IBM QRadar Security Intelligence Platform

为企业安全和合规性提供行动智能

IBM® QRadar® Security Intelligence Platform 可将 SIEM、日志管理、异常检测、漏洞管理、风险管理和事件取证集成为一个统一的解决方案。该解决方案通过使用智能化、整合化和自动化手段，提供 360° 安全洞察，可实现高级威胁检测、提高易用性并降低总体拥有成本。

QRadar Security Intelligence Platform 使用智能化、整合化和自动化手段实现安全性和合规性，这在当今物联化、互联化和智能化业务可收集、处理、使用和存储比以往更多信息的智能星球上是无价的。

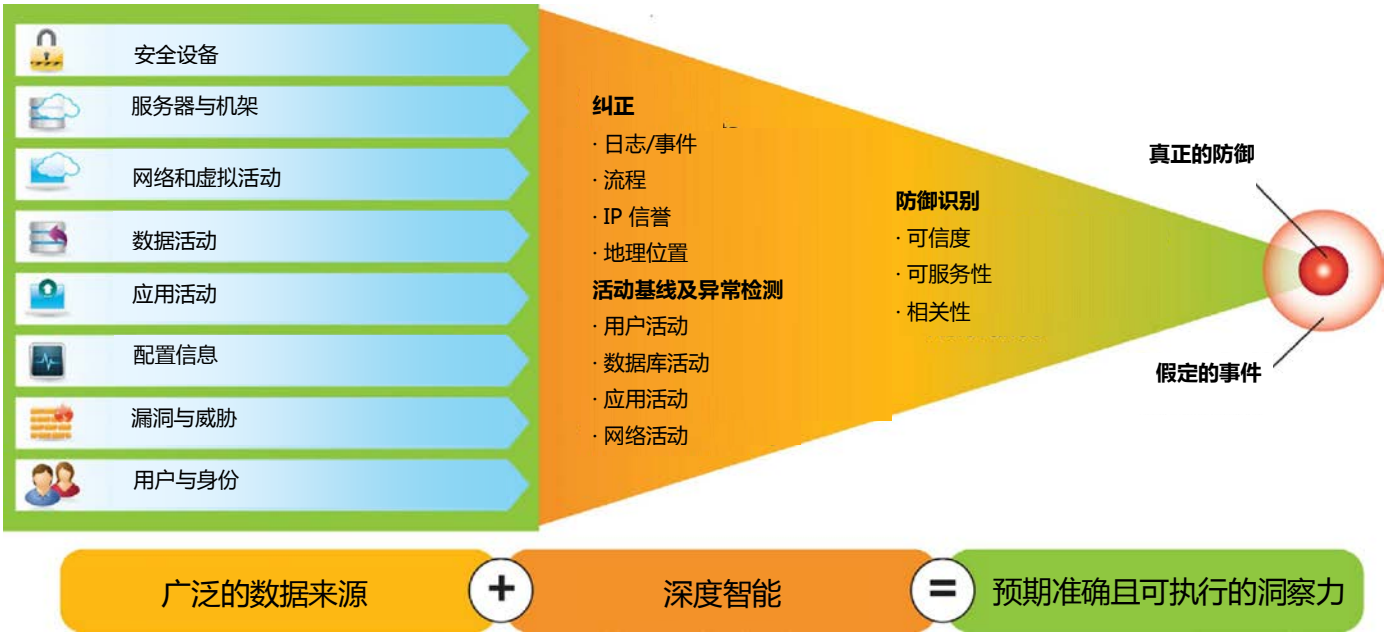
企业现在面临比过去更多数量和种类的攻击。高明的攻击者都很聪明、又有耐性，几乎不留痕迹。QRadar Security Intelligence Platform 是一个集成的系列产品，有助于检测可能错漏的威胁。它将复杂的分析应用于更多类型的数据，帮助检测和抵御威胁。这样，它就能帮助识别可能在嘈杂声中遗漏的高优先级事件。

IBM QRadar Security Intelligence Platform 能帮助解决大量业务问题，包括：

- 将数据竖井整合成一个集成解决方案
- 识别内部盗窃和欺诈
- 管理漏洞、配置、合规性和风险
- 对事件和侵犯进行取证调查
- 应对监管要求

亮点

- 将安全信息和事件管理（SIEM）、异常检测、日志管理、漏洞管理、风险管理和事件取证集成为一个单一、统一的解决方案。
- 利用单一的架构，分析日志、流量、漏洞、用户和资产数据
- 使用实时的关联和行为异常检测，以识别高级威胁
- 在数十亿个数据点之间进行高优先级事件识别
- 获得对网络、应用和攻击者活动的 360° 可视性
- 具有收集、关联和报告功能的自动化合规功能



实现智能化、整合化和自动化

QRadar Security Intelligence Platform 使用智能化、整合化和自动化手段实现安全性和合规性，这在当今物联化、互联化和智能化业务可收集、处理、使用和存储比以往更多信息的智能星球上是无价的。

整合数据竖井

尽管在企业的日志、网络流量和业务流程数据中存在着很多信息，但这些信息常保留在数据竖井之中，被忽视或未被充分利用。QRadar 将网络、安全和运营视图集中于一个统一、灵活的解决方案。它通过将日志与网络流量和大量其他数据相关联，打破竖井之间的间隔 ，将所有相关信息虚拟呈现在一个屏幕上。这有助于支持高级威胁检测和更丰富的企业活动视图。

检测内部欺诈

一些对企业而言最严重的威胁来自于内部，但企业经常缺少检测恶意内部人员或被盗用客户账户的外部人员所需的智能。通过将用户和应用监控与应用层网络可视性相结合，企业能更好地检测与正常活动的重大偏差，帮助在攻击完成之前制止攻击。

预测和修复风险和漏洞

安全、网络和基础架构团队力求通过在发生破坏之前识别漏洞和优先修复来进行风险管理。QRadar Security Intelligence Platform 以 SIEM 功能（包括关联和网络流分析）来整合风险、配置和漏洞管理，以帮助提供更好的关键漏洞洞察。如此一来，企业可更加有效且高效地修复风险。

进行取证分析

QRadar 集成式事件取证可帮助 IT 安全小组减少调查安全事件所需的时间，并减少专业培训的需要。它将安全数据搜索扩大至完整的数据包捕获，数字化储存文本、语音和图像文件涵盖在内。

这有助于清楚地呈现安全事件中何时、何人发生了何事，以及访问或传送了何种数据。如此一来，可以有助于修复网络漏洞并帮助防止其再次发生。

应对监管合规要求

许多企业在用日益贫乏的资源进行数据采集、监控和报告的同时，还要应对通过合规性审计。为了自动化和简化合规任务，QRadar 提供了对合规性相关活动的收集、关联和报告，并由大量立即可用的报告模板提供支持。

利用易用的安全分析

QRadar Security Intelligence Platform 可提供一个统一的架构来存储、关联、查询和报告相关日志、流量、漏洞、恶意用户和资产数据。它将复杂的分析与立即可用规则、报告和仪表盘相结合。对于世界 500 强企业和主要政府机构而言，它足够强大、可扩展；对中小型企业而言，它也是足够敏锐、灵活的。用户可以从可能的更快价值实现时间、更低总体拥有成本、更大的灵活度以及对安全和合规性风险的更好防护当中获益。

智能化

通过分析更多类型的数据和使用更多的分析技术，QRadar 常常能检测到其他解决方案漏掉的威胁，并帮助提供其他解决方案不能提供的可见性。

整合化

通过使用通用的应用平台、数据库和用户界面，该平台可提供大规模日志管理，而无需影响 SIEM 和网络行为分析的实时智能。它可为所有搜索、关联、异常检测和报告功能提供通用解决方案。单一、敏锐的用户界面可提供对所有日志管理、流量分析、事件管理、配置管理、风险和漏洞管理、事件取证、仪表盘和报告功能的无缝访问。

自动化

QRadar Security Intelligence Platform 可简化部署和管理，提供广泛的立即可用的集合模块和安全智能内容。该解决方案在提供立即可用规则和报告的同时，还可通过对许多资产发现、数据规范化和调整功能的自动化，降低那些经常会削弱其他产品功能的复杂性。

为什么选择 IBM?

IBM 运营着全球最大的安全研究、开发和交付组织。该组织有 10 个安全运营中心、9 个 IBM 研究中心、11 个软件安全开发实验室和 1 个高级安全研究所,在美国、欧洲和亚太地区均设有分部。IBM 解决方案可使企业减少其安全漏洞并更多地专注于其战略举措的成功实施。这些产品构建于 IBM X-Force® 研究和开发团队的威胁智能专业知识之上，以提供先发制人的安全捷径。作为在安全方面值得信任的合作伙伴，IBM 可提供相应的解决方案来使包括云在内的整个企业基础架构免于遭受最新的安全风险。

有关更多信息

如欲了解有关 IBM QRadar Security Intelligence Platform 的更多消息，请联系您的 IBM 代表或 IBM 业务合作伙伴，或访问以下网站：Partner, or visit: ibm.com/security

IBM Corporation
Systems Group
Route 100
Somers, NY 10589
2014 年 9 月编制于美国