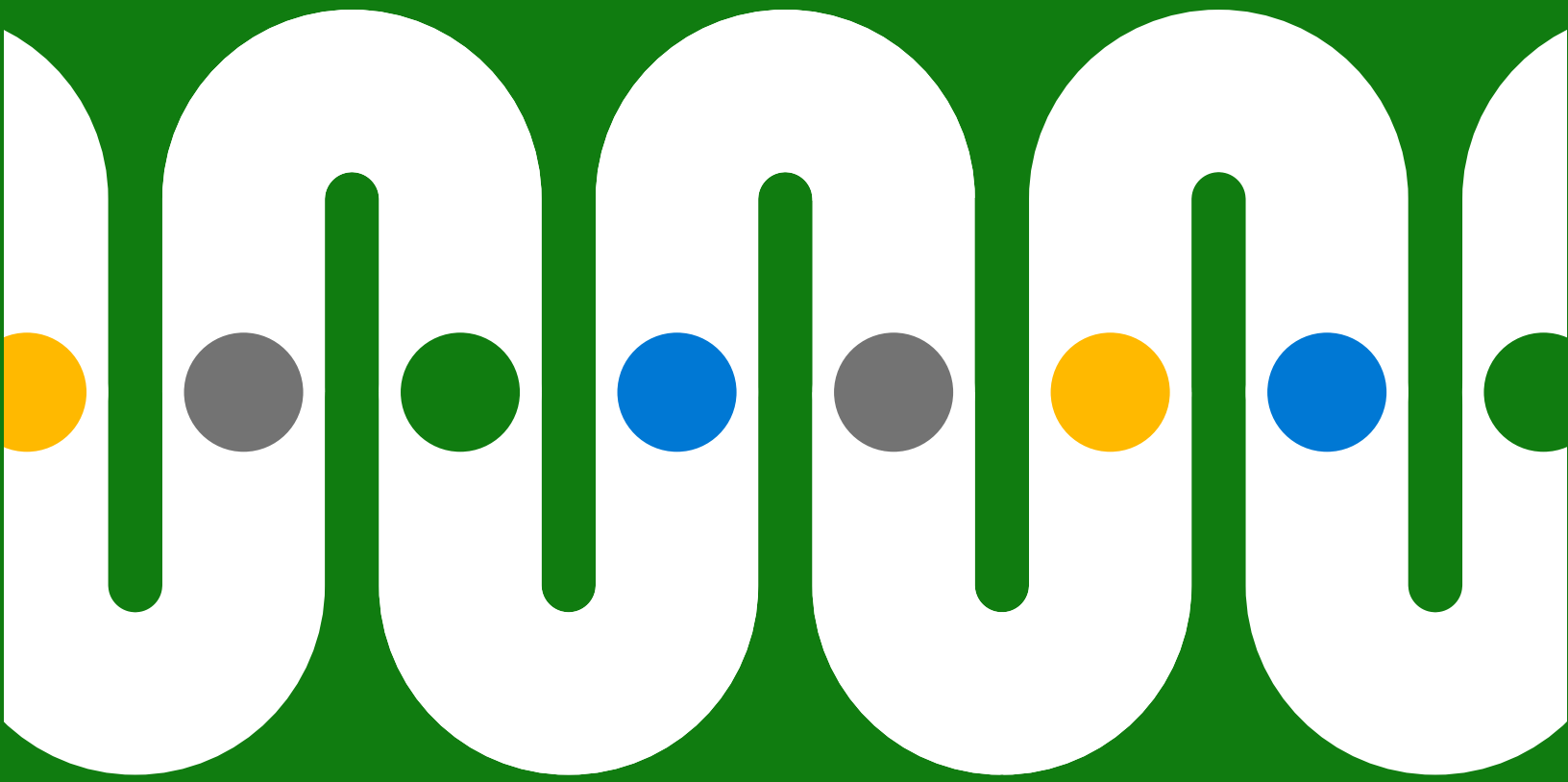
Microsoft Security

以端到端的方法保护数据的 3 个步骤



目录

针对合规性决策者开展的一项调查显示，95% 的决策者为数据保护挑战感到担忧。[2]

引言

混合办公模式使得组织的数字足迹大幅增长，远远超出了传统办公室的范围。

这引发了更多的数据碎片化和泄露问题，而所有这些问题又因大量应用程序、设备和位置的快速增长变得更加复杂。许多员工为了寻求更大的成就感或更高的灵活性而切换了角色，这无疑加剧了上述挑战，在日益增多的数据资产中带来了新的盲点。[1]

所有这些因素共同作用，使得 CIO 和 CISO 需要重新思考他们的信息保护方法。在针对 500 多名美国合规性决策者开展的跟踪调查中，几乎所有 (95%) 的决策者为数据保护挑战感到担忧。[2]

[1] “Microsoft 如何在 ‘大洗牌’ 期间帮助降低内部风险，Alym Rayani”，Microsoft 安全。2022 年 2 月 28 日。

[2] Vital Findings 在 Microsoft 委托下于 2021 年 9 月对 512 名美国合规性决策者进行的调查。

IT 和安全团队正在寻找更好的方法，以跨多云、混合云和本地环境管理整个数据生命周期。这种端到端方法涉及三个关键步骤：

第 1 步：识别数据

确定数据的位置、数据类型以及数据的使用或共享方式

第 2 步：对数据进行分类

对数据进行分类和标记，以便确定需要应用的正确策略和风险缓解措施

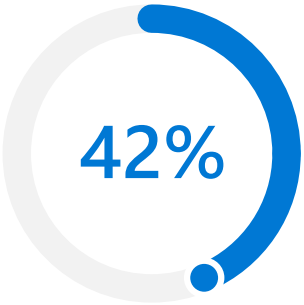
第 3 步：防止数据丢失

利用智能检测和控制，帮助员工在风险降低和灵活性之间取得平衡

这一方法的目标是什么？在不影响工作效率的情况下弥补漏洞并最大限度地降低风险。

第 1 步

识别数据



当被问及组织中的数据有多少是“暗数据”时，42% 的组织表示至少有一半。[3]

这些“隐藏”数据可能以电子邮件附件、客户通话记录、机器日志和录像片段等多种形式存在。

如果你无法识别数据的位置、数据类型以及数据的使用和共享方式，则无法对其应用正确的策略或保护。

现代组织不断生成大量数据。这些数据不仅是指文档、电子邮件和消息，还包括安保录像和地理位置数据中的所有内容，所有这些数据都会因本地和云中的应用、设备和存储的激增而更加复杂。

识别所有这些数据并非易事，42% 的组织表示，至少有一半的数据是“暗数据”。[3] 此类数据是指未知或未用于业务目的的已收集信息。有时，数据会在创建者切换项目或角色时变成暗数据；通常情况下，根本没有相应的系统来识别正在创建或修改的数据。

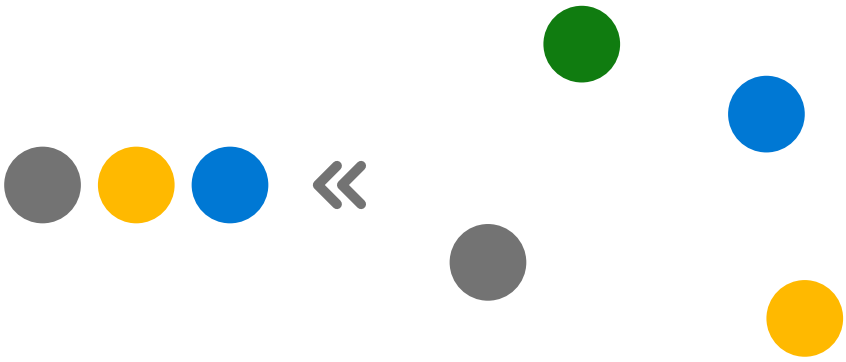
[3] “2022 State of Data Governance and Empowerment Report”，Enterprise Strategy Group。2022 年 7 月。

想要在一个平台上构建端到端数据发现工作流?

通过 **Microsoft.com** 了解 Microsoft Purview 中的数据发现。

这种挑战只会与日俱增。到 2026 年，创建、捕获、复制和使用的新数据量预计将增加超过一倍，企业数据的增长速度将是消费者数据的两倍多。[4]

人工智能 (AI) 和机器学习 (ML) 可以帮助识别敏感数据（如电子邮件地址、健康数据、信用卡号或知识产权）并对其进行自动分类。AI 和 ML 还可以提高分类准确性，并以追溯的方式审查数据。这些识别过程可以覆盖你的整个数据资产，在任何云中保存、收集、分析、审查和导出位于任何位置的内容。



[4] "Worldwide IDC Global DataSphere Forecast, 2022–2026: Enterprise Organizations Driving Most of the Data Growth"，John Rydning，IDC。2022 年 5 月。

第 2 步

对数据进行分类

分类和策略都需要对四处移动的数据进行跟踪。

例如，在一位员工将信用卡号从 Microsoft Word 文档复制到 Excel 中时，分类和策略将自动应用于这两个文档。

适当的数据分类可帮助你确定正确的策略和风险缓解措施，以确保不同类型的数据不会在未经授权的情况下被意外或有意滥用或访问。加密和水印可进一步保护数据，无论是静态、传输过程中还是使用中的数据。

但当数据在组织内部移动时，还需要通过分类和策略对这些数据进行跟踪。标记和保护策略不能局限于离散文档，而必须覆盖整个数字资产，包括本地和基于云的存储库，以及软件即服务 (SaaS) 和操作系统原生应用。

传统分类方法需要大量手动工作，这存在发生错误或无意中忽视关键数据的风险。内置且可训练的分类器可帮助实现此流程的自动化，而集成式解决方案可帮助管理员跨所有系统集中管理策略。

希望更好地管理和保护整个环境中的敏感数据?

通过 **Microsoft.com** 了解 Microsoft Purview 中的数据分类和保护。

第 3 步

防止数据丢失

DLP 策略可以防止不合规操作。

例如，在员工试图将带有信用卡卡号信息的电子表格下载到闪存驱动器或将其上传到云存储时，DLP 策略会将此活动识别为不合规活动并对其进行阻止。

想要智能检测和控制敏感信息?

通过 **Microsoft.com** 了解 Microsoft Purview 中的数据丢失防护。

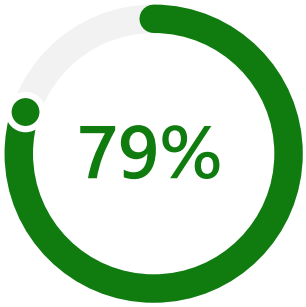
完成数据识别和分类后，数据丢失防护 (DLP) 解决方案可以实施端到端保护策略来减轻暗数据和数据泄露等威胁，以便现有员工和前员工不会（有意或无意）未经授权共享、公开或传输敏感数据。

智能 DLP 解决方案利用背景信息在提供选择灵活性与阻止高风险操作之间找到平衡点。例如，在收到有关潜在风险和适用策略的提醒后，个人可能仍可以继续操作。这有助于保护敏感数据，同时培训用户来更好地了解风险。

DLP 解决方案可帮助保护知识产权和其他关键业务数据，同时帮助组织更好地遵守《一般数据保护条例》(GDPR)、《健康保险流通与责任法案》(HIPAA) 和《加州消费者隐私法案》(CCPA) 等法规。

全面的 DLP 方法可在整个组织中采用一致的方式强制执行策略，保护数据生命周期中“最薄弱的衔接”点。

数据保护不应追加，而应内置。



针对合规性决策者开展的一项调查显示，79% 的决策者购买了多种合规性和数据保护产品。

大多数决策者购买了三种或三种以上的产品。[5]

许多组织都尝试采取了“追加式”的信息保护方法，使用多个解决方案来管理数据生命周期的离散部分。但这会使安全性、数据治理、合规性和法律团队强制拼凑在一起，不仅成效甚微，还会耗用大量资源。

“内置式”方法可以通过整合数据识别、数据分类和 DLP 来弥补这些不足。借助集成式解决方案，组织可以更轻松地集中管理和实施策略。它还减少了用户的培训时间，因为用户可以在应用程序中以熟悉的原生方式接收策略通知。

[5] MDC Research 在 Microsoft 委托下于 2022 年 2 月针对 200 名美国合规性决策者进行的调查（n = 100、599-999 名员工，n = 100、1000 多名员工）。

内置的集成式解决方案：Microsoft Purview

Microsoft Purview 提供一系列有助于治理、保护和管理整个数据资产的全面解决方案，可帮助你应对当今数据丰富的分散式工作场所带来的挑战。

并不止于数据治理。
详细了解如何借助 Microsoft Purview 保护数据 >

对数据保护特定领域感兴趣？详细了解 Microsoft Purview 的以下解决方案如何为你提供帮助：

数据发现 >

数据分类和保护 >

数据丢失防护 >

Microsoft Security