McAfee Web Gateway Cloud Service

云原生 Web 安全提供无处不在的保护

采用先进技术抵御复杂的网络威胁，但不必增加成本和复杂性。通过云提供网络安全保护，使安全团队可获得类似内部部署设备那样的高级威胁保护优势，并且还不需要硬件或资源维护成本。随着网络边界外部的网络访问增加，云成为设备和用户漫游时一致的联系点。通过云提供网络安全保护，并不是为流入单个位置的通信量提供安全保护，而是为终端输出的通信量提供更有效的安全保护。凭借针对云和 Web 采取一体化的访问控制和威胁防御措施，可以在创建高效且一致的安全管理体验的同时，支持贵公司的工作人员以最高的生产效率执行工作。

经济高效、无处不在的保护

管理内部部署网络安全设备不但成本高，而且还需要占用安全团队的时间，这对时间已经很紧张的安全团队而言无疑是雪上加霜。以云服务形式部署网络安全，可以降低总体拥有成本。不再需要购买、持有和维护硬件设备。以前维护设备，执行软件升级和安装修补程序等任务所使用的所有资源，可以重新分配给 IT 或 IT 安全组织内更具战略意义的计划。

在混合部署中可以将设备和云服务结合使用。大多数组织选择此模式，旨在继续持有和控制网络中的设备，并为小型远程办公室和漫游用户提供通过云提供的保护。

通过云提供网络安全保护的直接受益对象是，通过多协议标签交换 (MPLS) 电路回送远程办公室 Web 流量以使网络中的 Web 网关设备过滤流量的 IT 团队。通信量回送成本高，并增加了网络复杂性。现在远程办公室可以直接将通信量发送到提供保护的云，减少 MPLS 电路，并简化了网络体系结构。

最后，员工访问网络不再需要局限于网络边界，否则会导致脱机用户和设备脱离 IT 团队的保护和视线。将网络安全目标转向云，颠倒了网络边界。脱机用户和设备的 Web 流量可以从终端自动路由到云，不管用户是在家、在机场、在咖啡店还是在任何其他脱机位置工作都能保证安全连接。网络安全保护重点不再是物理网络围墙中的通信量。而是终端所到之处输出的通信量。

主要优势

- 最经济有效的网络安全部署方式—不需要使用内部部署硬件或软件。
- 超越基本保护—在处理通信量时通过行为模拟可在几毫秒内阻止零日恶意软件。
- 为脱机用户提供保护。通过云提供保护消除了传统的网络边界。
- 通过与 McAfee® MVISION Cloud (CASB) 控制台相结合，可提供高效且一致的安全管理体验。
- 经过实践验证的体系结构：McAfee Web Gateway Cloud Service 被构建为多租户版的 McAfee Web Gateway（全球企业所使用的受信任的内部部署设备）。

联系我们

全球高性能的体系结构

McAfee® Web Gateway Cloud Service 是专为企业构建的产品，与许多组织目前的内部部署体验相比，他们将获得更高水平的性能。例如，对于内部部署，在需要提升容量时，IT 团队需要购买和部署新设备，这需要数天乃至数周的时间。在云中，提升容量大约需要 15 分钟，这归功于内置于服务的弹性云设计。

当内部部署设备出现故障、需要维修时，如果故障消息在网络上公开，将会破坏互联网和安全计划。如果其中一个数据中心位置出现故障，我们的云服务会将所有 Web 流量重新自动路由到距离最近、传送速度最快的数据中心位置，确保当前的数据连续性。

我们的云服务体系结构还会构建到全球最大的互联网交换点 (IXP) 的互联网中枢“对等”点。这样可消除增加连接延迟的中间 Internet 服务提供商 (ISP) 的路由跃点。与用户直接连接到开放互联网相比，随着 Microsoft Office 365 和 Google 等受欢迎的内容提供商的跃点越少，他们通过我们的云服务建立连接的速度则更快。

McAfee Web Gateway Cloud Service 是全球服务。Web 内容可以使用本地区域语言提供，例如，不管用户在何处建立连接，他们都可以看到 Google 本地搜索结果。要查看处理 Web 流量的数据中心的当前位置和状态，请访问 https://trust.mcafee.com。

抵御复杂的威胁

安全团队通常跟不上避开传统防御的，极复杂的恶意软件和针对性攻击的步伐，不得不消耗资源不停“灭火”，无休止地修复终端。与阻止 Web 威胁的传统 URL 过滤和基于特征码的方法不同，McAfee Web Gateway Cloud Service 通过串联模拟 JavaScript 和 HTML 文件，保护终端免受零日和无文件恶意软件的威胁。此服务可防止零日恶意软件入侵用户系统，比 URL 过滤和基于特征码的解决方案的拦截率高 20% 左右。通过减少恶意软件事件的总数，降低了成本，提高了资源灵活性，安全操作因此受益匪浅。仍认为可疑的任何内容可以发送到 McAfee Cloud Threat Detection，我们基于云的高级威胁分析解决方案，作为补充方式，与 McAfee Web Gateway Cloud Service 一起提供原生集成服务。

Web 威胁通常是通过避开网络安全防御的加密通信量传递的。云存储或社会化媒体等几乎所有云应用程序都默认使用加密通信量。McAfee Web Gateway Cloud Service 可以完全解密和检查 HTTPS 加密通信量，在加密通道内启用恶意软件阻止功能和云应用程序监控功能。

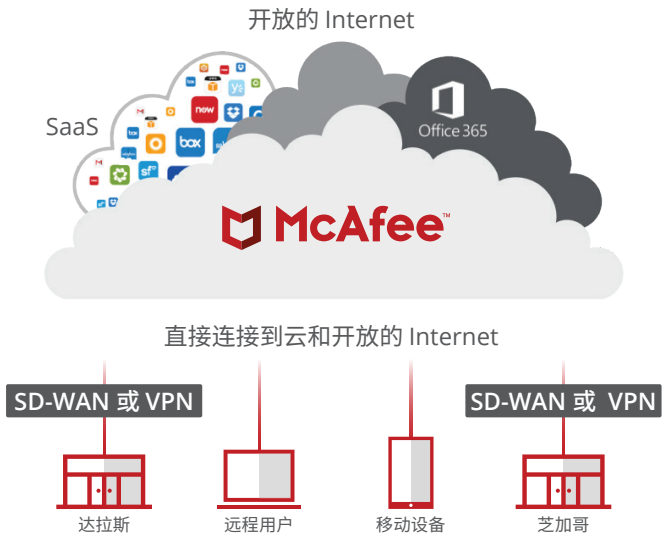

图 1. 适用于 Web 和云安全的云原生体系结构。

针对云和 Web 采取一体化的访问控制和威胁防御措施

云服务存在着多重风险；另外，无论是托管设备还是个人设备，都可以访问云服务。McAfee Web Gateway Cloud Service 与 McAfee MVISION Cloud (CASB) 的结合，实现了通过单个控制台就可以控制所有云服务的访问权限，并且可以抵御其中出现的各种威胁。这些合并后的策略可提供前所未有的云控制措施 — MVISION Cloud 负责通过 API 和反向代理，执行其批准的云服务可见性和控制；McAfee Web Gateway Cloud Service 负责通过正向代理，监控并阻止未经批准的云服务和 Web 流量。高风险的云服务将会遭到阻止，从而阻隔最终用户访问这些服务，以确保最终用户免遭意外数据丢失或恶意软件的侵扰。

全球哪些地方可提供 McAfee Web Gateway Cloud Service?

请访问 https://trust.mcafee.com，了解我们数据中心位置、可用性情况等内容的实时更新，并监控这些内容。

了解更多

有关详细信息，请访问 www.mcafee.com/cn/products/web-gateway-cloud-service.aspx。

北京市东城区北三环东路 36 号
北京环球贸易中心 D 座 18 层，100013
电话：8610 8572 2000
www.mcafee.com/cn

McAfee、迈克菲和 McAfee 徽标是McAfee, LLC 或其分支机构在美国和/或其他国家/地区的注册商标或商标。其他商标和品牌可能是其各自所有者的财产。
Copyright © 2020 McAfee, LLC. 4423_0220
2020 年 2 月