

## 保持可见性和控制权的同时，实现更好的安全自动化

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	Reach the next frontier of security automation while maintaining visibility and control		
原文作者	Andrew Lintell	原文发布日期	2019 年 12 月 19 日
作者简介	Andrew Lintell 是 FireMon 公司欧洲、中东和非洲地区副总裁兼常务董事。		
原文发布单位	Help Net Security		
原文出处	<a href="https://www.helpnetsecurity.com/2019/12/19/network-security-automation/">https://www.helpnetsecurity.com/2019/12/19/network-security-automation/</a>		
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 <a href="https://bbs.antiy.cn">bbs.antiy.cn</a> 安天公益翻译板块		
免责声明	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul>		

## 保持可见性和控制权的同时，实现更好的安全自动化

Andrew Lintell

2019 年 12 月 19 日

企业所依赖的技术不断发展，增长速度超过了企业保护它们的能力。面对这种不断增加的潜在风险，企业需要改变方法，自动执行更多网络安全操作以减少攻击面。

导致此问题复杂化的主要原因之一是 IT 人才短缺，这会导致企业的 IT 安全专家超负荷工作，增加人为原因导致的配置错误。安全分析师和工程师通常要花很大的精力来应对漏洞，但是 Gartner 认为，到 2023 年，在所有数据泄露事件中，99% 是由配置错误而非漏洞造成的。IBM 在最近的一项调查中指出，云配置错误导致的数据泄露增加了 424%，而云配置错误也是人为原因造成的。

这些事实证明，企业需要采用自动化网络安全策略管理流程来减少人为错误并提高效率。但是，一些企业担心会失去 IT 安全可见性和决策控制权，因此对是否采用自动化策略犹豫不决。幸运的是，他们无需在实现自动化和保持控制权之间二选一。

企业可以从与其当前 IT 安全功能相匹配的自动化方法着手，然后随着其信心和技术成熟度的提高逐步采用自动化程度更高的方法，从而避免上述问题。

### 改善网络控制，降低复杂性和错误

一些企业可能认为，自动化的网络安全操作会降低其对策略和流程更改的可见性和控制权，并降低其遵守安全和隐私法规的能力。实际上，自动化可以消除这些方面的猜测和手动管理，减少配置错误和风险增加的可能性，从而为企业提供更多控制权。

网络安全策略自动化能够为企业带来诸多好处，包括最大程度地减少人为错误、降低安全成本的同时提高运营效率、减少 DevOps 和 SecOps 之间的摩擦、提高整体安全敏捷性，以及在实施新更改之前主动检查法规和内部合规措施，减少违规情况。

### 创建自定义的网络安全自动化方法

我发现，并非每个企业都准备好了接受完全的自动化。对于这些企业，建议他们首先确认其当前的 IT 安全成熟度，然后逐步定义如何发展其自动化流程。这些决策应基于公司的

业务目标、人员配备、客户需求和技术水平。

下一步是将公司置于自动化转型曲线上，以确定其技术进步路径。我认为安全自动化分为四个关键阶段，这能够缩短实现安全流程所需的时间，提高效率。

## 1. 设计自动化

该阶段提供基本的自动化水平。在此基础上，安全专家仍然可以手动监控环境并对环境变化做出响应。同时，这种自动化系统能够提供智能设计建议以改善网络安全；并自动生成合规性和风险评分报告，以改善工作流程并缩短纠正时间。

## 2. 实施自动化

在该阶段，通过提供自动化的网络安全规则实施、验证和记录，企业可以继续提高速度和效率。该阶段仍主要由安全专家控制，但是增加了自动化程度，使安全专家可以将注意力转移到更关键的需求上。

## 3. 零接触自动化 ( zero-touch automation )

网络系统可以监控环境变化并对环境变化做出响应，但是安全专家仍然可以控制全局策略。在此阶段，企业可以将实施更改自动部署到所有设备，并且轻松定义基于意图的标准和黄金规则，以处理耗时的例行更改。

## 4. 自适应安全实施

一段时间以来，安全行业一直将“零接触自动化”视为终极目标，但是现在出现了超越这种自动化的新方法，该方法能够建立真正的自适应网络安全模型。这种自动化方法可跨系统扩展，并在自动检测任何基础网络和基础架构更改时重新校准全局安全策略。这种方法使企业能够保持对安全操作的控制，同时最大限度地提高效率并保持对安全策略的合规性。

通过这种多阶段的方法，企业可以按照自己的自动化步调来满足其当前的网络安全能力和未来期望。为了确定从哪里着手，企业应调查其要实现完全自动化、部分自动化或保持不变的流程类型。然后，企业可以在其舒适度范围内、在其系统允许的范围内尽快实现自动化。

## 探索网络安全自动化的新前沿

我认为，网络安全自动化的新前沿将帮助企业超越“零接触实施”，以不断调整其安全流程，获取实时可见性并控制全局网络变化，实现更高的效率，使 IT 安全专家能够专注于更具战略性的举措。

这种自适应网络安全模型还提供了响应重大事件所需的灵活性，并在事件发生时将其应用于所有环境。企业不必在速度或安全性之间二选一：通过不断监控和调整其网络系统，企业可以保护所有环境中的全局策略并保持合规性。

这种自动化网络安全策略管理解决方案可以满足每个企业的需求和能力。企业无需担心自动化会降低其对混合网络环境的控制权或可见性。通过为当前需求选择正确的自动化方法，企业可以减少人为错误，提高安全敏捷性，并为未来做好准备。

## 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，截止到 2019 年 9 月 30 日，安天的威胁检测引擎为全球超过六十万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>