天的威胁可以渗透每道防御。攻击者积极主动地了解部署哪些类型的安全解决方案， 并转向不太可见、内容不易检测的行为模式。根据**思科 2014 年度安全**报告，大多数的攻击者都有一项主要任务：窃取高价值的数据。[1]

同时，分布式企业的涌现和新业务模式（如云计算、移动性和自带设备 (BYOD) 环境）的兴起，削弱传统的安全边界并且正在使攻击面扩大。安全团队很难与时俱进。他们不知道如何确定要调查的威胁的优先级，错过许多他们完全看不到的威胁。

实时的预防性安全解决方案为什么不能为现代企业提供足够的保护，这点很容易理解。当然，没有任何一种检测方法是十全十美的，有些威胁肯定会足够复杂和隐蔽，能够渗透任何层的防御。需要什么？ 连续和追溯性的安全性，可以涵盖整个攻击过程：攻击前、攻击中和攻击后。

图 1. 整个攻击过程



[1] 思科 2014 年度安全报告：http://www.cisco.com/c/en/us/products/security/annual_security_report.html。

思科云 Web 安全基本版

思科® 云 Web 安全 (CWS) 帮助组织应对在扩展网络中保持持续安全的挑战。该解决方案为分布式企业提供行业领先的安全性和控制，并提供最广泛的可用部署选项。思科云 Web 安全是思科 Web 安全基于云的版本。思科云 Web 安全平台将 Web 安全扩展到移动设备和分布式环境。它通过思科全球威胁情报、高级威胁防御功能和漫游用户防护为用户提供保护。

思科 Web 安全提供多种直观的工具，可用来创建、实施并监控入站和出站 Web 策略，使企业完全控制最终用户以何种方式访问互联网内容。简而言之，思科云 Web 安全是在云中的安全边界。它提供详细的环境感知策略控制和实施。此外，它还：

- 实时、动态地阻止威胁
- 保护网络和用户免受不良 Web 内容的危害
- 通过减少带宽拥塞优化网络资源
- 帮助启用在线活动的全面报告和监控
- 避免组织泄漏数据

云 Web 安全与思科防火墙、分支机构路由器和基于客户端的软件集成，无论用户在何处工作，都可提供保护。所有流量 - 无论是否来自总部位置、分支机构、或移动或远程用户 - 都通过数据中心全局网络路由。云 Web 安全消除回程，加快 Web 安全的部署速度，并帮助拓展现有思科投资的价值。

由于最近收购了安全公司 Sourcefire 和 Cognitive Security，思科现已能够提供思科云 Web 安全的增强版本来阻止高级恶意软件威胁，尤其是在攻击过程中的“攻击后”阶段，还改进“攻击中”阶段的实时威胁检测。思科通过可选的高级版订用提供此解决方案，详情如下所述。

云 Web 安全高级版

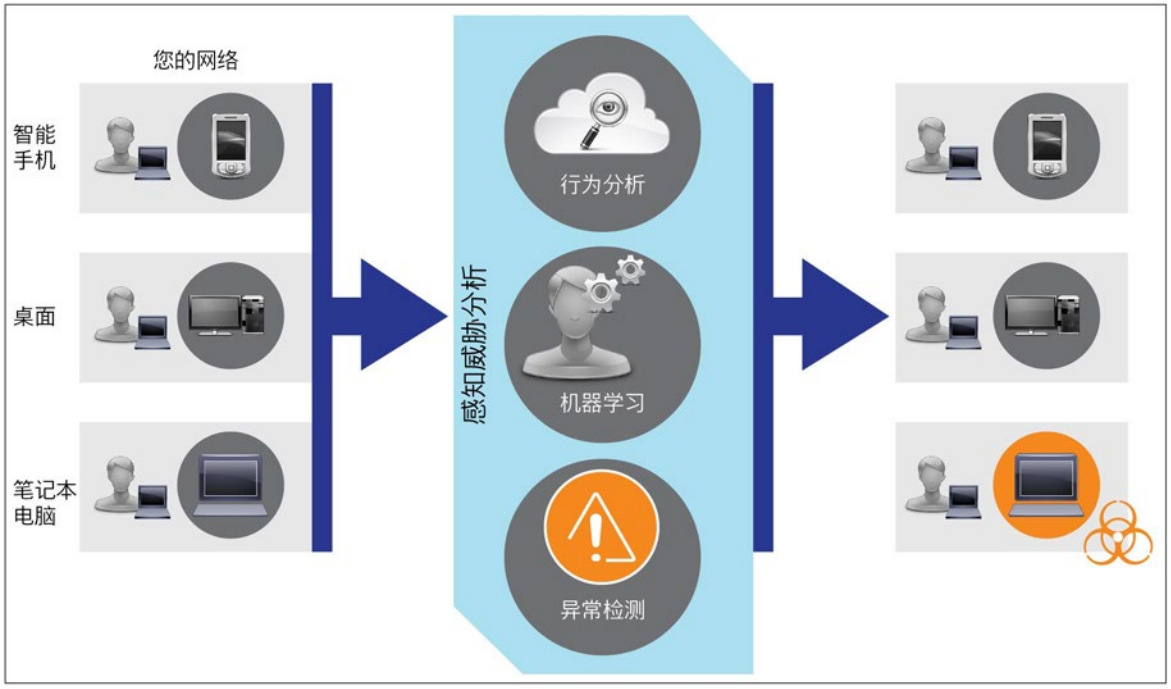
云 Web 安全高级捆绑包包括所有基本版捆绑包的功能，但还包含两个创新的恶意软件检测系统：认知威胁分析 (CTA) 和高级恶意软件防护 (AMP)。这些系统可以自动化搜索组织 Web 流量中的高风险威胁。思科云 Web 安全高级版提供额外的实时保护、追溯性的安全性和不间断分析，帮助组织查找和解决最重要的威胁。此外，它还缩短发现已在网络内部运行的威胁的时间。

安全团队现已能够提供不间断的 Web 安全，从而可以在整个攻击过程中保护系统。接下来让我们详细了解这两个恶意软件检测系统。

感知威胁分析

感知威胁分析 (CTA) 是由 Cognitive Security 开发的一个近实时网络行为分析系统。它利用机器学习和高级统计找到网络中的异常活动：感染症状。此解决方案不依赖规则集，这意味着无需人工干预来“调整”CTA。一旦 CTA 启用，它就会立即开始寻找威胁。系统会在云中关联数据，以提高 CTA 的异常检测功能的速度、灵活性和深度。

图 2. CTA 概述



CTA 从它发现的情报中学习。它随着时间的推移不断改变，从而能够识别安全行业以前检测不到的、新的指挥和控制通道。它评估实体（例个人用户）在网络中的行为，并使用行为建模预测这些实体应如何表现。CTA 使用长期的网络行为建模使看似不相干的活动相互关联。然后，它将这些相互关联的数据与整个特定客户网络中的各个用户行为进行比较，从而能够更快地检测威胁。

检测到的威胁可能是什么并不重要。如果预期行为的差异很大或持续存在，CTA 将标记此行为。CTA 的操作类似于安全团队力求在商店扒手有机会实施盗窃之前找到这个人：这个人的行为与其他购物者的行为有什么不同？ 拿着一个大袋子而不是推着购物车？ 试图从后门而不是前门出去？ 即使可疑行为可能证明是合法的，但也值得调查。

CTA 发现异常，然后引导安全分析师找到潜在问题，这有助于他们减少工作量和确定威胁的优先级。它还对思科现有的安全技术进行补充，使这些解决方案更准确、更能检测到网络中的未知或异常行为。因此，思科安全功能扩展到攻击过程中的“攻击后”阶段。最重要的是，CTA 帮助提供随着不断变化的威胁环境而发展的安全性。

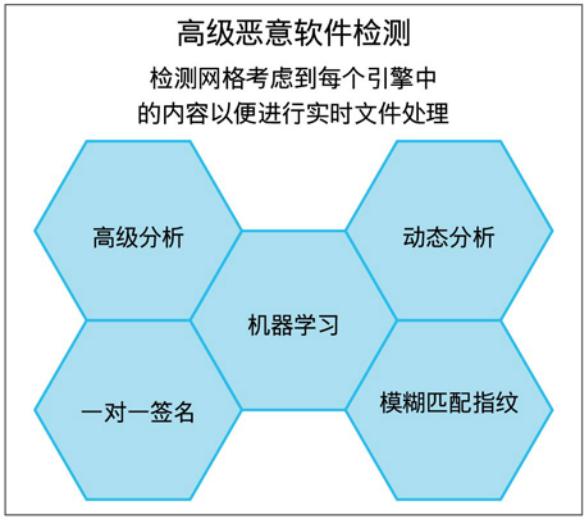
高级恶意软件防护

思科云 Web 高级版的第二个检测系统是来自 Sourcefire 的高级恶意软件保护 (AMP)。AMP 不依赖恶意软件签名，可能需要数周或数月分别为每个新的恶意软件示例创建此类签名。此解决方案结合使用文件信誉、文件沙盒和追溯性文件分析方法，来在整个攻击过程内识别和阻止威胁。

文件信誉

文件信誉是查看文件数据库以确定文件为 “clean”、已知是恶意软件或未知的功能。AMP 在它经过思科云 Web 安全服务时捕获每个文件的“指纹”，并查询思科和 Sourcefire 共同的基于云的智能网络以便获得信誉裁决或“得分”。使用这些结果，AMP 然后可以自动阻止恶意文件并应用管理员定义的策略。图 3 显示不同引擎致力于实时检测高级恶意软件和确定文件信誉。

图 3. 高级恶意软件防护



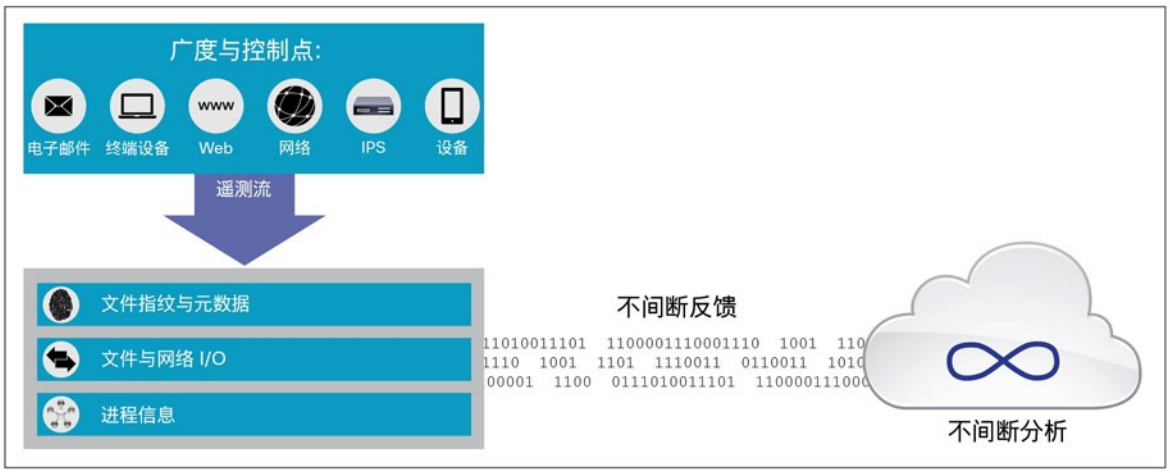
文件沙盒处理

文件沙盒处理是 AMP 的一项重要功能 - 也最终是云 Web 安全高级版的一项关键功能。借助文件沙盒处理，AMP 可以分析经过思科云 Web 安全的未知文件。在高度安全的沙盒环境中，AMP 可以收集精确详细的文件行为，然后将这些数据与详细的人工和机器分析结合，以确定文件的威胁级别。接着，这些信息被存储到思科和 Sourcefire 共同的基于云的智能网络，用于动态更新 AMP 云数据集。通过活动报告功能，安全团队可以查看数据丰富的、简单易读的有关分析文件的报告。

文件追溯

或许 AMP 最重要的功能是它的追溯性分析功能，使组织能够“及时追溯”以便确定攻击时间，然后评估损坏情况。文件追溯利用思科和 Sourcefire 基于云的智能网络中的实时更新，对经过安全网关的文件执行不间断分析。

图 4. AMP 的追溯性分析流程

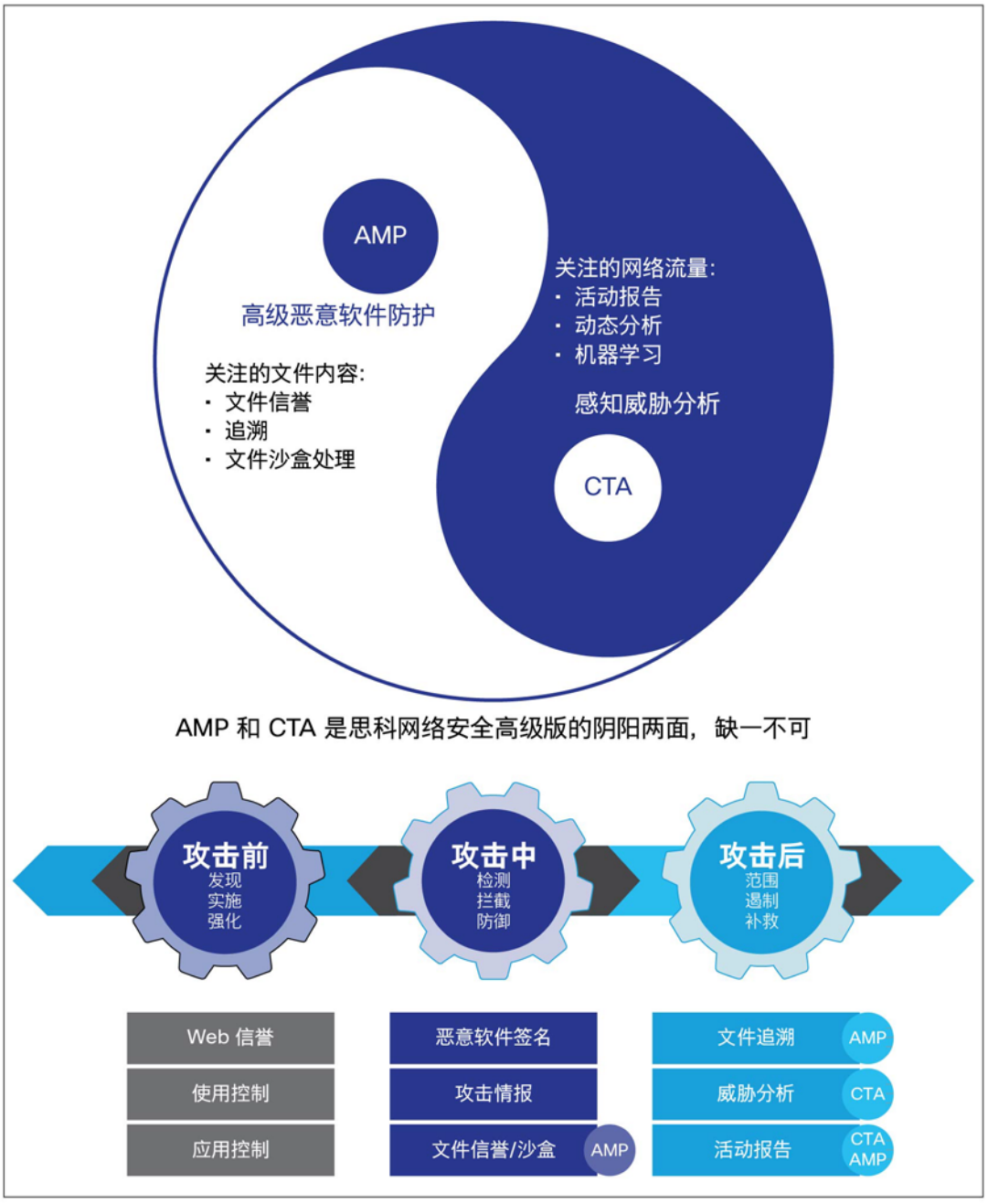


有时追溯性分析会揭露通过边界防御时视为 “clean”、但实际上是精心伪装的高级恶意软件的文件。AMP 将立即向安全管理员发出警报，确定网络中的哪些用户可能被感染以及何时感染。这样安全团队就能在病毒有机会传播前迅速解决攻击。

总结

包含 CTA 和 AMP 的思科云 Web 安全高级版与思科战略保持一致，帮助组织解决已知和新出现的安全挑战。它帮助组织检测、了解并找到威胁。不间断分析和实时安全情报是从云中提供的，并在所有安全解决方案间共享，从而提高了它们的效率。通过结合使用这三个解决方案，帮助组织识别安全行业以前检测不到的、新的指挥和控制通道，还帮助组织解决在整个攻击过程中遇到的安全挑战。

图 5. 带有 AMP 和 CTA 的云 Web 安全：覆盖整个攻击过程的安全



攻击前：发现、实施、强化

云 Web 安全提供 Web 信誉、使用控制、应用控制（包括微型应用的控制）、恶意软件签名以及攻击情报，从而在攻击前和攻击中提供安全性。

攻击中：检测、阻止、防御

AMP 借助自己的文件信誉和文件沙盒处理功能，增强了攻击过程中的“攻击中”阶段的安全性。它自动阻止恶意文件，并基于文件的已知信誉应用管理员定义的策略。它还分析经过网络的未知文件，并相应地更新威胁情报。这些功能有助于安全分析师确定要调查的威胁的优先级。

攻击后：范围、遏制、补救

CTA 和 AMP 都在攻击过程中关键的“攻击后”阶段实现不间断分析和补救。CTA 提供实时网络行为分析来确定网络中的异常行为。同时，AMP 的文件追溯功能也能解决恶意文件通过边界防御的问题。AMP 的活动报告功能提供已进入网络的文件的相关信誉和行为信息。安全团队可以更轻松地确定和评估攻击范围，然后立即采取补救措施。

接着，使用 CTA 和 AMP 在“攻击后”阶段提供的机器学习，来增强云 Web 安全高级版在攻击中应用的近实时监测功能。

更多详情

要了解更多有关思科云 Web 安全基本版和云 Web 安全高级版的信息，请访问 http://www.cisco.com/go/cws。

有关 CTA 的详细信息，请参阅 http://www.cisco.com/go/cognitive。

有关 AMP 的详细信息，请访问 http://www.cisco.com/go/amp。

美洲总部
Cisco Systems, Inc.
加州圣荷西

亚太总部
Cisco Systems (USA) Pte, Ltd.
新加坡

欧洲总部
Cisco Systems International BV Amsterdam.
荷兰

思科在全球设有 200 多个办事处。思科网站 **www.cisco.com/go/offices** 中列出了各办事处的地址、电话和传真。

美国印刷　　C11-734836-00　06/15