Forcepoint

产品资料

Forcepoint DLP

行业领先的数据泄露防护解决方案，实现跨渠道统一管理

数据安全至关重要，但无需繁琐操作。当前混合办公模式的员工需要通过任意设备、在任何地理位置安全获取到敏感信息。Forcepoint Data Loss Prevention (DLP)解决方案简化了了现代企业的数据保护，在确保零性能损耗与生产力影响的前提下，提供完整的本地化部署数据防泄露防护能力。

通过对端点、网络和储存之间的数据流动进行深度洞察，Forcepoint DLP 可以保护您的关键资产，并确保合规性。它具备独特的功能，能够将策略从Forcepoint Security Manager (FSM) 扩展更多渠道，从而在云 SaaS 应用程序和网络中实现无缝的数据保护，同时确保策略实施的一致性和统一性。获得高级取证分析功能、无缝系统集成性、弹性扩展架构以及随业务需求同步进化的解决方案。

简化数据合规工作

- → **监管覆盖范围**使用超过 1,800 个预定义模板、策略和分类器（包括超过 70 个覆盖国家专属 ID、凭证、密钥和令牌），轻松满足和维持超过 90 个国家和超过 160 个地区的合规要求。
- → 借助网络、云和端点发现，**查找并修复**受监管数据。
- → 在所有渠道（包括云、端点、网络、网络、电子邮件）中**集中控制**和一致的策略。

提供全面的数据保护

- → **发现并控制数据**无论数据存在于云端、网络、电子邮件或是终端。无论是在云端还是在网络中，还是在电子邮件还是在端点。
- → 使用**引导用户**行为的信息，指导员工做出明智决策，就策略对员工进行培训，并在与关键数据交互时验证用户意图。
- → 使用基于策略的自动加密技术，在数据传输到组织之外时保护数据，与受信赖的合作伙伴**安全协作**。
- → 通过与 Forcepoint Data Classification 和 Microsoft Purview Information Protection 集成，实现**数据标记和分类的自动化**。

启用高阶功能和控制项

- 嵌入策略引擎的**光学字符识别 (OCR)** 可在本地和云部署中识别图像中的静态或动态数据，从而简化基础设施并确保一致的混合实施。
- 针对个人身份信息 (PII) 的**强大识别功能**提供数据验证检查、真实姓名检测、邻近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）。
- **高级的文件扫描功能**通过检查大文件的随机部分来检测部分数据泄露，防止数据窃取者隐藏敏感信息。
- **与 Forcepoint Data Classification 集成**，与 Forcepoint Data Classification 集成，利用经过高度训练的 AI/ML 模型，通过 Forcepoint Data Security Posture Management (DSPM) 为正在使用的数据和静态数据提供高度精确的分类。
- **先进的生成式 AI** 能支持用户训导系统并构建自学习AI模型，通过自动化数据发现，多层级分类及智能标注，显著提升数据处理时效性与分类准确率。
- 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。
- **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。

发现并降低数据保护风险

- **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。
- **使用直接集成在解决方案中的人工智能驱动的智能搜索帮助工具**，无需离开管理控制台即可快速找到特定的支持信息。
- 通过在 Windows 和 macOS 上进行员工培训，**提高员工处理敏感数据和 IP 的意识**，此外，通过集成 Forcepoint Data Classification 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。
- **身份集成**支持云原生的 Entra ID，既适用于管理访问，也适用于终端用户的策略执行，从而提高安全性一致性并简化管理。

实现对您所有数据的全面可视性

- → **使管理员**能够识别并保护跨云应用程序、网络数据存储、数据库以及托管和非托管端点的数据。
- → **识别并自动阻止**向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。
- → 通过本地部署的数据丢失防护（DLP）解决方案及混合选项来**维护数据所有权**，将诸如指纹识别、机器学习和策略实施等高级功能扩展到云应用程序和网络渠道。它非常适合监管严格的行业，通过将事件及取证数据安全存储在您的数据中心内，确保数据主权，满足合规要求。
- → **通过公开的 REST API，使用第三方工具**查看和管理事件。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。

如欲了解更多关于我们 enterprise DLP（DLP）解决方案的信息，请申请演示。

附录 A：DLP 解决方案组件概述

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。依托DLP智能引导对话机制，实现员工对数据风险的自助式修复。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。包含嵌入策略引擎的 OCR，能够提供对图像中数据的可见性。与 Outlook、Notes 和电子邮件客户端完全集成。
Forcepoint CASB	借助 Forcepoint 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 Web Security	Forcepoint Web Security 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 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。包含嵌入策略引擎的 OCR，能够提供对图像中数据的可见性。
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。嵌入策略引擎的 OCR，能够提供对图像中数据的可见性。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。包含 OCR，能够在混合部署中提供一致的实施。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。

附录 B：DLP 解决方案组件概述

	FORCEPOINT DLP ENDPOINT	FORCEPOINT CASB	FORCEPOINT WEB SECURITY	FORCEPOINT DLP DISCOVER	FORCEPOINT DLP NETWORK	FORCEPOINT DLP FOR CLOUD EMAIL	FORCEPOINT DLP APP DATA SECURITY API
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。	在云端或云端交付的应用程序中发现数据并执行策略	通过发出的邮件，查看和控制动态数据	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	在内部自定义应用程序和服务中查看和控制数据
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	通过 API 以及所有其他主要应用通过代理上传、下载和共享 Office 365、Google Apps、Salesforce.com、Box、Dropbox 和 ServiceNow	HTTP(S)		电子邮件、打印机、FTP、Web：Http(S)、ICAP	电子邮件	内部自定义应用程序和自定义服务
在哪里保护使用中的数据?	Zoom、Webex、Google Hangouts、IM、VOIP 文件共享、M365 Teams 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 CASB	FORCEPOINT WEB SECURITY	FORCEPOINT DLP DISCOVER	FORCEPOINT DLP NETWORK	FORCEPOINT DLP FOR CLOUD EMAIL	FORCEPOINT DLP APP DATA SECURITY API
Risk-Adaptive Protection	插件		插件；目前在 Forcepoint Web Security 的 GRE/ IPSec 隧道中支持	插件	插件	插件	
光学字符识别				包含	包含	包含	
Data Classification 和标签集成	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）						
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						
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						