简译版

数据安全计划的五个最佳实践

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Don’t Torpedo Your Data Security Program: 5 Best Practices to Consider		
原文作者	莱斯利·威金斯（Leslie Wiggins）	**原文发布日期**	2020 年 10 月 29 日
作者简介	莱斯利·威金斯是 IBM Security 的项目总监。		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/posts/dont-torpedo-your-data-privacy-program-best-practices/		
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	• 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有方式，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。		

数据安全计划的五个最佳实践

莱斯利·威金斯

2020 年 10 月 29 日

大多数负责保护公司高价值数据的安全领导人，肯定问过这样的问题："恶意内部人员能否访问企业的敏感和关键数据"。确实，这是一个很好的问题——企业中可能隐藏着一些恶意内部人员，他们伺机窃取企业的高价值数据。

很少有企业能够实现完全的可见性，实时了解敏感和受监管数据发生了什么。如今，实现可见性并保护为企业赋能的数据，比以往任何时候都更为重要。随着数据安全市场的不断变化——为了应对越来越严格的客户要求、复杂的云迁移要求，以及越来越多的数据隐私和网络安全合规性要求，特定领域的市场参与者试图与其他市场参与者合并——我们很难客观地比较领先供应商。

这会对企业开发平衡、完整数据安全项目的能力，带来不可预知的影响。对企业来说，创建数据安全计划比以往任何时候都更加重要。为什么呢？主要是为了避免数据泄露，以及满足数据隐私和合规性要求，避免遭受罚款和丧失客户信任。有些供应商会告诉企业，有一种"万能的"数据隐私和法规合规性方法足以实现这些目标，而且可以提高客户的投资回报率（ROI）。

数据泄露的现实情况

现实情况是，数据泄露事件越来越多，成本也越来越高。最新研究表明，全球数据泄露平均总成本为 386 万美元。其中，内部人员导致的数据泄露事件占 50%，平均成本为 1145 万美元。这表明，与内部人员威胁有关的数据泄露会造成更大的损失。这是因为，内部人员（或冒充内部人员的人士）可以利用其凭证，访问更多的敏感和受监管数据，因此会造成更大的损失。

这些事实意味着，单一领域供应商（范围狭窄）无法满足当今复杂的数据安全、数据隐私和网络安全合规性要求。知道了这一点，我们就可以理解，一家试图开拓无代理数据安全解决方案（无法支持实时用例）的初创公司，为何要与提供传统 IT 技术的企业合并了。目前尚不清楚，这些迥然不同的架构该如何组合起来。因此，这种供应商组合可能会给客户带

来麻烦，他们难以通过多个传统架构部署稳健、灵活和现代的数据安全和合规性计划。

为应对这种新的、可能造成混乱的局面，企业可以采用以下最佳实践，满足特定的数据安全和保护用例。

1. 发现、阻止和防御

企业的数据安全解决方案是否可以实时监控数据活动？是否可以利用高级分析和行为分析，发现和阻止内部人员数据泄露或针对关键数据的应用程序劫持？

需要考虑的问题：无代理解决方案的被动数据收集方法，仅提供事后的有限合规支持。这种数据收集技术，支持对无关键数据的数据源的审计，但不足以支持涉及关键或受监管数据的合规性或安全用例。对于敏感用例，数据安全专家必须通过易于理解的分析，帮助企业识别用户行为异常和趋势。

上文提到的初创供应商，已将无代理数据收集用于所有用例。其合并可能标志着方向和策略的改变，其客户可能只能使用无代理数据安全方法了。但是，要想实现完整的数据安全计划，代理和无代理数据收集方法都是必需的。

2. 减轻负担

从连接到修复平台，打开故障单，到与第三方应用集成或创建报告，企业需要执行哪些操作？安全团队是否需要特殊技能来执行这些操作？

需要考虑的问题：企业用于各种计划的预算和资源通常是不足的。因此，企业应投资于易于使用，且需要较少专业技能就能维护的解决方案，这一点很重要。例如，阅读报表不需要高超的结构化查询语言（SQL）技能；查阅故障单不需要编写命令和代码。一些供应商对客户数据安全专家的期望正是如此。如果安全专家的注意力集中在高影响力的数据安全问题上，并且能够迅速提取和共享报告，企业就不再需要这种技能了。企业应考虑：安全团队能否使用此技术快速创建自定义报告？

3. 实现现代化以降低总拥有成本（TCO）

企业的业务压力已经改变，他们向 IT 团队施加压力，要求 IT 团队在支持混合环境的同时开始将基础架构迁移到云端。为了满足这些需求并实现 ROI，企业开始寻求现代化，以期降低总成本，使维护数据安全解决方案变得更加容易。

需要考虑的问题:架构现代化带来了一些内在的好处,使企业易于使用和维护解决方案。如今,企业应在本地部署解决方案,然后在需要时迁移到公有或私有云。现代化还可以提供诸如自动扩展、本地灾难恢复、高性能和低延迟、就地升级和多租户等优势,能够带来更好的体验并降低总拥有成本。目前,只有很少的供应商能够提供这种现代化的方法。其他供应商仍在支持各种传统架构,这可能会减慢客户的云迁移速度。

4. 快速使用数据

安全团队是否需要手动审计收集的数据,并在每次发布新的数据源时重新进行审计?多久需要重新审计一次?

需要考虑的问题:数据安全专家应随时在其数据安全解决方案中使用监控和审计数据。只有当解决方案自动将数据标准化并使用(例如用于报告和分析)时,这一点才有可能实现。这种快速访问支持审计要求和安全用例,不必花费额外的时间和费用来处理数据。

5. 打破孤岛

在数据越来越分散,威胁越来越多的时代,为了实现有效的数据安全,我们应打破孤岛。数据安全功能必须实现自动化,并作为更大的安全生态系统的一部分,以帮助安全团队进行协同。基本的集成不足以支持更广泛的数据安全生态系统,也无法整合企业希望使用的大量数据源和数据安全工具。

需要考虑的问题:由于无法支持自动化、编排和协同,安全团队使用的各种数据安全工具相互独立,这增加了成本,减慢了数据安全和保护活动,并延长了实现价值的时间。

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