

简译版

采用“全方位”思维来保护企业数据和隐私

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	Data Protection and Privacy: Think 360, Demand 360		
原文作者	Jim Gordon	原文发布日期	2019 年 8 月 19 日
作者简介	Jim Gordon 是英特尔公司安全生态系统战略与发展总经理。		
原文发布单位	Security Week		
原文出处	https://www.securityweek.com/data-protection-and-privacy-think-360-demand-360		
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。 		

采用“全方位”思维来保护企业数据和隐私

Jim Gordon

2019 年 8 月 19 日

当涉及数据和隐私的保护时，评估企业现状和企业目标非常重要。

如果你正在阅读本文，那么你可能就是一位了解并重视数据保护和隐私重要性（以及它们之间的区别）的人。我们都意识到，“保护数据和隐私”这一目标不断发展，而且受到法律、道德和经济的影响。因此，我一直在思考创建简单的框架，以帮助大家更好地保护数据和隐私。最终，我得出了一个结论：采取“全方位”思维。

对重要的内容设置口令，就能保护数据和隐私的日子早已过去。现在，我们需要采取全方位思维。这包括：防御攻击者、防止过度使用权限、防止员工和内部人员威胁，以及防止企业自身不当行为导致的威胁。如果漏掉了这些中的任何一个，则该企业的数据和隐私无法得到完整的保护。

防御攻击者无须赘述。防止过度使用权限，是指防止政府机构滥用其司法权利。防止员工和内部人员威胁，是指防止员工故意或无意地访问他们不应访问的信息，如薪资信息和受保护的知识产权等。最后，防止企业自身不当行为导致的威胁，是指防止由于企业自身的原因导致意外泄露信息。

考虑到所有这些方面（当然，肯定还有一些是我没有提到的）是一个很高的要求。在不久前，这基本是无法实现的。但是现在，这种全方位思维更有可能实现、更可行，也更经济了。我们只需了解数据和隐私保护的全方位性质，然后针对每个方面制定解决策略。一些技术和流程可以涵盖多个方面。但是我们也必须意识到，很多保护措施和流程只能保护一个方面，而忽略了其他方面。

我们以企业的云 CRM 提供商为例。云 CRM 提供商是如何保护企业数据不被其员工访问的？他们的特权员工能够访问吗？他们是否能够检测到数据访问和数据流动中的异常？他们如何回应政府传唤？如果被传唤，他们是否有权披露企业的数据？还是说，只有企业自己能够披露自己的数据？企业数据的物理安全措施如何？数据保存在哪些物理位置？他们的漏洞修补策略如何？这样的问题还有很多。虽然这些问题没有完美的答案，但是如果企业不知道要问什么问题，就永远不会知道其所处的现状……所以，请向提供商询问这些问题。

如果企业采取全方位思维，并试图使所有解决方案到位，那企业永远无法找到合适的方法。鉴于企业保护的内容、攻击者，以及攻击者使用的技术是不断变化的，因此企业需要定期进行检查和评估。企业不仅要采取全方位思维，还必须意识到这项工作永远没有尽头。尽管企业所处的环境非常复杂而且不断变化，但是企业还是需要经常对其自身进行评估。

在后续专栏文章中，我将更详细地探讨如何将此思维付诸实践，以及如何评估企业的现状以及企业的目标。无论是小型企业还是大型企业，都适用该框架。即使这些企业的工具和方法（当然还有成本）有很大的不同，但他们的考虑因素是非常相似的。无论如何，我希望这个全方位框架既可以作为一种工具和评估标准，最重要的是，也可以作为一种思维模式。这种思维模式不仅能够识别风险领域，还能够确定保护数据和保护需要采取的行动。

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,安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十五亿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>