Akamai

购买指南

如何选择基于云的安全 Web 网关

保护远程员工队伍并简化企业安全功能

目录

保护现代企业：
重新思考数据中心回传

云计算、软件即服务 (SaaS)、移动性和更新的网络架构已经彻底革新了业务实践。但这些技术也给 IT 团队制造了一个巨大的难题 - 他们试图保护员工队伍的安全，与此同时还要充分发掘这些新技术带来的价值。如今，企业面临新的挑战：对于许多企业而言，无论它们在数字化转型中处于什么阶段，它们都必须迅速进行调整，以应对 2020 年远程用户的急剧增加。

安全 Web 网关是用于保护企业员工的一种重要工具，但许多企业仍在使用部署在数据中心内的物理设备。这种硬件需要持续的管理、维护和升级，并且它们使用复杂的流量回传来检查和控制 Web 流量 - 这最终会降低性能。

企业需要采用现代化的优化策略来保护它们如今面对的全新分布式企业环境。解决方案：摒弃硬件设备，将安全 Web 网关功能转移到云端。

本买家指南介绍了基于云的安全 Web 网关的优势，以及现代 Web 网关技术需要具备哪些功能。

远程办公的普及催生了新的 IT 和安全需求

在过去十年中，企业的远程员工人数在稳步增加。这种趋势在新冠疫情影响下有所加快，并且预计在疫情后仍会延续。Gartner 发现，74% 的受访 CFO 在疫情结束后会将至少 5% 的原现场办公员工永久转移到远程岗位上。[1]

与此同时，网络钓鱼、勒索软件、恶意软件等复杂定向攻击的数量也急剧上升。在最近的一项调查中，53% 的受访者表示，自新冠疫情开始以来，他们目睹网络钓鱼活动出现增长。[2] 美国财政部最近的一份咨询报告指出，在新冠疫情期间，勒索软件索要付款的情况发生增长，因为网络攻击者将人们赖以正常开展业务的在线系统作为攻击目标。[3]

过去，企业会在数据中心安装安全设备（比如安全 Web 网关），以保证其主要办公地点和分支机构的现场办公用户和远程员工安全访问互联网。然后，他们将所有 Web 流量回传到该中心位置，以执行检查和控制。

企业借助这些安全 Web 网关，从用户发起的 Web 流量中过滤不必要的恶意软件，防止用户访问恶意网站，以及执行公司政策和监管政策。

这些网关解决方案最初针对现场办公环境设计和部署，在此环境中，大多数员工会在办公桌旁使用由企业管理的设备。但是，随着远程办公用户和分支机构用户数量增加，更多流量流向公共互联网以访问 SaaS 应用程序，企业开始在中央数据中心安装多个冗余的安全 Web 网关，以维持令人满意的性能。采购和管理这些设备的过程变得越来越复杂，成本越来越高，且耗费的时间越来越多。

> **“过去几年，数据中心预算在 IT 预算中的比例有所下降，现在只占总预算的 17%。”**
>
> - Gartner，《2019 年 IT 关键指标数据》

或者，企业也可能在其分支机构增设安全 Web 网关设备，并且将所有远程用户的流量回传。这种冗余导致了额外的设备泛滥和随之而来的成本，并且需要耗费大量人力去执行部署和管理。

在众多地点维持一致的安全策略也变得越来越困难。即使企业部署了虚拟化设备以减少设备蔓延，他们仍然不得不部署和管理额外的硬件。

第三种方法是混合部署，即：企业继续为主要办公地点使用本地安全 Web 网关，并将分支机构的 Web 流量发送到基于云的安全 Web 网关，并且仍然为远程员工回传流量。这种方法保留了现有的本地设备硬件投资。然而这会增加复杂性，因为企业最终需要管理不同的系统。额外的设备和增加的管理负担不仅导致了比单纯的云端方案高昂得多的成本，而且很难在本地和云系统之间维持一致的策略。

> **Gartner 预测，到 2025 年，80% 的企业将关闭传统的数据中心。[4]**

更糟糕的是，即使企业采用了这些越来越复杂的解决方案，他们也开始面临网络安全资源的匮乏问题。(ISC)[2] 的一项研究发现，要填补美国目前在安全人员方面的短缺，安全人员数量需要增加 62%。[5]

为什么要使用基于云的安全 Web 网关?

企业需要一种现代化的 Web 安全策略 - 与企业的云战略匹配，从而支持并实现远程工作模式。基于云的安全 Web 网关为企业带来了出色的安全性，同时降低了复杂性，因为它可以直接连接到互联网，从而无需部署多台设备，也无需执行回传。

通过基于云的安全 Web 网关，企业可以从以下方面受益：

降低安全复杂性：由于采用云服务的形式，这些安全 Web 网关无需部署硬件或虚拟设备，也无需配置、管理和每三年更换/升级一次硬件。

尽量减少性能瓶颈：基于互联网的安全 Web 网关无需增加额外的设备，即可应对增加的 Web 流量负载和不断增多的加密流量。客户可以根据需求添加额外的服务，同时尽可能减少对性能的影响。

减少昂贵的流量回传/绕行：基于云的安全 Web 网关无需回传流量即可为 Web 流量提供保护，它允许直接连接到互联网，从而降低了多协议标签交换的网络成本。

提高安全团队效率：由于云安全 Web 网关不需要对硬件或软件进行持续维护，因此，稀缺的安全人员有更多的时间去关注其他主动安全措施。

一致的安全策略：企业可以使用集中进行管理、在全球范围内部署的策略——适用于从任何设备发起连接的所有用户。即使企业对不同的区域设置了不同的策略，也可以使用相同的 UI 来管理所有策略。

安全 Web 网关的关键要求

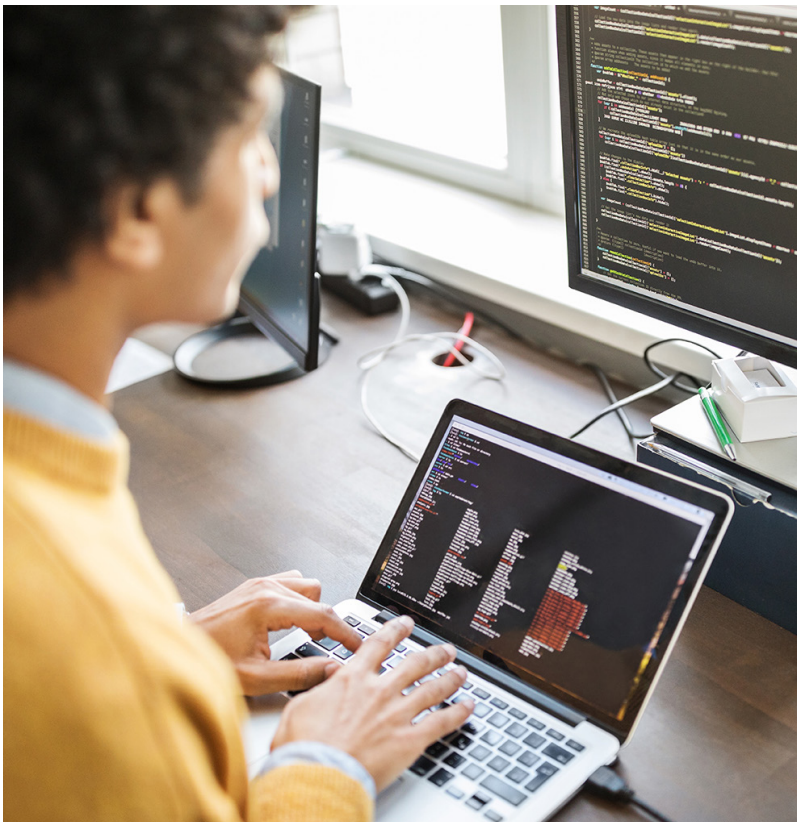
在选择基于云的安全 Web 网关时，必须认识到，安全性是关键要求。许多传统的安全 Web 网关包含多余的功能，用于解决如今已经不复存在的老问题。例如，它们包含带宽控制功能，这种功能适用于过去带宽成本高昂的时代。或者，它们可阻止员工在工作时间访问 YouTube 或 Facebook。如今，这些功能已经没有存在的必要，因为带宽十分充足，而且很多人都在使用他们的移动设备，因此企业根本不必费心在企业设备上禁止这些服务。

如今的企业需要基于云的安全 Web 网关，以专门处理现代安全问题。尤其是，该解决方案应采用纵深防御策略，通过多种安全措施来提供高水平的保护。这种策略应涵盖网络安全的方方面面，并提供完备的安全措施。这样一来，哪怕一道防线被攻破，仍有额外的防御层存在，以阻止攻击渗透到企业内部。这种分层策略可确保更早、更快地阻止恶意软件、勒索软件以及网络钓鱼等威胁，并在用户的设备遭到入侵之前阻止这些威胁。

部署了纵深防御策略的安全 Web 网关应提供以下安全功能：

对所有 DNS 请求和 URL 请求的评估

基于云的安全 Web 网关解决方案应根据实时威胁情报评估所有 URL 和 DNS 请求，并在击杀链中及早



阻止恶意请求。如果安全 Web 网关能够在建立出站连接之前阻止威胁，那么，Web 资源就不需要打开或检查任何返回的内容。这种高效处理避免了计算密集型流程，减少了安全 Web 网关在有效负载阶段必须分析的流量。结果如何？安全 Web 网关的整体性能得以提升。

威胁情报应可抵御恶意软件、勒索软件、网络钓鱼和基于 DNS 的低吞吐量数据渗透。它还应针对性地提供最新且相关的保护，并提供低误报率。

多种有效负载分析技术

由于每种威胁都各不相同，没有任何一种检测技术或方法可以应对所有类型的恶意软件，因此，安全 Web 网关解决方案应包含多种恶意软件分析引擎。这些引擎应使用各种识别技术（包括签名、无签名、机器学习和沙盒），以内联或离线的方式扫描 HTTP 和 HTTPS 有效负载。这种分析将针对潜在的恶意文件（比如可执行文件和文档文件）提供全面的零日威胁防护。

零日网络钓鱼检测

自新冠疫情爆发以来，远程员工持续面临越来越多的网络钓鱼攻击。恶意攻击者通过电子邮件、社交媒体和即时通信应用程序，以及通过在线文件共享和协作渠道发起这些攻击，以窃取企业凭据并借此进入企业网络。进入企业网络之后，攻击者可以横向移动，以寻找和渗透数据及知识产权，或传播勒索软件活动。

为了识别和阻止对网络钓鱼页面的访问，大多数安全供应商采取了以下措施：

1. 观察访问某个域的异常流量

2. 分析该域

3. 判断它是否是网络钓鱼域

4. 将其添加到阻止列表中

5. 向客户推送阻止列表更新

这个过程可能需要几个小时。更糟糕的是，如今的网络犯罪分子可利用网络钓鱼套件轻松创建并发起短期攻击，使得检测变得更加困难。在被攻击方发现网络钓鱼域或 URL 之时，攻击已经结束。事实上，网络钓鱼攻击越是复杂和有针对性，其持续时间就越短。

尽管这些攻击活动可能很快就会结束，但先进的零日网络钓鱼检测引擎仍能识别和阻止它们。在网络钓鱼页面的代码中，可以看到这些基于套件的攻击中反复出现的元素。利用这些信息，可以确定这些页面的“指纹”，从而实现精准识别。

安全 Web 网关解决方案应包含一个零日网络钓鱼检测引擎，该引擎可以分析请求的网页，并将这些网页与以前看到的网络钓鱼页面的“指纹”进行比较。

加密流量检查

互联网是一个天生就不安全的数据传输渠道。因此，如今 Web 流量加密无处不在，以阻止意图窃听、实施伪造或篡改流量的攻击者。传输层安全 (TLS) 是用于提供安全 Web 浏览的事实加密标准。TLS 在两个端点（比如客户端浏览器和 Web 服务器）之间建立一个安全隧道。

> **互联网上加密 Web 流量的比例在稳步上升，从 2014 年的 50% 左右增加到了现在的 80% 到 90% 之间。世界排名前 100 位的网站中，大部分 (96%) 都默认使用 HTTPS。**
>
> —《Google 透明度报告》，2020 年

但并非所有 HTTPS 流量都是良性的。攻击者和恶意软件编写者也使用加密来隐藏他们的活动，防止用户访问文件（借助勒索软件），以及保护恶意网络通信。最近的一项研究发现，近四分之一的恶意软件在建立互联网连接时使用 TLS 进行通信。[6]

为了主动检查和控制 HTTPS Web 流量，必须使用代理服务器（可信的中间设备）查看安全隧道内部情况，并检查加密流量。代理服务器应将 HTTPS 流量解密成纯文本，对其执行分析，重新加密流量，然后使用名为“中间机 (MITM)”的技术创建另一个安全连接。MITM 可检查请求的 URL（以判断它们是安全还是恶意），监测 TLS 加密流量，并保护企业免受威胁，同时还可保护源站流量的机密性和完整性。

MITM 检查需要充足的处理能力。因此，Web 浏览会因延迟而变慢。安全 Web 网关应提供可提高应用程序性能的服务。它应包括一个由服务器和智能软件组成的全球分布式网络，该网络位于靠近用户和全球数据中心的地方，以实现 Web 优化，进而提高应用程序性能和可用性。

此外，MITM 应检查云安全 Web 网关供应商是否维护了一个集中的域和 URL 列表，这些域和 URL 不能正常工作，应予以绕过。此外，对于特定类型的敏感 Web 内容（比如金融服务和医疗保健领域的敏感内容），云安全 Web 网关应能绕过 MITM 检查。

集成数据丢失防范

考虑到潜在的财务或声誉损失，必须主动防止个人身份信息 (PII) 和其他机密业务数据出现丢失。云安全 Web 网关应包括易于配置和可快速部署的集成数据丢失预防功能。频繁更新的字典应涵盖数据隐私和保护法规，比如 PII、PCI-DSS 和 HIPAA，同时，企业应能轻松创建自定义字典。

影子 IT 的识别和管理

用户可以轻松在托管设备上下载、安装和使用数十万种应用程序，而企业安全团队对此毫不知情。但使用未经批准的应用程序会大幅扩大企业的攻击面，使风险状况出现恶化。

> **一般公司使用超过 1295 个应用程序和云服务。由于没有 IT 管理权限，其中 95% 以上处于非受管状态。**
>
> — Cybersecurity Insiders，《云安全报告》，2019 年

云安全 Web 网关应能识别用户正在使用哪些应用程序，检测有多少用户安装了特定的应用程序，并突出显示可能存在潜在严重安全风险的应用程序。一旦完成识别，该解决方案应能阻止整个应用程序或特定的应用程序操作（例如，允许上传，但不允许下载）。

为任意设备随时随地提供保护

工作方式的灵活性在过去十年中呈现大幅上升趋势。现在，用户可以在任何地方使用任何设备开展工作。而且，由于疫情期间在家办公，企业有 59% 的最终用户计算正在转向移动设备，移动设备已经成为 PC 和笔记本电脑的有力补充，有些时候甚至会取而代之。据预测，即使在恢复办公室办公后，这种转变也会继续。[7]

向移动设备的迁移和 Wi-Fi 网络的使用增加会给所有企业的安全态势带来漏洞。企业需要能够在不影响设备性能的情况下，应用统一、通用的安全防护。

云安全 Web 网关应在用户加入的任何网络上，主动识别、阻止和缓解任意设备（iOS、Android OS、Chrome OS）上遭遇的定向威胁，比如恶意软件、勒索软件、网络钓鱼、DNS 数据渗透和零日攻击。该网关解决方案应在全球范围内提供无处不在的控制和优化的管理，同时帮助设备维持出色性能。

安全访问所有企业应用程序

云安全 Web 网关可以保护用户和设备在访问公共互联网时免受恶意软件的侵害。但这只是企业面临的安全难题之一。

要为整个企业创建一个整体式安全策略，企业还需要保护企业拥有和管理的应用程序 - 无论它们是驻留在企业数据中心内还是 IaaS 环境中，使其免受恶意攻击者的侵害。传统的网络安全工具可以保护网络防御层，但如果攻击者突破了网络防御层（例如，通过窃取用户凭据或在用户设备上安装恶意软件），他们就可以在网络内部自由移动。

企业网络钓鱼攻击呈上升趋势

观察到的攻击数量（2020 年 3 月至 10 月期间）

64%

攻击事件增加

（针对企业）

17%

攻击事件增加

（针对消费者）

来源：Akamai Enterprise Threat Protector 安全 Web 网关

企业需要适当的云安全 Web 网关 - 这种网关还能提供 Zero Trust 网络访问 (ZTNA) 技术来保护企业应用程序。ZTNA 是 Zero Trust 安全方案的一个重要组成部分，它可根据用户身份，只授予用户对特定应用程序（而不是整个网络或网段）的访问权限。该解决方案通过与身份和访问管理、多重身份验证 (MFA) 和单点登录技术的集成，为用户身份提供保护。通过使用 ZTNA 工具，企业可以消除以下操作的复杂性：安全管理设备，或维护复杂的广域网或虚拟专用网络连接。正确完成身份验证后，只允许用户访问他们需要的应用程序和数据，从而将应用程序攻击面缩减为 0，并尽可能减小用户出现横向移动的风险。企业在评估云安全 Web 网关时，应考虑供应商的 ZTNA 服务的功能。该服务能否提供对现代 Web 应用程序和传统非 Web 应用程序的访问？该服务能否与企业现有的身份提供商服务集成？它是否支持 MFA?

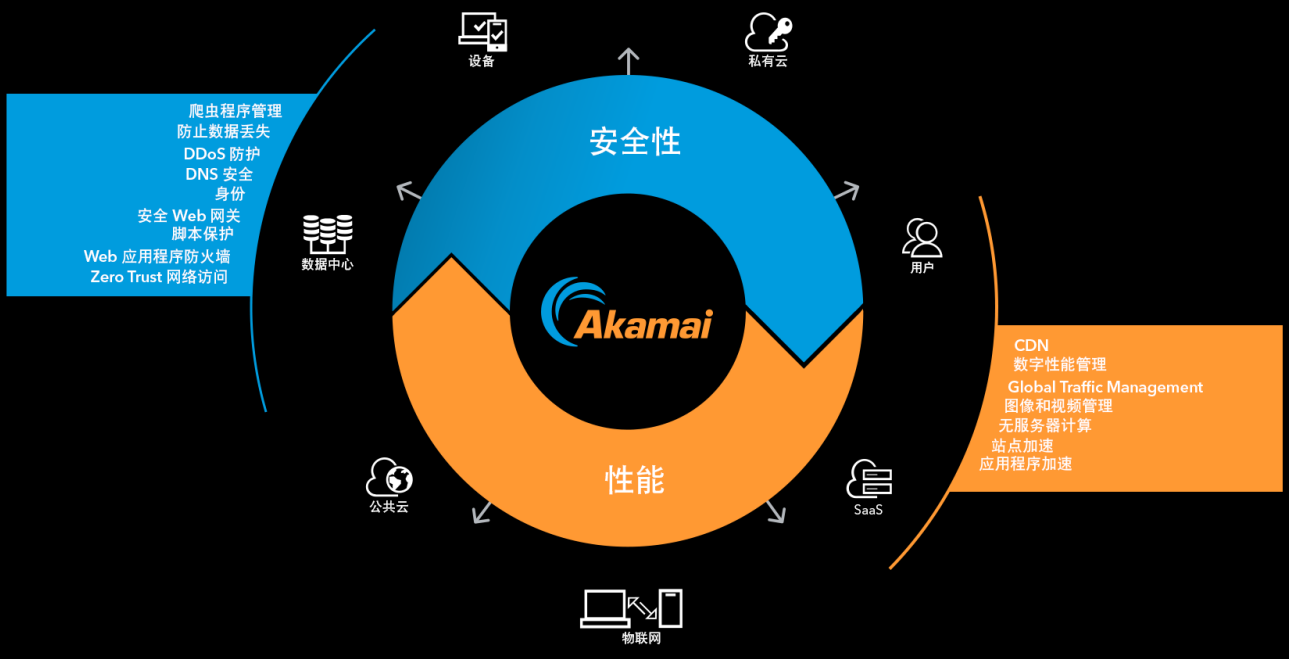
安全 Web 网关应与 ZTNA 服务集成并进行协作，这样一来，如果发现某台设备遭到入侵，就可以阻止该设备访问任何企业应用程序。安全 Web 网关的日志可以对其他威胁信号形成补充，从而更准确地揭示设备的安全态势。例如，如果设备正在调用命令和控制服务器，该解决方案应将此操作视为信号，以限制应用程序访问，直到设备完成安全修复为止。

通过添加安全 Web 网关和 ZTNA 功能，企业向采用安全访问服务边缘 (SASE) 框架迈进了一步。SASE 使得企业安全举措的侧重点不再是以数据中心为主导和硬件设备为主导的安全架构，毕竟这种架构已经不再适用于当今高度分布式的工作和业务环境。与此不同，SASE 根据用户和/或设备的身份提供基于策略的访问。SASE 还提供广泛的附加安全控制手段，包括 Web 应用程序防火墙、API 安全性、爬虫程序管理，以及为面向 Web 的应用程序提供的分布式拒绝服务攻击防护。

> **ZTNA 改善了应用程序访问的灵活性、敏捷性和可扩展性，使数字化业务得以蓬勃发展，而无需将内部应用程序直接暴露给互联网，从而降低了遭受攻击的风险。**
>
> - Gartner，《Zero Trust 网络访问的市场指南》，作者：Steve Riley、Neil MacDonald、Lawrence Orans，2020 年 6 月 8 日

此外，在 SASE 平台上提供安全控制措施，离用户只有一个互联网跃点的距离，可向用户、设备和云服务随时随地提供低延迟的访问。

Akamai 云交付 SASE



优化的性能

虽然安全性至关重要，但不能为此牺牲性能并进而对用户体验造成负面影响。除了提供纵深防御安全策略外，基于云的安全 Web 网关还应在不导致延迟的情况下提供上述服务。

为了避免延迟，云安全 Web 网关应在全球范围内部署，并在靠近所有用户联网位置的地方设置入网点。毕竟，用一种回传代替另一种回传的意义不大。

云平台还应具备快速扩展能力，哪怕在高峰期，也要避免影响最终用户的体验。在检查 HTTPS 流量时，这种能力尤为重要，因为 HTTPS 流量正在激增，并将最终构成几乎所有 Web 流量。在检查加密流量的同时，要尽可能减小对最终用户的影响，这一点至关重要，因为如今的绝大多数恶意软件都通过 HTTPS 交付。该平台还应提供 100% 可用性 SLA。

> 有 81% 的企业已过渡到云服务，而在这些企业中，Office 365 用户如今占总用户数的一半以上。[8]

Office 365 集成：必须确保 Microsoft Office 365 具备较高的安全水平和性能，这一点尤为重要，因为许多企业都依赖其服务作为基本的高效工作套件。部署云安全 Web 网关时会面临一个挑战：当用户通过转发代理（执行 TLS MITM 检查）访问 O365 的应用程序时，O365 与许多其他热门的 SaaS 应用程序一样，都会出现性能不佳的问题。

为了避免影响 O365 的性能，必须通过满足以下条件的全球边缘平台交付云安全 Web 网关：

- 使用请求的源 IP 将请求定向到地理位置最近的 Microsoft O365 数据中心，而不是使用回传 DNS 解决方案，将请求定向到离公司 DNS 解析器最近的数据中心；例如，用户从新加坡访问 O365，但被路由到位于纽约的 O365 服务器，这将产生糟糕的用户体验
- 确保安全 Web 网关服务器的位置位于靠近 Microsoft O365 数据中心的地方——并且，这些服务器和数据中心最好已相互连接
- 提供一键式 O365 流量优化设置，该设置使用 Microsoft 发布和更新的 O365 域和 IP 地址列表；对这些域的请求应按照 Microsoft 的建议直接发送到 O365 服务器，这样一来，当 Microsoft 添加新的域或 IP 地址时，用户无需手动更新防火墙和其他安全产品，从而节省时间和精力

将安全功能移到边缘

快速增长的远程员工队伍越来越容易受到网络攻击，而网络攻击也变得越来越频繁和严重。基于云的优秀安全 Web 网关解决方案将专门侧重于通过提供成熟的纵深防御功能来满足这些现代安全需求。它们还可随时随地为所有用户的互联网访问提供保护，从而支持 Zero Trust 和 SASE 等现代企业安全模型。

全面的云安全 Web 网关应评估所有 DNS 和 URL 请求、提供多种有效负载分析技术、解决零日网络钓鱼问题、检查加密流量、集成数据丢失防范功能、识别和管理影子 IT，并为任何设备提供无处不在的保护 - 与此同时提供高水平的性能，并与企业应用程序安全技术集成。借助此类解决方案，企业可以降低安全复杂性，消除昂贵的回传，提高安全团队效率，并支持一致的安全策略。

要详细了解 Akamai 基于云的安全 Web 网关 Secure Internet Access 并开始免费试用，请访问 akamai.com。

1. https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2
2. https://www.helpnetsecurity.com/2020/09/02/phishing-attacks-pandemic/
3. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf
4. https://blogs.gartner.com/david_cappuccio/2018/07/26/the-data-center-is-dead/
5. https://www.brinknews.com/a-global-shortage-of-cybersecurity-professionals-leaves-businesses-at-risk/
6. https://news.sophos.com/en-us/2020/02/18/nearly-a-quarter-of-malware-now-communicates-using-tls/
7. https://www.mobolize.com/2020/10/29/mobolize-announces-technology-partnership-with-akamai-to-enable-security-on-mobile-devices/
8. https://blog.goptg.com/microsoft-office-365-statistics#:~:text=According%20to%20Bitglass%2C%20usage%20of,the%20shift%20to%20cloud%20services

Akamai

Akamai 支持并保护网络生活。全球各大优秀公司纷纷选择 Akamai 来打造并提供安全的数字化体验，为数十亿人每天的生活、工作和娱乐提供助力。我们横跨云端和边缘的计算平台在全球广泛分布，不仅能让客户轻松开发和运行应用程序，而且还能让体验更贴近用户，帮助用户远离威胁。如需详细了解 Akamai 的安全、计算及交付解决方案，请访问 akamai.com 和 akamai.com/blog，或者扫描下方二维码，关注我们的微信公众号。发布时间：2022 年 6 月。

扫码关注，获取最新CDN前沿资讯