Forrester Wave™：安全性分析平台，2020 年第 4 季度

最重要的 11 家提供商及其排名情况

作者：Joseph Blankenship 和 Claire O'Malley

2020 年 12 月 1 日

为何应阅读此报告

在我们对安全性分析平台提供商的 27 项标准评估中，我们确定了 11 个最主要的平台 — Exabeam、FireEye、Gurucul、IBM Security、LogRhythm、Micro Focus、Microsoft、Rapid7、RSA、Securonix、Splunk，并对它们进行了研究、分析和评分。本报告中列举了每家供应商分别在哪些方面符合标准，并能帮助安全性风险专业人士选择适合其需求的产品。

关键要点

IBM Security、Splunk、Securonix、Exabeam 和 Microsoft 傲领群雄

Forrester 的研究发现，IBM Security、Splunk、Securonix、Exabeam 和 Microsoft 属于领导者；LogRhythm、Gurucul、Micro Focus、Rapid7 和 RSA 是表现出众者；FireEye 是竞争者。

自定义、ATT&CK 映射和 SaaS 成为关键优势所在

随着安全信息和事件管理 (SIEM) 技术的过时和效率降低，提供自定义检测功能的云交付安全性分析平台将决定哪些提供商成为行业领头羊。能够提供自定义功能、MITRE ATT&CK 映射和 SaaS 交付的供应商将更具优势，更有机会成功为客户提供改进的检测功能、更快速的调查和更高的灵活性。

Forrester Wave™：安全性分析平台，2020 年第 4 季度

最重要的 11 家提供商及其排名情况

作者：Joseph Blankenship 和 Claire O'Malley
Stephanie Balaouras，Alexis Bouffard 和 Peggy Dostie 合作编写
2020 年 12 月 1 日

目录

2 **安全性分析的未来在于云**
3 **评估摘要**
6 **供应商产品**
6 **供应商简介**
领导者
表现出众者
竞争者
11 **评估概述**
供应商入选标准
12 **补充材料**

相关研究文档

《Forrester Wave™：安全性分析平台》2018 年第 3 季度

《Now Tech：企业容器平台》2020 年第 3 季度

《网络安全现状：2018 年至 2019 年》

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | 传真：+1 617-613-5000 | forrester.com

安全性分析的未来在于云

过去，供应商将传统 SIEM 系统作为本地部署硬件或软件部署提供。因此，安全性专业人员很难管理和更新这些系统以及持续增加存储，来容纳不断增多的日志。在《帝国反击战》中，兰多·卡里斯西亚对利亚公主说："云端是你真正的归属。"这句话同样适用于安全性分析平台。随着企业将自己的工作负载迁移到云以利用其规模、灵活性和可用性，安全服务供应商终于开始跟进，基于云端交付其安全性分析解决方案。这种过渡和云原生供应商的出现表明，云端是安全性分析的归属。

在 Forrester 的 2020 年安全性分析平台市场评估中，大多数供应商都通过 SaaS 或云托管模型交付其产品。这一变化使供应商能够更快地向客户推出新功能，并降低这些系统的管理开销。要为其传统本地解决方案寻找替代品的安全专业人士应该寻找能够从云端提供大部分（即便不是全部）功能的供应商。在这些趋势的驱动下，安全性分析平台客户需要的提供商应该具备如下特点：

- **为客户提供定制能力。**大多数供应商都提供了开箱即用 (OOTB) 内容，企业可以对这些内容进行自定义，以满足它们的个性化需求。更高级的用户还希望针对特定情境开发自定义检测功能。一些供应商提供机器学习模型，可供客户自行定制，打造自己的专属模型。
- **提供真正的分析和运维服务。**许多安全性分析供应商提供基本分析服务，专注于用户行为，几乎没有自动化。最强大的供应商提供涵盖多种机器学习类型的分析功能，并包括安全编排自动化和响应 (SOAR)。分析和自动化功能的结合给安全性分析平台创造了机会，让它们可以提供能够识别并自动应对威胁的智能运维功能。
- **映射到 MITRE ATT&CK 框架。**安全专业人士很快就采用了 MITRE ATT&CK 框架，作为其安全运维的一部分。为了响应这种趋势，SA 供应商将其解决方案映射到该框架，以执行检测、调查、捕获威胁。掌握最先进功能的供应商还会显示客户环境中涵盖了哪些部分的 MITRE ATT&CK。
- **具备针对扩展检测和响应 (XDR) 的愿景。**端点检测和响应 (EDR) 和安全性分析长期以来一直在相向而行。这些功能的重叠将 EDR 与其他技术的分析功能相结合，提供大幅改进的遥测功能、快速调查和自动响应操作。

评估摘要

Forrester Wave™ 评估结果主要分为“领导者”、“表现出众者”、“竞争者”和“挑战者”四个类别。本次评估选取的对象都是市场上领先的供应商，并不代表所有供应商的总体情况。有关此市场的更多信息，请查看我们的报告《Now Tech：安全性分析平台》，2020 年第三季度。

此评估结果只是一个起点，我们鼓励客户使用基于 Excel 的供应商比较工具查看产品评估和调整标准权重（参见图 1 和图 2）。单击 Forrester.com 上本报告开头处的链接，即可下载此工具。

图 1 Forrester Wave™：安全性分析平台，2020 年第四季度

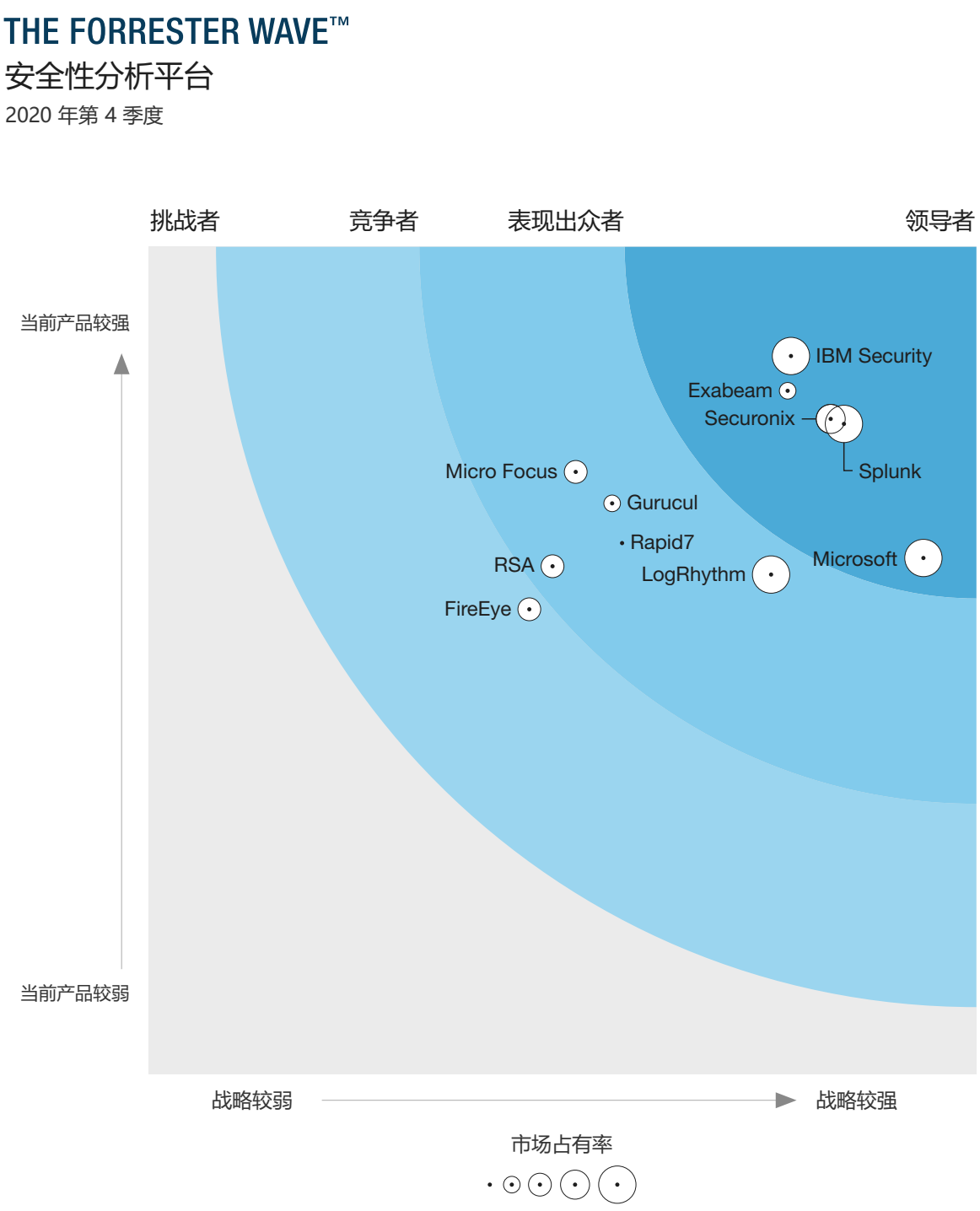

图 2 Forrester Wave™：安全性分析平台记分卡，2020 年第四季度

	Forrester 权重	Exabeam	FireEye	Gurucul	IBM Security	LogRhythm	Micro Focus	Microsoft	Rapid7	RSA	Securonix	Splunk
当前产品	50%	4.13	2.81	3.45	4.34	3.02	3.64	3.12	3.21	3.07	3.96	3.93
部署和数据架构	5%	3.40	3.40	3.80	3.40	3.40	2.20	4.20	3.80	1.80	5.00	2.20
可见性	10%	3.00	3.00	3.00	5.00	3.00	3.00	1.00	3.00	5.00	3.00	3.00
关联功能	10%	5.00	3.00	5.00	5.00	3.00	5.00	5.00	5.00	3.00	5.00	5.00
威胁检测	20%	4.60	3.00	3.40	4.60	4.20	4.20	2.60	4.20	3.00	3.80	4.20
ATT&CK 映射	10%	5.00	3.00	3.00	5.00	3.00	3.00	3.00	1.00	3.00	3.00	3.00
自定义检测	5%	5.00	3.00	5.00	5.00	3.00	3.00	3.00	1.00	3.00	5.00	5.00
安全编排	10%	3.00	5.00	1.00	5.00	1.00	3.00	3.00	3.00	3.00	3.00	3.00
合规性	5%	3.00	1.00	1.00	5.00	5.00	5.00	3.00	3.00	3.00	3.00	5.00
平台体验	5%	3.60	3.60	1.60	3.00	3.00	3.00	3.00	3.60	1.60	3.00	4.40
分析	10%	3.60	1.60	5.00	3.00	1.60	4.40	4.40	3.00	3.00	5.00	3.60
风险评分和优先排序	10%	5.00	1.00	5.00	3.00	3.00	3.00	3.00	3.00	3.00	5.00	5.00
战略	50%	3.86	2.30	2.80	3.88	3.76	2.58	4.68	2.86	2.44	4.12	4.20
产品愿景	25%	3.00	3.00	3.00	5.00	3.00	3.00	5.00	3.00	3.00	5.00	5.00
计划的增强	25%	5.00	3.00	3.00	3.00	5.00	3.00	5.00	3.00	3.00	3.00	5.00
性能	25%	5.00	1.00	3.00	3.00	3.00	1.00	5.00	3.00	1.00	5.00	3.00
商业模式	15%	3.40	3.00	3.00	4.20	3.40	2.20	4.20	3.40	2.60	3.80	3.00
技术合作伙伴	10%	1.00	1.00	1.00	5.00	5.00	5.00	3.00	1.00	3.00	3.00	5.00
市场占有率	0%	1.40	3.00	1.80	4.60	4.60	3.00	4.20	1.00	3.00	3.40	5.00
企业采用	80%	1.00	3.00	1.00	5.00	5.00	3.00	5.00	1.00	3.00	3.00	5.00
平均交易规模	20%	3.00	3.00	5.00	3.00	3.00	3.00	1.00	1.00	3.00	5.00	5.00

所有分数都在 0（弱）到 5（强）范围内。

供应商产品

Forrester 在本次评估中包括了 11 家供应商：Exabeam、FireEye、Gurucul、IBM Security、LogRhythm、Micro Focus、Microsoft、Rapid7、RSA、Securonix 和 Splunk（参见图 3）。Fortinet 和 McAfee 原本也在受邀之列，但因其谢绝参与本次 Forrester Wave 评估，因此我们无法对其实力进行足够充分的评估，也就无法将其作为未参与供应商纳入评估。

图 3 参与评估的供应商和产品信息

供应商	评估的产品
Exabeam	Exabeam Security Management Platform 2020.1
FireEye	FireEye Helix
Gurucul	Unified Security and Risk Analytics (USRA) 8.0
IBM Security	IBM Security QRadar 7.4.0; IBM Security Resilient v37
LogRhythm	LogRhythm NextGen SIEM Platform 7.5
Micro Focus	ArcSight 2020.2
Microsoft	Azure Sentinel
Rapid7	InsightIDR
RSA	RSA NetWitness Platform v11.4; RSA NetWitness Orchestrator v6.0
Securonix	Securonix Next-Gen SIEM 6.3
Splunk	Splunk Enterprise 8.0; Splunk Cloud; Splunk Enteprise Security (ES) 6.2; Splunk User Behavior Analytics (UBA) 5.0; Splunk Phantom 4.9; Splunk Mission Control (MC)

供应商简介

我们的分析表明，各个供应商分别存在以下优势和劣势。

领导者

› **IBM Security 正在云端构建一个开放式安全平台。**IBM 安全性分析平台的未来愿景以其 CloudPak for Security 平台为基础，该平台构建在 OpenShift 云原生架构之上，根植于其收购 RedHat 的举措，

这种收购的初衷就是在 IBM Cloud 中提供多种安全服务。IBM QRadar Advisor with Watson、X-Force 威胁情报及与 IBM 托管安全服务的集成等功能是关键的区别所在。SOAR 以 IBM Security Resilient 插件的形式提供。定价方案包括基于用量的许可证（收费由系统提取的事件数量决定），或者对提取、分析和存储量均无限制的许可证（收费由环境内的服务器数量决定）。

参考客户赞赏了 IBM 的全球影响力、技术支持和创新。不过他们也指出，许多新功能都是以应用程序的形式提供的，而不是对核心产品的改进，并且一些可视化效果看起来有些过时。他们提到的弱点包括本地安装较为复杂，以及找不到产品文档和支持页面。具有复杂安全需求的大型全球企业应该评估 IBM。

- **Splunk 以安全性分析为企业使命。**大多数企业在一定程度上使用 Splunk 进行基础架构监控、应用程序分析或安全。在安全性方面，Splunk 正围绕其基于云的统一安全平台 Mission Control 筹划未来。在云技术采用方面，Splunk 比本次评估中的其他供应商以及安全分析市场的云原生新秀要缓慢，但该公司现在正将云作为未来业务重点。Splunk 提供了一系列定价方案，包括基于工作负载、基于用例的定价，以及由平台所提取数据量决定的传统按用量付费模式。

  灵活性和快速搜索大量数据的能力是 Splunk 的主要特点。参考客户表示速度、多功能性和自定义是其关键优势。他们还赞赏 Splunk 庞大且活跃的用户社区。相比之下，定价问题仍然存在。Splunk 已努力改善定价方案并提供更多灵活性，但参考客户一致认为，成本是其一大薄弱环节。如果企业需要高度可自定义的解决方案，以快速搜索多个大型数据库，那么应该考虑 Splunk。

- **Securonix 提供基于 SaaS 的多租户安全性分析。**Securonix 最初于 2008 年作为 SUBA 供应商亮相，2016 年新增了 SIEM 功能，作为安全性分析平台参与市场竞争。此后，该供应商又额外提供了自动化产品，可作为附加功能交付，也可通过第三方集成交付。Securonix 已转向采用云优先 SaaS 部署策略，提供灵活的部署选项，包括多租户，因此对 MSSP 合作伙伴具有吸引力。该供应商采用基于所监控的身份数量收费的定价方案。

  参考客户指出，Securonix 的基于分析的方法、行为分析和实时数据充实是优势所在。在缺点方面，参考客户指出，日志提取延迟和用户界面中的小缺陷是其不足。寻求灵活的安全性分析平台或多租户解决方案的企业和中端市场公司应该评估 Securonix。

- **ExaBeam 在用户体验方面表现亮眼。**Exabeam 于 2014 年起步，重点关注 SUBA，并于 2017 年推出了 SIEM 和 SOAR 产品，发展迅猛。Exabeam 安全管理平台可将集成化分析、日志管理和 SOAR 结合在一起作为一个平台运行，也可分别作为独立解决方案提供。事件主要基于用户行为和资产，安全性分析师可以通过时间轴的形式查看事件，以开展调查。Exabeam 提供多种定价模式，包括基于受监控员工数量或所提取的数据量收费。

参考客户表示，可用性和对个人用户行为的深入了解可视为优势。他们还将该供应商的定价策略视为一项具有吸引力的特点。参考客户提醒说，该供应商的快速成长可能不利于其充分支持客户的能力，并评价说，新功能在最初发布时经常有很多小错误。寻求以用户行为为重点、模块化而又集成式的 SA 平台的中端市场公司和企业应该考虑 Exabeam。

› **Microsoft 进军安全性分析市场。**该供应商的 SA 解决方案 Microsoft Azure Sentinel 在 2019 年 RSA 安全会议上宣布，然后于 2019 年 9 月隆重推出。该供应商进军安全性分析领域，吸引了安全服务购买者的关注。Microsoft 推行大胆举措，允许免费将 Microsoft Azure 和 Microsoft Office 365 活动日志提取到 Sentinel 中，这使得该解决方案对已经投资于 Azure 和 Microsoft 365 的企业尤具吸引力。其他数据源的定价基于用量，由提取到平台中的数据量决定。仅仅一年时间，Microsoft 就形成了巨大的市场吸引力。

虽然 Azure Sentinel 具有创新性并充分利用了 Azure 基础机构，但它仍然是一种非常新的产品。其创新性表现在能够引入第三方日志等方面。参考客户指出，可跨 Azure、Microsoft 365 和 Windows Defender for Endpoint 等其他 Microsoft 产品轻松集成是一大优势。参考客户指出，自动化是另一个优势。Microsoft 进军安全领域确实给不希望单独一家供应商在多个层级（包括云、端点和电子邮件）提供安全服务的安全专业人士带来了问题。但是，寻求单一供应商解决方案的客户会喜欢跨技术的集成。在 Microsoft Azure 和 Microsoft 365 上投入大量资金的各种规模的企业都应该考虑使用 Microsoft 产品。

表现出众者

› **Logrhythm 为企业安全性分析提供了部署灵活性。**Logrhythm 于 2018 年 7 月被私募股权公司 Thoma Bravo 收购，是 SIEM 市场的老牌厂商。LogRhythm 素以中端市场解决方案而著称，提供了功能丰富的 SA 平台，适合各种规模的企业。该供应商将 SIEM、分析和自动化纳入基本许可证，但通过其 Cloud AI 交付的 SUBA 属于附加购买项。Logrhythm 可作为本地部署设备、虚拟设备、软件和 SaaS 的形式提供。2020 年，为了让客户享受灵活定价，LogRhythm 推出了 True Unlimited 数据套餐定价方案，这一模式承诺数据用量不受限，取代了价格由每秒消息量 (MPS) 决定的基于用量的定价模型。

参考客户评论说，该解决方案易于使用，并且可以很好地扩展以跟上增长步伐。他们还提到，该公司的客户支持服务较为出色。参考客户提到，所包含的自动化和快速响应功能与独立的 SOAR 解决方案不能相比，并且对第三方云和 SaaS 环境的支持不及预期。寻求具有灵活部署选项、全面功能的安全性分析平台的中端市场和企业客户应考虑 LogRhythm。

› **Gurucul 提供基于风险的数据分析。**Gurucul 于 2010 年成为大数据安全性分析供应商，并发展为涵盖 SUBA、SIEM 和 SOAR 的安全性分析平台提供商。Gurucul 提供自己的大数据架构，并支持客户提供的第三方数据存储。该供应商允许客户自定义其分析模型，或通过 Gurucul Studio 构建自己的模型。Gurucul 提供可自定义的机器学习行为剖析、预测性风险评分和风险优先级警报。Gurucul 部

署为可在客户提供的硬件或虚拟基础架构、设备或 SaaS 上运行的软件。该供应商提供订阅式许可、永久授权许可和 SaaS 许可。该解决方案的定价是模块化的，对于 SIEM、SUBA、自定义日志存储、SUBA 和 NAV 均有独立定价模块，此外还提供企业定价。监控服务的价格根据监控的身份/实体的数量而定。

参考客户反馈表明，Gurucul 在机器学习模型、风险评分和灵活性方面都有优势。参考客户提到的弱点包括解决方案过于复杂，以及供应商为进入市场所作的努力方面的不足。寻求强大、可自定义并具有基于风险的优先级排列功能的安全性分析工具的企业应该考虑 Gurucul。

› **Micro Focus 将安全性分析平台的各个部分整合在一起。**Micro Focus 战略性地收购了一家 SUBA 供应商 (Interset) 和一家 SOAR 供应商 (Atar Labs)，用来补充其原有的 ArcSight SIEM - 该产品几年来一直处于市场落后水平。长期以来，ArcSight 一直是一些全球最大企业和政府机构的首选供应商，尽管许多长期客户已离开该平台。Micro Focus 目前有所进步，但与本次评估中的其他供应商相比，采纳云交付方式的实际较晚。ArcSight 可以在虚拟环境和云环境中以硬件设备、容器或软件的形式部署。Micro Focus 目前正致力于提供完整的 SaaS 版解决方案。该解决方案的定价基于 EPS，而 SUBA 功能则作为附加产品销售，并按托管实体的数量发放许可。

Micro Focus 正在投资于安全性分析领域，为其平台增加了功能，这是一个令人鼓舞的迹象。参考客户提到，与其他产品的集成、关联和全球支持是其优势所在。他们也指出，搜索性能、支持和管理控制台存在不足。投资于 Micro Focus 产品组合其他部分的企业以及那些寻求在 SA 领域拥有悠久历史的供应商的企业应该评估 Micro Focus。

› **Rapid7 在云中结合了多种安全功能。**Rapid7 的 InsightIDR 平台完全采用云端交付形式，提供了日志管理、SIEM、SUBA 和 SOAR，并且集成其漏洞管理平台。该供应商还捆绑了端点可见性和检测功能、文件完整性监控和入侵诱骗功能。该供应商于 2019 年收购 NetFort，并由此获得了 NAV 能力，可提供网络流量和行为的可见性，这项功能目前作为附加产品提供。该供应商可以扩增服务，让客户能够获得交付专业知识和内部团队支持。其产品采用 SaaS 的形式提供，采用订阅模式，定价基于受监控资产的数量。

参考客户反馈表明，部署和操作的简便性是优势。客户提到的缺点包括，缺乏定制和报告能力有限。寻求基于 SaaS 的 SA 解决方案的中小型企业以及资源受限的大型企业应该考虑 Rapid7。

› **RSA 提供了统一的安全性分析平台。**2020 年 9 月，RSA 从 Dell Technologies 集团分拆出来，并被投资财团收购，现已独立运营。[1] 该供应商通过 RSA NetWitness Platform 产品提供 SIEM、NAV、SUBA 和 SOAR。RSA NetWitness 通过结合日志、端点和包数据分析，提供威胁检测功能和可见性。SOAR 通过 RSA NetWitness Orchestrator 提供，该产品通过与 Threat Connect 签订的 OEM 协议构建，Threat Connect 通过单独许可授权提供。该解决方案可以本地部署软件、硬件或

混合部署等形式提供。软件版本可以托管在私有云或公共云环境中，但不能作为 SaaS 产品提供，不过他们正在开发完整的 SaaS 功能。定价依组件的不同而有所不同，RSA NetWitness Logs 和 RSA NetWitness Network 的基于用量的定价模式，RSA NetWitness UEBA、RSA NetWitness Endpoint 和 RSA NetWitness Orchestrator 则采用基于用户数量的定价模式。

RSA 将 RSA NetWitness 与自有的 EDR 功能集成在一起，用于检测和响应，并支持第三方 EDR 供应商。参考客户赞赏该平台的统一性，还有结合日志和数据包分析等优势。参考客户指出，该解决方案很复杂，UI 不够直观，新用户的学习曲线可能十分陡峭。利用 RSA Archer 进行治理、风险和合规性 (GRC) 管理的组织以及希望对其网络流量和集成 EDR 拥有高度可见性的组织应考虑 RSA。

竞争者

› **FireEye 通过 Helix 提供了一套集成式方法。**FireEye 将其安全性分析和自动化功能结合到了 Helix 平台中。Helix 包括日志保留、SIEM、威胁情报、威胁捕获和 SOAR 等功能。该供应商将 Helix 作为独立的 SaaS 解决方案销售，也可将其与其他 FireEye 解决方案（如网络安全、电子邮件安全、端点安全和 Cloudvisory）打包销售。2019 年收购 Verodin 后，该供应商以附加销售项的形式为 MITRE ATT&CK 框架提供可视化覆盖情况的能力，不过 Helix 允许使用 ATT&CK 进行威胁捕获和自定义检测。另外还可以使用 Mandiant 服务增强 Helix，利用其安全专业知识或提供托管服务。该供应商的定价基于用量，与 EPS 挂钩。

参考客户赞赏其以下方面的优势：威胁情报、接洽 FireEye 专家的能力以及与其他 FireEye 安全工具的高集成水平。虽然该解决方案在 FireEye 产品组合中集成良好，但没有针对所有 FireEye 产品的中央管理控制台或仪表板，参考客户将此视为不足。参考客户还提到，Helix 的 SOAR 组件不当不够完善，具备管理该平台的娴熟技能的人才不足，这是一个问题。依靠该供应商提供其安全基础架构的其他部分的企业应该考虑 FireEye。

评估概述

我们根据 27 个标准条件对这些供应商进行了评估，这些标准分为三大类：

- **当前产品。**在 Forrester Wave 图中，每个供应商在垂直轴上的位置就表示其当前产品的优势情况。这些解决方案的关键标准包括部署和数据架构、可见性、关联能力、威胁检测、ATT&CK 映射、自定义检测、安全编排、合规性、平台体验、分析以及风险评分和优先级排列。
- **战略。**在水平轴上的位置表示供应商战略的优势情况。我们评估了产品愿景、计划的增强、性能、商业模式和技术合作伙伴等方面。
- **市场占有率。**图上标记的大小即代表了市场占有率分数，这也反映了每家供应商的企业采用率和平均交易规模。

供应商入选标准

Forrester 在本次评估中包括了 11 家供应商：Exabeam、FireEye、Gurucul、IBM Security、LogRhythm、Micro Focus、Microsoft、Rapid7、RSA、Securonix 和 Splunk。所有这些供应商都符合以下条件：

- **产品收入。**供应商的安全性分析平台必须有 5000 万美元的产品线收入。
- **核心功能。**供应商必须拥有一个包含成熟的 SIEM 和 SOAR 功能的安全性分析平台。所提供的 SOAR 功能可以作为解决方案的专有项或白标部分提供。
- **Forrester 客户认知度。**Forrester 客户经常在咨询和访谈期间讨论到参与评估的供应商。为了确保与 Forrester 客户的相关性和所提供参考的质量，我们要求产品在过去六个月内处于正式发布状态，并且未发生重大变化。

与分析师交流

通过与 Forrester 思想领袖合作，将我们的研究成果应用于您的特定业务和技术计划，让您对自己的决策更具信心。

分析师问询

在 30 分钟电话会议中直接与分析师就您的问题展开讨论，或者也可以选择通过电子邮件获得分析师的回复，帮助您将研究成果付诸实践。

了解更多。

分析师咨询

通过定制战略会议、研讨会或演讲等特定形式，与分析师合作将研究成果转化为具体行动。

了解更多。

网络研讨会

参加我们的在线会议，了解对您的业务产生影响的最新研究。每次会议都包括分析师问答和幻灯片材料，可按需提供。

了解更多。

针对 iOS 和 Android 的 Forrester 研究应用程序。
在动态竞争中保持领先地位。

补充材料

在线资源

我们将所有 Forrester Wave 得分和权重都发布在一个 Excel 文件中，其中提供了详细的产品评估和可定制排名；单击 Forrester.com 上该报告开头处的链接，即可下载此工具。我们设定的这些得分和默认权重只是作为一个参考，读者可以根据个人需要来调整相应权重。

Forrester Wave 方法指南

Forrester Wave 是一套可供技术市场中的买家在做出购买决策时参考的指南。为了提供一个对所有参与者都公平的流程，Forrester 遵循《Forrester Wave™ 方法指南》对参与的供应商进行评估。

在审查中，我们首先开展初步研究，制定出一份考虑评估的供应商列表。然后根据入选标准，逐渐缩小范围，确定最终的供应商名单。接着，通过详细的问卷调查、演示/简报以及客户参考调查/采访，收集详细的产品和战略信息。在这些信息输入的基础上，我们借助分析人员在相关市场中的丰富经验和专业知识，对这些供应商进行评分，此过程中用到了相对评级系统，即将每个供应商与评估中的其他供应商进行比较。

每份 Forrester Wave 报告的标题中都清楚地列出了 Forrester Wave 发布日期（季度和年份）。在本次 Forrester Wave 评估中，参与的各供应商在 2020 年 8 月 18 日之前向我们提供的材料方可作为参考依据，该时间点之后不允许提供其他信息。我们鼓励读者评估市场和供应商产品随时间的变化情况。

根据《Forrester Wave™ 供应商审查政策》，Forrester 要求供应商在发布之前对调查结果进行检查，以确保准确性。Forrester Wave 图中，标记为未参与的供应商是指符合我们定义的入选标准，但谢绝参与评估或只参与了部分评估的供应商。我们根据《Forrester Wave™ 和 Forrester New Wave™ 未参与和未完整参与的供应商政策》对这些供应商进行评分，并将他们的定位情况与其他参与的供应商一起发布。

操守政策

我们遵循公司网站上发布的《操守政策》开展包括 Forrester Wave 评估在内的所有研究。

尾注

[1] 资料来源：《RSA® 在被 Symphony Technology Group 收购完成后成为独立公司》(RSA® Emerges as Independent Company Following Completion of Acquisition by Symphony Technology Group)，RSA 新闻稿，2020 年 9 月 1 日 (https://www.rsa.com/en-us/company/news/rsa--emerges-as-independent-company)。

我们与商业和技术领域的众多领导者携手，推动以客户为本的愿景、战略和措施的落实，以推动业务不断增长。

产品和服务

- 研究和工具
- 分析师参与
- 数据和分析
- 同行协作
- 咨询
- 活动
- 认证计划

› Forrester 可根据您的工作职责和关键业务计划提供量身定制的研究和洞察。

我们所服务的角色

营销和战略制定专业人士

CMO
B2B 营销
B2C 营销
客户体验
客户洞察
电子商务和渠道战略

技术管理专业人士

CIO
应用程序开发和交付
企业架构
基础架构和运营
› 安全和风险
采购和供应商管理

技术行业专业人士

分析师关系

客户支持

有关打印件或电子重印本的信息，请联系客户支持部门：致电 +1 866-367-7378、+1 617-613-5730 或发送电子邮件至 clientsupport@forrester.com。学术机构和非营利性机构可享受批量折扣和特价优惠。