Forrester 总体经济影响调研报告，
由 IBM 委托撰写
2018 年 5 月

IBM QRadar Security Intelligence Platform 之总体经济影响分析报告

IBM QRadar 实现的成本节省与业务效益

FORRESTER®

目录

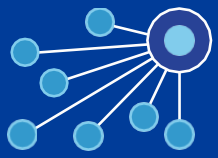
项目总监：
Sean McCormick

关于 FORRESTER CONSULTING

Forrester Consulting 提供独立客观的研究咨询，助力企业领导取得成功。无论是简短的战略对话，还是定制项目，Forrester 的咨询服务都能让您直接体验到调研分析师的专家洞察，轻松应对特定的业务挑战。要了解详细信息，请访问：forrester.com/consulting。

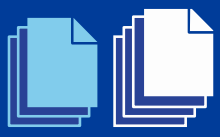
FORRESTER®

收益与成本



提高威胁检测能力：

1,631,344 美元



减少调查工作量：

2,025,461 美元

IBM Qradar 许可成本

5,048,986 美元

概述

IBM 的网络安全情报平台帮助客户加强安全流程，提高检测威胁以及采取行动的能力。IBM 委托 Forrester Consulting 开展了“总体经济影响”(Total Economic Impact™, TEI) 调研，深入分析企业通过部署 QRadar 可能实现的投资回报（ROI）。本次调研旨在为读者提供一个框架，用于评估 QRadar 对其组织的潜在财务影响。

为了更好地了解与此项投资相关的收益、成本和风险，Forrester 采访了一家拥有多年 QRadar 使用经验的客户。IBM QRadar Security Intelligence Platform 是一个产品系列，内含 QRadar 以及将安全信息和事件管理（SIEM）、异常检测、事件取证、事件调查和漏洞管理等解决方案集成在一起的统一架构。QRadar 能够从 450 个数据源获取数据，可以在内部环境和云环境部署，还可以通过软件即服务（SaaS）的形式进行部署。基本产品中包含高级安全分析引擎，用于检测复杂威胁。QRadar User Behavior Analytics 作为应用，负责监控用户行为。该平台还包含一些案例管理工作流，以及 IBM 近期通过收购 Resilient 而获得的一些自动化与指挥工具。[1]

使用 QRadar 之前，这家受访客户一直依靠非 IBM 的外包安全服务提供商 (MSSP) 执行安全监控和响应任务。但多年之后，这家 MSSP 已无法满足他们的需求，该客户仍需大量内部资源来确保准确地向这家 MSSP 提供日志。更重要的是，安全威胁常被遗漏，致使客户不得不单独处理某些事件。该受访客户表示：“有很多真正的威胁都被漏掉了。发现一个安全事件往往会漏掉两到三个。”在决定内包安全监控和响应任务之后，该受访企业部署了 IBM QRadar。因为该产品能够满足其所有要求，并且标准功能运用起来更加灵活。他们很快便发现 QRadar 在威胁检测方面更有效，令公司的安全运营中心（SOC）能够更快地针对威胁采取行动。该客户表示：“... 以前，我们每天检测到 30 起事件，其中许多是误报。而现在，我们每天可检测到 50 起事件，并且准确率及可操作性都比以前大有提高。”

主要发现

可量化的收益。根据风险对现值（PV）进行调整之后，这家受访企业取得了以下可量化的收益：

- **IBM QRadar 提高了检测威胁的速度和有效性。**与之前的解决方案相比，IBM QRadar 可以帮助该受访企业更快地检测到更多事件，从而降低了发生严重事件或违规事件的总体风险。该企业告诉 Forrester，以前的解决方案平均会漏掉 3/4 的威胁。但 QRadar 却将检测到的事件数量增加了近 75%，其中可采取行动的威胁占了很大比例。IBM QRadar 帮助该受访企业在三年中规避了超过 160 万美元的风险。

FORRESTER®

ROI
35%

收益现值
1,410 万美元

净现值
360 万美元

回报期
17 个月

› **QRadar 可一站式地提供更多信息，帮助该客户将事件响应时间缩短了 75%。**部署 QRadar 之前，这家受访企业只能访问 MSSP 工具的简单视图，因此不具备以适当方式响应事件所需的全部信息。内包监控和响应任务后，他们不但可以访问所有信息，还能在 SOC 中成立全天候的内部监控和响应团队。二者结合在一起，已帮助该企业将事件响应时间缩短了 75%，每年可规避超过 65.6 万美元的风险。

› **减少了终端取证调查工作，三年间节省成本 200 万美元。**检测效率的提高和响应时间的缩短，帮助减少了终端取证调查工作量。这意味着这个拥有 16 名全职员工的工作团队可腾出更多时间去执行其他增值任务，如安全规则的进一步细化和定义。根据总体估算，此类取证调查工作减少了 50%，三年内可帮助企业节省 200 万美元的成本。

› **通过 IBM QRadar 提高合规报告效率，帮助企业节省了 13.5019 万美元的生产力成本。**这家受访企业负责执行“萨班斯 - 奥克斯利法案”(SOX) 的季度内部审核，并且接受每三年一次、持续两个月的外部合规审核。据称，IBM 的内置报告功能帮助这家企业以一半的人员满足了合规要求，从而在三年内节省了 13.5019 万美元的成本。

› **节省了 870 万美元的原有技术成本。**与之前的 MSSP 相比，在采用 IBM QRadar 并内包监控和报告任务后，该企业避免了近 870 万美元的花费。

不可量化的收益。这家受访企业还获得了本次调研未进行量化的以下收益：

› **提高了网络安全流程的有效性和成熟度。**该企业利用 IBM QRadar 改进了网络安全流程，提高了威胁检测和事件响应的有效性。他们表示，采用 IBM QRadar 之后开展的成熟度评估显示，该企业的安全成熟度从之前的 2.1 分增加至 3.3 分（满分为 5 分）。

› **通过与其他第三方应用集成，帮助企业提高了生产力，并实现了自动响应。**QRadar 与许多第三方应用预先集成，使该客户能在一个系统中直观了解整个环境的情况。该受访者表示：“我们发现 QRadar 运行许多非常有用的应用，能帮助我们更好地了解整个网络中的攻击情况。”

成本。这家受访企业经过风险调整后的现值成本如下：

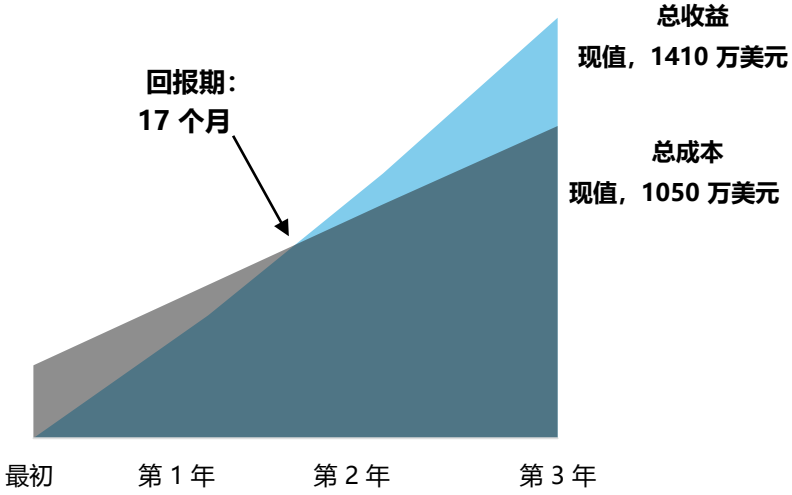
› **IBM QRadar 的初始许可、附加许可以及面向大客户的长期支持和维护费三年总计约 500 万美元。**作为 IBM 最大的客户之一，该客户最初购买的设备和许可支持每秒处理 5 万起事件。第 2 年和第 3 年增至每秒 10 万起事件，并且还投资购买了 IBM QFlows，每分钟可处理 190 万个事件流，因此每年会产生 100 万美元的额外成本。此外，IBM 还以大约占初始许可费 20% 的价格为客户提供年度支持与维护服务。三年以来，这家受访企业共向 IBM 支付了 504.8986 万美元的 QRadar 相关费用。如果是小客户，通常三年花费大约 15.5 万美元，中型部署大约为 64.5 万美元。

› **实施和部署期间的专业服务成本为 70.1250 万美元。**实施和部署大约耗时五个月。在此期间，IBM 全球服务部受雇帮助客户开发监控和响应规程，编制运行手册并开展培训。客户总共向 IBM 支付了 55 万美元的实施费，并且还因为调拨内部人员提供部署支持而耗费了 15.125 万美元。

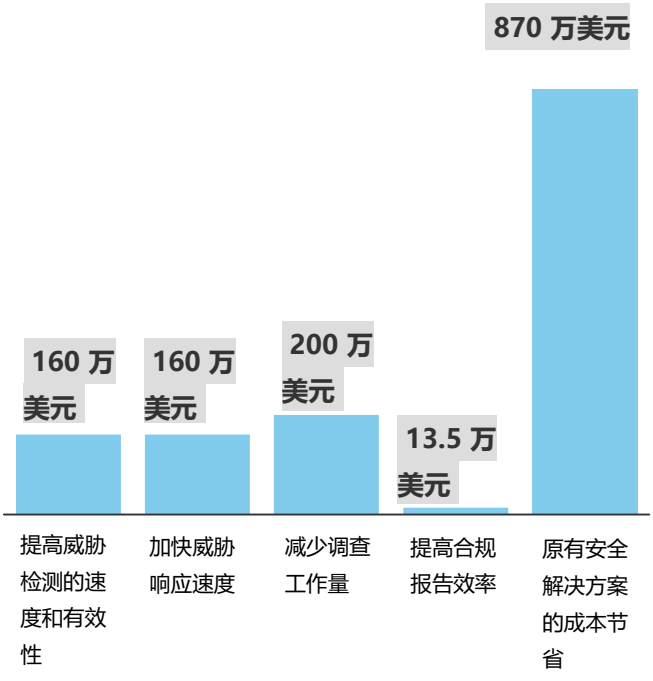
› **客户因内包监控和响应任务而额外增加了 14 名安全工作人员。**当决定内包监控和响应任务而不再聘用 MSSP 时，这家受访企业需要招聘新员工。新招聘了 3 名安全工程师和 11 名拥有不同经验的安全分析师，平均全勤年薪为 11 万美元。三年总计为 460 万美元。

通过开展访谈以及随后进行财务分析，Forrester 发现这家受访企业在三年内获得了 1,410 万美元的收益，而成本为 1,050 万美元，净现值 (NPV) 等于 360 万美元，投资回报率为 35%。

财务摘要



收益（三年）



FORRESTER®

TEI 框架与方法

根据访谈中得到的信息，Forrester 为考虑实施 IBM QRadar 的企业构建了“总体经济分析”(Total Economic Impact™, TEI) 框架。

该框架旨在确定影响投资决策的成本、收益、灵活性和风险因素。Forrester 采用多步骤方法来评估 IBM QRadar 可能对企业造成的影响：

TEI 方法帮助企业向高级管理层和其他主要业务利益相关方展示、证明并实现 IT 计划的切实价值。

尽职调查

采访 IBM 利益相关方和 Forrester 分析师，以收集与 QRadar 相关的数据。

客户访谈

采访了一家使用 QRadar 的企业，以获取有关成本、收益和风险的数据。

财务模型框架

使用 TEI 方法根据代表性的访谈构建财务模型，并根据受访企业的问题和关注点对财务模型进行风险调整。

成功案例

我们采用 TEI 的以下四个基本要素模拟 IBM QRadar 的影响：收益、成本、灵活性和风险。考虑到企业对 IT 投资开展相关的 ROI 分析变得越来越熟练，因此，Forrester 的 TEI 方法旨在帮助客户全面了解采购决策的总体经济影响。有关 TEI 方法的更多信息，请参阅附录 A。

QRadar 客户体验之旅

投资 QRADAR 前后对比

受访企业

在本次调研中，Forrester 采访了 IBM 最大的 QRadar 客户之一：

› 一家总部位于美国的公用事业企业，年收入超过 200 亿美元。

› 他们雇佣了 3.2 万人，包括合同工。

› 运营着拥有 3 万个工作站的企业网络，以及连接工业控制系统和其他公用事业系统的运营网络。

› 安全运营中心 (SOC) 拥有 150 名员工，其中 35 人专门负责安全监控和事件响应工作。 该团队是 IBM QRadar 的主要用户。

主要挑战

部署 QRadar 之前，这家受访企业利用外包安全服务提供商进行安全监控，遇到了以下挑战：

› **服务不灵活，对业务缺乏了解。**这家 MSSP 使用预先构建的一组安全监控用例，基本上没有能力根据受访企业的需求对这些用例进行定制。此外，由于在运营控制系统方面缺乏特定的技能或专业知识，他们还缺乏对业务的了解。这意味着他们无法理解设备（终端）及防火墙的行为和原因，导致误报数量比准确警报的数量还要多。

› **低效的威胁检测带来攻击漏洞。**抛开高居不下的误报率不说，MSSP 还漏掉了很多真正的威胁。据受访者称，只有 1/4 的真正威胁被发现。这使他们很容易受到攻击和不断升级的事件的影响。

› **内部支持任务繁重。**面对如此众多的误报和不断升级的攻击，受访企业的安全负责人不得不安排内部人员来响应和跟踪警报和事件。16 人组成的安全团队投入大量的时间开展现场调查和取证工作。他们没有能力查看开展调查所需的日志数据，并且无法访问由 MSSP 创建的故障凭单中的详细安全背景信息，从而导致事故调查充满挑战且效率低下。

> “很多真正的威胁都被漏掉了。发现一个安全事件往往会漏掉两到三个。”
>
> *—家公用事业企业的网络安全总监*

解决方案需求

受访企业所期望的解决方案必须能够：

› 支持他们使用大多数现成可用的规则和用例，以内包方式执行安全监控和响应任务，无需太多的定制和调整。

› 威胁检测有效性高于现有 MSSP 的水平。

› 灵活地满足他们的需求。

在对五到七家主要的 SIEM 供应商开展了广泛的 RFP 和商业案例流程评估之后，该企业挑选并开始部署 IBM QRadar。

› 最初，该企业聘用了 14 名全职安全人员。 其中 3 位安全工程师填补了系统管理员和安全分析师之间的空白。这些工程师帮助企业定义监控和响应用例，制定规则和配置，并且确定日志和事件源。此外，该公司还聘用了 11 名市场上稀缺的监控和响应分析师。整个招聘工作耗时约两个月，由网络安全主管与人力资源部门共同起草职位描述、审核简历以及面试候选人。该受访企业的相关招聘人员估计这占用了自己大约 20% 的时间，然而，由于人员流失的原因，这些岗位总有大约 10% 的空缺，需要他长期抽出 10% 的时间开展招聘工作。

› 聘请 IBM 全球服务部在 QRadar 的实施和部署过程中提供专业服务支持。IBM 开发了监控和响应规程、手册和培训材料，并引入了适当的变更管理实践。IBM 全球服务部总共与该受访企业合作了五个月。

› 除 IBM 全球服务部的专业服务支持外，该企业还安排了 3 名全职人员，花费六个月的时间专注开展 QRadar 设备的集成、部署和配置工作。 这包括开发特定于业务的定制，以增强安全性并减少误报。

主要成果

这次访谈揭示出投资 QRadar 的以下主要成果：

› **提高了威胁检测的有效性和速度。**通过采用 IBM QRadar，这家受访企业增加了能够检测到的威胁数量，即真正威胁的数量，同时减少了误报数量。部署 QRadar 之前，MSSP 每天平均检测到 30 起事件，其中大多数是误报、已知的异常活动，或者并不总是可采取行动的事件。QRadar 提高了该企业根据业务需求定制规则的能力，从而能够降低误报率，提高威胁检测能力。此外，该企业还集成了 QRadar Qflow，即第 7 层网络活动监控功能。添加 Qflow 使分析人员能够更好地了解网络和应用行为，而不仅仅是日志数据中捕获到的行为。这种可视性的提升帮助该企业增强了威胁检测能力，同时帮助分析师提升了快速响应威胁的能力。该企业指出，这种组合使他们平均每天能够检测到 50 起事件，并且这些事件比 MSSP 检测到的 30 起事件更具可操作性。

> “QRadar 帮助我们显著提高了响应效率。我们现已能够利用 QRadar 更快速、更有效地解决问题。”
>
> *一家公用事业企业的网络安全总监*

› **加快事件响应速度，降低事故升级的风险。**在该企业内包监控和响应任务之前，MSSP 支持高优先级事件 24x7 上报，但内部 SOC 每周仅工作 40 小时。通过内包，该受访者得以建立一支 24x7 不间断运行的内部 SOC 团队。从而帮助他们改进了事件响应 SLA。以前，他们的 SLA 为 8 小时，事件响应平均需要 4 小时。借助 24x7 式 SOC 以及 IBM QRadar 提供的数据，他们平均可在 1 小时内响应事件。此外，通过为分析师提供事件描述、日志数据和流数据以及威胁情报等更为详细的威胁信息，提高了事件响应的效率。该受访者表示：“QRadar 可提供现成的日志和流数据，因此加速并提高了我们的响应事件能力。”以前，在聘用 MSSP 时，分析人员无法访问完整的工具，只能通过供应商的故障凭单门户网站获得简单视图。该门户网站仅包含 MSSP 认为有用的最新日志文件，但分析人员无法通过该工具访问事件。该受访者表示：“QRadar 帮助我们显著提高了响应效率。我们现已能够利用 QRadar 更快速、更有效地解决问题。”总的来说，他们将响应时间缩短了 75%，降低了小事件升级为大事件的风险。

› **提高了调查及合规报告的效率。** 通过提高威胁检测和响应的效率，以及分析 IBM QRadar 中的日志和网络流量的能力，该受访企业将本地调查和终端取证调查的工作量减少了 50%。这使得 SOC 的全职员工能够将调查的事件数量翻一番。最终推动企业制定了新规则，以便扩大检测规则的广度和深度。此外，作为受到严格监管的组织，这家受访企业还改进了合规报告流程。通过更好地了解网络流量和日志文件，该企业能够持续轻松获得开展内部 SOX 控制以及收集监管证据所需的数据。该公司大约每三年开展一次为期两个月的特别审核。虽然这段时间的工作量较平时会显著增加，但他们预计 IBM QRadar 能帮他们提高 50% 的工作效率。该受访者说道：“我们充分利用 QRadar 来实现合规性。该产品确实能帮我们更快速更轻松地收集到所需的证据，从而加快 SOX 审核流程。”

› **通过增加功能，提高了安全成熟度。**通过投资 IBM QRadar，这家公司获得了新功能，从而能够更灵活地定义规则。该受访者表示：“QRadar 的标准功能使我们能够灵活决定要实施哪些规则以及如何调整配置。”QRadar 附带的应用还支持该企业通过单一界面更好地了解环境情况。此外，他们现在还可以整合异常检测功能，动态构建基线，并将系统设置成在活动超过基线时发出警报。通过部署 QRadar，该企业改进了安全流程。该企业在部署 QRadar 前后分别开展了安全成熟度评估。结果表明，以 5 分制为满分，部署 QRadar 帮助他们将成熟度得分从 2.1 分提升至 3.3 分。该受访者表示：“QRadar 让我们真正做到了事半功倍。”

“我们充分利用 Qradar 来实现合规性。该产品确实能帮我们更快速更轻松地收集到所需的证据，从而加快 SOX 审核流程。”

一家公用事业公司的网络安全总监

收益分析

量化的收益数据

总收益

参考号	收益	第 1 年	第 2 年	第 3 年	总计	现值
Atr	提高威胁检测的速度和有效性	655,988 美元	655,988 美元	655,988 美元	1,967,963 美元	1,631,344 美元
Btr	加快威胁响应速度	655,988 美元	655,988 美元	655,988 美元	1,967,963 美元	1,631,344 美元
Ctr	减少调查工作量	792,000 美元	815,760 美元	840,233 美元	2,447,993 美元	2,025,461 美元
Dtr	提高合规报告效率	49,500 美元	61,182 美元	52,515 美元	163,197 美元	135,019 美元
Etr	原有安全解决方案的成本节省	2,375,000 美元	3,562,500 美元	4,750,000 美元	10,687,500 美元	8,672,051 美元
	总收益（根据风险调整后）	**4,528,475 美元**	**5,751,417 美元**	**6,954,722 美元**	**17,234,614 美元**	**14,095,219 美元**

上表显示了下列领域的所有收益总额，以及贴现 10% 之后的现值 (PV)。预计该受访企业根据风险调整后的三年总收益将超过 1,410 万美元。

收益 1：提高威胁检测的速度和有效性

借助 IBM QRadar，安全分析师可在单个界面中访问更多信息。这可以帮助他们进一步完善和制定新规则，以提高威胁检测的有效性和速度。该受访企业表示，在实施 QRadar 之后，他们的威胁检测有效性提高了 75%。这帮助他们降低了小事件演变成重大违规事件的几率。

为了对这项收益的价值建模，我们假设：

› 涉及 1 万条以上记录的违规事件或严重事件的平均成本为 735 万美元。 这是 Ponemon 在其 2017 年调研报告中公布的特定于美国企业的结果。[2]

› 企业在指定年份发生涉及 1 千条以上记录的违规或严重事件的平均概率为 14%。[3]

具体的威胁检测改进幅度可能因以下因素而异：

› 威胁的类型以及先前解决方案检测这些威胁的有效性。

› 企业所属的行业，因为某些行业具有更高的事件发生概率和违约成本。

为了抵消这些风险，Forrester 将此项收益调低了 15%，根据风险调整后的三年总现值为 1,631,344 美元。

IBM QRadar 将威胁检测有效性提高了 75%。

影响风险是指可能因投资无法满足企业的业务或技术需求而降低总体效益的风险。不确定性越大，收益估算结果的潜在范围越大。

提高威胁检测的速度和有效性：计算表					
参考号	**指标**	**计算/来源**	**第 1 年**	**第 2 年**	**第 3 年**
A1	违规或严重事件的平均成本	Ponemon 调研	7,350,000 美元	7,350,000 美元	7,350,000 美元
A2	违规或严重事件的平均概率	Ponemon 调研	14%	14%	14%
A3	使用 QRadar 提高的威胁检测率（百分比）		75%	75%	75%
At	提高的威胁检测的速度和有效性	A1*A2*A3	771,750 美元	771,750 美元	771,750 美元
	风险调整	↓15%			
Atr	**提高的威胁检测的速度和有效性（根据风险调整后）**		**655,988 美元**	**655,988 美元**	**655,988 美元**

收益 2：加快威胁响应速度

仅次于威胁检测有效性的是响应时间。该受访企业将威胁响应时间缩短了 75%。借助 24x7 式 SOC，分析师可以更快地访问重要数据，从而将事件的平均响应时间从 4 小时缩短到 1 小时。

对于该受访企业，Forrester 假设：

› 涉及 1 万条以上记录的违规事件或严重事件的平均成本为 735 万美元。这是 Ponemon 在其 2017 年调研报告中公布的特定于美国企业的结果。[4]

› 企业在指定年份发生涉及 1 千条以上记录的违规或严重事件的平均概率为 14%。[5]

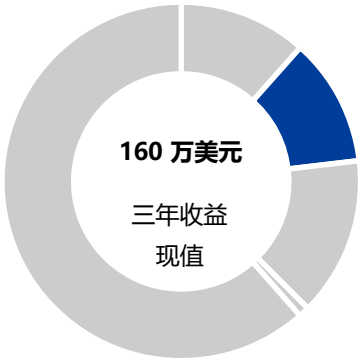
› 通过采用 IBM QRadar，这家受访企业将威胁响应时间缩短了 75%，这帮助他们降低了事故升级的可能性，并有助于降低事故的总体成本。

软件开发成本的降低幅度因以下因素而异：

› 先前解决方案可以应对的威胁类型和数据可用性。

› 企业所属的行业，因为某些行业具有更高的事件发生概率和违约成本。

为了抵消这些风险，Forrester 将此项收益调低了 15%，根据风险调整后的三年总现值为 160 万美元。



加快威胁响应速度：
12% 的总收益

FORRESTER®

加快威胁响应速度：计算表

参考号	指标	计算/来源	第 1 年	第 2 年	第 3 年
B1	违规或严重事件的平均成本	Ponemon 调研	7,350,000 美元	7,350,000 美元	7,350,000 美元
B2	违规或严重事件的平均概率	Ponemon 调研	14%	14%	14%
B3	使用 QRadar 加快的威胁响应速度（百分比）		75%	75%	75%
Bt	加快的威胁响应速度	B1*B2*B3	771,750 美元	771,750 美元	771,750 美元
	风险调整	↓15%			
Btr	**加快的威胁响应速度（根据风险调整后）**		**655,988 美元**	**655,988 美元**	**655,988 美元**

收益 3：减少调查工作量

随着威胁检测有效性和响应速度的改进，该受访企业将取证调查的工作量减少了 50%。从而能够腾出更多的人手去开展规则和配置改进工作，最终创建更安全的环境。如此周而复始，帮助他们节省了更多的时间，并支持分析师主动而非被动地应对威胁。

对于该受访企业，Forrester 假设：

› 16 名全职员工参与终端取证和现场威胁响应活动。

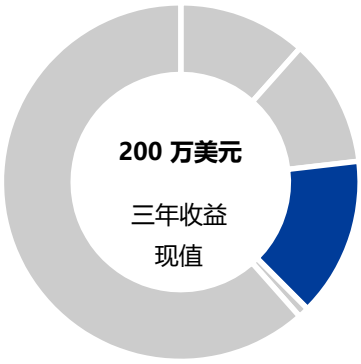
› 全勤的全职安全分析师年平均成本为 11 万美元。

› IBM QRadar 可将调查数量减少 50%。调查工作量的减少幅度因以下因素而异：

› 最初发生的调查数量和设备位置。

› 全职调查人员的数量。

为了抵消这些风险，Forrester 将此项收益调低了 10%，根据风险调整后的三年总现值为 2,025,461 美元。



减少调查工作量：**14%** 的总收益

减少调查工作量：计算表

参考号	指标	计算	第 1 年	第 2 年	第 3 年
C1	参与调查的全职员工数量		16	16	16
C2	减少的调查工作量百分比		50%	50%	50%
C3	每名全职员工的平均成本		110,000 美元	113,300 美元	116,699 美元
Ct	减少的调查工作量	C1*C2*C3	880,000 美元	906,400 美元	933,592 美元
	风险调整	↓10%			
Ctr	**减少的调查工作量（根据风险调整后）**		**792,000 美元**	**815,760 美元**	**840,233 美元**

FORRESTER

收益 4：提高合规报告效率

在受到严格监管的行业中，该受访企业必须满足持续的 SOX 审核要求以及每三年一次的特定于行业的审核要求。长期以来，由于该企业必须从 MSSP 请求特定的数据才能满足测试要求，因此，这一直都是一项耗时耗力的工作。IBM QRadar 不仅可以帮助分析师更为快速轻松地访问所需信息，而且还能制作报告，向审核人员证明公司满足了要求。对于该受访企业，Forrester 假设：

› 在投资 QRadar 之前安排一名全职人员开展持续的 SOX 审核工作，并安排另一名全职人员参与为期两个月的特定于行业的审核。

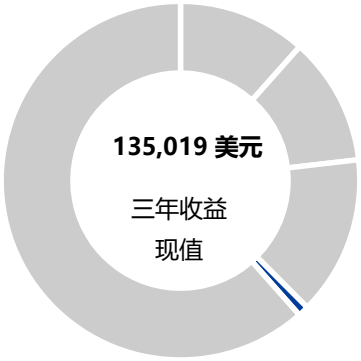
› 该受访企业可将合规报告效率提高 50%。

合规报告效率的提升幅度可能因以下因素而异：

› 企业过去访问所需信息的能力以及现有报告的复杂程度。

› 企业所属的行业，因为某些行业需要满足不同的法规要求。

为了抵消这些风险，Forrester 将此项收益调低了 10%，根据风险调整后的三年总现值为 135,019 美元。



提高合规报告效率：
1% 的总收益

提高合规报告效率：计算表

参考号	指标	计算	第 1 年	第 2 年	第 3 年
D1	日常的季度合规报告（全职员工人数）		1.0	1.0	1.0
D2	三年一次的审核工作（全职员工人数）	1 名全职员工 / 12 个月 * 2 个月	0.00	0.20	0.00
D3	合规报告效率提高		50%	50%	50%
D4	每名全职员工的平均成本		110,000 美元	113,300 美元	116,699 美元
Dt	提高合规报告效率	(D1+D2)*D3*D4	55,000 美元	67,980 美元	58,350 美元
	风险调整	↓10%			
Dtr	**提高合规报告效率（根据风险调整后）**		**49,500 美元**	**61,182 美元**	**52,515 美元**

FORRESTER

收益 5：原有安全解决方案的成本节省

虽然许多企业选择将 QRadar 的运营工作外包给 MSSP，但这家受访企业却选择在采用 IBM QRadar 之后内包安全运营工作。以前，该企业一直使用非 IBM MSSP，每年花费约 250 万美元。虽然为了取代 MSSP 而招聘内部员工也会产生成本，但这家受访企业发现这部分成本低于他们支付给 MSSP 的费用。此外，他们现在还能更好地控制数据和安全性。

对于该受访企业，Forrester 假设：

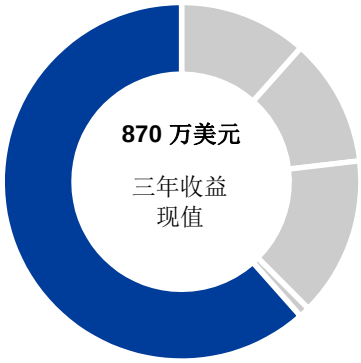
› 停止使用 MSSP 之后，该公司第一年就避免了 250 万美元的成本。

› MSSP 成本规避金额可能因为 IBM QRadar 许可成本之类的使用需求而增长。

原有安全解决方案成本节省的减少可能因以下因素而异：

› MSSP 使用的数据量以及 MSSP 的定价模式。

为了抵消这些风险，Forrester 将此项收益调低了 5%，根据风险调整后的三年总现值为 8,672,051 美元。



原有安全解决方案的成本节省：61% 的总收益

原有安全解决方案的成本节省：计算表

参考号	指标	计算	第 1 年	第 2 年	第 3 年
E1	原有安全解决方案 (MSSP) 的年度成本		2,500,000 美元	2,500,000 美元	3,750,000 美元
E2	年度需求增长率			50.0%	33.3%
Et	原有安全解决方案的成本节省	E1*(1+E2)	2,500,000 美元	3,750,000 美元	5,000,000 美元
	风险调整	↓5%			
Etr	**原有安全解决方案的成本节省（根据风险调整后）**		**2,375,000 美元**	**3,562,500 美元**	**750,000 美元**

灵活性

灵活性的价值显然因客户而异，价值衡量标准因组织而异。许多情况下，客户都是先行选择实施 QRadar，然后才意识到该产品的其他用途和商机，包括：

› **IBM QRadar Advisor with Watson 使企业能够加速事件分析并快速响应威胁。**通过 IBM Watson，企业可借助人工智能 (AI) 主动分析威胁，确定威胁的相关性，并为分析人员提供有关威胁的其他背景信息。这种额外的分析和背景信息收集功能有助于加快调查速度，并为分析人员提供事件处理指导。鉴于安全领域技能短缺，企业可选择利用 IBM Watson 来减少误报，提高分析人员的工作效率并缩短响应时间。

根据 TEI 的定义，灵活性是指企业投资增加额外的容量或功能，可转化为商业利益，产生更多的投资价值。这使得企业有“权利”或能力规划未来投资，但并非强制。

FORRESTER®

› **借助 IBM 的 User Behavioral Analytics (UBA) 解决方案，企业可以清晰了解可能表示内部人员威胁的行为异常。**UBA 可以帮助安全团队分析用户活动，并查明内部人员的行为是否可疑或可能存在恶意。将 UBA 与日志、事件和流数据相结合，分析人员就能够检测到可疑行为并开展有效调查。此外，行为分析还能帮助检测到可能被纯规则方法所遗漏的可疑行为。

如果作为特定项目的组成部分进行评估，灵活性也可被量化（附录 A 中有详细说明）。

成本分析

量化的成本数据

总成本

参考号	成本	最初	第 1 年	第 2 年	第 3 年	总计	现值
Ft	IBM QRadar 许可成本	1,400,000 美元	1,280,000 美元	1,480,000 美元	1,680,000 美元	5,840,000 美元	5,048,986 美元
Gtr	实施和部署成本	731,500 美元	0 美元	0 美元	0 美元	731,500 美元	731,500 美元
Htr	SOC 人力成本	313,133 美元	1,709,400 美元	1,760,682 美元	1,813,502 美元	5,596,718 美元	4,684,754 美元
	总成本（根据风险调整后）	**2,444,633 美元**	**2,989,400 美元**	**3,240,682 美元**	**3,493,502 美元**	**12,168,218 美元**	**10,465,240 美元**

上表显示了下列领域的所有收益总额，以及贴现 10% 之后的现值 (PV)。预计该受访企业根据风险调整后的三年总成本将是不到 1,050 万美元的现值。

成本 1：IBM QRadar 许可成本

这家受访企业以 140 万美元的初始价格购买了 IBM QRadar。作为最大的 IBM 客户之一，他们所购买是基于使用量的许可，每秒可处理 5 万起事件。在接下来的三年中，该企业的需求增长到每秒超过 10 万起事件。此外，他们还进一步投资购买了 IBM QFlow，用于分析网络数据。该许可涵盖每分钟 190 万个数据流。

对于该受访企业，Forrester 假设：

› 该公司将评估占到初始许可成本 20% 的年度支持和维护费用。

› 初始许可中包含具有高可用性 (HA) 功能的 QRadar SIEM 设备、具有 HA 功能的事件处理能力以及每秒处理 5 万起事件的能力。

› 附加许可包含更多数据节点、具有完整数据包捕获功能的 QRadar Incident Forensics 以及每秒额外处理 5 万起事件的能力。

› IBM Qflows 的许可支持每分钟处理 190 万个数据流。

许可成本将随所需的每秒事件处理数和每分钟数据流处理数而变化。此外，该受访企业的规模远远大于客户平均规模。对于每秒只需处理 2,500 起事件的典型企业而言，初始许可成本接近于 7.704 万美元。对于每秒需要处理 1 万起事件以及每分钟处理 20 万个数据流的典型企业而言，初始许可成本接近于 35.95 万美元。下表列出了典型中小型部署的三年期成本。

面向小型企业的 IBM QRadar 典型许可成本

参考号	指标	计算	最初	第 1 年	第 2 年	第 3 年
X1	每秒处理的事件		2,500		2,500	
X2	每分钟处理的数据流					
X3	客户支付给 IBM 的许可和基础架构费用		77,040 美元		35,400 美元	
X4	长期维护和支持成本	20%*X3上一年 +X4上一年*1.1		15,405 美元	16,949 美元	25,724 美元
Xt	**面向小企业的 IBM QRadar 许可成本**	**X3+X4**	**77,040 美元**	**15,405 美元**	**52,349 美元**	**25,724 美元**

面向中型企业的 IBM QRadar 许可成本

参考号	指标	计算	最初	第 1 年	第 2 年	第 3 年
Y1	每秒处理的事件		10,000	5,000		
Y2	每分钟处理的数据流		200,000			
Y3	客户支付给 IBM 的许可和基础架构费用		359,500 美元	70,800 美元		
Y4	长期维护和支持成本	20%*Y3上一年 +Y4上一年*1.1		71,900 美元	93,250 美元	102,575 美元
Yt	**面向中型企业的 IBM QRadar 许可成本**	**Y3+Y4**	**359,500 美元**	**142,700 美元**	**93,250 美元**	**102,575 美元**

IBM QRadar 许可成本: 受访企业成本计算表

参考号	指标	计算	最初	第 1 年	第 2 年	第 3 年
F1	客户支付给 IBM 的许可和基础架构费用		1,400,000 美元	1,000,000 美元	1,000,000 美元	1,000,000 美元
F2	长期维护和支持成本	20%* Sum(F1初始成本 :F1上一年)		280,000 美元	480,000 美元	680,000 美元
Ft	**IBM QRadar 许可成本**	**F1+F2**	**1,400,000 美元**	**1,280,000 美元**	**1,480,000 美元**	**1,680,000 美元**

成本 2：实施和部署成本

该受访企业花费了六个月的时间实施 QRadar。他们安排了 3 名全职员工在公司内部支持部署工作，并与 IBM 全球服务部签署了五个月的服务合同，帮助他们制定规则和配置系统。

Forrester 对这家受访企业假设如下：

› IBM 专业服务费为每月 10 万美元，为期五个月。

› 全勤的全职安全分析师年平均成本为 11 万美元。

具体的实施和部署成本因以下因素而异：

› 部署的复杂性和所需的配置数量。

实施风险是指可能因建议的投资偏离最初或预期需求而导致成本高于预期的风险。不确定性越大，成本估算结果的潜在范围越大。

› 聘请的第三方专业服务以及所提供服务的质量。

› 内部人员与第三方工作量的对比情况。

为了抵消这些风险，Forrester 将此项成本调高了 10%，根据风险调整后的三年总现值为 731,500 美元。

实施和部署成本：计算表

参考号	指标	计算	最初	第 1 年	第 2 年	第 3 年
G1	IBM 专业服务的月成本		100,000 美元			
G2	实施和部署工作所需的时间（月）		5			
G3	实施工作所需的内部人员（全职员工数）		3			
G4	每名全职员工的平均成本		110,000 美元			
Gt	实施和部署成本	G1*G2+(G3*(G4/12*6))	665,000 美元	0 美元	0 美元	0 美元
	风险调整	↑10%	❑			
Gtr	**实施和部署成本（根据风险调整后）**		**731,500 美元**	**0 美元**	**0 美元**	**0 美元**

成本 3：SOC 人力成本

这家受访企业在采用 IBM QRadar 之后便不再与之前的 MSSP 合作，转而内包监控和响应活动。SOC 总监最初花了两个月的时间招聘分析师和工程师，组建自己的团队。该总监共招聘了 14 名安全员工。然而，维持一个完整的 SOC 团队是一场无休止的战斗，受访者表示，他们通常只能保持 90% 的产能，因为总有人离职。

Forrester 对这家受访企业假设如下：

› SOC 总监最初招聘到 20% 的全职员工，并长期保持对 10% 的空缺岗位进行招聘。

› 全勤的全职安全分析师年平均成本为 11 万美元。全勤的招聘经理年平均成本为 14 万美元。

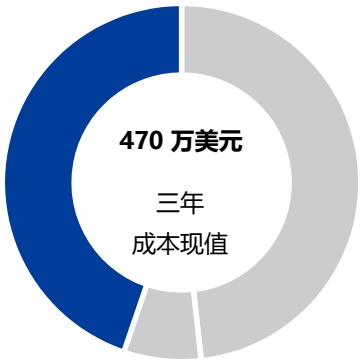
› 支持安全工作内包需要另外招聘 14 名员工。

员工招聘的成本和工作量因以下因素而异：

› 工作地点和同等岗位的当地薪资。

› 人才的稀缺程度和专业水平要求。

为了抵消这些风险，Forrester 将此项成本调高了 10%，根据风险调整后的三年总现值为 4,684,754 美元。



SOC 人力成本：
45% 的总成本

FORRESTER

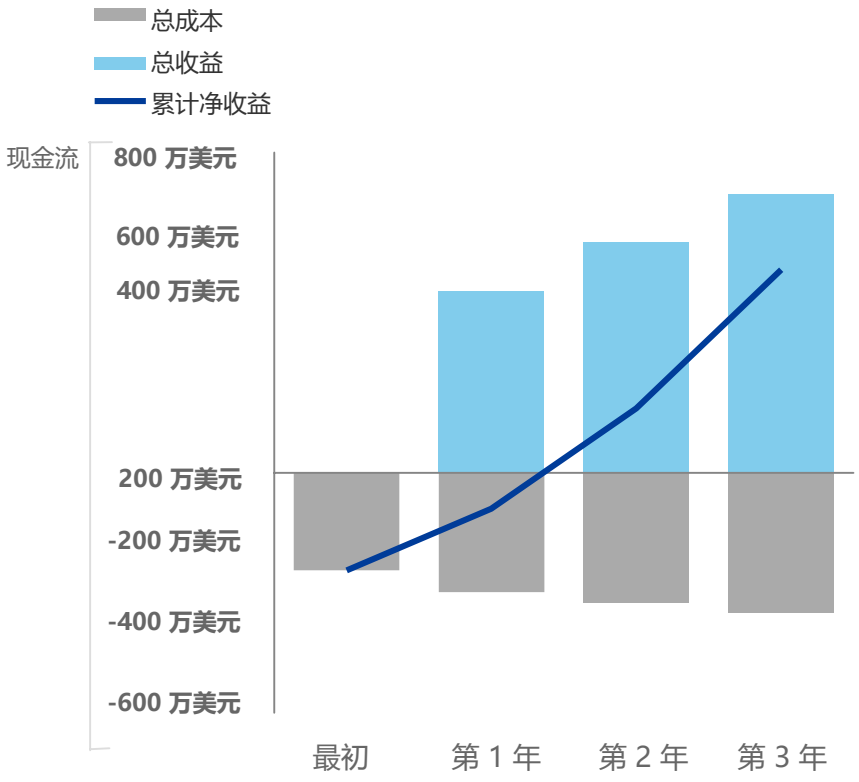
SOC 人力成本：计算表

参考号	指标	计算	最初	第 1 年	第 2 年	第 3 年
H1	最初招聘和持续招聘所需的资源（全职员工数）		0.2	0.1	0.1	0.1
H2	招聘全职员工的平均成本		140,000	140,000	144,200	148,526
H3	招聘 SOC 人员的成本	H1*H2	28,000 美元	14,000 美元	14,420 美元	14,853 美元
H4	SOC 需要的额外人手		14	14	14	14
H5	需要这些人员多少个月		2	12	12	12
H6	每名全职员工的平均成本		110,000 美元	110,000 美元	113,300 美元	116,699 美元
H7	额外人力资源的成本：	H4*H5*H6	256,667 美元	1,540,000 美元	1,586,200 美元	1,633,786 美元
Ht	SOC 人力成本	H3+H7	284,667 美元	1,554,000 美元	1,600,620 美元	1,648,639 美元
	风险调整	↑10%				
Htr	SOC 人力成本（根据风险调整后）		313,133 美元	1,709,400 美元	1,760,682 美元	1,813,502 美元

财务摘要

根据风险调整后的三年期综合指标

现金流图（根据风险调整后）



“收益”和“成本”部分所计算的财务结果可用于确定该受访企业的投资回报率、净现值和投资回收期。Forrester 假设此分析的年贴现率为 10%。

这些根据风险调整后的投资回报率、净现值和投资回报期是通过将风险调整因子应用于每个“收益”和“成本”部分中的未调整结果而算得的。

现金流图（根据风险调整后）

	最初	第 1 年	第 2 年	第 3 年	总计	现值
总成本	(2,444,633 美元)	(2,989,400 美元)	(3,240,682 美元)	(3,493,502 美元)	(12,168,218 美元)	(10,465,240 美元)
总收益	0 美元	4,528,475 美元	5,751,417 美元	6,954,722 美元	17,234,614 美元	14,095,219 美元
净收益	(2,444,633 美元)	1,539,075 美元	2,510,735 美元	3,461,220 美元	5,066,397 美元	3,629,979 美元
ROI						35%
投资回报期						17 个月

FORRESTER

IBM QRadar：概述

以下信息由 IBM 提供。Forrester 并未验证任何声明，也不为 IBM 或其产品背书。

IBM QRadar Security Intelligence Platform 是全面的安全分析解决方案，旨在帮助企业过滤网络“噪音”，提供有关环境中风险和威胁的切实可行的实时洞察。

该解决方案的核心是 QRadar Security Information and Event Management (SIEM)，用于收集海量的网络、资产、云和用户数据，并应用一系列高级分析来识别威胁，发现可能表示攻击的异常行为。这个灵活的平台可部署在内部环境和公共云环境中，也可作为 SaaS 使用。您可通过轻松添加可选组件来扩展监控功能，增加新用例，无需进行大规模的基础架构变更。可选组件包括：

- **QRadar User Behavior Analytics：**无缝地在 QRadar SIEM 上运行，用于检测可能表示内部人员存有恶意或其凭证已被窃取的异常用户活动。
- **QRadar Advisor with Watson：**使用 AI 自动执行调查流程中的步骤，快速发现威胁的根源和范围，深入了解威胁发起人、可能的最终目标以及环境中的其他相关观察迹象，以加速解决问题。
- **QRadar Vulnerability Manager：**通过将漏洞数据映射到资产和资产配置信息，丰富漏洞扫描的结果，帮助企业确定补救工作的优先级。
- **QRadar Network Insights：**实时检查网络活动，以检测网络钓鱼、内网漫游、数据渗漏、重构会话内容等攻击，深入洞察应用级的活动，帮助开展取证调查。
- **QRadar Incident Forensic：**使用完整的数据包捕获数据，一步步追溯攻击者的行为，使分析人员能够更轻松、更深入地开展取证调查。
- **QRadar Data Store：**充当日志数据湖，用于规范化和存储日志数据，使安全分析人员能够运行高级搜索查询，并可选择使用 QRadar SDK 来开发自己的定制分析方法。

IBM QRadar Security Intelligence Platform 的组件完全集成，使客户能够自行选择起步规模，并根据需求的变化轻松扩展或收缩。借助 500 多项经过验证、现成可用的集成和预先配置的规则，客户可以快速启动并运行系统，并通过 IBM Security App Exchange 轻松添加新功能。如欲了解更多信息，请访问：www.ibm.com/qradar。

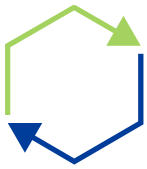
附录 A：总体经济影响

“总体经济影响”(Total Economic Impact) 是 Forrester Research 开发的一种方法，旨在增强企业的技术决策流程，帮助供应商向客户传达其产品和服务的价值主张。TEI 方法帮助企业向高级管理层和其他主要业务利益相关方展示、证明并实现 IT 计划的切实价值。

“总体经济影响”方法

收益表示产品给企业带来的价值。TEI 方法对收益和成本的评估给予同等的重视，旨在全面审视技术投资对整个企业的影响。

成本表示相关产品实现预期价值或收益所需的全部费用。TEI 方法中对成本的分类可捕捉现有环境中的增量成本，用于计算与解决方案相关的持续成本。



灵活性表示企业在现有初始投资的基础之上可以通过未来追加投资而获得的战略价值。如果具有实现此类收益的能力，就具备可估算的现值。

风险用于衡量收益和成本估算的不确定性，包括：1）估算符合最初预测的可能性；以及 2）估算可长期跟踪的可能性。TEI 风险因素基于“三角分布”。

“初始投资”列中包含“时间 0”或“第 1 年”开始时的未贴现成本。所有其他现金流均使用年底的贴现率进行贴现。计算每个总成本和收益估算的现值。汇总表中的净现值计算是初始投资及每年贴现现金流的总和。考虑到四舍五入，最终算得的总收益、总成本和现金流表的总和及现值可能不完全等于各项直接相加之和。

现值 (PV)

按利率（贴现率）给出的（贴现的）成本和收益估算的现值或当前值。成本和收益的现值是计算现金流总净现值的基础。

净现值 (NPV)

给定利率（贴现率）的（贴现）未来净现金流的现值或当前值。如果项目的净现值为正，通常表明应该进行投资，除非其他项目具有更高的净现值。

投资回报率 (ROI)

项目按百分比计算的预期回报。投资回报率的计算方法是将净收益（收益减去成本）除以成本。

贴现率

现金流分析中使用的利率，旨在将货币的时间价值考虑在内。企业通常使用 8% 到 16% 的贴现率。

投资回报期

投资的盈亏平衡点。是指净收益（收益减去成本）与初始投资或成本持平的时间点。

附录 B：补充材料

Forrester Research 的相关调研资料

[1] 来源： “Vendor Landscape: Security Analytics (SA),” Forrester Research, Inc., 2016 年 11 月 15 日。

网上资料

[2] 来源：Ponemon Institute 的“2017 Cost of Data Breach Study: Global Overview” (https://www- 01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN)。
[3] 来源：The True Cost of Compliance with Data Protection Regulations (https://www.ponemon.org /news-2/80)。
[4] 来源：Ponemon Institute 的“2017 Cost of Data Breach Study: Global Overview”（https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN)。
[5] 来源：The True Cost of Compliance with Data Protection Regulations (https://www.ponemon.org /news-2/80)。

扫一扫，
关注 IBM 安全微信， 获取应对企业安全问题的全球资讯

致电垂询 IBM 安全专家

400 810 1818 转 2395

（工作日 9:00 – 17:00）

即刻访问 IBM 安全官方网站

https://www-03.ibm.com/security/cn-zh/?lnk= mpr_buse_cn-zh&lnk2=learnquick

FORRESTER

IBM Security

IBM

IBM QRadar

借助最先进的安全分析平台感知并检测各种现代威胁

IBM 安全白皮书

征服未知问题

安全专业人员生活在一个不断出现悬念的世界中。其组织的每个角落时时刻刻都在遭受各种威胁和攻击。执著的攻击者攻破防线后，他们就会缓慢地潜行。他们搜寻有价值的数据并掩盖自己的一切行踪。事实上，最近的一项调查发现，识别一次攻击的平均时间为 256 天，而阻止它的平均时间为 82 天。[1] 所以，安全操作中心 (SOC) 的压力非常大；许多团队就是不知道对他们来说到底哪些是未知的。

安全团队只要封锁边界，就能禁止许多形式的互联网访问并对抗最新威胁的时代已一去不复返。如今的企业要求用几乎无处不在的连接来保持企业运行，同时阻止高级威胁，识别欺诈和恶意的内部人员，并确保持续合规。新的需求要求企业分析尽可能多的信息，以检测潜伏在表面下的威胁性活动 — 并更快地进行响应。SOC 分析师必须具备一种敏锐的能力，可检测与正常活动的偏差，并且他们选择的解决方案必须能够扩展，可触及企业的每个角落且只使用单个紧密结合的平台。

[1] “2015 年数据泄露成本研究：全球分析” *Ponemon Institute 研究报告*，2015 年 5 月。

感知威胁并采取行动

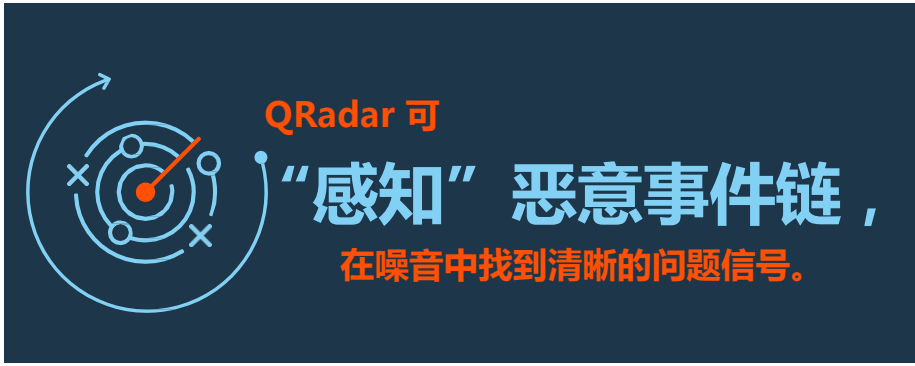
要想始终领先一步，企业要能够“感知”到恶意活动链，就像人们在看到、听到、嗅到或感觉到棘手状况时感知危险一样。因此企业需要的安全平台要能够：

- 快速部署在整个网络中，包括基于云的资源
- 检测环境中的细微差别，比如潜伏的入侵者或恶意的内部人员
- 在不依赖少数训练有素的专家的情况下发现攻击
- 收集、标准化和关联数十亿个事件，确定少数优先考虑的问题
- 识别重要漏洞和风险，防止数据泄露

从好的方面讲，如今的 SOC 分析师不必再单枪匹马地战斗。就像攻击者联合起来共享其洞察和技术一样，安全社区也以类似的共享资源作为响应。这些新的威胁情报和应用共享工具的出现，帮助人们限制了新恶意软件和漏洞攻击工具包的有效性，并且限制了零日或一日漏洞的影响。许多 SOC 分析师仍受限于老旧的日志管理系统或基本的安全信息和事件管理 (SIEM) 解决方案，一个可疑行为实例就会让这些解决方案生成大量的警报。

使用分析消除威胁

最严重的安全破坏不是突然出现的。相反，网络罪犯会发起可能持续数月的“低频而缓慢的”攻击。如果您能找出环境中细微但相关的变化，然后在开始发生怪异的事情时提醒安全团队，岂不是更好？



IBM® QRadar® Security Intelligence Platform 是唯一由 IBM Sense Analytics™ 提供支持的安全解决方案，它可以：

- 开发用户和资产概要信息作为合法活动的基准
- 在人员（包括内部人员、合作伙伴、客户和访客）、网络、应用和数据间检测异常行为
- 将当前活动与历史可疑活动关联起来，提高事件识别的准确性
- 检索并重放网络活动，以最初的数据包格式调查数据包内容
- 在薄弱环节被人利用之前找到并优先进行处理

执行即时分析的单点解决方案是不可靠的；它们不能将新的网络活动与“危险”用户关联起来，比如那些声誉不佳的已知过往站点访问者。Sense Analytics 可将用户行为与日志事件、网络流、威胁情报、漏洞和业务上下文相匹配，从而帮助企业消除威胁。通过在噪音中找到清晰的问题信号，让企业能够专注于最直接和最危险的威胁 — 并指导他们执行补救工作来最大限度降低任何潜在的损害。

Sense Analytics 的工作原理

没有数据，分析就毫无用处；没有大量的数据，分析也会软弱无力。一些数据来自您的网络操作，一些数据存储在应用中，一些源自以前的分析，还有一些作为信息提要来源于外部。QRadar 从网络内的每个设备、应用和用户处收集原始安全数据 — 无论这些设备、应用和用户位于企业的内部还是托管在云环境中的系统上都是如此。

Sense Analytics 能够：
- 分析安全数据
- 理解上下文
- 探查使用情况

收集数据后，QRadar 设备执行实时分析来搜索直接的危险信号，然后将结果与已存储的其他有关任何所涉及网络、用户或文件元数据的情报进一步融合。QRadar 让安全团队能够理解当前活动与过去已发生的活动有何关联，而且感知变化的一个重要方面是能够为基准活动提供正确的参数。

分析安全数据以感知威胁

有了 Sense Analytics 作为后盾，QRadar 使用基于状态的高级分析将当前的安全数据转换为有意义的洞察。安全团队可定义多种类型的条件，帮助他们感知潜在的恶意活动，包括：

- 行为变化，以捕获与正常模式的偏差
- 可能揭示新网络流量或突然终止的流量的异常
- 阈值违反情况，以查找哪些活动超出了既定的级别

使用 QRadar，一家国际能源公司每天能够分析

20 亿个事件–

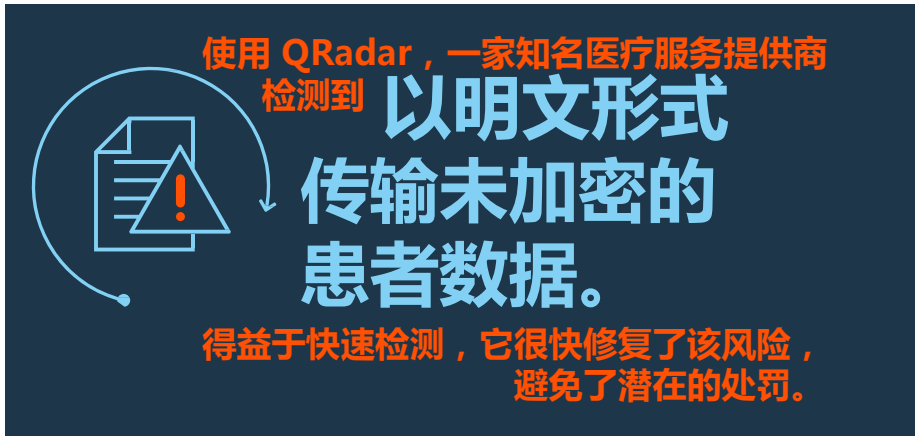
实时关联数据 — 以识别

20 到 25具有最大危险的潜在攻击。

用户或身份的常规行为变化，常常是网络被破坏或某些个人凭证可能被损害的初期迹象之一。Sense Analytics 不仅会对比实时活动与历史模式，它还检测新的应用使用情况、新的网站访问和新的文件传输活动。它还能从企业身份系统中拉取数据，允许 SOC 分析师查看最新报告或个人的角色变化，从而帮助企业排除误报结果。

通过分析事件、数据流和数据包来理解上下文

一种强大且常被忽视的上下文来源可能源自原生网络流数据 — 标识 IP 地址、端口、协议，甚至应用或流经网络的“载荷”内容的数据 — 所有这些数据都通过直接的深入数据包检查或事故后的完整数据包恢复来捕获。这让安全团队能够：



- 探查“正常的”网络流量并在条件变化时收到报警
- 找到与恶意 IP 通信的新的或已被攻陷的主机
- 检测新的安全威胁，而不使用签名
- 回放被检测到的入侵者或恶意用户的逐步操作
- 深入了解应用层并检测可疑内容或不当的使用情况

Sense Analytics 使用网络数据来提供每个事件、事故或相关攻击的上下文。它可以检测 Web 服务器是否停止对通信的响应，识别常用服务的活动水平是否有重大变化，以及在网络上出现新服务或协议时生成警报。此分析还会揭示应用的类型，识别端口和协议失配 — 这可帮助企业加快调查速度。

探查使用情况，以存储洞察并帮助管理风险

一个为快速搜索实时数据而设计的安全解决方案会遗漏大量的事故，要捕获这些事故，需要提前了解关键应用及其使用人员、典型性能水平和关联的主机，还需要了解这些关键应用何时处于快速活动周期、何时处于缓慢活动周期。知晓这些参数对获得可操作的洞察至关重要。

QRadar 帮助一家信用卡公司

保护其关键数据

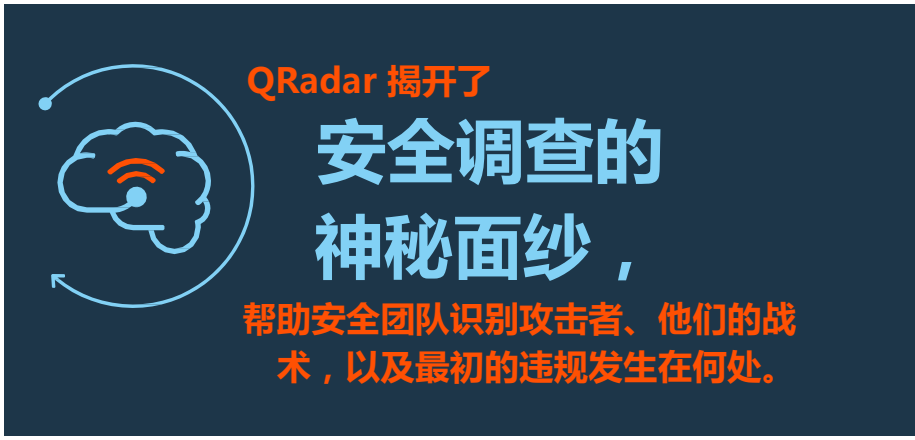
和基础架构远离高级威胁 — 同时还实现高达 50% 的部署、调优和维护成本节省。

能够通过探查资产和个人来获得知识，是 Sense Analytics 的一个基本特征。QRadar 使用网络流数据和漏洞扫描来自动发现资产并创建资产概要文件。此概要文件定义了资产是什么，识别它如何与其他资产通信，列出允许操作的应用和存在的任何已知漏洞。然后 QRadar 使用所有这些情景来减少噪音，提供高度准确的事故信息。

积累网络用户当前行为的知识，对攻击和破坏检测同样宝贵。QRadar 可跟踪 IP 和 MAC 地址、电子邮件 ID 和聊天句柄等信息，并且可以利用其他 IBM 或第三方身份和访问管理程序来为事故调查提供宝贵的情景资料。它可使用所有这些关联信息来限定其分析的范围，包含或排除与（当前发生或最近观察到的）可疑活动有关的个人或角色。

可展现 Sense Analytics 强大功能的用例

在许多环境中，安全实践方面的自满和过失意味着关键资产的安全性不一定达到了它们能够达到或应该达到的水平。企业需要限制不可避免的违规情况所造成的负面影响。他们需要涵盖整个环境且没有任何盲点的解决方案。



从安装那一刻开始，QRadar 就开始构建可操作的安全洞察，这些洞察可帮助您加强企业的防御。该解决方案提供了快速价值的用例包括：

- 高级威胁检测
- 关键数据保护
- 内部威胁监视
- 风险和漏洞管理
- 未授权流量检测
- 取证调查

用例：
高级威胁检测

使用实时分析，安全团队可以检测主机是否访问了一个潜在的恶意域，但仅仅一次访问可能不需要发出警报。然而，如果同一主机开始表现出报警行为 — 使用长期历史分析检测出来 — 而且它也开始传输异常高的数据量，与其行为基准不符，所有这 3 个条件相结合，QRadar 就能生成单个加强型警报。

QRadar 也可以感知网络流量的突然变化，比如主机上出现一个新应用或一个典型服务终止了，并捕获它作为异常条件。安全团队在搜索系统日志时不太容易发现异常 — 这些异常不同于恶意软件签名或针对已知漏洞的其他既定攻击。根据定义，异常是指一种奇怪现象，它只能被可监视和探查所有用户与实体操作的安全解决方案所发现。

用例：
关键数据保护

在晚上，一个新应用开始在一个网络主机上运行。此活动可能是一个新的业务需求或某人安装了一个聊天应用所导致的。但是如果该主机能够访问关键数据，而且还有一个相关的已知漏洞，QRadar 可创建一个高优先级警报来提示安全团队调查该事件。

QRadar 快速检测事件流量何时超出特定的活动水平并生成一个警报。可根据 QRadar 中已收集的任何数据来确定该阈值或限制，如网络设备配置、服务器、网络流量遥测、应用，以及最终用户及其活动。而且像行为改变或异常一样，QRadar 可使用用户身份、正在使用的端口和协议、IP 声誉和已报告的威胁活动来提供更多警报线索，为安全团队提供该事件更深入的信息。

用例：
内部威胁监视

一位客户服务代表突然开始从客户信息系统下载两倍于正常数量的数据，这可能是某个新的销售分析活动的一部分。但是如果 QRadar 知道该代表最近访问了一个潜在的可疑网站，而且现在正看到少量数据被发送到竞争对手的网站，就可在大量信息被泄露之前通知安全人员。

通过在单位和个人中的评测，QRadar 在众多安全产品中脱颖而出。一组全面的数据、业务情景和威胁情报的组合 — 加上能够检测与正常行为的偏离并识别哪些行为不被允许或者是不当的 — 提供了非常强大的事件检测能力。

用例：
风险和漏洞管理

网络上出现一个新实体时，QRadar 通过探查日志和流数据可自动感知它的存在。借助其无缝集成的漏洞扫描器，QRadar 可触发对这个新实体的一次扫描，以发现它是否有任何紧急或高风险的漏洞暴露给潜在的威胁来源。

例如，将一个新服务器添加到网络时，QRadar 可检测它是否遗漏了关键的补丁或者具有默认的管理凭据。然后 QRadar 可通知合适的团队进行补救和/或计划一次修补，如果没有及时执行该任务，则升级该问题。

而且，会自动地将新公布的漏洞与现有数据相关联，而无需重新扫描，这有助于提高检测的速度和准确度。这样所带来的操作节省让安全分析师能够将更多的时间集中在主动战术上，比如风险分析和漏洞修补活动。

用例：
未授权流量检测

随着大部分企业现在都支持自带设备 (BYOD) 端点，安全团队正看到越来越多与社交媒体应用相关的网络流量。用户常常访问他们的企业电子邮件系统，通过 Facebook、LinkedIn、Twitter 和其他服务与好友保持联系，所有这些都在同一台设备上完成。QRadar 收集和分析此数据，并留意互联网聊天会话何时开始通过端口 80 连接（举例而言），该端口通常用于传输 HTTP 流量。与已知的僵尸网络服务器的进一步连接可快速证实恶意软件已被注入，应提示安全团队采取行动。

QRadar 从网络层和端点管理系统收集和分析来自移动以及 BYOD 设备的数据。它可检测潜在的威胁 — 比如一个被越狱的设备、安装在设备上的可疑应用或潜在的恶意互联网通信 — 然后触发对设备进行隔离和/或将问题升级到合适的安全团队来采取行动。

用例：
取证调查和威胁搜寻

在攻击调查期间，安全分析师发现一位或多位员工受到了网络钓鱼攻击，攻击者已成功入侵并扩展到一个内部服务器主机。该模式与 X-Force 已识别的一种模式相符，称为注入远程访问特洛伊 (RAT) 软件，该软件很难检测。

通过单击几次鼠标，QRadar 恢复了所有与该事件相关的网络数据包并重构了攻击的逐步过程 — 向安全分析师清晰透明地展示出安装该 RAT 软件的位置和时间。取证工作流让分析师能够快速且轻松地构建丰富的恶意软件概要信息，并通过链接分析将注入路径衔接起来，识别出“第一感染源”和任何其他受感染方。结果是，安全团队能够快速补救损害，将此事件的再现几率降到最低。

IBM 提供了可操作的情报来实现主动出击和更强的防护

信息安全是董事会级的优先事项，但许多企业仍依赖于数十个单点产品来获取即时洞察。受过深入培训的人员正在使用搜索引擎来筛查海量数据，但攻击者越来越普遍地在成功打开缺口后，通过将IP、协议、端口和应用切换到锁存状态来逃避检测，进而大肆收集宝贵数据。

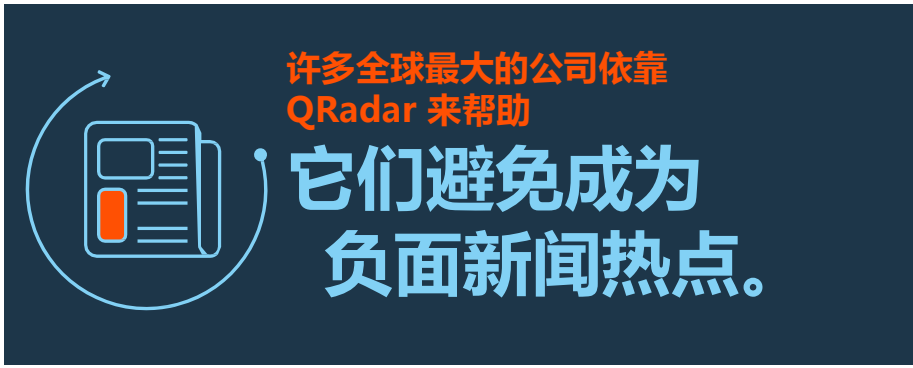
IBM QRadar 与众不同。无论网络的规模如何，它都可以快速部署并在几小时内开始交付结果。它的认知能力和已存储的情报可关联从同一来源传来的或对应于相同目标数据的相关攻击。QRadar 提供了这些可操作的洞察来满足当前和未来的需求 — 从高级威胁检测到内部威胁监视、欺诈检测、风险和漏洞管理、取证调查以及合规性报告。

安全领导者选择 QRadar 的主要原因包括：

- 一个易于使用的安全仪表板，突出显示了最重要的威胁，支持快速、有效的调查和补救工作流
- 几乎无限的可伸缩性，由 X-Force 威胁智能和 IBM X-Force Exchange 的协作功能提供支持
- IBM Security App Exchange，包含 IBM 和合作伙伴开发的应用，它扩展了 QRadar 的功能而没有增加复杂性
- 具有全局可见性的单个集成平台，提供了有关网络、应用和用户活动的洞察

让最重要的威胁无处遁形

一旦检测到威胁、攻击或破坏，就是采取行动的时候了。QRadar 为安全团队提供了一个基于 Web 的用户界面，该界面在整个平台上外观一致。platform.在监视日志活动、观察网络活动、审核高度相关的攻击，运行风险和漏洞分析，或执行取证分析之间进行切换非常容易，只需单击一个选项卡就能显示一个信息丰富的仪表板屏幕。每个仪表板都拥有丰富的安全情报信息，这些信息被组织到高度直观的最新活动显示界面中，只需单击几次鼠标即可轻松开始调查工作。



您可以花几分钟时间查看突出的事件或深入研究所报告攻击的细节。安全团队可快速了解重要问题的性质；被利用的任何漏洞；注入的任何僵尸网络、RAT 或其他恶意程序；以及任何数据丢失的程度。现在是时候在造成实际损害之前采取行动了。

获得大规模采取行动的能力

使用更大的 QRadar 平台，安全团队可清晰地理解已发生的事件，以及不快速采取行动会面临哪些风险。通常只需一次单击即可使用威胁监视、风险和漏洞管理及合规性报告等关键功能，并且可以在彼此之间传递相关数据。而且，QRadar 与 X-Force 威胁智能紧密集成，能够每小时更新全球攻击技术和恶意软件种类。

QRadar 包含各种硬件、软件和虚拟应用模型，可实现

更快的部署速度。

发生破坏事件时，QRadar 集成的取证技术为 SOC 分析师提供了相关攻击的成套数据，详细且准确清晰地描述了入侵者的逐步行动。打败一些威胁只需拦截与一个外部 IP 地址的通信，但其他威胁需要动员应急响应团队来隔离和重新配置主机，禁用恶意软件并修补漏洞。但是如果您的团队不知道要做什么怎么办？此时就应该寻求帮助，与同行协作，寻求一个解决方案，甚至雇佣专业服务团队了。

QRadar 开放框架以及 IBM Security App Exchange 有助于促进与 IBM 和第三方解决方案实现更紧密的集成。例如，站点上的一个应用将 QRadar 攻击数据传递给 Resilient Systems 的事故响应平台，以便立即采取行动。另一个应用通过 Carbon Black Enterprise Response 端点管理解决方案提供一种类似的数据共享功能。

借助 IBM Security App Exchange 扩展各种功能

IBM Security App Exchange 显著提高了 QRadar 的灵活性。这个最重要的协作站点允许客户、开发人员和业务合作伙伴共享应用、安全应用扩展和对 IBM Security 产品的增强。

借助 IBM Security App Exchange，企业能够：

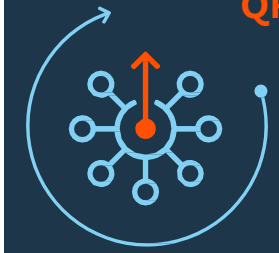
- 获取各种应用，扩展 IBM Security 解决方案的功能
- 共享最佳实践并向他人学习
- 找到各种解决方案和用例，增强安全操作的战略价值

IBM 会针对已设定的条件审查所有代码，然后才会将代码上传到站点上。安全团队可独立下载和安装解决方案 — 在官方产品发布周期外。这样，他们就可以应用新的安全用例，而不会添加不必要的解决方案的复杂性。

具体来讲，QRadar 用户可从 IBM Security App Exchange 下载特定于行业、威胁、设备和供应商的内容。而且，他们可以访问定制报告、仪表板、专业分析和威胁信息。

部署一个具有全局可见性的平台

当今的安全环境充满着复杂性 — 安全数据常常分散在不同供应商的多款产品中，这些产品具有不同的接口和数据存储格式。要想有效地检测现有和新兴的威胁，安全团队需要此数据的统一视图，并且还要结合使用全面的威胁检测分析和响应功能。QRadar 使用单个连锁的数据库来存储所有安全数据，该数据库专门从内部部署系统和云系统可扩展地收集数据，并且具有出色的存储、报告和非常快的调查搜索性能。此外，QRadar 针对实时和历史事故分析进行了优化，在事故发生后几秒即可检测出来 — 而不是几小时、几天或几周。



QRadar 可以快速部署而无需众多专家，提供了一个

单一的控制台指挥中心

QRadar 还提供了一组紧密整合的安全用例，更多的用例可通过 IBM Security App Exchange 获得。安全团队可使用单个基于仪表板的控制台控制所有功能，这些功能包括实时安全监视，主动风险和漏洞管理，以及事故检测、取证和补救。这个安全操作和响应中心融合了来自 IBM 和第三方产品的智能 — 由一个一致的用户界面和工作流提供支持 — 使您的安全操作团队工作更加富有成效。

更多信息

要了解由 Sense Analytics 提供支持的 IBM QRadar Security Intelligence Platform 的更多信息，请联系您的 IBM 销售代表或 IBM 业务合作伙伴，或者访问：**ibm.com**/security

关于 IBM Security

IBM Security 提供了最高级和一体化的企业安全产品和服务组合之一。该产品组合（由享誉全球的 X-Force 研发团队提供支持）提供了安全智能来帮助企业整体性地保护其人员、基础架构、数据和应用，为身份和访问管理、数据库安全、应用开发、风险管理、端点管理、网络安全等提供了解决方案。这些解决方案让企业能够有效地管理风险，为移动、云、社交媒体和其他企业业务架构实现一体化的安全保护。IBM 运营着全球最大的安全研究、开发和交付组织之一，每天监视着 130 多个国家的 150 亿个安全事件，拥有超过 3,000 项安全专利。

IBM Security
Route 100
Somers, NY 10589

美国印刷
2016 年 4 月

WGW03211-CNZH-00