Forcepoint Data Loss Prevention

无边界环境中的数据保护

Forcepoint

手册

forcepoint.com/zh-hans

Forcepoint Data Loss Protection (DLP)

使用 Forcepoint 保护您的人工智能转型

世界各地的组织正在经历一场由人工智能（特别是基因人工智能应用程序和技术）集成到其业务流程中的变革之旅。虽然这有望大幅提高生产力，却也带来了新的数据安全挑战。例如，用户可以输入敏感数据或将机密文件上传到 GenAI 应用程序，这可能导致数据泄露。Forcepoint 提供一种解决方案，允许您利用人工智能的潜力，而不会损害您最有价值的资产：您的数据。

借助 Forcepoint，我们尖端的人工智能网格技术可确保无与伦比的数据分类准确度和效率。这能让您在应对人工智能转型的复杂问题时高枕无忧。无论您使用的是 ChatGPT、Copilot、Gemini 或其它 GenAI 应用程序，Forcepoint 都能提供集中式可视化和控制，在所有环境中保护您的敏感数据。

无论您的人员工作和数据所在何处，都能确保数据安全

Forcepoint DLP 可解决各种规模的组织所面临的关键数据安全挑战。随着监管要求的紧缩，保护个人身份信息（PII）和受保护的健康信息（PHI）等敏感信息变得至关重要。云应用程序、混合设置和自备设备趋势等现代工作环境使数据保护更加复杂。

不断扩大的攻击面需要全面的可见度和控制。Forcepoint DLP 通过管理跨主要渠道（端点、网络、云、web、私有应用程序和电子邮件）的全球策略，为数据安全团队提供支持。我们的预定义模板和分类器简化了事件管理，让您专注于生产力，同时最大限度地降低风险。无论您的员工工作和数据位于何处，Forcepoint DLP都能确保可见度和控制。

数据保护必须：

- 通过一个控制点来**保护受监管的数据**，适用于员工创建、存储和传 数据的所有应用程序。
- 使用先进的 DLP **保护敏感数据**，该 DLP 能分析人们如何使用数 据，指导员工正确处理数据，并根 据风险优先级处理事件。
- 通过实施强大的 DLP 控制和策略，**确保生成式** AI 的安全使用，以在所有位置和应用程序（从端点到 Web 和云）中保护其使用。

简化合规性

为数据保护赋能

高级检测和控制

响应和化解风险

安全使用 GenAI 应用程序

简化合规性

对于力求遵守众多全球数据安全法规的企业来说，现代 IT 环境存在艰巨的挑战，尤其是在采用云应用程序和移动劳动力时。很多安全解决方案提供某种形式的集成 DLP，例如 CASB 和 SWG 应用程序中的 DLP。

但是，当安全团队在端点、云应用程序和 Web 流量中部署并管理独立且不一致的 DLP 策略时，他们将面临复杂情况和附加成本。Forcepoint DLP 通过提供比任何其他主要供应商更多的立即可用的预定义分类器、策略和模板，加快您的合规性工作速度。初始 DLP 部署更加迅速，DLP 管理更加简单。

- → **监管覆盖范围**，使用超过1700个预定义模板、策略和分类器，轻松满足和维持90个国家和超过150个地区的合规要求。
- → 在所有渠道（包括云应用程序、Web、电子邮件和端点）**集中控制**并统一策略。

为数据保护赋能

只有预防性控制的 DLP 让用户感到头疼，他们有时会仅为完成一个任务而规避这些控制。绕过安全控制会造成不必要的风险和意外数据泄露。

Forcepoint DLP 认识到您的员工正处于当今网络威胁的最前线。

- → **发现和控制**无论是在云应用程序、Web 流量、电子邮件还是端点中的数据。
- → **使用自定义消息引导用户行为，让员工**了解策略，并在用户与关键数据交互时验证其意图，从而指导员工做出明智的决策。
- → 使用基于策略的自动加密技术，保护传输到企业外部的数据，从而与受信赖的合作伙伴进行**安全协作**。
- → 通过与 Forcepoint Data Classification 和 Microsoft Purview Information Protection 整合，实现**数据标记和分类自动化**。

跟踪数据的高级检测和控制

恶意和意外数据泄露是复杂事件，而非单一事件。Forcepoint DLP 被 Forrester、Radicati Group 和 Frost & Sullivan 认可为 DLP 解决方案行业领导者。其中一个关键功能是 Forcepoint DLP 能够识别静态、动态和使用中的数据。关键数据识别包括：

- → **光学字符识别 (OCR)**，识别嵌入图像中的静态或动态数据。
- → 对于个人身份信息 (PII) 的**强大识别**提供数据验证检查、真实姓名检测、接近性分析和上下文标识符。
- → **定制加密识别**暴露隐藏在发现和适用控制之外的数据。
- → **累积分析**用于滴漏式 DLP 检测（即随着时间缓慢泄露的数据）。
- → **更智能的执行机制**识别与数据交互相关的用户行为变化，例如个人电子邮件使用量的增加。借助风险自适应保护功能，Forcepoint DLP 利用行为分析来了解用户风险，进而依据用户风险等级实施自动化策略执行，这使得该系统变得更加高效。这使得安全团队能够实施动态策略，与静态的全局策略相比，这些策略是个性化的。

人工智能网格

释放人工智能的潜力，同时不损害企业最珍贵的资产：您的数据。借助 Forcepoint，我们尖端的人工智能网格技术可提供无与伦比的数据分类准确度和效率，让您高枕无忧。我们的集中式可视化和控制可保护您各处的数据，包括 ChatGPT、Copilot、Gemini 和其他许多 GenAI 应用程序。使您的团队安全使用 GenAI 和其他应用程序，从而提高工作效率。通过简化操作和统一策略来降低成本。

- → **与 Forcepoint 数据分类同步**，利用训练有素的人工智能网格和 LLM 模型，通过 Forcepoint 数据安全态势管理 (DSPM) 为使用中的数据和静态数据提供高精度分类。

识别、管理和纠正数据保护风险

大多数 DLP 解决方案缺乏强大的预定义分类库和对所有数据的敏感可见性，导致用户被错误报告所困扰，同时错过了处于风险中的数据。除了降低安全团队的效率之外，这也使得员工或最终用户感到沮丧，因为他们将安全解决方案视为对他们业务生产力的阻碍。通过利用分析技术以及业内最大的预构建模板和策略库，Forcepoint DLP 大幅减少了误报，这有助于提高安全操作的效率。为了提高员工的安全意识，DLP 支持员工培训并与数据分类解决方案集成。

- → 通过优先处理的事件，**让响应团队专注于**最大的风险，这些事件突出显示了负责风险的人员、处于风险中的关键数据，以及用户间常见的行为模式。
- → **员工培训**以弹出窗口的形式进行，可以个人化设置组织的名称，以简短说明弹出窗口的原因，以及用户可以点击的网址，以查找有关组织相关安全策略的更多信息。
- → 通过基于电子邮件的分布式事件工作流程，**使数据所有者和业务经理**能够审核和响应 DLP 事件。
- → 通过匿名化选项和访问控制来**保护用户隐私**。
- → 通过与 Forcepoint Risk-Adaptive Protection 的深度 成，将**数据的上下文添加**到更广泛的用户分析中。

实时防止数据泄露

数据泄露可能在瞬间发生，其后果无论是在经济上还是声誉上，代价都可能极为高昂。Forcepoint DLP 为您的组织提供工具，以便在数据泄露发生的瞬间识别并阻止它们，从而确保敏感数据的安全无虞。通过提供先进的实时防护和简化的管理，我们助力您的团队在不断演化的威胁面前始终领先一步。

- → **实时监控和阻止：**在敏感信息泄露之前，检测并阻止数据泄露事件的发生。
- → **统一策略管理：**借助单一控制台简化安全管理，以便在整个环境中为“数据安全无处不在”而管理各项策略。
- → **跨渠道事件可见性：**全面洞察 网络、云端、电子邮件和端点间数据的流动情况，以便对威胁做出快速响应。
- → **取证：**揭示数据流动的全貌，以调查事件、防范违规行为、强化策略并确保合规性。
- → **风险自适应保护：**根据用户行为和风险等级动态调整安全控制措施，确保敏感数据在得到保护的同时不影响工作效率。

随时随地实现数据可视化，包括云端和本地

当今的企业面临着复杂的环境挑战，数据无处不在，需要在企业无法管理或不拥有的地方保护数据。Forcepoint ONE Data Security for CASB 和 SWG 将分析和 DLP 策略扩展到关键云应用程序和 Web 流量，无论您的数据存放在何处，都可以得到保护。

- → 借助 Forcepoint ONE for Email 和 Forcepoint ONE for Endpoints，**专注于响应团队，以识别并保护**云应用程序、Web 以及电子邮件和端点中的数据。
- → **识别并自动阻止**对外部用户或未经授权的内部用户共享敏感数据。
- → 实时**保护数据**，包括上传和下载到关键的云应用程序，如 Office 365、Teams、SharePoint、OneDrive、Salesforce、Box、Dropbox、Google Apps、AWS、ServiceNow、Zoom、Slack等等 。
- → 通过单一的控制台**统一策略实施**，定义并应用数据在传输和数据发现策略，涵盖所有通道，包括云、网络、终端、Web和电子邮件。
- → **部署由 Forcepoint 托管的解决方案**，将 DLP 策略功能扩展到云应用程序，同时可以选择在您的数据中心内保留事件和取证数据。

了解有关 DLP 的更多信息

获取演示

Forcepoint 数据安全解决方案

Forcepoint ONE Data Security (DLP SaaS)	Forcepoint ONE 数据安全是一种云原生解决方案，可保护敏感数据、防止数据泄露并确保全球合规性。通过快速部署和策略管理，它可以简化数据保护。它可以在云应用程序、Web、电子邮件和端点中实现统一管理。通过 Forcepoint Risk-Adaptive Protection，它可以提供实时用户风险洞察。借助 Forcepoint ONE 数据安全，降低成本、风险并提高效率。
Forcepoint DSPM	Forcepoint DSPM 通过提供无与伦比的可见度和控制，应对跨云平台和服务器的数据扩散挑战。它使用人工智能网格技术来不断提高数据发现和分类精度。它还自动化了补救和报告等任务，以简化流程并降低成本。
Risk-Adaptive Protection	与传统的以政策为中心的 DLP 解决方案不同，我们的 Risk-Adaptive Protection (RAP) 将人员置于最前沿，了解行为以主动降低风险。RAP 优先考虑高风险用户，提供实时风险计算、130 多个行为指标和无摩擦部署。通过易于阅读的仪表板获得洞察力，通过细粒度的策略实施提高效率，并通过动态自动化主动降低内部威胁。
Forcepoint ONE Data Security for Email (DLP SaaS)	Forcepoint ONE Data Security for Email 可防止关键电子邮件渠道中的敏感数据泄露。这种完全云原生的解决方案通过端点和移动设备防止电子邮件泄露和数据泄露。与流行的电子邮件提供商无缝集成，通过预构建的安全策略、分类器和模板来简化管理。
Forcepoint ONE Data Security for Cloud Apps and Web (DLP SaaS)	Forcepoint ONE Data Security（面相云应用和网络）提供与Forcepoint One Data Security（面向端点）以及Forcepoint Data Security（面相电子邮件）相同的完全云原生数据丢失防护（DLP）解决方案，使您能够从单个用户界面管理4个渠道中的任意一个或全部，并从同一策略管理控制台同步所有策略。一次编写策略，并在所有 Forcepoint ONE Data Security渠道中部署，可节省在多个服务中同步策略的时间和资源。
Forcepoint Data Classification	Forcepoint 数据分类化通过人工智能网格实现精度和自动化，重新定义数据分类，消除手动错误并提高 DLP 效率。我们利用人工智能网格技术和大型语言模型来提供卓越的分类精度。通过不断学习和改进，它提供自信的建议，加强政策执行和合规性。无缝集成您的工作流程，提高生产力并减少误报。
Forcepoint DLP Endpoint	Forcepoint DLP Endpoint 保护您在企业网络内外的 Windows 和 Mac 端点上的关键数据。Forcepoint DLP – 终端 保护您存储在公司网络内外的 Windows 和 Mac 端点上的关键数据。它包括对静态（发现）、动态和使用中数据的高级防护和控制。它与 Microsoft Azure 信息保护集成，以分析加密数据并应用适当的 DLP 控制。它能让员工依据 DLP 指导对话中的指引，自行纠正数据风险问题。该解决方案监控 Web 上传，包括 HTTPS，以及上传到 Office 365 和 Box Enterprise 等云服务的操作。与 Outlook、Notes 和电子邮件客户端完全集成。
Forcepoint DLP Discover	Forcepoint DLP Discovery 现功能可识别并保护文件服务器、SharePoint(本地部署和云端)、Exchange（本地部署和云端）中的敏感数据，还能在诸如SQL Server 和 Oracle 等数据库中进行检测。先进的指纹识别技术能够识别静态状态下的受管制数据和知识产权，并通过应用适当的加密和控制来保护这些数据。Discovery 还包括 OCR 技术，可视化图片中的数据内容。
Forcepoint DLP Network	Forcepoint DLP Network 络提供关键的执行点，阻止通过电子邮件、网络渠道和文件传输协议（FTP）进行动态数据窃取行为。该解决方案帮助识别并防止数据泄露以及外部攻击或内部威胁导致的意外数据泄露。OCR 识别图像中的数据。分析提供滴漏式 DLP，以逐条停止数据的窃取，同时还可以识别其他高风险的用户行为。
Forcepoint DLP for Cloud Email	Forcepoint DLP for Cloud Email，阻止通过出境电子邮件泄露您的数据和IP。您可以与其他 Forcepoint DLP 通道解决方案（如端点、网络、云和 Web）相结合，以简化 DLP 管理，编写一个策略，并在多个渠道中部署该策略。Forcepoint DLP for Cloud Email 在无法预见的电子邮件流量爆发中实现了巨大的可扩展潜力。这也允许你的外发电子邮件流量随着业务的增长而增长，无需配置和管理额外的硬件资源。
Forcepoint DLP App Data Security API	Forcepoint DLP App Data Security API 使组织能够轻松地在其内部自定义应用程序和服务中保护数据。它支持对文件和数据流量进行分析，并强制执行 DLP 操作，例如允许、阻止、通过个性化弹出窗口请求确认、加密、取消共享和隔离。这是一个 REST API，易于理解且简单易用，无需经过广泛培训或了解复杂的协议。它也是语言无关的，可以在任何编程语言或平台上进行开发和使用。

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint 为全球企业和政府简化安全工作。Forcepoint 一体化的、真正的云原生平台使您能够轻松采用 Zero Trust，并防止敏感数据和知识产权被盗或丢失，无论工作地点在哪里。Forcepoint 总部位于德克萨斯州奥斯汀市，为150 多个国家的客户及其员工创建安全、可信的环境。在 www.forcepoint.com, Twitter 和 LinkedIn 上了解 Forcepoint。