CLOUDFLARE

白皮书

简化我们保护 SaaS 应用的方式

如何 Zero Trust 方法保护用户和数据

内容

简介

在当今的分布式环境中，软件即服务（SaaS）应用为组织提供了更大的灵活性，以支持世界各地的企业员工和承包商。目前最著名的 SaaS 应用套件包括通信（电子邮件传输、聊天平台）、生产力（文档、电子表格）和协作（在线存储）。Gartner 预测，到 2025 年，85% 的企业将以云第一的原则运营其业务——以 SaaS 作为访问管理部署的首选工具[1]。

虽然 SaaS 应用让组织更灵活，但转移到云带来相关的安全和性能风险，尤其是在组织同时使用多个旨在独立运作的点解决方案时。安全、网络和 IT 团队肩负着实施和管理数十个乃至数百个应用的重任，时间上往往捉襟见肘，难以获得对整个组织的可见性，还要努力解决非原生设计为协同工作的服务造成的安全和连接漏洞。

因此，许多组织都在寻求更好的方式来整合其 SaaS 领域的安全产品——以改善效率，降低管理和实现的复杂性，并获得统一的支持。

Garner 预测，到 2025 年，80% 的企业将转向单一供应商的解决方案，其中将来自安全服务边缘（SSE）平台的 Web、云服务和专用应用访问统一起来[2]。

开始简化 SaaS 安全之旅需要考虑几个重要的因素。当今的员工队伍沟通和操作的方式需要一种简单的、可扩展的安全方法，这种方法旨在领先于新兴风险，减少来自 SaaS 应用程序的事件，并使安全团队更容易监控和预防对其组织的威胁。

继续阅读，以了解集成云访问安全代理（CASB）和云电子邮件安全（CES）能力的 Zero Trust 平台如何提供一种最简单的方式，阻止数据丢失、网络钓鱼、勒索软件、影子 IT 和横向移动。

[1] Gartner，“预测分析：全球信息安全与风险管理。”分析师：Shailendra Upadhyay，Mark Driver，Christian Canales，Ruggero Contu，Lawrence Pingree，Elizabeth Kim，John A. Wheeler，Nat Smith，Rahul Yadav，Swati Rakheja，Dave Messett，Mark Wah，Shawn Eftink。2021 年 8 月 12 日。Gartner。
[2] Gartner，“2022 年预测：统一的安全平台才是未来。”分析师：Charlie Winckless，Joerg Fritsch，Peter Firstbrook，Neil MacDonald，Brian Lowans。2021 年 12 月 1 日。Gartner。

CASB 的演变

全面的 SaaS 安全要求几种关键技术，以便安全团队能获得对整个 SaaS 环境的可见性，轻松监测和缓解威胁，并保护对敏感数据和系统的访问。任何 SaaS 安全策略最重要的组成部分之一是云访问安全代理（CASB），为组织的云托管服务和应用提供数据安全控制和可见性。

SaaS 安全 101：CASB

CASB SaaS 允许 IT 和安全团队从单一仪表板查看其所有数据设置和用户活动。其能力因供应商而异，但通常包括如下属性[1]：

- **数据保护：**CASB 保护敏感数据，防止其离开公司控制的系统。
- **访问控制：**CASB 帮助控制用户在公司控制的应用中可以看到的内容和可以进行的操作。CASB 也可提供身份验证能力，以确保用户是他们所声称的身份。
- **影子 IT 检测：**CASB 帮助识别员工用于业务目的的未经授权的系统和服务（通常称为“影子 IT”）。通过对这些系统进行编目，他们可以检测和减轻以前未知的安全风险。
- **威胁检测：**CASB 使用反恶意软件检测、沙箱、包检测和其他技术来帮助阻止数据泄露和外部攻击。
- **态势管理：**CASB 为安全团队提供有关用户行为分析和应用态势控制的洞察，以便轻松地调查移动和跟踪 SaaS 环境中的威胁。
- **合规：**通过识别错误配置来帮助组织满足法规要求（例如 SOC 2、HIPAA、GDPR 等），从而避免违反法规的相关处罚和罚款。

[3] 这并非 CASB 产品可能包含之功能的详尽列表。

理解现代 CASB 挑战

随着 SaaS 采用增加，组织需要保护的攻击面也在扩大。不同于以往使用单一数据库来储存有价值的数据，目前数据分散到第三方管理的各种应用中（例如 Dropbox、Google Drive 等），无论这些应用是否被企业使用沙箱隔离以供使用。

虽然 CASB 有助于在 SaaS 应用程序中保护企业数据和用户，但其仍然不能完美地对付所有威胁。由于企业使用 SaaS 应用处理更多有价值的数据，攻击者日益瞄准这些应用，从而造成数据泄露和其他威胁。简单的配置错误和用户错误也会向这些攻击敞开大门：

Gartner 预测，到 2025 年，超过 99% 的云入侵都将源于可预防的配置错误或用户造成的错误[4]。

在预测和补救用户配置错误和现代 SaaS 攻击方面，很多 CASB 依然力有不逮。为了解决这个问题，一些供应商已经开始提供云或 SaaS 安全态势管理（CSPM 或 SSPM[5]）服务。此类服务旨在跟踪控制平面上的配置和合规错误。然而，这种做法还没有普及，致使很多组织缺乏所需的检测和补救能力。

此外，一些 CASB 产品未能在数据泄露前加以识别，导致安全团队落后于攻击者，增加了补救成本和数据损失。

[4] Gartner，“2021 年云安全技术成熟度曲线。”分析师：Tom Croll，Jay Heiser。2021 年 7 月 27 日。Gartner。
[5] 这些服务和特性通常与 CASB 产品一起提供，或者更常见的是，作为 CASB 产品的一部分提供——为应用程序提供内联和基于 API 的保护。

CASB 实施和集成的问题

随着 SaaS 供应商加强其内置安全产品的功能，两大障碍仍然存在：集成和可见性。这些供应商使数据易于访问和使用，但仍然给组织带来了以易于管理的方式巩固安全能力的负担。对于采用多个点解决方案的组织来说，当这些解决方案没有设计成相互集成或具有不同级别的可见性时，跟踪跨不同平台的威胁就会变得更加困难。

这增加了应用环境的复杂性，以至于即使是最基本的攻击也变得更难预测和缓解——因为攻击者只需要识别安全平台之间的漏洞，就可以在不被发现的情况下进行攻击。通过 CASB，组织可从同一地方访问安全产品，对整个安全堆栈获得更佳的可见性和缓解能力。

即使如此，CASB 也只是更大的 SaaS 安全策略的一部分。为了覆盖完整的 SaaS 领域，组织需要将 CASB 功能与其他 Zero Trust 技术融为一体，而不增加不必要的复杂性，也不迫使安全团队手动配置和维护每个工具。成功地大规模控制 SaaS 不能是一个人工的过程——需要通过自动化来补充 SaaS 管理平台和 CASB 工具，使组织能够有效地缓解各种威胁，而不会有团队负担过重或用户配置不当和错误的风险。

电子邮件安全的演变

与大多数 SaaS 服务一样，电子邮件通信已经发展成为各种规模组织的基本业务应用。随着向云计算和远程办公的转变，越来越多组织转向 Microsoft 365 和 Google Workspace 中的云电子邮件解决方案——根据 Gartner 的数据，全球多达 70% 的组织正在使用云电子邮件解决方案[6]。

因此，电子邮件现在是最广泛采用的 SaaS 应用，并构成了最大的攻击面之一——吸引网络钓鱼、恶意软件、欺诈、商业电子邮件入侵（BEC）和其他现代威胁。

然而，对安全团队来说，防范电子邮件攻击可能是一项乏味而艰巨的任务，在攻击者继续使用更复杂的手段来对付毫无戒心的员工时更是如此。为了保护用户和数据免受这些威胁，安全主管应该考虑将电子邮件集成到他们的 SaaS 安全平台上，以增加可见性，并提供更健壮和简化的保护。

SaaS 安全 101：电子邮件安全

现代电子邮件安全包括一组工具、过程和技术，用于保护电子邮件帐户和内容，防范恶意攻击和未经授权的访问。以下是一些最常见的电子邮件安全技术：

- **安全电子邮件网关（SEG）：** SEG 处理和过滤 SMTP 通信，并要求组织更改其 MX 记录以指向其邮件传输代理。
- **云电子邮件安全（CES）：** CES 分析电子邮件内容（通过对云电子邮件提供商的 API 访问，）而不需要更改 MX 记录。（注：Gartner 将这一类别称为“ICES”，即“集成 CES”。）
- **基于域的邮件身份验证报告和一致性 （DMARC）：** DMARC 通过检查域的 SPF （发件人策略框架）和 DKIM （域名密钥识别邮件)记录来对邮件进行认证。在这个系统中，没有通过 SPF 或 DKIM 检查的电子邮件被标记为垃圾邮件或被阻止到达预期收件人。
- **电子邮件数据保护（EDP）：** EDP 解决方案使用加密，以帮助防止意外数据丢失和对电子邮件内容的未经授权访问。

[6]Gartner，“电子邮件安全市场指南。” 分析师：Mark Harris，Peter Firstbrook，Ravisha Chugh，Mario de Boer。2021 年 10 月 7 日。Gartner。

了解现代电子邮件安全挑战

电子邮件最初是通过本地软件平台发送的，但现在越来越多地转向云原生的发送系统。许多组织已经转向功能丰富的生产力套件，如 Microsoft 365 和 Google Workspace，它们让用户更有效地工作和协作。

由于电子邮件已经存在了很长一段时间，即使是普通用户也意识到他们可能通过电子邮件遇到的一些更普遍的威胁——包括可疑电子邮件、恶意链接等等。因此，攻击者已经发展了策略，使合法和恶意消息更难识别。这些混合的威胁通过多个通信渠道，以显得更合法（例如，电话钓鱼，短信钓鱼等），往往能成功地欺骗用户提供敏感信息。

电子邮件使用量的增加也让企业面临被入侵的风险：一旦攻击者获得了某个电子邮件帐户的权限，他们往往能轻易在企业内部横向移动，并破坏或窃取敏感数据。虽然云电子邮件供应商提供有限的内置安全功能，旨在缓解常见的威胁，如垃圾邮件、恶意软件和网络钓鱼，但在应付遭入侵的内部发件人在收件箱之间进行横向移动，这些内置安全功能几乎无济于事。

为了对抗这些威胁，电子邮件安全解决方案也在不断发展。本地云电子邮件平台提供了基本的内置安全功能，可以处理常见的垃圾邮件和恶意软件攻击。

Gartner 估计，到 2023 年，至少 40% 的组织将依赖于这种内置保护，而非采用 SEG 那样的独立工具[7]。

许多组织选择通过放弃 SEG 来简化他们的电子邮件安全对战，转而寻找阻止高级钓鱼和 BEC 攻击的安全产品，同时通过 API 与他们的云电子邮件环境紧密集成。Gartner 估计，到 2023 年，20% 的反钓鱼解决方案将通过与电子邮件平台集成的 API 交付[8]。

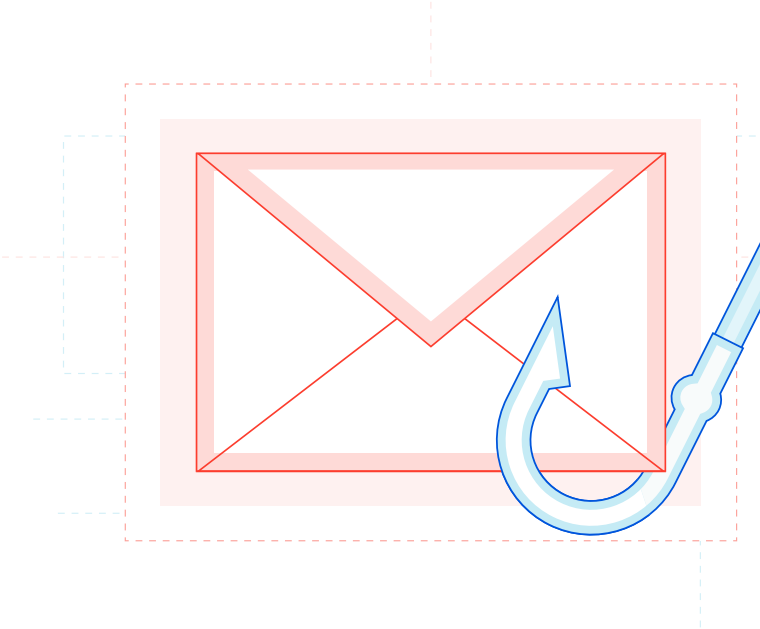
[7]Gartner，“电子邮件安全市场指南。” 分析师：Mark Harris，Peter Firstbrook，Ravisha Chugh，Mario de Boer。2021 年 10 月 7 日。Gartner。[8]Gartner，“电子邮件安全市场指南。”

电子邮件安全实施与集成的问题

虽然这些内置功能让组织稍为安心，但它们远远不足以对抗现代电子邮件威胁。所有类型的攻击——比如鱼叉式网络钓鱼、BEC 等等——都需要专门的安全平台，而这些平台是电子邮件提供商所不提供的。传统的电子邮件安全解决方案在设计上无法实现规模化、应对云原生挑战或拦截高度针对性的攻击。

即使安全团队精确定位旨在捕捉现代威胁的电子邮件安全工具，他们仍可能会遇到额外的问题：复杂的配置要求、耗时的部署过程和繁琐的策略维护挑战。例如，众所周知，部署 SEG 产品来对抗电子邮件攻击极其困难，因为拦截每一种攻击变体需要维护不断加长的策略列表，这是不可行（不可扩展）的。检测高级攻击需要大规模使用只有云原生服务才能处理的算法。

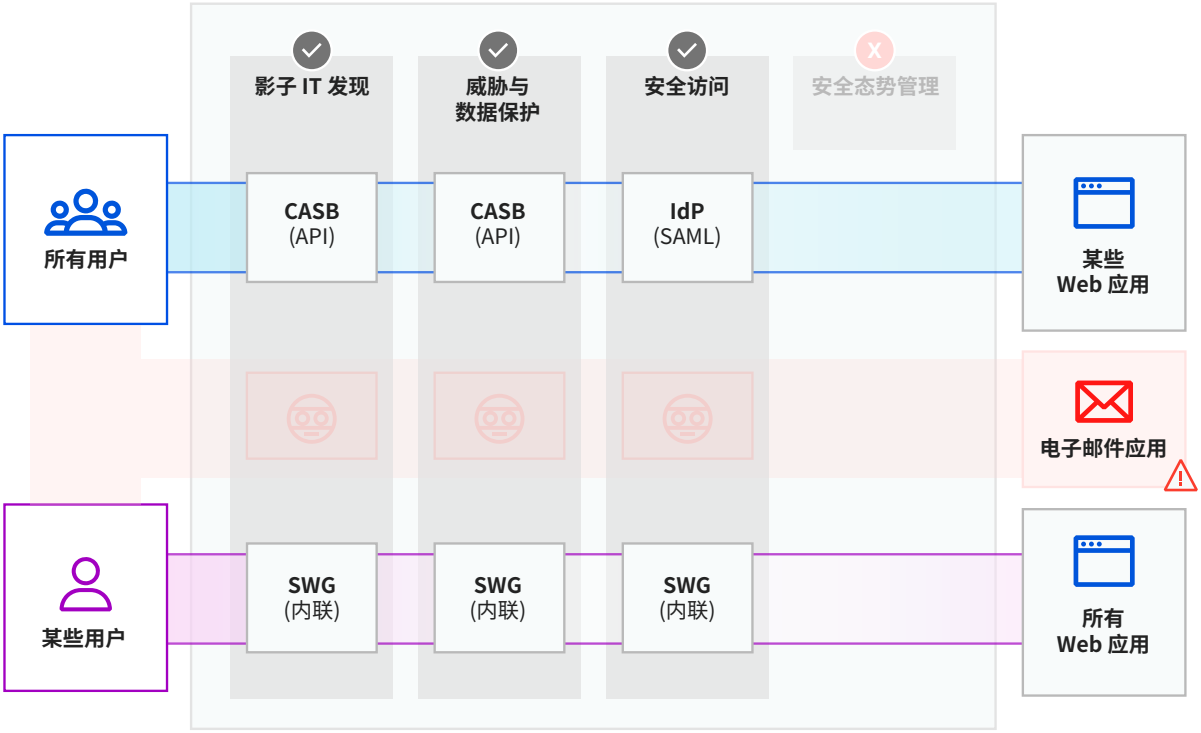
为了保护企业电子邮件系统免受这些攻击——既不使安全团队带来负担过重，不需多层使用传统硬件产品，也不需要依赖员工来捕捉每一条恶意消息——企业需要一种 Zero Trust 方法，其中集成了云原生的电子邮件安全功能，减少了对电子邮件通信的隐式信任。



实现 SaaS 安全的更佳方式

从通信平台到电子邮件传输系统，SaaS 应用程序构成了当今商业运营的相当大一部分。然而，保护这些应用免受日益复杂的威胁对安全团队来说可能是一场噩梦，他们常常被要求使用的多种工具并非旨在相互原生集成，也不能提供对组织整个 SaaS 环境的可见性。

传统 SaaS 安全

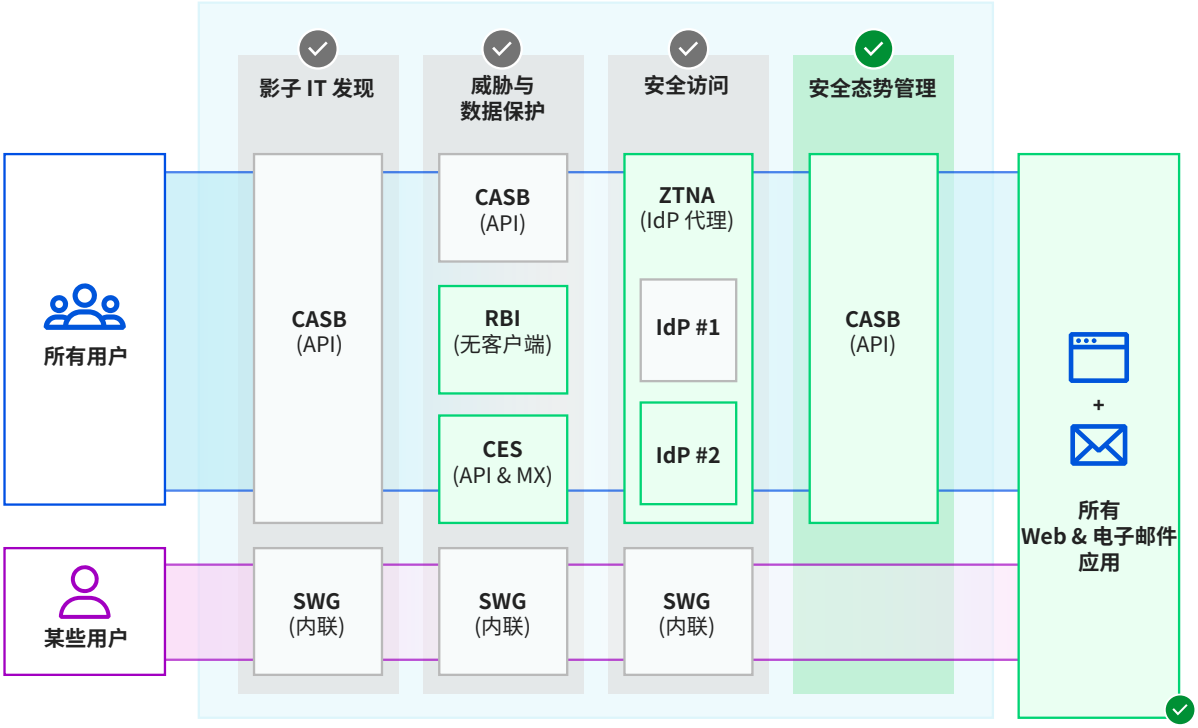


SWG = 安全 Web 网关 | CASB = 云访问安全代理 | IdP = 身份提供商

随着供应商打造出更健壮的 SaaS 安全工具，IT 和安全团队的任务是将这些一流的解决方案整合在一起，以保护他们的应用和数据。这往往需要相当多的时间和内部资源来实施和管理——而且，虽然点解决方案能够解决个别层面上的威胁，但缺乏一个总体平台提供多供应商支持和对整个组织的可见性。

通常情况下，传统的 SaaS 安全措施也不能完全将其保护扩展到电子邮件平台，导致组织很容易受到复制关键业务流程、冒充可信合作伙伴和用户的针对性攻击，并且很容易绕过现有的电子邮件分类系统和内置控制。如果没有这些解决方案之间的本地集成——或者对整个威胁环境的可见性——保护应用免受现代威胁就会给安全团队留下更多需要弥补的缺口。

现代 SaaS 安全



SWG = 安全 Web 网关 | CASB = 云访问安全代理 | IdP = 身份提供商 | RBI = 远程浏览器隔离
CES = 云电子邮件安全 | ZTNA =Zero Trust 网络访问

为了弥补传统 SaaS 安全和管理解决方案留下的漏洞，组织需要现代威胁保护，旨在从单一互联网原生平台保护应用和数据。这种现代方法的一个关键组件是健壮的安全态势管理，它允许安全团队更好地确定用户如何访问关键资源，并获得对外部和内部威胁的可见性和控制。

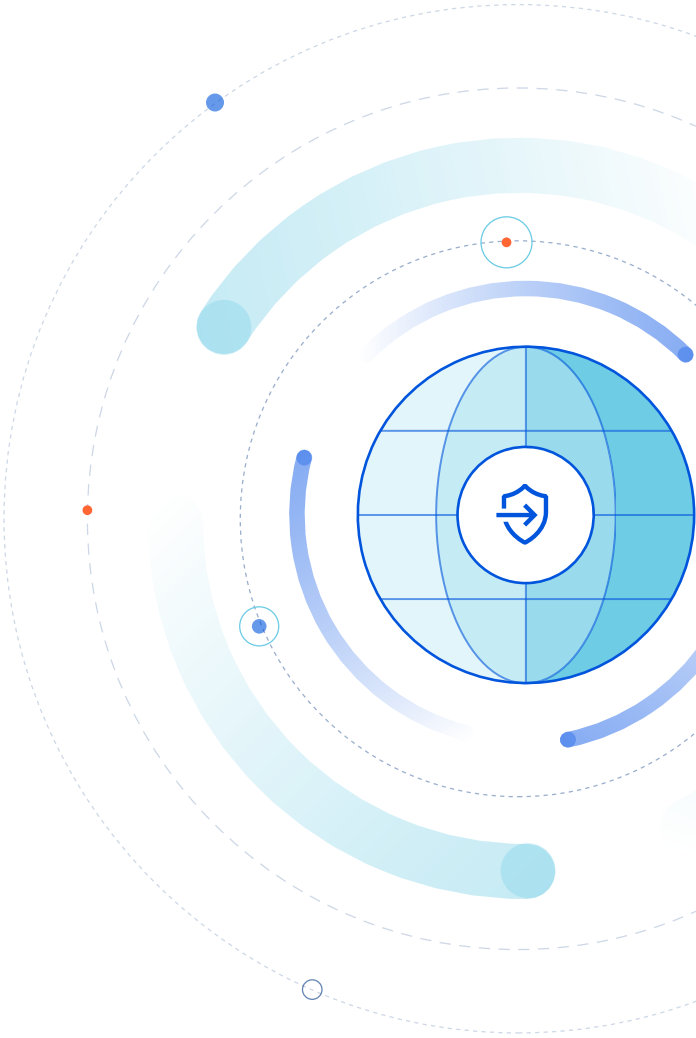
SaaS 安全平台并不要求组织使用单一解决方案工具来修复单个威胁，而是扫描应用程序，检测配置、权限和共享中的异常，然后让安全团队管理应用程序访问、缓解电子邮件攻击、阻止内部威胁和高风险数据共享，等等。

这种方法不仅为 SaaS 应用程序提供了更健壮、更全面的保护，还能为组织节省分类工单的时间、自动化安全流程，并专注于战略计划，而不必担心数据泄漏和攻击，也无需费心进行手动配置和维护。

以 Zero Trust 方式实现 SaaS 安全

开发正确的 SaaS 安全方法需要对现代 SaaS 和基于云的威胁有全面的了解，但是，对 IT 和安全团队来说，根据组织的需求定制现有的解决方案可能是一项艰巨的任务。组织机构需要一个简化、易于管理、能够预测和缓解现代威胁的安全平台，而不是在个别层面上抗击威胁，或者依赖于各种独立工具的东拼西凑。

虽然 CASB 和云电子邮件安全功能都是 SaaS 安全策略的重要组成部分，但它们在 Zero Trust 体系结构中工作得最好——其中，每项技术协同使用都胜于单独运行。如能正确实施，这种分层还有助于通过消除安全差距、节省安全团队带宽和自动化威胁监视来帮助缓解相邻的问题。



Cloudflare 如何保护 SaaS 应用

Cloudflare 为保护整个 SaaS 环境提供了最简单的途径，允许组织控制用户如何访问关键资源，如何保护这些资源免受外部或内部攻击，以及如何实时监控和降低风险。

*加入我们的 DLP 等候名单

使用 Cloudflare Zero Trust 保护 SaaS 应用

为了确保传输中数据的安全，Cloudflare Zero Trust 在云和 SaaS 应用程序前放置访问（ZTNA）、网关（SWG）和浏览器隔离（RBI）控制，作为内联 CASB 部署架构提供支持和运行。

为了保护 SaaS 应用静态数据的安全，易于配置的 API 驱动集成持续扫描高使用率应用，以检测漏洞和潜在威胁。

将 Cloudflare Area 1 电子邮件安全与 Cloudflare Zero Trust 结合起来

Cloudflare Area 1 电子邮件安全是具有代表性的 ICES 供应商，可根据组织的电子邮件安全需求为其提供更高的灵活性。其做法是通过 API 集成，更改 MX 记录来充当网关，以便以内联方式验证、过滤、检查和隔离电子邮件流量。

Area 1 主动扫描互联网，以识别攻击基础设施和网络钓鱼活动，从而提前数天预防钓鱼攻击和保护收件箱。

如需进一步了解 Cloudflare 如何帮助保护 SaaS 应用，
请访问 https://www.cloudflare.com/zh-cn/products/zero-trust。

来源

1. Gartner，“预测分析：全球信息安全与风险管理。”分析师：Shailendra Upadhyay，Mark Driver，Christian Canales，Ruggero Contu，Lawrence Pingree，Elizabeth Kim，John A. Wheeler，Nat Smith，Rahul Yadav，Swati Rakheja，Dave Messett，Mark Wah，Shawn Eftink。2021 年 8 月 12 日 Gartner。

2. Gartner，“2022 年预测：整合安全平台才是未来。”分析师：Charlie Winckless，Joerg Fritsch，Peter Firstbrook，Neil MacDonald，Brian Lowans。2021 年 12 月 1 日 Gartner。

4. Gartner，“2021 年云安全成熟度曲线。”分析师：Tom Croll，Jay Heiser。2021 年 7 月 27 日 Gartner。

6. Gartner，“电子邮件安全市场指南。”分析师：Mark Harris，Peter Firstbrook，Ravisha Chugh，Mario de Boer。2021 年 10 月 7 日 Gartner。

7. Gartner，“电子邮件安全市场指南。”分析师：Mark Harris，Peter Firstbrook，Ravisha Chugh，Mario de Boer。2021 年 10 月 7 日 Gartner。

8. Gartner，“电子邮件安全市场指南。”分析师：Mark Harris，Peter Firstbrook，Ravisha Chugh，Mario de Boer。2021 年 10 月 7 日 Gartner。

010 8524 1783 | enterprise@cloudflare.com | www.cloudflare.com

REV:BDES-3303.2022JUN24