cpl.thalesgroup.com

THALES

使用Thales CipherTrust数据发现和分类的10大理由

遵守不断演变的数据隐私法律法规非常具有挑战性。如果您完全依赖人工方式，若想了解所有敏感数据所在的位置就会面临耗时且成本高昂的持续性工作。如果不考虑这一点，那么最大限度降低数据蔓延所带来的风险将是一个非常困难的过程。

好消息！CipherTrust数据发现和分类可以随时为您提供帮助，为您带来诸多益处，其中包括：

- 发现合规性差距以帮助您降低风险
- 第一时间协助您对高风险数据进行保护
- 随着数据足迹的增长，您可以按需添加更多扫描位置

CipherTrust数据发现和分类通过在异构数据存储环境中高效的数据发现、分类和风险分析能力，帮助你的组织对现有的敏感数据实现全面了解。我们在下面列出了您应该立即考虑实施CipherTrust数据发现和分类的10大理由。

增强安全性

1 发现合规性差距

为避免因违反繁杂的数据隐私法律和法规可能带来的重大业务风险，了解您拥有哪些敏感数据及其所在的位置至关重要。借助针对各种数据法规（包括CCPA、GDPR、HIPPA和PCI DSS）的预定义模板，您可以使用CipherTrust数据发现和分类快速设置全面扫描，以识别数据存储空间中任意地点的各种敏感数据。您发现的大多数合规性差距都可以利用数据保护方法（例如CipherTrust透明加密）立即得到补救。

2 提示安全风险

准确了解您的基础设施中存在哪些类型的敏感数据及其风险级别，提供实现额外层面保护所需的深入洞察力。当您根据监管合规性、隐私法规或内部业务要求，对各类数据集明确存储位置和分类依据时，CipherTrust数据发现和分类使您能够为数据分配具体的敏感度级别（无、公共、内部、私有、受限）。运行扫描后，信息可以按您定义的风险级别进行排序，以帮助突出显示潜在的安全风险，例如尚未进行访问控制或加密时。随后，您可以开始采取适当的补救措施，并且知晓您正在消除组织的安全风险。

3 识别策略错误配置

将数据（尤其是敏感数据）的访问权限局限于仅允许需要的人访问，这是公认的正确安全做法。但是，如果以人工、临时的方式进行彻底调查可能需要很长时间，并且可能无法提供所需的有关访问控制策略配置错误的所有证据。而这时，CipherTrust数据发现和分类可以通过其全面扫描和相关报告大显身手。您可以轻松审阅报告数据，准确查看需要更严格控制敏感数据访问权限的位置，或需要纠正的访问权限错误配置。

4 丢弃不需要的数据

数据以不受控制的方式蔓延的情况很容易发生，这不仅会导致您在存储上花费大量资金，并且还会增加破坏性数据泄露的风险 – 保留您真正需要的数据是PCI DSS要求中建议的内容。通过过滤由CipherTrust数据发现和分类扫描事件生成的报告数据，您可以查明需要从相关数据存储中删除、存档或移除的特定信息 – 通常是重复的、陈旧的或冗余的信息。CipherTrust数据发现和分类通过使用CipherTrust加密、令牌化或数据屏蔽工具为您提供了具备先见之明的适当行动。

提高效率

5 利用风险因素

发现敏感数据本身并不是最大的挑战，最大的挑战是知道要如何根据风险因素对意外敏感数据泄露做出反应。为了实现这一点，您需要一个基础来定义与任何给定数据集相关的风险因素。CipherTrust数据发现和分类能够使用标签对数据进行分组，为每个单独的数据存储设置风险级别，并根据数据存储中保存的数据元素类型对风险进行分类。通过这种方式，您可以运行多个扫描并将各个扫描结果汇总成一个报告进行分析。与大多数CipherTrust数据发现和分类用户一样，您可以按风险因素对数据进行降序排序，深入了解组织中的最高风险因素，从而能够适当地优先安排各项保护措施。

6 集中协调行动

在发现敏感数据并对其分类后，需要在实施访问控制和数据保护机制的同时，快速、高效地进行补救。CipherTrust数据发现和分类属于更大的CipherTrust数据安全平台解决方案的一部分，该解决方案通过CipherTrust Manager使用中央控制台功能，使您可以在其中为各种类型的用户定义全面的数据访问控制策略。市场领先的数据保护解决方案（例如CipherTrust透明加密）也通过CipherTrust Manager进行配置和管理，为您提供确保对所选操作进行集中协调所需的工具。

7 减少整合工作

如果您需要能够发现您拥有的敏感数据的所在位置，并随后保护您识别的数据，然后严格控制访问以降低风险，无需处理来自不同供应商的多种产品当然能带来优势，因为不同产品不能轻易整合或者需要完全专有的管理工具。CipherTrust数据安全平台在一站式平台中提供您所需的一切 – 实现一站式发现、保护和控制。CipherTrust数据发现和分类发现的敏感数据可以由适当的CipherTrust数据保护代理（都在集中式CipherTrust Manager的控制下）快速补救（使用加密、令牌化或数据脱敏）。可以将不同的CipherTrust数据发现和分类组分配给不同的数据存储，以帮助缩短运行和分析扫描数据所需的时间。这种方法使组织能够将复杂的活动拆分为可管理的分块，每个分块由不同的专家团队负责，同时提供跨团队功能以实现连贯的解决方案流程。

借助针对各种数据法规（包括CCPA、GDPR、HIPPA和PCI DSS）的预定义模板，您可以使用CipherTrust数据发现和分类快速设置全面扫描，以识别数据存储空间中任意地点的各种相关敏感数据。

如果不属于标准的数据分类，CipherTrust数据发现和分类能够为敏感数据创建自定义的规则。

固有的可扩展性

8 增加新来源

随着数据足迹的扩大以及使用不同类型的数据存储，您需要确保您的数据发现功能可以随时查找敏感数据并对其进行分类，尤其是在您的数据存储需求不断变化的情况下。无论您的数据是属于结构化还是非结构化，CipherTrust数据发现和分类都能使您随时添加各种不同的数据存储（本地、网络、数据库、大数据、云）以覆盖您的最新存储位置，从而让您可以确保正在进行的扫描覆盖了敏感数据所在的所有位置。

9 扩展发现能力

经常会出现需要分析的新型信息。例如，您的数据足迹可能会发生变化，包含更多基于云的存储位置。您需要定期更新的解决方案，以保持跟进不断变化的需求和技术进步。如果不属于标准的数据分类，CipherTrust数据发现和分类能够为敏感数据创建自定义的规则。我们将此功能称为“自定义信息类型”，它使您可以找到几乎任何内容。您可以扫描本地和多个云数据存储中的数据。本地和代理发现客户端的组合可用于帮助简化部署工作、提高性能并使您能够在需要时快速扩展。

10 解决专有需求

您可能拥有超出预定义模板的敏感数据，这些数据也需要定位和补救。您可能还有一些需要保护的组织专有的敏感数据（例如知识产权）。除了能够编辑我们开发的预定义分类配置文件之外，CipherTrust数据发现和分类还提供了添加新的自定义分类配置文件的功能，让您鱼和熊掌兼得。此外，您还可以为预定义标签未涵盖的数据类型添加新的自定义标签。这是一款真正能够支持您现在和未来所有潜在需求的发现和分类解决方案。

关于Thales

您信赖的隐私保护者依靠Thales来保护其数据。在数据安全方面，各个组织面临着越来越多的决定性时刻。无论是制定加密策略、迁移到云还是满足合规性要求，您都可以依靠Thales来为您的数字化转型提供安全保障。

决定性时刻的决定性技术。

THALES

联系我们

请访问 cpl.thalesgroup.com/contact-us
查阅所有办事处的地点和联系方式

> cpl.thalesgroup.com <

© Thales - September 2021 • EHV2