没有网络边界？
现在该怎么办？

鉴于云应用程序、移动设备和远程工作人员消除了网络边界的概念，
是时候跳出安全框思考安全问题。

Symantec™

第 1 章

云时代网络安全

运用专为云时代打造的网络安全防护，对抗狂风暴雨般的安全挑战

如何保护移动设备、远程办公室和云应用程序安全？如何满足不断演变的合规义务，同时应对无休止且日益复杂的网络安全攻击？

回传分支和远程互联网通信至企业数据中心的首选，充分应用安全性和威胁防护策略。随着公司逐渐迁移业务到云端，这种模式慢慢退役，因为通过专有多协议标签交换 (MPLS) 链路回传通信非常昂贵，而且回传会产生延迟问题，从而影响尝试访问云应用和网络的异地员工。或者，员工可以直接访问基于云的安全服务，从而消除回传；当通信直接传递到 Web 和云应用程序时应用安全策略。

建议：

- 选择基于云的 Web 安全网关作为安全基础架构的基础，全面保护用户和数据，无论其身在何处
- 获得自己所需的安全性，同时不牺牲网络性能或成本优势
- 确保您拥有业界领先的威胁防护技术
- 通过统一安全策略保护本地和远程/移动用户
- 选择全面的解决方案，实现有效无缝的保护

2017 年

1/13

网关每分析 13 个 URL，就能发现 1 个恶意 URL。

而在 2016 年，这一比例仅为 1/20。

恶意软件隐藏在加密通信中时，就可以渗透传统的网络防御并大肆破坏。当下的大多数互联网通信都实行了加密，而恶意分子也越来越多地使用加密来传播恶意软件。

第 2 章

围绕基于云的高级安全 Web 网关构建防御

云时代离不开 Web 安全网关 (SWG)，它涵盖的不仅仅是网络和云应用程序安全基本功能。

Web 安全网关 (SWG) 可将安全数据流快速传送至 Web 和云应用程序，以独特方式扫描通信（即使通信加密也无妨），查找恶意软件和信息安全违规情况。这就是为何 SWG 是网络安全堆栈的完美基础。基于云的高级 Web 安全网关超越了传统的基本功能，例如强制实施企业可接受的网络使用策略。它使用威胁情报数据评估 URL 的风险，阻止员工打开有风险的网站，并且融合了检测技术以检查通信中有无网络威胁和数据泄露风险。部分 SWG 融入了 Web Isolation 等创新技术，为用户增添额外的威胁防护。全功能版 SWG 可提供全面功能，解决您面临的关键安全和合规难题。最重要的是，它采用云形式交付，因此您可始终通过该解决方案路由用户通信，确保他们无论位于何处、采用何种设备都能得到妥善保护。

建议：

- **选择性地检查加密通信，准确扫描内容以查找恶意软件和违规行为。**
  - 快速安全地检查 SSL/TLS 加密通信，解决企业的保护需求和用户的性能需求。现在，大部分互联网通信都实行加密，因此您的网络安全解决方案务必可解密通信并协调通信至安全和数据合规检查引擎。此外，企业还务必保护用户远离以网页浏览器为目标的新兴威胁。
- **支持员工以受保护的方式访问可能存在风险的网站。安全访问电子邮件中嵌入的网址，以免在钓鱼网站中输入企业访问凭据。**
  - 使用 Web Isolation 功能，阻止以用户网页浏览器为目标的威胁和网络钓鱼攻击入侵员工设备。Web Isolation 可以脱离端点执行各种 Web 会话，仅将安全呈现信息发送给用户浏览器，因此可以有效阻止任何网站发送的零日恶意软件侵入您的设备。

第 2 章

围绕基于云的高级安全 Web 网关构建防御

- **自动在所有网络通信中应用数据隐私和保护策略，无论数据加密与否，并使用管理面板和在线报告监控活动。**
  - 将解密的 SSL/TLS 通信发送至任何数据泄露防护 (DLP) 系统以进行准确快速的分析。支持法规遵从并保护数据。
- **准确识别在用的云应用程序，评估风险，并按用户、组和位置等属性控制访问权限。**
  - 通过云访问安全代理 (CASB) 控件保护云应用程序，保护与公有云交互的数据。监控员工使用的所有云应用程序、已知的云（例如 Office 365）以及“影子 IT”云（员工自己置备），确保其遵守公司的云使用政策。
- **将云 SWG 与本地和移动端点保护相整合。**
  - 将网络安全与端点安装的安全解决方案相集成，实现全面多层网络到端点防护，简化移动设备应用程序管理。创建多层防御以全面保护企业端点，包括直接连网的移动用户和远程用户。
- **将远程/分支办公室的员工连接到网络，同时充分发挥 SD-WAN 性能和灵活性优势。**
  - 通过可选 SD-WAN 和类似设备将远程通信路由至云安全解决方案，轻松保护远程办公室和移动员工的通信安全。像更改防火墙或代理上的配置一样轻松入门，或者在用户设备上进行轻微调整。

第 3 章

卓越安全性和性能，同时享受低成本优势

采用以云形式交付的网络安全即服务，运用全部功能保护员工。

强制实施高度一致的策略，无论用户位于何处、采用何种设备。最重要的是，由于全面网络安全堆栈以云形式交付，因此完整的安全功能也可实现云的速度和简单性优势。所需的一切功能均整合到一款高性价比的服务中，日后只需为新用户增添订购即可扩展部署。

直接连网的高效率

基于云的安全性可为办公室和移动用户交付卓越性能，因为员工会在试图访问网络位置或云应用程序的途中连接到安全服务，这就称为“直接连网”安全性。同时还要选择集成了 SD-WAN 产品的服务，以便将办公室轻松连接入云。

高效 SSL/TLS 加密扫描

切勿让重要的 SSL/TLS 通信检测出现不必要的延迟，占用计算资源。采用不合适的设备（例如下一代防火墙）可能会严重降低性能。

单一代理网络安全访问

越来越多的员工通过日益增长的远程和移动设备连接网络。为何还要通过额外的代理来连接至基于云的网络服务？单一轻量型代理就可解决这个问题，它不仅带来全面的端点安全性，还可将您的网络通信重定向至云中的网络安全堆栈。

第 4 章

实现 Office 365 等应用程序的可见性、最大限度降低风险、维持合规性

采用 CASB 控件准确识别在用的云应用程序，评估风险，并按用户、组和位置等属性控制访问权限。

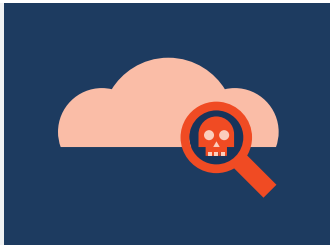
维持合规要求企业不但要洞察环境，而且要时刻掌控散落在各个角落的敏感数据。这包括云应用程序中共享文档的数据，即使是未经 IT 部门批准的员工采用的应用程序（所谓的影子 IT）。CASB 功能可保护与公有云应用程序交互的数据，例如 Office 365。

准确识别在用的应用程序

深入了解各种云应用程序和服务中的用户活动，并强制实施粒度内容和基于上下文的策略。持续监控云应用程序使用情况并在共享敏感数据时深入检测。确保员工遵守云使用政策。

评估云应用程序风险

检查员工在用的每个云的数十种属性。识别并实时拦截有风险的活动、恶意行为或恶意软件威胁，保护信息安全。



控制云应用程序访问权限

根据云属性数据按用户、组、位置和更多指标设置访问权限和控制策略。识别并分类关键合规相关数据，监控数据在云应用程序中的上传、下载或共享方式。

第 5 章

统一安全策略管理，兼顾简便性和一致性

跨本地环境和云环境快速定义和实施策略，适应快速变化的法规要求和企业要求。

直面现实，更改安全基础架构从操作层面上来说可能非常复杂。如果您没有提前计划，最终会出现需要不同策略的云和本地平台，并且您将无法维护两个独立的系统。选择一款可在本地和云中部署类似功能，且可以通过一套策略管理两个平台的解决方案，可大大简化您的管理。如果您要完全迁移至云，则不妨寻找一款可让您一键将现有安全策略迁移至云网络安全服务的解决方案。

简化迁移到云安全方案的流程

指定要自动迁移到基于云的新安全方案的内部部署策略。

创建并管理高度一致的策略

定义一次即可制定新策略，然后推送至全部安全网关，并在混合的本地和云安全环境中实行高度一致的策略实施。

最大限度利用现有投资

充分发挥现有的安全系统优势。利用对 DLP 的投资，但现在可将其扩展至云。如果可以的话，将本地 SWG 留在主数据中心，但将分支机构和移动用户迁移至云。通过单一管理控制台管理任何环境，无论是私有、公有、物理、虚拟还是云，亦或任何环境的混合。

第 6 章

结论：没有边界？无需担心！基于云的网络安全方案带来牢不可破的防护

赛门铁克基于云的 Web Security Service 以高性能的全球云服务，通过强大的企业级安全功能全面保护中央位置、分支机构、远程和漫游用户以及无处不在的公司数据。

无可匹敌的网络安全功能

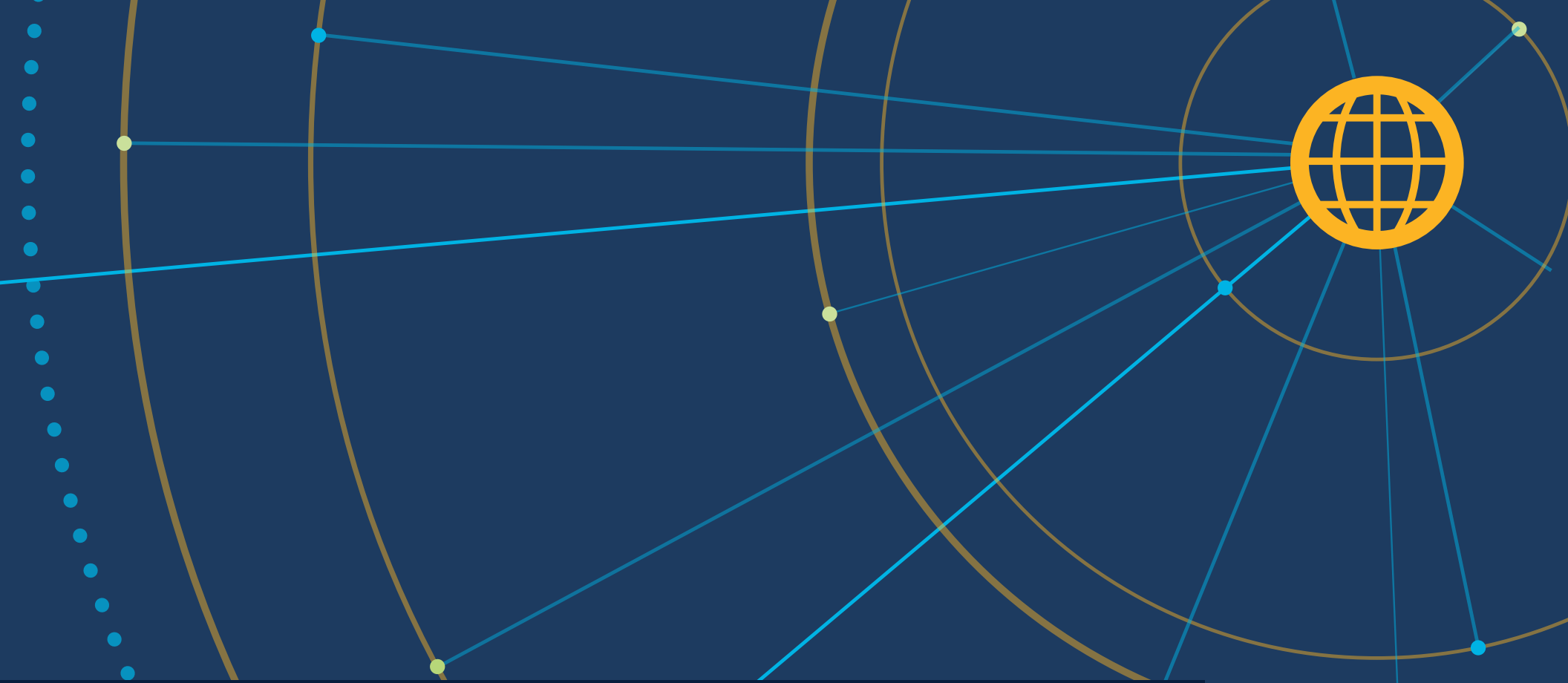
基于云的 Web Security Service 采用与 Symantec ProxySG 相同的高级代理技术，这是连续 11 年在 Gartner“Web 安全网关”魔力象限中荣列领导者象限的产品。这是完整网络安全方案堆栈的基础：高级 Web 安全网络作为核心，融入恶意软件分析、沙盒检测、Web 隔离、云应用程序控制（又称 CASB）、数据泄露防护、集成式 SD-WAN 等功能，所有这些功能都采用独一无二的威胁情报，确定员工试图访问的网站是否存在风险。

全球云网络：可靠的性能

在分布式且极具韧性的全球云数据中心基础架构的支持下，我们可以交付 99.999% 的运行时间 SLA。我们优化了性能，例如与 Microsoft、Amazon、Google 等平台的网络对等连接，同时 TCP 窗口优化可在大文件在云存储应用程序之间移动时加快处理速度。

集成式保护，深度简化您的运行

我们认识到，您还需要在端点上部署安全解决方案。这正是我们将屡获殊荣的 Symantec Endpoint Protection (SEP) 与 Web Security Service 相集成的原因。产品组合运行时，您即可减少要在端点上安装和管理的代理。SEP 可配置为将网络通信路由至 Web Security Service，这样即可实施网络安全策略。这就形成了赛门铁克独一无二的端点和网络深度防御服务，旨在保证您的用户在无边界的环境中安全无虞。



如需了解更多信息，请访问
symantec.com/zh/cn/products/web-and-cloud-security

关于赛门铁克

赛门铁克公司（纳斯达克：SYMC）是全球领先的网络安全企业，旨在帮助个人、企业和政府机构保护无处不在的重要数据安全。全球企业都青睐选用赛门铁克的战略性集成式解决方案，在端点、云和基础架构抵御复杂攻击。同时，全球 5000 多万的个人和家庭也在使用赛门铁克的 Norton 和 LifeLock 产品，保护家庭各类联网设备安全，畅享无忧数字生活。赛门铁克经营的在全球规模数一数二的威胁情报网络，能够发现和抵御最高级威胁。如欲了解其他信息，请访问 www.symantec.com.cn 或通过 weibo.com/SymantecChina 联系我们。

赛门铁克中国地区办事处 | 北京 电话:(010)58746999 | 上海 电话:(021)60377266
广州 电话:(020)28017160 | 安全产品售后技术支持热线: 800 810 3992 | www.symantec.com

19C210137_SB_VANISHING_PERIMETER_CN