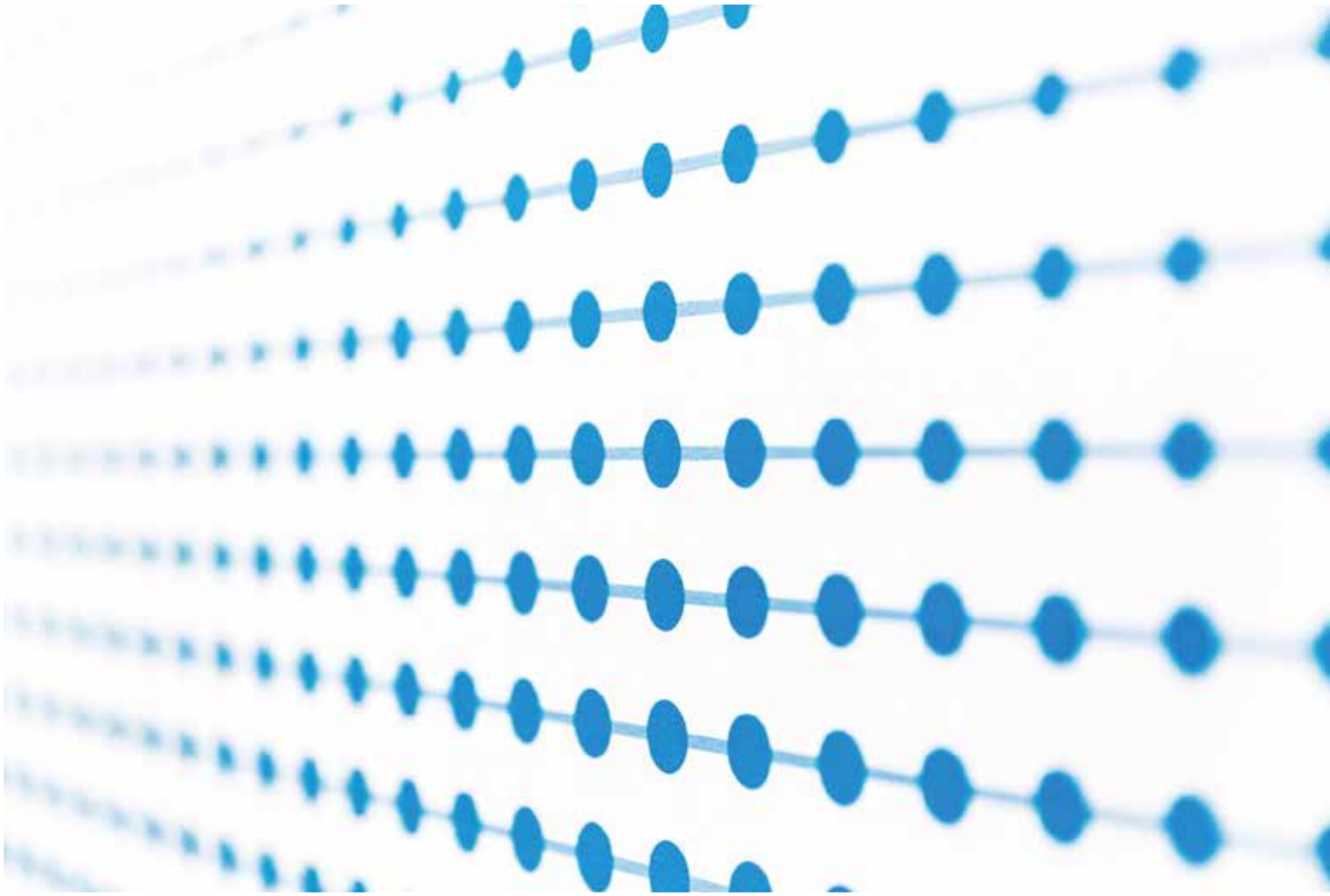
Google Cloud 白皮书
2021 年 2 月

使用 BeyondCorp Enterprise 安全访问 SaaS 应用程序



Google Cloud

目录

免责声明

本白皮书适用于 cloud.google.com 上描述的 Google Cloud Platform 产品。此处包含的内容截至 2021 年 2 月是正确的，并代表截至其撰写时的现状。随着我们不断改进对客户的保护，Google 的安全政策和系统可能会在未来发生变化。

引言

由于 COVID-19 大流行，74% 的公司计划永久转向以远程的方式工作。在远程工作已成为新常态的时代，确保用户安全并确保他们能够适当地访问数据对于企业 IT 领导者来说变得比以往任何时候都更加重要。普通企业的员工使用超过 400 个 SaaS 应用程序，或者可能多达 1,800 个影子 IT SaaS 应用程序，IT 和安全管理员面临着不断增长的保护环境。事实上，在最近的一项研究中，84% 的 IT 领导者表示，当员工在家工作时，数据丢失防护更具挑战性。

通过将我们最好的安全技术与零信任产品相结合，Google 可以帮助组织的员工通过任何网络从几乎任何设备以简单、安全、可靠地的方式访问 SaaS 应用程序，而不必担心恶意软件、网络钓鱼或数据丢失等威胁。

BeyondCorp Enterprise，是 Google 的零信任产品，提供对应用程序和云资源的简单安全访问，并提供集成的威胁和数据保护，包括允许用户执行以下操作的关键安全功能：

- 管理访问基于 SAML 的应用程序的因素如设备和用户信任
- 在访问应用程序和数据时防止有意或意外的数据泄露
- 防止不受信任的网站窃取企业信息
- 防止凭据泄漏到网络钓鱼站点或未经批准的应用程序
- 防止恶意软件通过 SaaS 应用程序传输
- 通过包含应用程序的安全性来阻止跨网络的横向移动

这些功能与 Chrome 浏览器完全集成，不需要额外的代理或破解 SSL 的代理。

用例

企业 IT 领导者正在寻找能够保护他们的员工和扩展员工访问 SaaS 应用程序的解决方案，无论是被批准的还是未经批准的。下面我们将概述 BeyondCorp Enterprise 支持的一些关键 SaaS 应用程序用例。

管理对经批准的 SaaS 应用程序的零信任访问

Google 自己的零信任实施 BeyondCorp 的基本原则是根据我们对用户和设备的了解授予对服务的访问权限。这意味着分配给单个用户和/或单个设备的信任级别是从各种属性动态推断的，这些属性包括用户身份、用户组、硬件、软件、策略、完整性、位置和其他类似标准。

Google 的上下文感知访问功能让您可以精细控制对 SaaS 应用程序的访问，包括 Google Workspace 和其他流行的 SaaS 应用程序，例如 Salesforce 或 Box。如果用户身份、位置、设备安全状态和 IP 地址等属性符合根据创建的访问策略设置的规则和标准，员工和扩展员工（包括承包商和供应商）可以访问支持 SAML 的应用程序。

例如，当您想要执行以下操作时，可以使用上下文感知访问策略：

- 仅允许从公司配发的设备访问应用程序。
- 仅当用户存储设备已处于加密状态时才允许访问云端硬盘。
- 限制从公司网络以外访问应用程序。

您还可以将多个条件组合到一个策略中。例如，您可以创建一个访问策略，要求设备为公司所有、加密并满足最低操作系统版本，以便访问某些应用程序。

用例

企业 IT 领导者正在寻找能够保护他们的员工和扩展员工访问 SaaS 应用程序的解决方案，无论是被批准的还是未经批准的。下面我们将概述 BeyondCorp Enterprise 支持的一些关键 SaaS 应用程序用例。

通过两步验证保护对 SaaS 应用程序的访问

所有 SaaS 应用程序都可以通过两步验证 (2SV) 进行保护，这在您的组织和试图窃取用户名和密码以访问敏感数据的网络犯罪分子之间设置了额外的障碍。 启用两步验证是您可以采取的最重要的一项措施来保护您的业务。 管理员可以启用 2SV 作为其员工访问某些 SaaS 应用程序的要求。

Google 的 2SV 功能支持多种验证方法，包括：

- 安全密钥 - 最安全的 2SV 形式是硬件安全密钥（我们推荐来自 Yubico 等全方位服务企业硬件提供商的密钥）或手机的内置安全密钥。安全密钥是防止网络钓鱼威胁的良好方法。
- Google 提示 - 用户可以将其 Android 或 Apple 移动设备设置为接收登录提示，然后在手机上点击通知以确认其身份。
- 验证码生成器 - 用户在硬件令牌上或通过移动设备上的 Google Authenticator 等应用程序生成一次性验证码。然后，用户输入代码以登录到他们的计算机和其他设备。
- 短信或电话 - Google 通过短信或语音电话向移动设备发送两步验证码。
- 备用验证码 - 如果用户没有移动设备或在无法携带移动设备的区域工作，他们可以提前生成备用验证码。

除了启用 2SV 访问 SaaS 应用程序外，管理员还可以设置上下文感知访问级别，在允许访问某些应用程序之前需要特定级别的身份验证强度。 例如，为了访问某些金融应用程序，管理员可以设置上下文感知策略，要求在授予访问权限之前使用硬件安全密钥对用户进行身份验证。

防止敏感数据从 SaaS 应用程序中泄露

保护敏感的个人信息，例如受保护的健康信息 (PHI) 或个人可识别信息 (PII)，不仅对我们的客户，而且对他们的最终用户而言都极为重要。 例如，《通用数据保护条例》(GDPR)和《加州消费者隐私法》(CCPA)等法律规定了处理个人数据的要求。

无论您的数据是在本地还是在云端，通过将云数据丢失防护(DLP)功能直接嵌入 Chrome 浏览器，BeyondCorp Enterprise 可以更好地控制敏感的个人信息，因为它在端点设备和应用程序之间传输。DLP 集成使用户能够控制可以共享哪些数据，包括可以上传或下载的敏感数据，或复制、粘贴、拖放或删除的内容。管理员还可以设置策略以阻止使用敏感信息（例如社会安全号码或信用卡号码）的操作。

Google 的 BeyondCorp Enterprise 数据保护功能包括：

- 文件上传、下载和内容粘贴保护
- 每个保护规则的实时警报
- 审核、警告和阻止操作
- 支持不同的文件格式，包括文档、图像文件类型、压缩/存档文件和自定义类型
- 数百个内置敏感数据检测器，及自定义正则表达式和列表
- 实施 URL 过滤器和完整内容检查等条件

防止不受信任的网站跨站信息窃取

我们的现代化无代理方法利用了 Chrome 浏览器及其众多安全功能。例如，Chrome 的站点隔离是一项默认启用且可供所有 Chrome 用户使用的安全功能，旨在通过将不同网站的页面分开来阻止不可信的网站访问或窃取通过浏览器访问的网站和 SaaS 应用程序的信息。与保护站点之间的同源策略相结合，此功能提供了多层防御，用以降低此类攻击成功的可能性。

站点隔离确保来自不同网站的页面总是被放入不同的进程中，每个进程都在一个沙箱中运行，该沙箱限制了允许该进程执行的操作。 它还可以阻止从其他站点传输某些类型的敏感数据。 因此，恶意网站会发现从其他网站窃取数据要困难得多，即使它可以在自己的进程中违反某些规则。

Chrome 浏览器中的以下行为使这种保护成为可能：

- 无论导航是在当前选项卡、新选项卡还是 iframe（即，一个嵌入在另一个网页中的网页），跨站点文档始终被放入不同的进程中。
- 跨站点数据（特别是 HTML、XML、JSON 和 PDF 文件）不会传递到网页的进程，除非服务器表示应该允许（使用跨域资源共享 (CORS)）。
- 浏览器进程中的安全检查可以检测并终止行为不端的渲染器进程。

检测和防止 SaaS 应用程序密码泄露和重用

使用被盗凭据是许多攻击中首先采用的策略之一。作为安全管理员，您需要确保员工和承包商没有使用以前泄露的凭据，并且不会意外地将他们的公司 SaaS 密码输入未经您的组织授权的危险网站。

当用户登录特定页面时，Chrome 可以执行两个特定操作。首先，Chrome 以保护隐私的方式检查输入的用户名和密码，与 Google 的泄露凭据数据库进行对比。如果用户输入的凭据已被公开泄露，则会警告用户。

其次，Chrome 会生成密码指纹或哈希，并将其缩短为 37 位，如果在危险或不允许的网站上重复使用，这足以识别密码。然后，Chrome 会使用操作系统级别的用户名（如果可用）对部分哈希进行加密。当用户在钓鱼网站或授权列表之外的网站上使用保存的密码时，Chrome 会向用户显示警告并提示他们更改密码。此外，如果用户在您不允许的网站上输入密码，您可以提示用户更改密码。

通过阻止这两个攻击媒介，BeyondCorp Enterprise 可以保护您的组织免受帐户受损，并确保您的用户在安全环境中访问敏感信息。

防止访问嵌入在电子邮件或应用程序内容中的网络钓鱼 URL

网络钓鱼是恶意攻击第一步中采取的首要行动，也是最重要的社会工程策略。根据 2020 年 Verizon 数据泄露调查报告，67%或更多的泄露事件中使用了网络钓鱼、社交攻击和使用被盗凭据。因此，IT 管理员确保用户不会访问嵌入在电子邮件中或在 SaaS 应用程序中共享的不安全 URL，这一点至关重要。

Google 的]技术保护全球数十亿台设备免受不安全 URL 访问，使其成为最大的威胁情报数据库之一。它还不断爬取互联网和网站来分析和识别新的网络钓鱼或恶意网站，并在识别出不安全的网站时实时更新数据库。

BeyondCorp Enterprise 利用此威胁情报数据库和不安全 Web 资源列表来提供实时安全检查，以确定 URL 属于恶意 URL 还是网络钓鱼 URL，以及该站点是否包含欺骗性内容或恶意软件。

防止恶意软件通过批准的应用程序进行转移和横向移动

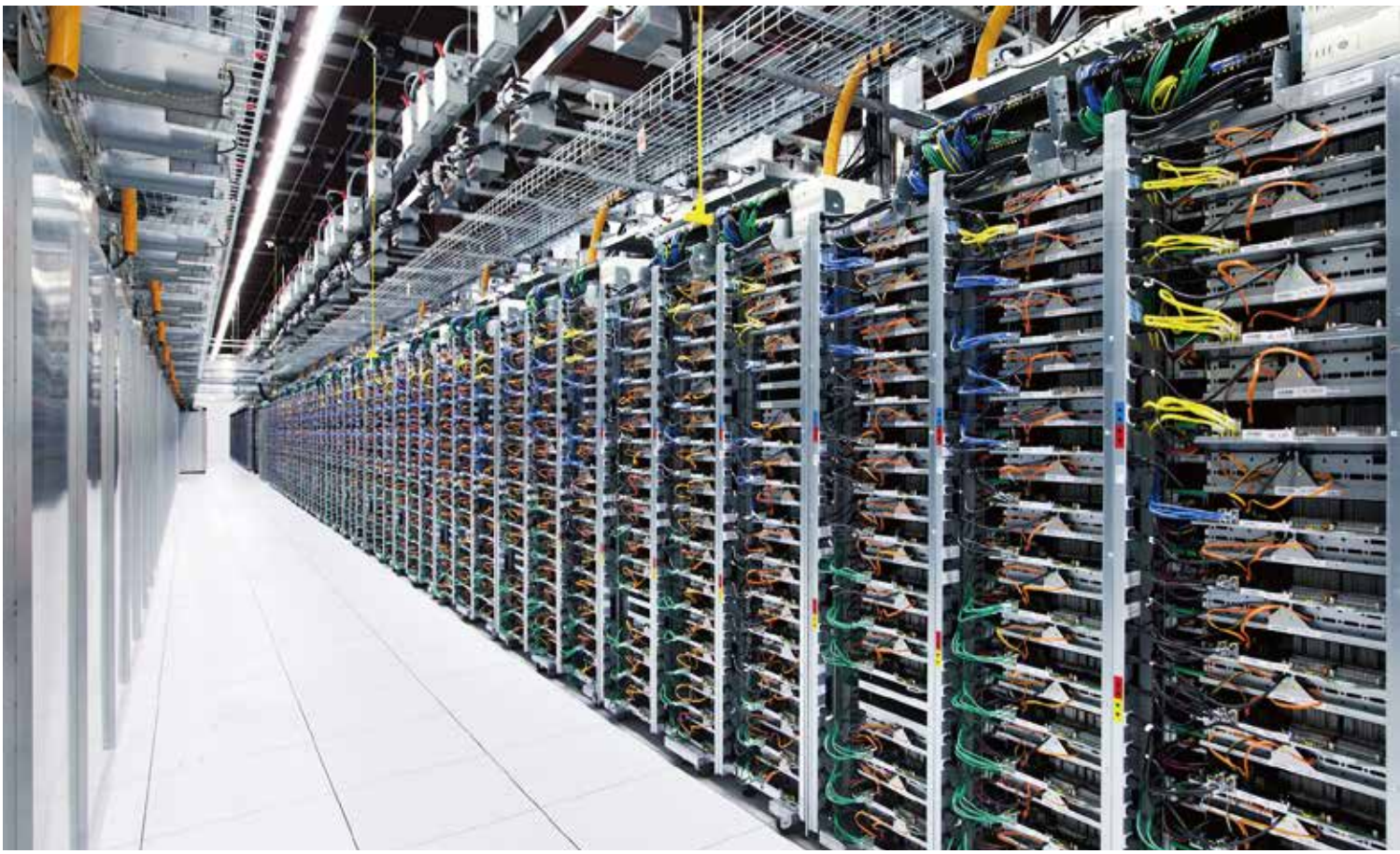
恶意软件或勒索软件的使用通常是恶意攻击第二步中采取的首要行动。根据 2020 年 Verizon 数据泄露调查报告（第一步通常是网络钓鱼或使用被盗凭据），17% 的成功泄露事件中也使用了恶意软件。

IT 和安全管理员必须确保任何 SaaS 保护解决方案都可以检查、检测和阻止所有上传或下载文件中的恶意软件和勒索软件。 这将最大限度地减少用户意外感染或传播恶意软件的机会。

BeyondCorp Enterprise 采用多阶段恶意软件防护架构，包括：

1. 信誉检查 - 使用 URL 信誉和签名匹配检查下载文件的网站的安全性
2. 静态分析 - 根据多个签名数据库和二进制字符串静态分析规则库检查签名以及文件内容
3. 云沙箱 - 使用先进技术引爆云沙箱中的文件，以观察恶意或可疑行为，例如文件加密活动

这些恶意软件防护功能支持 Windows 可执行文件、文档（例如 PDF、Office.docs）和存档文件，并且适用于所有主要桌面操作系统，包括 Windows、Mac、Linux 和 ChromeOS。



捕获和监控不安全或登录活动以进行调查取证

不安全用户活动的可见性是安全程序最关键的方面之一。您无法控制您看不到的东西。

因此，BeyondCorp Enterprise 为安全管理员提供详细的审计日志，以监控、审查和分析用户活动和行为。这些审核日志包括：

- 上下文感知访问审计日志，跟踪所有被拒绝的用户对应用程序的访问请求，以便管理员可以排除故障并确定根本原因。
- 威胁和数据保护审计日志，提供所有不安全活动的详细审计跟踪，例如恶意软件传输、不安全的站点访问、敏感数
- 据传输、密码重用或更改以及未扫描的内容。
- 数据保护规则审核日志，跟踪用户试图进行共享、下载、上传或粘贴敏感数据操作。
- 登录审核日志，用于跟踪用户登录事件，例如登录成功和失败、密码泄露和可疑登录。
- 设备审核日志，报告用于访问组织数据的计算机和移动设备上的活动，包括设备安全状况信息和密码策略违规。

此外，安全管理员可以利用安全中心调查工具来报告、汇总、过滤和分类收集到的安全事件。管理员可以使用预先构建的报告或创建自己的报告。预建报告包括：

- Chrome 威胁防护摘要 - 提供所有威胁类别以及各种计数的高级概览。目标是让分析师和高管快速了解整个威胁形势。
- Chrome 数据保护摘要 - 提供 DLP 事件的高级概览，以及前五大数据保护规则的事件数，并按触发的操作排列。
- 高风险用户 - 提供遇到过最多不安全 Chrome 相关事件的用户的概览。
- 高风险域 - 提供对组织风险最高的域的概述，按不安全尝试次数排名。

最后，由于许多组织使用集中式安全信息和事件管理 (SIEM) 解决方案来整合事件视图，Google 提供了不同的方式来导出安全事件以进行额外分析：

- 导出 API，允许管理员为上述审计日志检索特定客户帐户的活动列表。
- BigQuery 导出，允许管理员每天将特定的审核日志导出到 Google Cloud BigQuery 表。

结论

Google 的 BeyondCorp Enterprise 解决方案为企业提供零信任安全，结合 Google 的最佳安全技术，包括上下文感知访问，数据保护，网站隔离以及恶意软件，网络钓鱼和勒索软件预防，为您的员工和扩展员工提供用以访问 SaaS 应用程序的端到端安全环境。

开始使用

我们在概述用例中所反映的完整解决方案需要 BeyondCorp Enterprise，Google Workspace Enterprise Standard 或 Plus（或Cloud Identity Premium）和 Chrome（浏览器和/或Chrome OS）。

要了解如何使用 BeyondCorp Enterprise 管理对 Google Cloud 上、托管在其他云或本地的 SaaS 应用程序的访问，以及如何根据用户、设备和其他上下文因素定义和执行访问策略，请访问产品文档。

要立即开始，请执行这些步骤或与我们联系，与我们团队的人员交谈。