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)

在员工工作和数据存放的每一个地方都实现数据安全

数据安全是当今各种类型和规模的组织面临的一个主要问题。一方面，IT组织需要遵守法规，保护个人身份信息（PII）、受保护的健康信息（PHI）以及其他类型的受规管信息，以免遭受针对性的恶意攻击和意外的数据泄露。另一方面，他们必须适应宏观 IT 趋势，比如采用云应用、混合云环境和 BYOD（自带设备）趋势，这些都增加了数据可能从组织泄露的方式。

这种不断扩大的攻击面对保护关键数据构成了最大的挑战。数据安全团队必须考虑数据从组织' 内部' 到数据现在所在和流动的所有地方和渠道的爆炸性增长。必须获得云端和本地所有数据的可见性。数据安全团队还必须通过单一管理点，在所有渠道（端点、网络流量、网络、电子邮件、云应用程序和私有应用程序）上实现可见性和控制。

Forcepoint DLP 作为业界最受信赖的解决方案，能够让您轻松地在各主要渠道（包括端点、网络、云、网页、私有应用程序和电子邮件）上管理全球政策，为您提供了必要的工具。在行业中，我们提供的预定义模板、策略和分类器数量超过任何其他 DLP 提供商，能够极大地简化您的工作流程。这样可以大大简化您处理事件的流程，让您集中精力处理最重要的事情，即消除风险，以便使您的团队工作效率更高。Forcepoint DLP 通过在您的员工工作的每个地方和您的数据所在的任何地方提供可见性和控制来应对风险。

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、存储和传输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。

保护重要渠道

- **自定义应用程序**
- **云应用程序**
- **私有应用程序**
- **端点**
- **网络**
- **发现**
- **Web**
- **电子邮件**

加速实现合规性

为数据保护赋能

高级检测和控制

响应和化解风险

加速实现合规性

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，例如云应用程序中的 DLP。

但是，当安全团队在端点、云应用程序和网络中部署并管理独立且不一致的策略时，他们将面临复杂情况和附加成本。Forcepoint DLP 提供超过 1600 个预定义分类器、策略和模板，让您快速完成合规工作。初始 DLP 部署更加迅速，DLP 管理更加简单。Forcepoint DLP 可有效保护敏感的客户信息和受监管的数据，让您自信地证明组织持续满足合规性要求。

- → **监管覆盖范围**，使用超过 1600 个预定义模板、策略和分类器，轻松满足和维持 83 个国家和超过 150 个地区的合规要求。
- → 使用网络、云和端点发现**查找和修复**受监管的数据。
- → 在所有渠道（包括云、端点、网络、Web 和电子邮件）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。

- → **发现并控制**所有数据，无论数据存在于云端、网络、电子邮件或是终端。
- → 使用消息引导用户行为，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、Gartner、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）。
- → **与Forcepoint 数据分类集成**，利用经过高度训练的 AI/ML 模型为正在使用的数据提供高度精确的分类。

- → **机器学习**允许用户训练系统以识别相关的、以前从未见过的数据。用户提供正面和负面示例，以标识相似的商业文件、源代码等。
- → 对结构化（例如数据库）和非结构化（例如文档）数据进行**指纹**识别，使数据所有者能够定义数据类型，并在商业文件、设计计划和数据库之间识别完全和部分匹配，然后应用与数据匹配的正确控制或策略。
- → **分析**发现用户在数据交互方面的行为变化，例如个人电子邮件使用的增加。 通过 Risk-Adaptive Protection，Forcepoint DLP 变得更加有效，因为它利用行为分析来理解用户风险，然后根据用户的风险等级来实施自动化策略实施。” 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。

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。
- → 通过在 Windows 和 macOS 上进行员工培训，**提高员工**处理敏感数据和知识产权的意识，此外，通过集成 Forcepoint 数据分类和 Microsoft Purview 信息保护等分类解决方案，使员工能够更好地应对挑战。
- → 在远程工作终端和企业云应用中**实施先进的 DLP 数据**识别能力，例如指纹识别技术。
- → 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 的深度集成，将**数据的上下文添加**到更广泛的用户分析中。

无处不在的可见性，包括本地数据和云端数据

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 CASB、SWG 和 ZTNA 将分析和 DLP 策略扩展到关键的云应用程序、网络流量和基于网络的私有应用程序，以确保无论数据位于何处，都能得到保护。REST API，如 Forcepoint DLP App Data Security API，为内部自定义开发的应用程序带来可见性和 DLP 执行能力。

- → **专注于响应团队，以识别和保护**云应用程序、网络数据存储、数据库以及受管理和未受管理的终端中的数据。
- → **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**，将包括指纹识别和机器学习在内的 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。
- → 通过公开的 REST API，**查看事件并管理第三方工具**。通过自动化和服务工具（如 ServiceNow、Nagios 和 Tableau）以及 SIEM/SOAR 解决方案（如 Splunk 和 XSOAR），实现事件管理工作流自动化，并支持依赖 DLP 事件的业务流程。

Forcepoint DLP 在每次部署时都包括来自单一控制点的高级分析和监管策略模板。云应用程序、网络流量和基于网络的私有应用程序，因此无论数据位于何处，都能得到保护。

附录 A：DLP 解决方案组件概述

Forcepoint DLP Endpoint	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。它使员工能够根据 DLP 培训对话中的指导，自行纠正数据风险。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 ONE CASB	借助 Forcepoint ONE CASB 的支持，将 Forcepoint DLP 的高级分析和单一控制扩展到合规的云应用程序，包括 Office 365、Salesforce、Box、Dropbox、Google Apps、Amazon AWS、ServiceNow、Zoom、Slack等众多应用。无论用户身在何处或使用何种设备，都能持续控制关键业务数据。
Forcepoint ONE SWG	Forcepoint ONE SWG 允许您安全访问任何网站或下载任何文档，同时获得您的团队依赖的高速网络性能。与 RBI 集成，以安全容器渲染风险网站，并与 Zero Trust CDR 集成，以完全清理所有可下载的文档。
Forcepoint ONE ZTNA (coming 2H 2023)	Forcepoint ONE ZTNA 为管理和非管理设备提供简单、安全和可扩展的零信任远程访问，无需跨 VPN 即可访问内部和私有云应用程序。
Forcepoint DLP —Discover	Forcepoint DLP - Discovery 识别并保护文件服务器、SharePoint（本地和云端）、Exchange（本地和云端）以及数据库（如 SQL Server 和 Oracle）中的敏感数据。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 - 网络提供了关键的执行点，用于阻止数据在电子邮件、Web 渠道和 FTP 传输中的泄露。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。与非云解决方案不同，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。它可以分析文件和数据流量，并执行 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。

附录 B：DLP 解决方案组件概述

	FORCEPOINT DLP ENDPOINT	FORCEPOINT ONE CASB	FORCEPOINT DLP—DISCOVER	FORCEPOINT DLP—NETWORK	FORCEPOINT DLP FOR CLOUD EMAIL	FORCEPOINT ONE SWG	FORCEPOINT DLP APP DATA SECURITY API	FORCEPOINT ONE ZTNA (COMING 2H 2023)
主要功能是什么?	在用户的端点上通过应用程序、网络、打印、可移动介质等渠道，实现数据发现和执行数据保护策略。	在云端或云端交付型应用程序中，发现数据和实施策略	发现、扫描和修复数据中心和其他本地环境中静态数据	通过网页和网络电子邮件，查看和控制动态数据	通过网页和网络电子邮件，查看和控制动态数据	通过发出的邮件，查看和控制动态数据	在内部自定义应用程序和服务中查看和控制数据	对企业私有应用程序内移动中的数据（上传和下载）进行可见性和数据保护策略实施
在哪里发现/保护静态数据?	Windows 端点 MacOS 端点	OneDrive、Sharepoint Online、Exchange、Google Drive、Box、DropBox、Salesforce、ServiceNow	本地文件服务器和网络存储、Sharepoint 服务器、Exchange 服务器、数据库（如 Microsoft SQL Server、Oracle 和 IBM Db2）					
在哪里保护传输中的数据?	电子邮件、Web：HTTP(S)、打印机、可移动介质、文件服务器/NAS	Office365、Google Apps、Salesforce.com、Box、Dropbox、ServiceNow 通过 API 上传、下载和分享；所有其他主要应用程序通过代理上传、下载和分享		电子邮件、打印机、FTP、Web：Http(S)、ICAP	电子邮件	HTTP(S)	内部自定义应用程序和自定义服务	通过 ZTNA Connector 将文件上传和下载到私人应用程序
在哪里保护使用中的数据?	Zoom、Webex、Google Hangouts、IM、VOIP 文件共享、M365 团队共享、应用程序（云存储客户端）、OS 剪贴板	使用云应用程序进行创建、修改和协作					内部自定义应用程序和自定义服务	

附录 B：DLP 解决方案组件特征比较

	FORCEPOINT DLP—ENDPOINT	FORCEPOINT ONE CASB	FORCEPOINT DLP—DISCOVER	FORCEPOINT DLP—NETWORK	FORCEPOINT DLP FOR CLOUD EMAIL	FORCEPOINT ONE SWG	FORCEPOINT DLP APP DATA SECURITY API	FORCEPOINT ONE ZTNA (COMING 2H 2023)
Risk-Adaptive Protection	插件		插件	插件	插件	插件；目前在 Forcepoint ONE SWG 的 GRE/ IPSec 隧道中支持		
光学字符识别			包含	包含	包含			对 DLP 增强的 OCR 支持（2023下半年）
Data classification 与标记的集成	Forcepoint Data Classification 和 Microsoft Purview Information Protection.							
哪些数据可以指纹识别?*	结构化（数据库）、非结构化（文档）、二进制（非文本文件）							2023 年下半年推出
统一策略管理	从端点到云应用程序，通过单一控制台进行策略配置和实施							2023 年下半年推出
可靠的策略库	从行业最大的合规策略库中获取发现和实施							

Forcepoint

forcepoint.com/contact

关于 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。