聚焦安全防护：人为错误的成本和自动化的优势

为什么政府机构正在重新审视手动管理安全防护的方式，智能自动化将如何帮助防范潜在威胁，避免产生代价高昂的安全漏洞

下一个

在本电子书中：

01 简介：日益严峻的网络犯罪形势

网络犯罪案例正呈上升趋势。上一财年，澳大利亚网络安全中心（ACSC）收到了超过 67,500 份网络安全报告，同比增长 13%，自报损失总额超过 330 亿美元[3]。其中，大约有四分之一的事件对澳大利亚关键基础架构相关的实体造成了不利影响。

许多政府机构越来越多地采用新兴技术，并采用混合工作模式，与此同时，网络攻击者也在不断改变其攻击手段。员工队伍和计算资源愈加分散，IT 基础架构格局迅速演变，这为不法分子创造了利用安全缺陷和漏洞的新机会，企业和机构为防范数据泄露而付出的成本也水涨船高。即使企业和机构拥有强大的安全态势，在这样的环境中也会面临诸多风险。

针对网络犯罪分子的主动安全防护

网络犯罪分子不断研发新手段来攻击受保护的系统和数据，企业和机构面临着内部和外部的双重压力，需要制定更具战略性和主动性的网络攻击保护策略。事实上，数据安全和隐私措施必须遵守更全面的法规和条例要求。

例如，“新南威尔士（NSW）网络安全政策”现在要求根据 ACSC Essential Eight（ACSC 八项基本网络安全措施）中的风险缓解策略[1] 来落实和提供成熟度评估。Security Legislation Amendment of Australia’s Critical Infrastructure Bill（澳大利亚关键基础架构法案之安全立法修正案）可能会增加负责管理或运维关键基础架构的政府机构的监管负担[2]。

强化防御机制

需要改善网络安全的企业和机构首先需要识别现有漏洞。即使全面的防护策略已落实到位，但人为错误和培训不足也常常会危及安全。若放任不管，微不足道的错误也可能会造成系统风险，让问题变得更加复杂。因此，许多企业和机构正采用自动化方法来增强其安全策略的可靠性并降低相关风险。

在本电子书中，我们将探讨人为错误导致的风险将如何影响对网络犯罪的打击效果。我们还将讨论自动化关键网络安全风险缓解策略将如何增强安全防护，同时减少耗时费力的任务，减轻 IT 团队的负担。

网络犯罪给澳大利亚带来的损失。

67,500

网络攻击报告数量[3]

330 亿美元

自报损失数额[3]

13%

攻击案例数量同比增长率[3]

1. 新南威尔士州政府。“DCS-2021-02 NSW Cyber Security Policy（DCS-2021-02 NSW 网络安全政策）”。2021 年 2 月。
2. 澳大利亚议会。“Security Legislation Amendment (Critical Infrastructure) Bill 2021（安全立法修正案（关键基础架构）法案 2021）”。2021 年。
3. “ACSC 年度网络威胁报告 2020-21”。澳大利亚网络安全中心，2021 年 9 月。

02 有效的安全防护策略需要人人参与

人人都会犯错

IT 团队中的成员也经常低估或误解其系统的漏洞以及由此产生的安全风险。无法准确评估风险可能会使企业和机构产生巨大的成本。

举个例子，想象一下，技术人员在手动更新防火墙时，犯了一个不以为意的小错误，并且这个漏洞一直未得到妥善解决。他们并没有意识到，这个微小的错误会发展成为企业 IT 系统的关键漏洞，给网络犯罪分子带来可乘之机。

在这种情况下，技术人员的小错误可能会导致各种负面结果，包括数据泄露、违反行业和政府数据安全法规、导致服务中断和系统停机，而所有这些后果都要由企业和机构来承担。

从修补应用和更新防火墙，到设置和执行管理权限，如果全都依靠手动方式，安全防护难题的许多方面都有可能出错。网络犯罪分子识别漏洞的能力越来越强，仅依靠运维团队来处理这些任务可能会造成无法挽回的破坏性后果。

人才短缺加剧了安全漏洞

网络安全人才供不应求，这进一步增加了手动任务期间出现人为错误的可能性。经过专业培训、掌握相关技能，并有能力评估和解决安全风险的能人才干远远不够。（ISC）[2] 网络安全劳动力研究指出，澳大利亚需要增加 25,000 名 IT 安全工作人员来填补其网络安全缺口[4]。

网络安全专家的长期短缺让政府机构更加难以妥善管理风险。IT 团队早已不堪重负，根本没有时间在整个企业和机构中实施安全流程，更不用说在第一时间建立相关安全流程了。

为安全团队配备自动化工具

手动安全流程和技能短缺正在不断增加企业和机构的风险，如何解决这两个问题是打击网络犯罪的关键，而自动化解决方案在两方面皆大有可为。随着深入了解，我们发现自动化安全流程可提供整个企业和机构迫切需要的一致性、准确性和可扩展性。

手动安全措施的风险

“2021 年，在未实施安全防护自动化的企业和机构中，平均泄密成本为 671 万美元；而对于完全部署安全防护自动化的企业和机构，平均泄密成本仅为 290 万美元。”[5]

4. “弹性网络安全职业规划的前进之路”，（ISC）[2] 网络安全劳动力研究，2021 年。
5. “2021 年数据泄露成本报告”。IBM，2021 年。

03 风险管理的常见挑战

政府机构需要更有效的风险管理措施

为了确保官方信息的机密性、完整性和可用性，政府机构必须能够准确高效地识别和管理风险。安全威胁不断演变，企业和机构需要实施精准的风险分析，拥有灵活应变的安全态势。实现自动化运维是快速响应这些变化的关键。

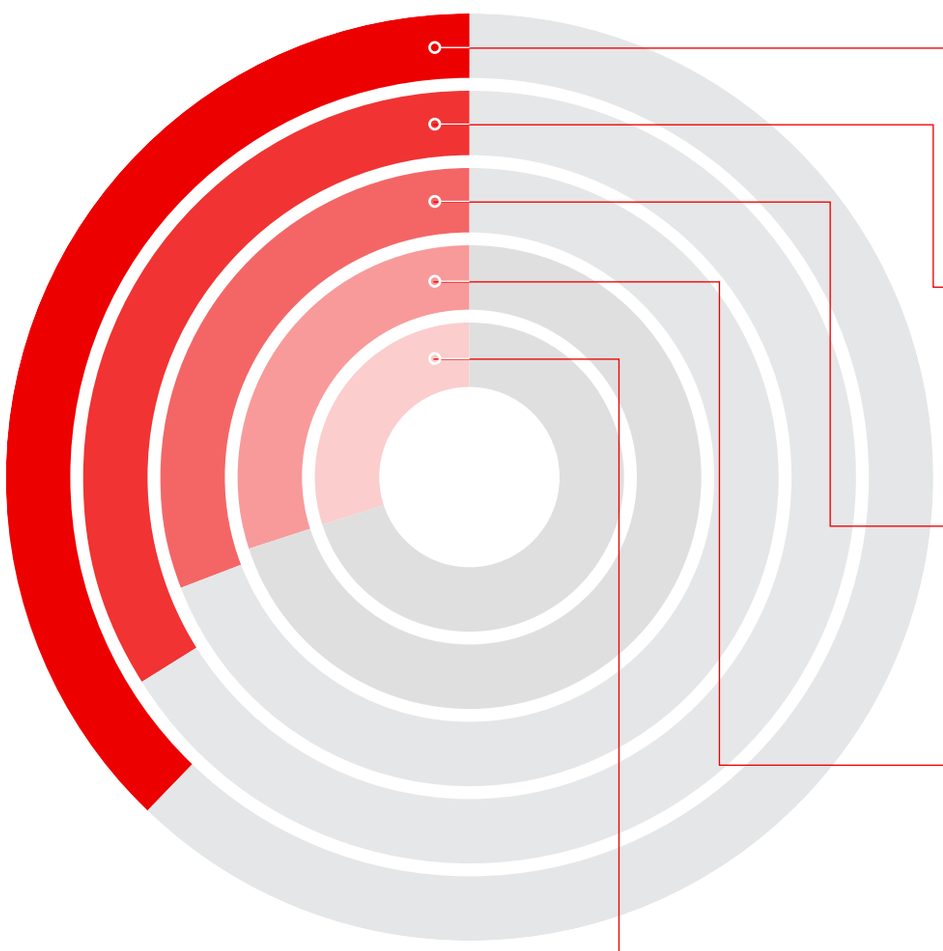
阻碍安全实践改变的障碍

在加强安全防护的过程中，政府机构需应对多方面的挑战，首当其冲的是变更管理。常见问题包括：

- 如何扩展团队以实施全新网络安全计划？
- 我们应如何为企业和机构中的不同部门提供支持，以确保不违反新的安全协议？
- 采用企业和机构所需的现代安全策略的同时，我们可以采取什么措施来更有效地保护提供关键服务的现有系统？
- 我们可以在现有架构中部署与零信任类似的策略吗？

但是，企业和机构不应将这些考虑因素视为负担，而是应该将不断变化的安全环境视为重新评估其安全实践和实施更严格协议的机会。

常见网络安全挑战



38%

盯紧瞬息万变的威胁[6]

34%

有关风险和行为的指导[6]

31%

巩固内部网络安全态势[6]

30%

网络安全培训的必要性[6]

30%

数据泄露的法律/财务后果[6]

6. “2021 年渠道报告”。CompTIA，2021 年 8 月。

04 借助自动化增强安全态势

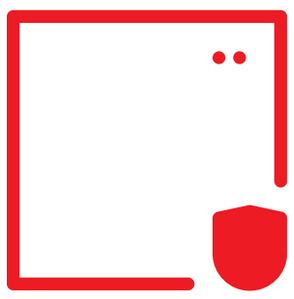
自动化网络安全战略的关键要素

政府机构正在借助网络安全自动化的力量，降低风险并帮助打击网络犯罪。自动执行常规的重复工作，可以让网络安全团队专注于更关键的战略任务。此外，自动化有助于减轻 IT 团队的工作量，从而更大限度地减少人为错误并降低安全风险。

ACSC Essential Eight 中详细说明了应如何借助自动化来强化网络安全战略。在落实 Essential Eight 时，许多企业和机构都因为资源有限、技术匮乏而无法持续地减少或消除人为错误。

为解决这一问题，IT 负责人认识到，可以且应该对其安全框架中的部分环节进行自动化。以下示例说明了应以何种方式对哪些环节进行自动化：

自动执行 ACSC Essential Eight

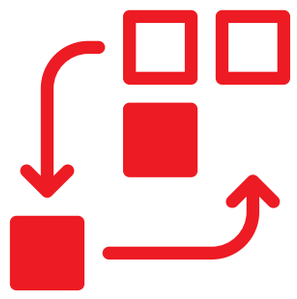


应用控制

跨混合云自动变更应用控制状态

修补应用和运维系统

自动执行预检、内容升级以及更新后的验证和测试



备份和恢复

自动执行备份、恢复和验证测试

改进修补流程

为了帮助防范攻击，Essential Eight 中建议企业和机构定期修补并更新应用以避免发生恶意安全问题。在有可用更新后立即修补应用不仅是最佳实践，通常也是法规要求。但是，手动修补总是容易发生人为错误，并且在大型企业和机构中也非常耗时费力。

安装补丁是非常适合借助自动化工作流完成的任务。企业和机构还能自动执行验证和测试，而无需依赖 IT 员工来执行测试、设置预检和运行修补程序。再加上其他相关的安全措施，这样便可以确保所有步骤都顺利高效地进行。

掌管管理员权限

为了限制攻击范围，Essential Eight 建议企业和机构对管理员权限加以限制。控制特权访问有助于保障基础架构和应用的安全，高效地推进业务流程，并维护敏感数据和关键基础架构的机密性。

机构中应仅有少数人拥有全局控制权。确定谁应拥有特权并不简单。预测安全事件的影响范围，并评估该潜在事件的总体影响也并非易事，但如果能做到，您就可以预测有人滥用凭据时可能造成的后果。随后，便可由 IT 团队来部署相关安全措施，以确保类似事件不会对整个企业和机构产生影响。

通过自动执行特权访问管理工作流，并集中存储访问凭据，而不必注入到存在泄漏风险的应用中，将使整个过程变得更加可控、可靠。

05 红帽在网络安全管理方法中扮演的角色

建立适应未来发展的网络安全实践

红帽® 解决方案将帮助您自动执行现有的手动流程，减少因企业和机构 IT 团队负担过重、人手短缺而导致的疏忽问题，从而降低风险。我们的开源产品提供了跨云环境和架构的灵活性和可扩展性，支持企业和机构在当前和未来的环境中进行部署。

通过在任何网络安全成熟度模型的基础上使用自动化，企业和机构可以采取实际步骤，以迭代方式快速添加自动化层，取代手动流程。红帽解决方案可以帮助缓解和响应风险。

红帽 Ansible 自动化平台

红帽 Ansible® 自动化平台使用人类可读的自动化语言 Ansible，可将复杂的手动流程转化为自动执行的工作流。Ansible 自动化平台让 IT 团队可以在整个公司中自动执行并整合不同的安全协议。此平台将帮助企业和机构利用精选模块、角色和 Playbook 集合，以协调统一的方式来调查和应对威胁。

红帽 Ansible 自动化平台将帮助企业和机构对以下任务进行自动化：

- 根据通用漏洞披露（CVE）进行修补。
- 应用控制部署。
- 备份和恢复或验证流程。

Ansible 自动化平台可提供兼具安全性和稳定性的企业级框架，帮助实现从混合云到边缘环境的大规模构建及运维 IT 自动化。该自动化解决方案允许整个企业和机构的用户创建、共享和管理 Ansible Playbook，无论是开发和运维团队还是安全和网络团队，均可参与其中。IT 主管可以提供将自动化应用于各个团队的指导，而自动化创建者则可以利用现有的知识编写任务。

此外，Ansible 自动化平台中包含来自 CyberArk、IBM 和 Splunk 等众多经认证合作伙伴的内容，可作为安全解决方案的集成点，帮助自动化管理和整合不同的安全技术。

进一步了解 Ansible 自动化平台 >

红帽企业 Linux

红帽企业 Linux® 为在裸机、虚拟环境、云端以及边缘环境之间扩展现有应用并部署各种新兴技术提供了基础。

为应对安全挑战，红帽企业 Linux 主要围绕三个方面采取了切实措施：

- 缓解风险：管理安全防护，同时降低被入侵的风险，以避免发生数据泄漏、系统漏洞或声誉受损。
- 提供保护：大规模自动化安全控制，并对其进行持续维护，最大程度减少停机时间。
- 符合标准：针对处在监管严格的环境的企业和机构，高效精简合规标准。

红帽企业 Linux 内置符合信息安全手册（ISM）和 Essential Eight 等 ACSC 指南的安全策略，旨在通过简单、一致地向新数字化服务自动部署安全控制，帮助政府机构更有效地管理风险。

进一步了解红帽企业 Linux >

Red Hat

上一个

红帽助您强化安全防护

红帽将竭尽所能，助您提高数字化服务的安全防护

红帽可以帮您自动执行 ACSC 指南中的相关措施，并通过自动化安全集成优化风险管理。

欢迎随时联系我们以了解更多信息 ›