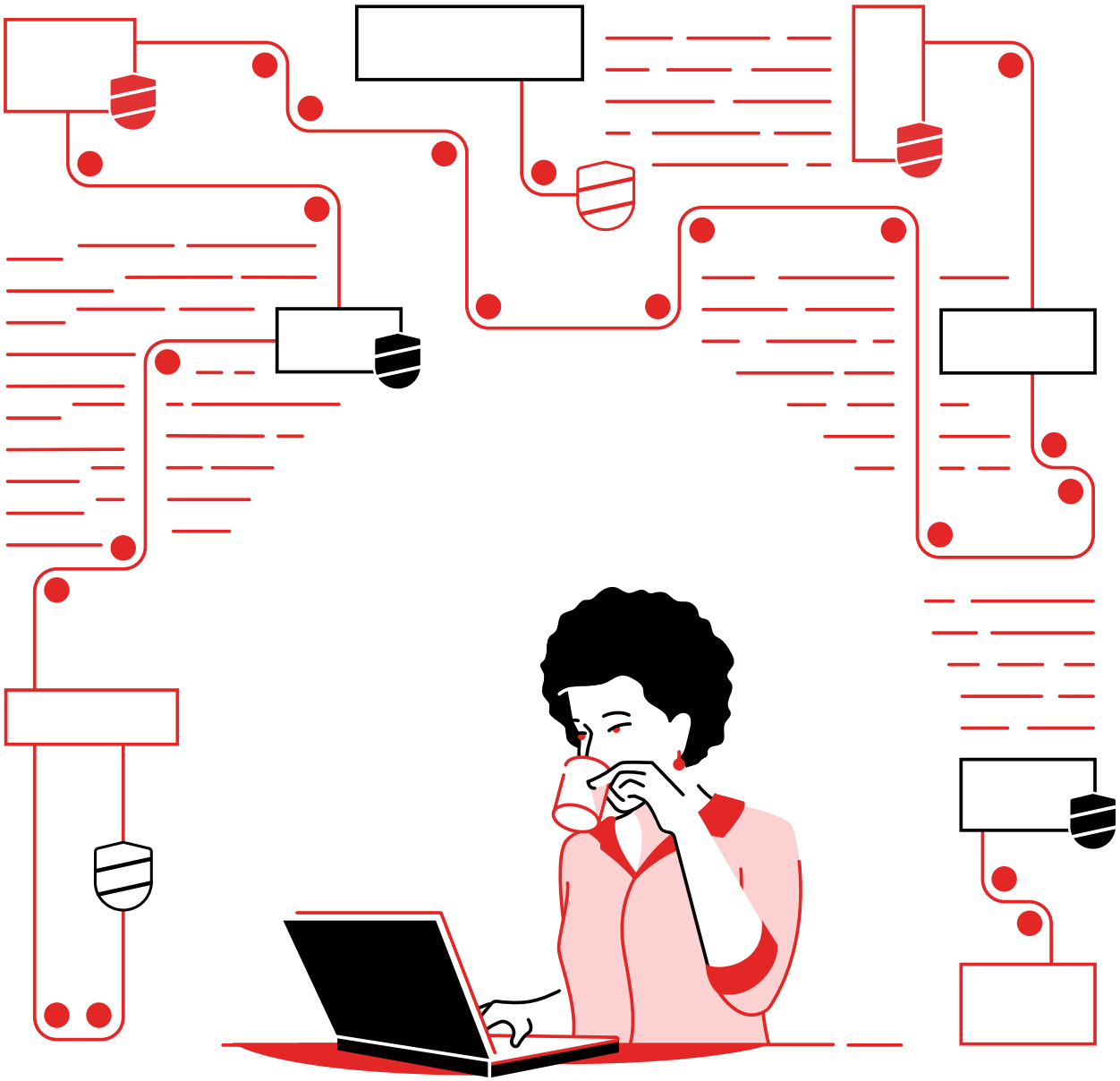
简化您的安全防护运维中心

通过统一的自动化平台加快速度、节省时间、保障安全



Red Hat

目录

IT 安全防护是头等大事

对大多数企业而言，安全防护是头等大事。实际上，33% 的首席执行官密切关注网络威胁。[1] 这种担心并非毫无根据：32% 的企业在过去两年里遭遇了重大的网络攻击。[2]

企业安全防护至关重要，但经常困难重重。安全防护团队必须组建、维护、管理和调整复杂的环境，而且通常要使用来自彼此竞争的不同供应商所提供的多种工具和服务。产品数量年年增多，团队必须随着安全格局改变不断调研、评估和整合新的产品。

此外，数据泄露在数量、严重性和成本上不断攀升。两年内遭遇数据泄露的概率为 29.6%，比 2014 年的 22.6% 有所上升。[3] 2019 年与 2018 年相比，每次数据泄露涉及的记录平均数增加了 3.9%。[3] 数据泄露的平均成本在 2019 年上升到了 392 万美元。[3]

大多数企业以人工方式处理安全防护运维。一旦需要人为介入，安全防护相关任务都会比较耗时、繁琐，也容易出错。因此，安全防护团队不堪重负。他们面临着无数工具发出的威胁警报，警报数量也是日益增多。实际上，60% 的安全防护团队每天收到 5,000 多条警报，16% 的团队甚至每天收到超过 100,000 条警报。[4]

另外，基础架构规模在增大，复杂性也在提高，这让识别漏洞和验证数据泄露变得愈加困难。大多数安全防护工具不能相互集成，安全防护团队必须投入更多人力。事故调查和响应时间也随之延长。2019 年，识别和控制数据泄露平均需要 279 天，比 2018 年增加了 4.9%。[3] 而且，难以找到新的人才来拓展或维系团队；2019 年，39% 的企业报告了网络安全技能方面的短缺。[2] 最后，用于网络安全防护活动的预算也捉襟见肘。只有 33% 的企业反映有充足的资金来实现高层次网络弹性。[5]

因此，典型的安全防护团队只能评估和响应他们所获警报中的 48%，而且只有 50% 的合理威胁得以修复。[4] 这使得许多企业仍然处于易受攻击的境地。

77% 企业计划在其安全防护生态系统中增强自动化，以进行简化并加快响应时间。[4]

无效安全防护的影响

安全漏洞在数量、严重性和成本上也不断攀升。

392 万美元
2019 年数据泄露平均成本[3]

279 天
2019 年识别和控制数据泄露平均用时[3]

122 万美元
识别和控制泄露后节省成本

200 天
或更短[3]

29.6%
两年内遭遇数据泄露的概率[3]

50%
合理威胁得到修复的比例[4]

1 *PWC，“第 23 届年度全球 CEO 调查：驾驭不确定的全球形势”，2020 年。*https://www.pwccn.com/zh/research-and-insights/ceo23/china-report.html。

2 *Harvey Nash 与 KPMG，“2019 全球CIO调查报告：变化中的视角”，2019 年。*home.kpmg/xx/en/home/insights/2019/06/harvey-nash-kpmg-cio-survey-2019.html。

3 *IBM Security，“2019 年数据泄露成本报告”，2019 年。*ibm.com/security/data-breach。

4 *思科，“思科基准研究：守护当前和未来”，2020 年 2 月。*cisco.com/c/en/us/products/security/ciso-benchmark-report-2020.html。

5 *Ponemon Institute（IBM Security 赞助），“网络弹性组织”，2019 年 4 月。*ibm.com/account/reg/us-en/signup?formid=urx-37792。

什么是安全防护自动化?

所谓安全防护自动化，就是自动执行保障业务安全性相关的手动任务。它包含了多种实践方法，我们将之划分为四大类别：

响应与修复
由事件驱动的活动，需要安全分析师的参与或指导

安全防护运维
由技术团队在安全基础架构上执行的日常流程和策略驱动的活动

安全防护合规
旨在确保基础架构符合安全防护策略和规范要求的活动

强化
用于将自定义安全防护策略应用到基础架构的活动，具有有针对性的意图和目标

本电子书重点关注对响应和修复活动及安全防护运维进行自动化。

进一步了解安全防护合规和强化

阅读以下资源，了解自动化对安全防护合规和强化的帮助：

- **《增强混合云安全性》电子书**
- **《开展安全防护与合规自动化的原因》概述**
- **红帽服务：《自动化安全防护和可靠性工作流》产品规格说明**

自动化安全防护运维、响应和修复活动的优势

提升速度和效率

自动化能够简化任务，剔除人工干预的需求，加快安全防护运维速度，并让员工重新聚焦于高价值行动计划。也能降低 IT 基础架构复杂度：40% 的高度自动化企业反映它们拥有数量恰当的安全防护解决方案和技术。[6]

大规模加强安全性

在安全防护基础架构中应用自动化可以加强一致性，让您以对安全性做到统筹兼顾。每名员工都能管理更多的工具、设备和系统，因此您可以开展大规模运维活动。自动化也能降低人为出错风险，提高准确性。

降低数据泄露的风险和成本

广泛开展自动化的企业具有更强的能力来预防安全事故和业务中断。[6] 全面部署安全防护自动化可以使数据泄露平均成本降低 95%。[7] 因此，52% 的企业部署了一定数量的安全防护自动化，另有 36% 计划在未来 24 个月完成部署。[7]

6 Ponemon Institute（IBM Security 赞助），“网络弹性组织”，2019 年 4 月。ibm.com/account/reg/us-en/signup?formid=urx-37792。

7 IBM Security，“2019 数据泄露成本报告”，2019 年。ibm.com/security/data-breach。

自动化集成您的安全防护工具、系统和流程

通过一致且灵活的平台统一人员、流程和工具

自动化平台可用作您安全防护团队，工具和流程之间的集成层。灵活、互操作平台让您：

- 连接安全防护系统、工具和团队。
- 从系统收集信息并将它快速转到预定义的系统和位置，无需人工干预。
- 从中央化界面快速更改和传播配置。
- 创建、维护和访问与您的安全防护工具和流程相关的定制自动化内容。
- 在检测到威胁时自动触发多个安全防护工具的操作。

在企业内使用一致的自动化平台和语言还可以增强沟通和协作。如果安全防护产品组合中的所有解决方案都通过同一语言进行自动化，分析师和操作员就能在不同的产品间迅速执行一系列操作，最大程度提升安全防护团队的整体效率。此外，通用的框架和语言还能让安全防护和 IT 团队在企业内外轻松地共享设计、流程和想法。

图 1. 自动化平台能够集成您的安全防护系统、工具和团队。

成功的自动化 = 人员 + 流程 + 平台

最大程度提高自动化价值需要的不仅仅是工具，您还需要考虑人员、流程和平台。

- **人员**是任何业务行动计划的核心。员工积极参与团队内和跨团队活动，可以更加高效地共享理念并开展协作。
- **流程**让您企业中的项目从头至尾顺利开展。有效自动化离不开条理清晰、记录完善的流程。
- 自动化**平台**提供相应的功能来帮助您构建、运行和管理自动化资产。与简单的自动化工具相比，自动化平台让您的企业获得统一的基础，可以大规模创建、部署和共享一致的自动化内容与知识。

阅读电子书

安全防护自动化之旅

在企业的任何层面实施自动化不会一蹴而就，也不适合孤注一掷。安全防护自动化之旅企业将各取所需在不同的地方开始（或停止）。这些需求也决定了每个企业可以采取的路径。尽管如此，不论您处于哪个阶段，即使在安全防护自动化投入少许力量也能产生效益。

评估您的安全防护自动化成熟程度

安全防护成熟度分为三个主要阶段，大多数企业都能归入其中一个阶段。确定企业当前所处的阶段可以帮助您在恰当的时机采用正确的工具和流程，确保您的自动化之旅更加圆满。

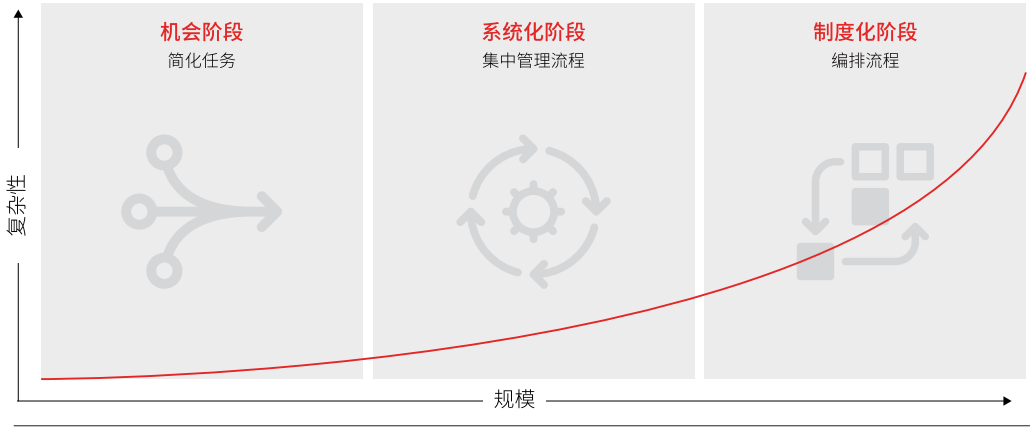


图 2. 安全防护自动化成熟度的不同阶段

阶段 1：化挑战为机遇

这个阶段的重点是通过自动化安全防护运维来节省时间。常见的目标包括标准化相似设备和技术之间的安全防护操作，以及简化在来自不同供应商的产品之间执行的手动任务。

第 2 阶段：系统化

这个阶段的重点是通过采用一系列安全防护运维工具和服务来改进流程并提高效率。常见的目标包括将安全防护流程构建为更高层次的工作流，并且集中处理安全防护响应流程。

第 3 阶段：制度化

这个阶段的重点是在企业内加强协作并集成安全防护。常见的目标包括创建自动化的编程式工作流，以覆盖安全防护的所有层面，也包括集成您的安全防护和 IT 技术。

阅读博客文章

用例和集成

定义您的路径实现安全防护自动化

安全防护自动化的常见高级用例

这些用例中的每一个都可以作为您安全自动化旅程的起点。关键是从小处着手，从简单开始，再日积月累。

调查详实

调查安全警报和事故涉及从各类安全防护系统收集信息，以评估是否发生了合理的事件。信息通常通过一系列用户界面、电子邮件和通话来收集。这样的低效率流程可能会延误抵御威胁的行动，让企业停留在易受攻击的境地，并且增加与数据泄露相关的潜在成本。通过自动化，您可以用编程方式从各种安全防护系统汇总信息，并以按需辅助的方式来支持通过安全信息和事件管理（SIEM）系统执行的分类活动。如此一来，您可以更快的速度评估和响应警报与事故。

搜寻威胁

搜寻威胁涉及以主动的方式来识别和调查潜在安全威胁。与事故调查一样，员工在许多系统之间手动收集和发送信息。借助自动化，您可以自定义和简化警报、相关搜索和签名操作，更快地检查潜在威胁。还能自动创建和更新 SIEM 相关查询及入侵检测系统（IDS）规则来改进检测。这样，您可以更加频繁、更有效率地更新企业的安全防御举措，为业务提供更好的防护。

事故响应

事故响应涉及采取措施来阻止泄露继续发生。检测到数据泄露时，安全防护员工必须快速响应，并通过规模化手段将其控制。然而，响应举措通常包含多项人工任务，这延缓了修复时间，并让企业在更长时间内处于易受攻击的状态。借助自动化，您可以将各种操作编写为可重复执行并且预获批准的 playbook，从而迅速响应。您可以加速执行各种任务，如拦截发出攻击的 IP 地址或网域，允许没有威胁的流量，冻结遭到泄露的凭据，以及隔离可疑工作负载以作进一步调查，从而减轻与事故相关的损害。

必要的集成

统一的自动化方法需要在您的自动化平台和安全防护技术之间进行集成。必要的集成包括：

- **防火墙**，控制网络之间的流量流，以保护对互联网公开的应用。自动化可以加快执行策略和日志配置变更。
- **入侵检测与防护系统（IDPS）**，监控网络流量中的可疑活动，发布威胁警报并阻止攻击。自动化可以简化规则和日志管理。
- **安全信息和事件管理系统**，收集和分析安全事件以帮助检测威胁并做出响应。自动化可以提供对数据源的编程化访问。
- **特权访问管理（PAM）工具**，监控和管理特权帐户和访问。自动化可以简化凭据管理。
- **端点防护系统**，监控和管理设备以增强其安全性。自动化可以简化常见的端点管理任务。

了解更多

利用红帽 Ansible 自动化平台简化您的安全防护运维中心

可用的自动化解决方案有许多，但并非全部包含有效安全防护自动化所需要的功能。寻找具备以下特征的自动化平台：

- **通用的、易于访问的自动化语言。**语言要易于理解和编写，从而方便您记录信息，并在具有不同专业领域的安全防护团队成员之间共享。
- **开放且公正的方法。**若要发挥作用，自动化平台必须能与您的整个安全防护基础架构和供应商生态系统进行交互操作。
- **可扩展的模块化设计。**模块化的平台允许您分阶段部署自动化。可扩展性则有助于您日后根据需要融合来自其他供应商的额外安全防护工具。

在红帽协助下发展您的安全防护企业

红帽® Ansible® 自动化平台是构建和运作自动化服务的基石，提供所有的必要工具和功能来帮助您实施安全防护自动化。它将简单、易读的自动化语言与可信、可组合的执行环境相结合，同时融合了专注于安全性的共享与协作功能。拥有开放的基础让您几乎能够连接和自动化您的安全防护与 IT 基础架构中的一切，打造一个通用的平台供整个企业参与和共享。红帽 Ansible 自动化平台也在其他方面提供切实的成果，如 IT 和网络运维以及 DevOps 等。

该平台附带一系列**以安全为本的 Ansible 集合**，包括各种模块、角色和 playbook，受到红帽的支持。这些资产可以协调多类安全防护解决方案的活动，从而以更加统一的方式来响应网络威胁和安全防护运维：

- 串联工作流和 playbook 以实现模块化可复用性。
- 整合和集中管理日志。
- 支持本地目录服务和访问控制。
- 利用 RESTful 应用编程接口（API）集成外部应用。

红帽 Ansible 自动化平台也包含协助您优化自动化的工具和功能。**自动化分析**提供有关企业的自动化使用情况的深入见解。**自动化中心**让团队成员通过一个中央存储库访问认证的自动化内容。另外，**内容集合**可以简化自动化资产的管理、分发和使用。

获取专家的帮助

红帽可以帮助您以更快的速度圆满部署自动化。

- **红帽服务计划：自动化采用**提供了一个掌控企业范围内自动化之旅的框架。
- **红帽培训与认证**提供实训课程和实践认证，帮助您更加有效地利用自动化。
- **红帽支持**与您携手合作，确保您在 IT 之旅上顺利前行。备受赞誉的 Web 支持[8] 让您能够访问各种最佳实践、文档、更新和安全警报和补丁。您还能与支持工程师或大客户技术经理联络，以解决问题并获得特别指导。
- **认证合作伙伴内容精选**协助您做好准备，对来自众多供应商的硬件和软件进行自动化。这一值得信赖的预构建自动化内容通过“自动化中心”提供，由合作伙伴和红帽联合提供支持。

8 红帽客户门户奖励与表彰，access.redhat.com/recognition。

自动化应用

红帽 Ansible 自动化平台所能带来的业务价值久经验证

红帽 Ansible 自动化平台提供高效又精简的方式，协助您对安全防护运维中心开展自动化。分析师对使用红帽 Ansible 自动化平台的企业进行了研究，结果表明它能带来可衡量的业务价值。实际上，IDC 就红帽 Ansible 自动化平台的使用体验采访了多位决策者，结果发现每家企业都通过自动化实现生产力、敏捷性和运营收益的显著提升。

IT 安全防护团队效率和生产力提升[9]

缓解安全事故的效率提升[9]

安全补丁部署的效率提升[9]

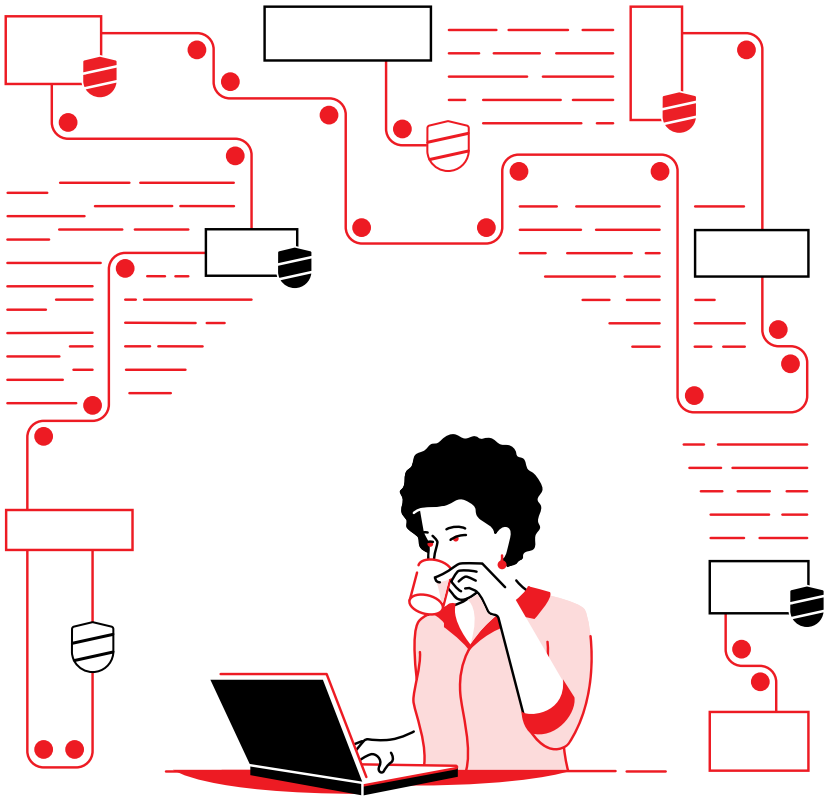
“红帽 Ansible [自动化平台] 太棒了，能够凝聚我们不同 IT 团队的力量。服务器、安全、网络和数据库团队可以各自处理负责的层面，然后使用红帽 Ansible 自动化创建自己的 playbook。”[9]

阅读分析师报告

9 IDC 白皮书，红帽赞助。“红帽 Ansible 自动化可提升 IT 敏捷性并加快产品上市”，2019 年 6 月。
redhat.com/zh/resources/business-value-red-hat-ansible-automation-analyst-paper。

准备好简化您的安全防护运维中心了吗?

自动化可以帮助您以更快的速度大规模识别和响应日益加剧的安全威胁。红帽提供统一的可协作自动化平台，让您整合安全防护团队、工具和流程来保护您的业务。



了解如何使用红帽 Ansible 自动化平台实现安全防护自动化：
red.ht/automate-security

版权所有 © 2020 Red Hat, Inc。红帽、红帽 logo 和 Ansible 是红帽或其子公司在美国和其他国家/地区的商标或注册商标。

F24343_0720_KVM

Red Hat