

通过 AI 技术缓解数据生命周期风险和挑战

非官方中文译文·安天技术公益翻译组 译注

简译版

文档信息			
原文名称	How AI can alleviate data lifecycle risks and challenges		
原文作者	克里斯·拉里 (Kris Lahiri)	原文发布日期	2020 年 8 月 3 日
作者简介	克里斯·拉里是 Egnyte 公司的首席服务官。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2020/08/03/how-ai-can-alleviate-data-lifecycle-risks-and-challenges/		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	<ul style="list-style-type: none"> 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。 		

通过 AI 技术缓解数据生命周期风险和挑战

克里斯·拉里

2020 年 8 月 3 日

全球企业数据量正在以惊人的速度增长——一些研究表明，企业的数据量每年都在翻番。随着时间的流逝，每家公司都会生成并积累海量的数据、文件和内容；有些数据无关紧要，而有些则高度敏感和机密。

在整个数据生命周期中，企业需要管理各种风险和注意事项。企业生成的数据越多，就越有必要寻求一种方法，以更好地跟踪和存储数据，防止数据窃取、泄漏和不合规等问题。

面对海量的数据增长，大多数企业不能再依靠手动流程来管理风险。许多公司采用了大量的跟踪、端点检测、加密、访问控制和数据策略工具来维护数据的安全性、隐私性和合规性。但是，部署和管理诸多不同的解决方案会带来极大的复杂性和矛盾性，给 IT 和安全团队以及最终用户带来麻烦。在大规模管理企业文件和内容所需的集成度和智能性方面，这种方法就显得不足了。

下面，我们来探讨一下当今企业面临的几种最常见的数据生命周期挑战和风险，并分析如何应对这些挑战。

维护数据安全

鉴于公司不断生成大量敏感文件和内容，其数据泄露的风险呈指数级增长。智能数据监管意味着，在风险最大的方面维护数据安全，包括确保公司数据和内容的完整性，保护所有有权访问数据的用户等。企业文件共享、协同和存储的每一个层面都必须受到控制措施的保护，这些控制措施包括自动用户行为监控（以防止内部人员威胁和受感染账户）、多因子身份鉴别、在经过认证的数据中心安全存储数据、端到端加密、基于特征的恶意软件检测和零日恶意软件检测等。

数据分类和合规性

企业要求用户对公司文件和内容进行标记或分类，或要求 IT 人员管理和手动执行数据策略的日子已经一去不复返了。手动进行数据分类和管理不仅不切实际，而且有很大的风险。

企业可能有数百万个文件，而这些文件被数以万计的用户访问——文件数量实在太多了，用户的范围也太广了。此外，诸如 GDPR、CCPA 和 HIPAA 等法规给出了错综复杂的（有时甚至是相互矛盾的）要求，为数据保护增加了更多的复杂性。仅 GDPR 下的 PII（个人信息）的定义就包含数百条信息，一个错误就可能会导致巨额罚款。

错误的分类会引发各种问题，包括数据窃取和监管处罚等。幸运的是，机器可以在几秒钟内（IT 人员可能需要花费数年的时间）完成分类工作，而且往往具有更高的准确性。人工智能（AI）和机器学习（ML）技术可以帮助公司跨数据存储库快速扫描文件，以识别诸如信用卡号、地址、出生日期、社保号以及与健康数据等敏感信息，并对数据进行自动分类。这些技术还可以跨热门数据源（例如 OneDrive、Windows File Server、SharePoint、Amazon S3、Google Cloud、GSuite、Box、Microsoft Azure Blob 和通用 CIFS/ SMB 存储库）跟踪文件，帮助企业实现更好的可见性和数据控制。

数据保存

在过去的 10 年中，数据存储成本暴跌；许多企业陷入了“存储所有内容”的怪圈，他们认为这样做的成本很低。但实际上，这种方法带来了诸多安全和监管风险以及潜在成本。我们的研究表明，泄露 1 TB 的数据会造成 129,324 美元的损失。现在，企业需要认真考虑他们究竟存储了多少 TB 的数据了。企业保存敏感文件的时间越长，这些文件被破坏或窃取的风险就越大。

根据各种客户合同和法规标准，某些类型的数据必须在特定时间段内保存。例如，HIPAA 法规要求，从文档创建之日起，企业可以保存 6 年。GDPR 没有给出具体的时间要求，但是指出保存数据的时间不得超过处理数据所需的时间。

保存数据超过必要的时间不仅会带来风险，还会导致存储成本迅速增加。AI 技术可以跟踪数据的保存期限，并通过自动保护或删除所有需要（或允许）的旧文件或冗余文件，来最大程度地降低风险。通过精简数据保存流程，企业可以降低存储成本，降低安全和违规风险，优化数据处理性能。

持续监控和管理

长期的良好数据安全实践，有助于实现强健的数据监管。但是，由于企业要在多个不同的存储库和存储平台上管理大量文件，因此实时跟踪风险和可疑活动会有些困难。企业应创

建专用策略，确定在哪些位置存储哪些数据、哪些用户可以访问数据，以及与之共享数据的所有各方。这有助于企业节省时间，使其将精力放在降低风险上。通过 AI 技术，企业可以消除手动监控流程，获得更好的数据使用情况可见性。如果敏感内容在外部或在未经许可的情况下被共享，AI 技术还会发出告警。AI 技术使企业更容易识别和应对威胁和风险行为，帮助其及时对受感染账户采取措施，移动或删除共享范围太广或存储在未经授权位置的敏感内容等。

数据生命周期管理的关键

如今，企业不断生成和管理大量数据、文件和内容，这会带来极大的复杂性和风险。企业必须了解他们有哪些数据、数据存储在哪里、哪些用户可以访问数据、何时共享数据、哪些文件可以删除、哪些文件需要根据法规要求存储等。任何一个方面出现问题，都会导致重大的运营、经济和声誉损失。

幸运的是，最新的 AI 和 ML 技术能够帮助公司简化数据监管，从源头查找和保护敏感数据，感知并响应潜在的恶意行为，保持合规性并适应不断变化的监管标准。由于人工流程和单点解决方案存在不足，企业可以采用 AI 技术监管数据，以减少用户和管理员的麻烦，在以数据为中心的世界中获得所需的可见性和控制权。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队,始终坚持自主先进的能力导向,依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累,研发智甲、探海、镇关、捕风、追影、拓痕等系列产品,为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系,依托全面持续监测能力,建立系统与人员协同作业机制,指挥网内各种防御机制联合响应威胁,实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合,协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设,支撑起协同联动的实战化运行,赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方,全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴,目前,安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点,在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面,实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体(如 APT 组织)及其攻击行动,进行持续监测和深度解析,协助客户在“敌情想定”下形成有效防护,通过深度分析高级网空威胁行为体的作业能力,安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可,已连续六届蝉联国家级安全应急支撑单位,是中国国家信息安全漏洞库六家首批一级支撑单位之一,亦是国家网络与信息安全信息通报机制技术支撑单位,国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日,在习近平总书记主持召开的网络安全和信息化工作座谈会上,安天创始人、首席架构师作为网络安全领域发言代表,向总书记进行了汇报。2016 年 5 月 25 日,习近平总书记在黑龙江调研期间,视察了安天总部,并对安天人说,“你们也是国家队,虽然你们是民营企业”。

安天实验室更多信息请访问:

<http://www.antiy.com> (中文)

<http://www.antiy.net> (英文)

安天企业安全公司更多信息请访问:

<http://www.antiy.cn>

安天移动安全公司 (AVL TEAM) 更多信息请访问: <http://www.avlsec.com>