借助 IBM QRadar on Cloud 确保可控性

目录

智能 SIEM 即服务

对于任何规模的组织来说，保护内部环境和云端数据和网络的安全都是一项艰巨的任务。几乎每天都会发现新的漏洞；一旦针对旧脚本编写了检测脚本，就会开发出新的恶意软件菌株；网络罪犯可以在背靠专业支持团队的暗网上购买预先打包的漏洞利用工具包。作为安全分析人员，您需要部署多款旨在保护网络边缘的解决方案。您需要确保可视性和洞察力，还需要在事情变得异常时洞悉它们的“直觉”。

IBM® QRadar® on Cloud 在这些方面的表现非常出色。该解决方案具有强大的安全信息和事件管理 (SIEM) 功能，可通过诸多功能帮助您确保数据和网络安全，这些功能可以向您展示谁在在何时何地做什么。它的仪表板和高级可视化功能将成千上万个离散事件压缩为可疑故障的简单指示器，同时保留所有可疑活动的详细记录，以供将来分析。同时，该解决方案的高级日志记录功能和报告生成工具，可帮助您快速实现与法规报告要求等基本要求的合规性。

[了解有关 IBM QRadar on Cloud 的更多信息 →]

QRadar on Cloud 每秒可处理超过

500,000 起事件。[1]

IBM QRadar on Cloud 的关键优势

“CIO是否必须将其质疑范围从‘云是否安全’转变为‘我是否正在安全地使用云？’”

Gartner
Gartner.com

探索优势 →

同时满足合规与安全需求

您可能已经在网络外围部署了基本的安全措施，以防范简单攻击，但是大多数端点都存在安全漏洞，而且一些用户也无法拒绝点击恶意链接。设备和凭证经常会被攻击，为数据丢失和潜在的业务中断打开了方便之门。

部署数据收集和合规报告系统非常容易，但是若要让审计人员满意并保护组织的关键数据却并非易事。系统越高级，就越能更全面地准备需要调查和事件响应的常规活动和异常网络漏洞的管理。

通过 IBM X-Force Threat Intelligence® 获取有关当今企业威胁的更多洞察力 →

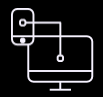
观看并发现有关高级持续威胁的更多信息 →

“使用认知功能处理和关联非结构化数据将会为我们提供更多情境信息，进而为您提供更准确的可执行建议，并让日常工作中的安全分析人员的工作更加轻松。”

Christophe Bianco，
Excellium Services 管理合伙人兼首席技术官

阅读案例研究 →

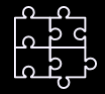
QRadar on Cloud 所提供的功能：



从资本开支转为运营开支模式

解决技能差距

高可视性、合规性和安全性



超过 500 个开箱即用型集成件

基于 AI 的数据驱动型洞察力

灵活性和扩展性

获取深入洞察力，保护您的云端关键资产

检测和消除恶意软件并建立防火墙规则，进而确保子网安全非常重要。这就是为什么您可能要投资外围安全的原因。不过安全分析软件基于以下基本概念，即：外围不连接到互联网肯定是真正安全的，并且组织必须具备检出行为更改和异常的能力。

借助云模型，您的组织可以部署安全性高的数据网关，并将您的安全数据发送到经过专业部署和管理的云环境中，并且每月的运营费用均可预测。云模型可以帮助您确保可控性，而且允许您的员工投入更多的时间来监控环境、调整威胁检测规则、自定义法规或管理报告，而无需运用软件补丁和执行数据备份。

紧跟法规变化，确保合规 →

IT 决策者每天几乎花费

2 个小时的时间来寻找相关数据。[2]

69% 的公司

将合规性视为必须投入开支的事项。[3]

让组织为合规做好准备

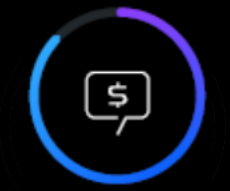
QRadar on Cloud 解决方案具有一项主要的业务驱动功能。通过保护数据并以可审计的形式保存支持保护的安全实践和事件记录，它可以帮助组织遵守政府和行业法规。一旦忽略了这些必须实施的措施，组织就会面临惩罚，就像恶意软件可以令组织遭受数据丢失一样。

您可以通过一系列旨在保护消费者个人与财务信息、提高公司透明度要求和最佳实践标准来治理收集、存储和保护客户与组织数据的方式。萨班斯奥克利法案（SOX）、支付卡行业数据安全标准（PCI DSS）、医疗保险可携性和责任法案（HIPAA）、欧盟的通用数据保护条例（GDPR）和其他法规，意味着企业可能会面临民事或刑事处罚、禁止使用支付卡以及其他风险，其中包括因不合规行为而造成严重的业务中断。

查看 IBM QRadar 针对 GDPR 进行的内容扩展 →

违反 HIPAA 的行为可能会遭受刑事处罚，每次违反最高可能会被处以 50,000 美元的罚款，每年的罚款最高可达到

150 万美元。[4]



88% 的公司

为应对 GDPR 而投入的开支超过 100 万美元。[3]

协助对威胁进行优先排序

您可以借助用于解决各种安全问题的专用工具，从策略上解决某些安全威胁。这些工具有助于解决已定义的威胁和已知问题，而且可能会生成非常简单的响应，例如选择性地阻止网络端口、删除恶意软件实例或修补已识别的易受攻击资产。

不过，QRadar 软件相比单点解决方案而言更具价值，因为它能够收集范围广泛的安全数据，而且基本上可在所有安全智能模块之间共享这些数据。一旦观察并计算出了网络上数据流规范的阈值，它便会自动检测违反这些阈值的事件并向安全人员发出警报。

阈值规则可以帮助我们检测异常增多的出站数据传输、带宽使用、应用更改或来自意外互联网协议（IP）地址的大量可疑登录尝试。QRadar 还能够监控关联事件，例如比较用户身份、源 IP 地址和目标 IP 地址以及活动发生所在的地理位置。它能够审查这些关联事件的情境信息，进而从新行为的一次性实例中找出真正的攻击。

阅读有关 IBM X-Force 2020 年安全预测报告的更多信息 →

网络安全比以往任何时候都要复杂。在 2019 年，识别和遏制数据泄露事件所需的平均时间为

279 天

全球数据泄露事件的平均成本大约为

390 万美元。[5]

医疗保健是数据泄露成本最高的行业，单条丢失或被盗记录的成本高达

429 美元。[5]

通过基于云的安全软件采用新的开支模式

软件对于 IT 和企业运营而言至关重要，但是对于大多数组织来说，将安全软件保留在内部将会增加额外的工作量，进而从实际上会妨碍其核心安全任务。减少和简化安全人员需要扮演的混合角色，可能是采用基于云的替代方案的一个重要动机。

提升安全性总是需要一定程度的人力和技术资源投入，但是使用基于云的托管解决方案，可以减少安全人员投入到日常工作上的时间和相关费用，将其用于分析和规划。

阅读该白皮书，了解有关 QRadar on Cloud 这款灵活且高度可扩展的 SaaS 解决方案的更多信息 →

成本对比
内部部署与云端部署

启动成本	内部部署	SaaS
定制化	●	●
硬件	●	
实施	●	●
IT 员工	●	
生命周期管理	●	
维护	●	
软件许可	●	
培训	●	●

经常性成本		
持续 IT 成本	●	
持续维护成本	●	
补丁和修复成本	●	
升级成本	●	
订阅成本		●

“我们的平均总成本所有增加，但我们觉得这种增加并不一定是坏事。长期以来，我们一直在对数据保护进行投资，因为我们知道数据泄露是不会消失的。”[6]

Ponemon 于 2018 年针对南非工业领域的 IT 主管进行的数据泄露成本调研

阅读该案例研究 →

使用其他安全工具扩展 QRadar

QRadar on Cloud 继承了 IBM 在过去十年开发的 500 多个现有集成件，不仅可响应内部部署客户的请求，而且能够与用以补充安全智能平台的第三方解决方案保持一致。经验丰富的专业人员在完成云部署后，几乎无需开发任何新的支持模块，便可开始接受资产和应用中的数据。大多数客户会在达成协议后的数天内开始实现价值。

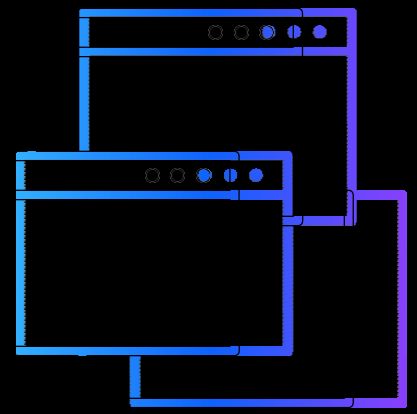
您可以从 IBM Security App Exchange 下载并安装新的扩展件或应用，这些扩展件或应用能够增强您的网络监控功能，而且 IBM Cloud™ 维护团队也将会为您提供此类技术扩展的相关支持。这些受支持的扩展件目前有数十种之多，包括新的可视化扩展、集成、补丁、自定义规则和完整的新应用，例如 IBM QRadar User Behavior Analytics 应用。该站点的所有内容均已由 IBM Security 通过“Ready for IBM Security Intelligence”验证流程进行了审核。

通过 IBM Knowledge Center 了解有关 QRadar 插件和扩展件的更多信息 →

QRadar 能收集来自

500 多个

应用和设备的日志事件和网络流信息。[7]



借助 AI 解决技能差距

近年来，网络安全技能的差距急剧拉大。IBM QRadar Watson Advisor App 旨在帮助组织更快地检测威胁。

该应用采用人工智能（AI）来协助用户进行事件与风险分析、分类和响应，并帮助安全运营团队实现事半功倍，同时提升准确性。结果如何呢？安全团队可以将调查事件所花费的时间从数天、数周大幅缩短到数分钟或数小时。

此外，安全团队仅需投入较少的时间便可处理安全运营中心（SOC）的常规任务，而将更多的时间投入到其他战略重点。

了解 QRadar Advisor with Watson 如何帮助您的 SOC 团队实现事半功倍，同时提升准确性。观看视频 →

探索 QRadar Advisor with Watson V2.5.0 →

到 2022 年，网络安全岗位缺口预计将达到

180 万。[8]

最近的一项调研结果显示，全球网络安全人员的数量需要

增加 145%

才能弥补技能差距。在美国，安全人员的数量需要增加 62%。[9]

“Cargills Bank 能够通过 IBM QRadar SIEM 及 QRadar Advisor with Watson 收到实时的、经过优先排序的警报，进而克服这些限制。“IBM 最佳的认知安全产品组合将会帮助我们预防威胁并减缓风险，助力我们发展为领先的数字银行。”

Rohan Muttiah
Cargills Bank 首席运营官

阅读该案例研究 →

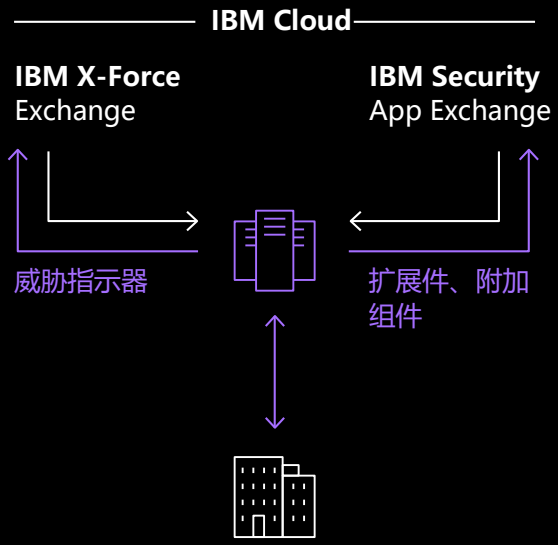
提升灵活性和可扩展性

购买软件即服务（SaaS）产品有助于实现可扩展性和灵活性方面的优势，因为这意味着容量变更不会再拘泥于现场基础架构，并且对内部人员可用性的依赖也大大降低。如此一来，企业便可在这种经济中迅速变革。借助 QRadar on Cloud 解决方案，无论是因并购而导致的偶尔流量激增，或是工作负载的永久变化，企业都可以根据需求扩展其计算能力。由于基础架构部署在云端且在设计时考虑了容量变更，因此无需在本地更改软件。企业可以在短时间内增加或降低容量，几乎不需要客户参与其中。

QRadar on Cloud 产品亮点

- 弹性升级；快速实现价值
- 专用 DevOps
- 24x7 全天候运行状况监控
- 系统管理：升级、补丁
- 支持 450 多款安全与 IT 集成件
- 高级威胁检测
- 可配置的 SOC 及管理仪表板
- 全球存在点覆盖
- 面向服务提供商的多租户模型支持

IBM QRadar on Cloud



客户的内部或云端资产

- 安全设备
- 服务器和云资源
- 网络和虚拟活动
- 数据活动
- 应用活动
- 漏洞和威胁
- 用户和身份

“以前，我们的安全一直都比较滞后，而现在我们变得更加主动。”

Michael Warrer
NRGi 首席信息官

阅读该案例研究 →

访问托管服务

对于其安全人员没有时间也不具备专业知识来满足其所需功能的组织，我们还可提供可选的附加管理服务。QRadar on Cloud 集成了 IBM Managed Security Services，通过 24x7 全天候安全威胁监控和响应提供完全托管服务。组织可以选择将其安全运营外包给第三方的 IBM 托管安全服务提供商 (MSSP) 合作伙伴。MSSP 能够提供全面的安全管理和监控解决方案，以及涵盖基本用例或高级用例的广泛补充性威胁监控服务。

IBM 再次入围 2019 年 Gartner 全球托管安全服务魔力象限。

下载该报告 →

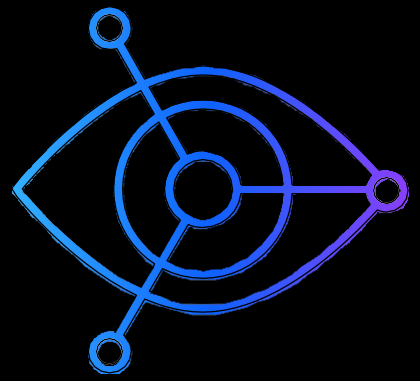
IBM 通过本地交付功能在全球范围内提供托管安全，帮助您保护您的混合云和多云环境。

了解有关 IBM Managed Security Services 的更多信息 →

QRadar on Cloud 的基础架构由可信的 IBM 专业人员进行

24x7

全天候监控。[10]



转向云优先的运营开支模式

IBM QRadar on Cloud 充分运用从数千次 QRadar 内部部署中获得的经验来满足您的环境需求。

无需维护或调整内部部署的安全软件。借助自动软件更新和按需可扩展性，QRadar on Cloud 可帮助您从庞大的资本开支 (CAPEX) 模式转化为基于运营开支 (OPEX) 的、更加灵活的模式，可以帮助 IT 安全人员简化他们的工作流程。

该系统能够实现企业级分析，其功能包括：

- 数据收集、关联和报告功能，可帮助您实现合规性
- 确保最大的每秒处理事件数 (EPS)，可满足全球数百个不同位置的客户的需求
- 具有服务级别承诺及正常运行时间保证的高可用系统配置
- 通过 IBM Security App Exchange 提供各种应用、附加组件和扩展件
- 通过随附的 X-Force 威胁情报源扩充警报

下一步行动

参加 QRadar on Cloud 解决方案为期 14 天的测试，了解其高级检测功能。

开始免费试用 →

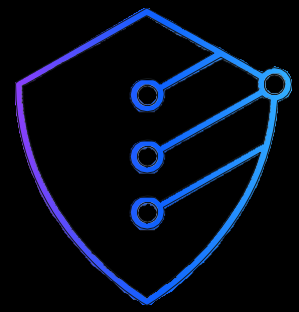
为什么选择 IBM?

IBM Security 可以提供最先进、集成的企业安全产品和服务组合。该产品组合由享誉全球的 X-Force Research 提供支持，能够提供安全智能，帮助组织全面保护其基础架构、数据和应用的安全。IBM Security 提供了各种解决方案，涵盖身份与访问管理、数据库安全、应用开发、风险管理、端点管理、网络安全等多个领域。

这些解决方案可以帮助企业有效管理风险，为移动、云、社交媒体和其他企业业务架构落实集成安全。IBM 作为世界上覆盖范围最广的安全研究、开发和交付企业之一，每天对 130 多个国家/地区的 150 亿次安全事件进行监控，并拥有 3,000 多项安全专利。

此外，IBM 全球融资部可提供各种支付选项，进而帮助您获取开发业务所需的技术。我们可提供 IT 产品和服务的全生命周期管理（从收购到处置）。有关更多信息，敬请访问 ibm.com/financing。

如欲了解有关云端部署的 IBM QRadar Security Intelligence Platform 的更多信息，请联系您的 IBM 代表或 IBM 业务合作伙伴，或访问以下网站：ibm.com/software/products/en/qradar-on-cloud。



免费咨询热线 400-810-1818 转 2395

服务时间 9:00-17:00

IBM Corporation
New Orchard Road
Armonk, NY 10504

美国印刷
2020 年 2 月

1 IBM Knowledge Center. https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/c_siem_vrt_ap_ov.html

2 “Data management challenges are having a severe impact on profitability”，Help Net Security，2019 年 3 月 13 日。https://www.helpnetsecurity.com/2019/03/13/data-management-challenges/

3 Josh Fruhlinger，“Top cybersecurity facts, figures and statistics for 2018”，CSO，2018 年 10 月 10 日。https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

4 HIPAA Violations and Enforcement，American Medical Association，访问于 2019 年 12 月。https://www.ama-assn.org/practice-management/hipaa/hipaa-violations-enforcement

5 2019 Cost of a Data Breach Report：https://www.ibm.com/security/data-breach

6 2018 年数据泄露成本调研：全球概述。由 Ponemon Institute 执行。https://www.intlxsolutions.com/hubfs/2018_Global_Cost_of_a_Data_Breach_Report.pdf

7 QRadar On Cloud 概述，YouTube。https://www.youtube.com/watch?time_continue=53&v=dCTnR_hHToU&feature=emb_logo

8 Marten Mickos，“The Cybersecurity Skills Gap Won't Be Solved in a Classroom”，Forbes，2019 年 6 月。https://www.forbes.com/sites/martenmickos/2019/06/19/the-cybersecurity-skills-gap-wont-be-solved-in-a-classroom/#353d37bd1c30

9 “Cybersecurity Workforce Needs to Grow 145% to Close Skills Gap”，SECURITY，2019 年 11 月。https://www.securitymagazine.com/articles/91224-cybersecurity-workforce-needs-to-grow-145-to-close-skills-gap

10 IBM Managed Services - https://www.ibm.com/security/services/managed-security-services

WGW03245-CNZH-02