简译版

通过集成的安全策略保护数字工作场所

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	Protecting the digital workplace with an integrated security strategy		
原文作者	朱尔斯·马丁（Jules Martin）	**原文发布日期**	2021 年 3 月 1 日
作者简介	朱尔斯·马丁是 Mimecast 生态系统与联盟副总裁。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2021/03/01/protecting-digital-workplace/		
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。		

通过集成的安全策略保护数字工作场所

朱尔斯·马丁

2021 年 3 月 1 日

新冠疫情推动 IT 世界狂飙向未来。那些原本考虑慢慢实现数字化转型计划的企业，被迫加快了转型步伐，以便保护“禁足令”下远程办公的员工。

这种运营变化已在许多方面对业务领域产生了积极影响，但同时也带来了新的安全挑战。如今，IT 安全团队正在努力应对这些挑战。例如：

- 大规模分布和流动员工已使“未来的数字办公室”成为现实。电子邮件平台的使用急剧增加，特别是 Microsoft Office 365，现在每月有超过 2.5 亿的活跃用户。
- 协同工具（例如 Microsoft Teams、Slack 和 Zoom）的使用大大增加。相应地，通过这些渠道交换的敏感信息的数量也大大增加（曾经在办公室交换的信息，现在通过数字渠道交换了）。
- 由于业务环境的变化，网络犯罪分子转变了攻击策略，开始针对这些云服务和远程员工。

此外，疫情爆发之前 IT 安全团队面临的成本、复杂性和技能短缺挑战也未消失。而如今，企业迅速过渡到数字办公，又导致攻击面大大扩展。

当 IT 安全团队仍致力于保护旧工作场所时，他们有能力来保护这个新的数字工作场所吗？答案是肯定的，但不必通过购买更多安全工具来实现这一点。安全团队可以将现有工具集成，从中获得更多价值，以便轻松共享信息，同时减少管理费用。

借鉴过去的经验教训

从历史上看，企业通常采取孤立的方法来防御网络威胁。当出现新的威胁时，IT 安全团队就会购买新的解决方案来进行应对。虽然单点解决方案是一种快速、简便、即用的解决方案，但它们带来了一系列长期的业务和安全挑战。

对于初始者来说，针对每一种新威胁购买新产品的成本会很高。而且，购买如此多的工具会导致企业的基础架构非常复杂，大多数企业都没有时间、资源或预算来管理这种架构。

（据统计，普通企业的生态系统中平均有 75 个安全解决方案。）此外，使用单点解决方案，威胁数据就会分散在各个工具中，导致 IT 安全团队难以（甚至无法）获得企业范围的可见性来检测和修复威胁。

好消息是：随着安全控制迁移到云中，我们有机会摆脱这种传统方法了，我们可以重新考虑在此新环境中如何实施、整合安全以及相关的 IT 和安全控制，并实现其自动化。

整合安全生态系统

就像俗话说的“人多力量大”，将所有安全工具的威胁情报整合在一起，能够使它们更聪明、更有效地克服数字工作场所的挑战，进而检测和响应威胁。棘手的问题是：虽然向基础架构中添加技术很容易，但要使其协同工作却并非易事。要想实现这种性质的安全集成，关键是采用开放且普遍的 API 安全策略。

API 能够在包括 SIEM（安全信息和事件管理），SOAR（安全编排、自动化和响应），端点安全和 ITSM（IT 服务管理系统）解决方案在内的各种安全工具之间，实现数据整合和交换的自动化。API 平台与集成的安全策略相结合，可以极大地提高安全基础架构的有效性，同时还能够提供整合的管理功能——这正是保护数字工作场所安全的两个方面。这种安全方法的主要优势包括：

- **获得整个安全生态系统的可见性。**威胁情报是共享和集中的，企业可以更深入地了解整个安全生态系统，从而更快、更有效地进行威胁预防、检测、调查和响应。
- **自动执行重复任务。**任何企业都不希望员工在缓慢、重复或手动的威胁检测和响应任务上（例如浏览海量的产品报告来查找潜在威胁）浪费精力。通过开放的 API 集成来实现这些流程的自动化，不仅可以提高 IT 安全团队的效率，还可以提高安全工具的有效性。
- **精简基础架构。**集成安全工具有助于整合基础架构管理，从而降低其复杂性并节省 IT 安全团队的精力，使其可以专注于诸如威胁预防、检测和响应等战略计划。
- **加速威胁检测和响应。**与“一次使用一个工具”的方法相比，许多开放的 API 平台可以在几分钟内生成有关企业综合安全生态系统的报告，从而大大减少安全专家针对潜在威胁做出重要决策所需的时间。

- **防御多向量攻击。**通过 API，企业能够获得检测和防御多向量攻击（网络犯罪分子攻击多个入口点）所需的跨工具可见性。如果没有这种威胁情报整合，那么每个工具中的数据就都是分散的，安全团队可能无法及时发现攻击活动。

- **建立自定义的网络弹性策略。**通过安全集成和 API，企业可以利用各个供应商提供的最佳解决方案，来构建与其特定风险环境相匹配的网络防御计划。

需要团队协作

企业可能会认为，依靠一家供应商来满足所有安全需求，似乎比集成多家供应商的解决方案要容易得多。但是，“单点联系”策略有其自身的劣势——特别是缺乏重点和创新能力，因为它们是要出售一堆商品，而非特定商品的最佳方案。此外，这些产品通常不是整合的，这违背了与单个多产品供应商合作的初始目的。

具有开放式 API 策略的安全集成可实现最佳的安全性，以及集成基础架构带来的预期收益。这能够有效地减轻 IT 安全团队的负担、从安全投资中获取更多价值，并更充分地管理新旧企业 IT 环境中的固有风险。

要想领先于攻击者一步，不仅需要安全厂商和工具之间的协作，还需要团队之间的协作。通过集成的安全策略，企业能够消除业务部门之间的现有孤岛，建立一个强大的团队，使其在出现巨变的情况下（如一夜之间实现数字化工作场所）能够更聪明地工作，更快地做出响应并保持敏捷。

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