FORRESTER®

Forrester Wave™：2024 年第二季度网络安全风险评级平台

重点关注的 10 家供应商及其排名

发布时间：2024 年 5 月 19 日

编辑人员：Cody Scott、Amy DeMartine、Caroline Provost 和 Peter Harrison

摘要

在 Forrester 对网络安全风险评级（Cybersecurity Risk Ratings，CRR）平台供应商的 25 项标准评估中，Forrester 确定了重点关注的 10 家供应商，对它们进行了研究、分析和评分。这份报告展示了每家供应商的表现，并帮助安全和风险专业人员选择符合他们需求的供应商。

信任将决定网络安全风险评级的未来

如果在一个坐满 CISO 的房间里提起网络安全风险评级，您就会发现意见众多，有热烈表达的，也有冷静评述的，但没有人是冷漠的。CRR 市场已存在十多年，它的崛起就像是西西弗斯一次又一次推着巨石上山，不断地努力，却很难取得进展，不是平稳地走向成熟。即使在 2021 年，Forrester 仍然认为市场还不成熟，并指出由于重大的技术限制，网络安全风险评级还没有准备好进入黄金时段。但是，时代在变化。技术挑战依然存在，但供应商正在重新调整其交付方式，在技术准确性和效率方面进行更多投资，并扩展其服务和支持，以满足更相关的安全和第三方风险管理（Third-Party Risk Management, TPRM）需求。而且，买家现在从这些平台中发现了更多价值：当今，大多数 CRR 客户都使用这些平台来增强其第三方网络风险评估和监察能力。CRR 市场正在慢慢从“帮助我理解”转变为“帮助我做得更多”。

由于这些趋势，CRR 客户应该寻找具有以下特点的供应商：

- **建立和维护信任。**Forrester 不是指那些“戴着玫瑰色眼镜”看待评级的华丽公关活动，而是指 CRR 供应商把信任作为他们开展业务的必要条件。首先要认识到评级在当今监管机构、保险提供商、政府、合同和各种商业关系中占据了非常重要的位置。通过发布公开的评级，CRR 供应商承担了与诚信、一致性、能力和透明度相关的类似受托责任和尽职调查的责任。有差异化的供应商开始认真对待这一角色，但这是一个持续的过程，不是一个可以一步到位的目标。
- **不断改进发现和归因方法。**CRR 供应商如何发现、归因并验证资产和发现，决定了优秀与卓越的区别。但多年来，客户不得不忍受刚刚好的情况。一般公司的安全团队既没有时间也没有资源从误报中找出准确的结果，但其商业伙伴、监管机构和领导层却要求其承担责任，挫败感无处不在。然而，一些有差异化的供应商已经开始认真对待这些问题，并开始使用外部攻击面管理（Attack Surface Management, ASM）方法，帮助被评级的实体更好地控制其数据。

- **了解风险评级和风险量化之间的区别。**风险评级不是对风险的定量衡量。相反，它是基于与风险相关的安全指标的分数。风险是具有一定可能性（威胁行为者通过攻击向量影响资产）和影响（导致不同形式的实质损失）的场景。评级中衡量的安全指标专注于可能性方面（即，增加或减少损失可能性的安全控制）。另一方面，网络风险量化（Cyber Risk Quantification, CRQ）直接衡量风险场景的概率和实质性影响。它们是相关的，评级数据可以用于 CRQ 分析，但它们并不相同。

评估总结

Forrester Wave™ 评估突出了领导者、表现出色者、竞争者和挑战者。这是对市场上顶尖供应商的评估，这不代表整个供应商环境。您可以在《2024 年第一季度网络安全风险评级平台格局》报告中找到更多关于该市场的信息。

图 1：Forrester Wave™：2024 年第二季度网络安全风险评级平台

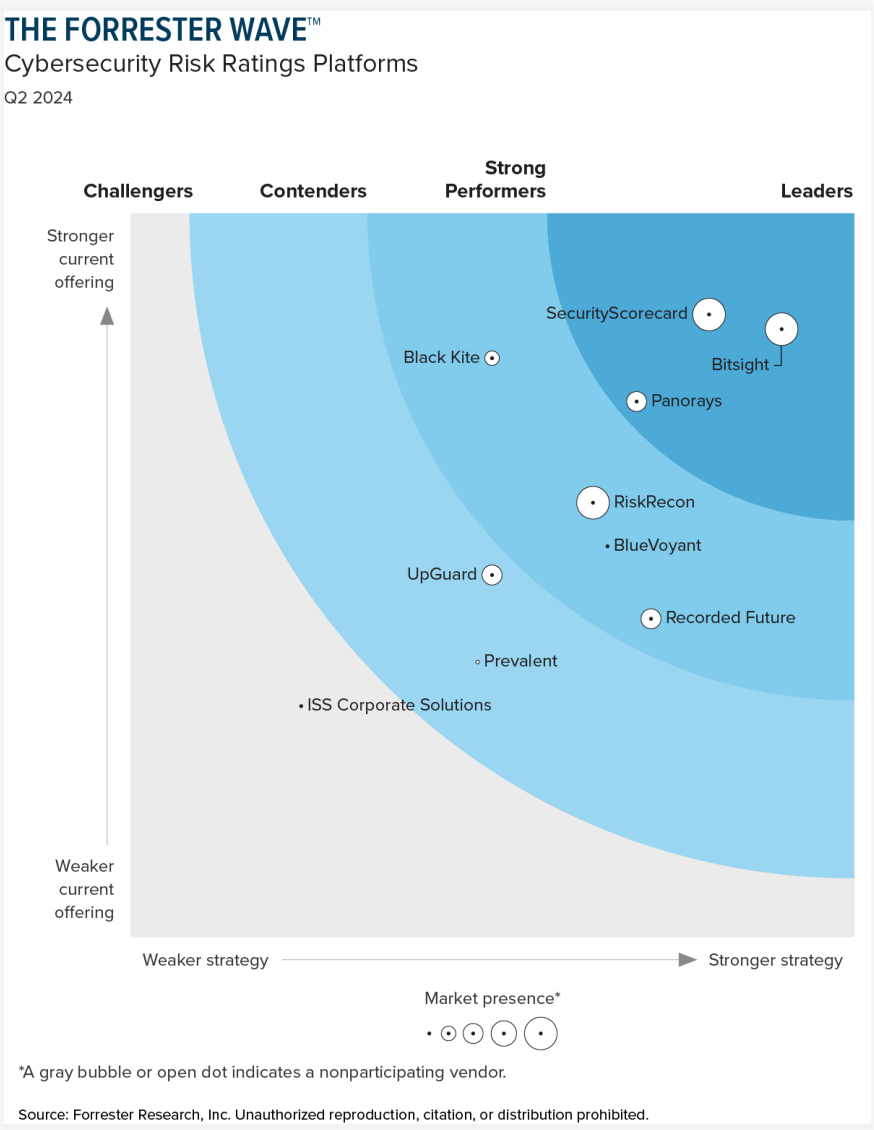

图 2：Forrester Wave™：2024 年第二季度网络安全风险评级平台 评分表

	Forrester's weighting	Bitsight	Black Kite	BlueVoyant	ISS Corporate Solutions	Panorays	Prevalent*
Current offering	50%	4.20	4.00	2.70	1.60	3.70	1.90
Asset discovery and attribution	10%	5.00	3.00	3.00	1.00	5.00	1.00
Data source variety	5%	5.00	3.00	3.00	3.00	3.00	1.00
Ratings correlation testing and results	5%	5.00	5.00	1.00	3.00	3.00	1.00
Ratings trust and transparency	10%	3.00	3.00	1.00	3.00	1.00	1.00
Ratings dispute resolution	5%	5.00	3.00	3.00	3.00	5.00	1.00
Vendor discovery and mapping	10%	3.00	5.00	5.00	1.00	5.00	3.00
Security assessment questionnaire	10%	3.00	5.00	3.00	1.00	5.00	5.00
In-platform collaboration	5%	5.00	5.00	3.00	1.00	3.00	3.00
Standards-based alignment	5%	3.00	5.00	3.00	1.00	3.00	1.00
Security performance analytics	10%	5.00	5.00	3.00	1.00	3.00	1.00
Exposure prioritization and remediation	5%	5.00	3.00	3.00	3.00	5.00	3.00
Third-party cyber risk quantification support	5%	5.00	5.00	1.00	1.00	1.00	1.00
Integrations and interoperability	5%	3.00	3.00	1.00	1.00	5.00	3.00
Reporting and visualization	5%	5.00	3.00	3.00	1.00	3.00	1.00
User experience	5%	5.00	3.00	3.00	1.00	5.00	1.00
Strategy	50%	4.50	2.50	3.30	1.10	3.50	2.40
Vision	15%	5.00	3.00	3.00	1.00	5.00	3.00
Innovation	15%	5.00	3.00	3.00	1.00	3.00	1.00
Roadmap	15%	5.00	3.00	3.00	1.00	3.00	1.00
Partner ecosystem	10%	5.00	3.00	3.00	1.00	5.00	3.00
Adoption	15%	5.00	1.00	3.00	1.00	3.00	3.00
Pricing flexibility and transparency	5%	1.00	5.00	3.00	3.00	3.00	1.00
Community	10%	5.00	3.00	3.00	1.00	3.00	1.00
Supporting services and offerings	15%	3.00	1.00	5.00	1.00	3.00	5.00
Market presence	0%	5.00	2.00	1.00	1.00	3.00	1.00
Revenue	50%	5.00	1.00	1.00	1.00	3.00	1.00
Number of customers	50%	5.00	3.00	1.00	1.00	3.00	1.00

	Forrester's weighting	Recorded Future	RiskRecon	SecurityScorecard	UpGuard
Current offering	50%	2.20	3.00	4.30	2.50
Asset discovery and attribution	10%	3.00	3.00	5.00	3.00
Data source variety	5%	5.00	3.00	5.00	3.00
Ratings correlation testing and results	5%	1.00	5.00	5.00	1.00
Ratings trust and transparency	10%	1.00	1.00	3.00	3.00
Ratings dispute resolution	5%	1.00	3.00	5.00	3.00
Vendor discovery and mapping	10%	3.00	3.00	3.00	1.00
Security assessment questionnaire	10%	1.00	1.00	3.00	3.00
In-platform collaboration	5%	1.00	3.00	5.00	3.00
Standards-based alignment	5%	3.00	5.00	5.00	3.00
Security performance analytics	10%	3.00	3.00	5.00	3.00
Exposure prioritization and remediation	5%	1.00	3.00	5.00	1.00
Third-party cyber risk quantification support	5%	1.00	5.00	3.00	1.00
Integrations and interoperability	5%	5.00	3.00	5.00	3.00
Reporting and visualization	5%	1.00	5.00	5.00	3.00
User experience	5%	3.00	3.00	5.00	3.00
Strategy	50%	3.60	3.20	4.00	2.50
Vision	15%	3.00	3.00	5.00	1.00
Innovation	15%	5.00	1.00	3.00	3.00
Roadmap	15%	1.00	3.00	5.00	3.00
Partner ecosystem	10%	3.00	3.00	5.00	1.00
Adoption	15%	5.00	3.00	3.00	5.00
Pricing flexibility and transparency	5%	5.00	3.00	3.00	3.00
Community	10%	5.00	5.00	5.00	3.00
Supporting services and offerings	15%	3.00	5.00	3.00	1.00
Market presence	0%	3.00	5.00	5.00	3.00
Revenue	50%	3.00	5.00	5.00	3.00
Number of customers	50%	3.00	5.00	5.00	3.00

All scores are based on a scale of 0 (weak) to 5 (strong).
*Indicates a nonparticipating vendor

供应商产品

Forrester 评估了以下产品。

图 3：评估的供应商和产品信息

Vendor	Product evaluated	Product version evaluated
Bitsight	Security Performance Management, Third Party Risk Management, Professional Services	N/A
Black Kite	Black Kite Cyber Risk Platform	N/A
BlueVoyant	BlueVoyant Supply Chain Defense	SCD.2024.March
ISS Corporate Solutions	ISS Cyber Risk Score	V5.0
Panorays	Panorays	N/A
Prevalent	Third-Party Vendor Risk Monitoring	N/A
Recorded Future	Recorded Future Intelligence Cloud	N/A
RiskRecon	RiskRecon	N/A
SecurityScorecard	SecurityScorecard	N/A
UpGuard	UpGuard	N/A

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

供应商简介

本报告揭示了各个供应商的优势和劣势，具体如下：

领导者

- **Bitsight 通过先进的分析和行业推广建立信任。**Bitsight 于 2011 年推出，是 CRR 市场的先驱，并有着在数字经济中创建信任的雄心壮志。它拥有无与伦比的创新承诺，迄今为止拥有 58 项专利、员工专利激励计划以及与其他供应商相比最大的研发投资。其合作伙伴生态系统、采用率和社区战略都以构建和推广评级信任为中心，通过培训和支持帮助客户取得成功，还支持全行业的研究和信息共享计划。然而，其定价模型相对复杂，并且基础产品不包括同行基准测试和第四方数据功能。其路线图优先考虑加强其风险管理深度、推出信任管理中心以及使用人工智能扩展分析工具。

Bitsight 专注于评级模型验证和相关性研究，以不断测试其评级与实际事件的一致性。它利用政策审查委员会来管理发现的争议并公开发布案例摘要。该平台具有协作仪表板，可简化与第三方的交互和计划。其领先的安全性能分析模块可提供对控制性能的深入洞察。它还具备本地网络风险量化工具，可根据网络损失数据衡量财务风险。相关客户赞扬了其执行报告和分析，但指出 Bitsight 数据通过治理、风险和合规（GRC）集成共享时，与 Bitsight 平台上的数据不匹配，导致需要额外工作来验证报告。Bitsight 最适合希望集中其攻击面管理、第三方风险管理和网络保险用例的客户。

- **SecurityScorecard 通过将见解转化为行动来颠覆评级。**SecurityScorecard 的使命是改变世界衡量和管理网络风险的方式，自上次 2021 年 Forrester Wave™评估以来，SecurityScorecard 已在攻击面管理、威胁情报、数字取证和事件响应方面进行了战略性转变。其路线图没有显示出放缓的迹象，因为它专注于重新构想第三方网络风险，从评级扩展到解决方案，并增强人工智能驱动的洞察力。该公司拥有强大的合作伙伴生态系统，可提高用户采用率和体验。其社区策略独特，涉及 17 个行业信息共享中心。近年来的这些转变，使 SecurityScorecard 接触到传统上不会考虑 CRR 平台的新买家，SecurityScorecard 需保持其发展势头，才能赢得他们的青睐。

SecurityScorecard 是此次评估中唯一一家发布实时指标的供应商，实时指标包括其响应时间、调查结果驳斥率以及 IP 和域名错误归因率，这对信任和透明度大有裨益。由于其丰富的内部历史数据和强大的扫描功能，其平台在资产发现、数据源多样性和评级相关性测试方面表现出色。它还在安全性分析和平台内协作功能方面与众不同，并配备强大的报告工具，以便于风险沟通。它使用评级数据来验证问卷答复，但缺乏人工智能解析工具来自动评估上传的证据文件。相关客户喜欢其 UX 功能，但指出在扫描的 IP 和主机名报告相同资产时防止重复发现存在挑战。SecurityScorecard 最适合希望增强攻击面和供应链用例的客户。

- **Panorays 优先考虑第三方网络风险管理的业务环境。**尽管该公司比其他公司更关注第三方风险，但其卓越的愿景突显了供应链的复杂性以及从第一方和第三方角度确保供应链安全所需的深层技术功能。其前瞻性的合作伙伴战略强调与专家行业团体的合作，使客户始终处于最佳实践内容和标准的前沿，以应对不断变化的监管要求。Panorays 的相关客户对其平台的整体商业价值给予了最高的满意度评价。其大部分战略重点与市场一致，与同行相比差异化程度较低。其路线图包括增强供应链发现、风险评估、威胁检测、修复和协作功能。

Panorays 的优势之一是人工智能主导的资产和供应商发现的强大功能，其中包括对所有发现结果分配置信度评分，以及在每条记录中发布源详细信息以提高透明度。它的人工智能文档验证工具可以评估供应商的调查问卷答复，以验

证观察到的数据是否支持该答复，从而简化确定修复措施优先级的工作。此外，它还拥有各种集成选项——涵盖 GRC、IT 资产管理、采购、隐私和分析工具，以及凭借强大的用户体验来加速评估工作流程。然而，它的评级信任度和透明度较弱，因为它不公开自己的评级绩效指标，并且缺乏本地风险量化工具。相关客户赞扬了该平台详细的修复计划，但希望有更多的动态报告功能。Panorays 最适合企业的第三方风险管理计划。

表现出色者

- **Black Kite 的技术能力飙升，但其战略过于保守。**如果 Forrester Wave™ 颁发最大进步奖，Black Kite 就会获奖。自上次 Forrester Wave™ 评估以来，该公司已大大增强了其平台的技术深度和广度。尽管通过强有力的创新取得了这一成功，但其大部分战略重点仍与市场相当。Black Kite 的独特之处在于其简单的两层定价模式（无限用户）和增值标准许可证（包含比大多数供应商标准套餐更多的功能）。其路线图优先考虑增强和扩展协作、自动化风险响应、漏洞管理和合作伙伴集成。Black Kite 在采用战略方面相对较弱，缺乏与其他公司相比的专门教育关注点，其支持服务通过托管服务提供商交付。

  Black Kite 独特的关注点是基于标准的评级，直接解决了行业评级完整性的问题。它是本次评估中唯一一家客户对其评级准确性一致满意的供应商。但这主要归功于其基于标准的方法，因为其资产发现策略和数据源多样性与大多数供应商相当。它在第三方供应商发现和安全评估调查问卷方面表现出色，包括一款人工智能文档解析工具，可以分析合规文档以简化评估流程。此外，它还具备本地的基于 FAIR 的第三方风险量化功能，以及增强其安全性分析的勒索软件敏感性指数。然而，相关客户提到了页面加载和性能缓慢的问题。Black Kite 非常适合偏好基于标准方法和基于 FAIR 的量化的安全和第三方风险管理团队。

- **RiskRecon 提供了一个全面的平台，但创新不足。**自 2019 年 Mastercard 收购 RiskRecon 以来，RiskRecon 的强劲增长、全球覆盖和多行业扩张一直是 Mastercard 重新定位为网络安全公司的关键驱动力。从战略上看，由于其集成的网络安全产品组合，它以其支持服务和产品而脱颖而出。它的愿景和路线图强调了向多维风险评级的转变，包括威胁情报、主动监察和附加保护服务等关键增强功能，以满足当今的客户需求。RiskRecon 拥有卓越的社区战略，与其客户群和各种行业协会建立了思想领导地位。但其较弱的创新战略导致产品开发是被动的，而不是主动的，并且缺乏对颠覆性功能的长期关注。

  RiskRecon 的优势包括其领先的报告生成器模块及其基于标准的一致性，该模块跨框架控制企业风险数据。这使得深度功能能够评估控制有效性，同时让用户灵活定义自己的框架，并通过评级数据分析绩效。RiskRecon 还通过其

Cyber Quant 产品整合了财务损失估计，从而实现了差异化。但其评级信任和透明度方法不及其他公司，在促进信任方面投入的资源和外联工作较少。此外，它还缺乏本地安全调查问卷模块，而是使用合作伙伴解决方案。相关客户赞扬了该平台的报告工具和同行基准测试，但提到了理解资产归属方面的挑战。RiskRecon 非常适合注重控制的安全和风险团队，也适用于当前的 Mastercard 客户。

- **BlueVoyant 在 CRR 风险运营方面表现出色，但仍需要争夺市场份额。**作为一家新兴的 CRR 供应商，BlueVoyant 于 2022 年推出了供应链防御（Supply Chain Defense）平台，以解决持续监察和修复中的差距。从战略上看，该供应商在支持服务方面表现出色，这要归功于其在托管检测和响应（Managed Detection and Response, MDR）以及数字风险保护方面的产品专业知识，还有其广泛的专业服务。其愿景和路线图与市场保持一致，强调安全运营的发展，并对其平台、分析和人工智能功能进行了坚实的增强。该供应商在 MDR 市场的定位为其提供了独特的优势，能够以当今大多数评级公司无法做到的方式接触安全运营商。但为了抓住这个机会，BlueVoyant 需要加强其创新和社区战略，以赢得市场份额。

BlueVoyant 的平台在自动化供应商发现方面也表现出色，使用人工智能从多个数据源中识别供应商关系。其 Terrain Explorer 工具提供了领先的可视化和数据查询功能，用于探索供应商和产品集中度以及第 n 方关系。其资产发现和安全性能分析处于同一水平。其评级方法较弱，因为它缺乏对实际事件的相关性测试。其问卷管理解决方案，包括智能审核工具，是通过合作伙伴提供，而不是本地提供，它们都用于确定合规证据满足问卷标准的程度。然而，相关客户希望看到调查问卷工具与供应链防御（Supply Chain Defense）平台完全集成。BlueVoyant 非常适合希望弥合采购和第三方风险管理安全差距的安全运营团队。

- **Recorded Future 基于情报的见解表现出色，但评级和修复措施滞后。**Recorded Future 应用其广泛的人工智能驱动的情报工具来生成网络风险见解。其创新方法独具特色，强调了全面的研发投资战略。它提供高度灵活的定价模型，按受监察方的层级定价。但相关客户表示，该产品在添加支持服务时相对昂贵。Recorded Future 还因其采用和社区策略而与众不同，其中包括 RF University、Intelligence Kit 最佳实践、免费工具、精选新闻、初创公司种子基金和全球活动。然而，其路线图不及市场水平。它包括许多计划中的增强功能，这些增强功能已经在市场上存在。

Recorded Future 的产品与 GRC、第三方风险管理、攻击面管理、分析工具广泛集成。虽然它在资产发现技术和自动供应商映射方面不相上下，但由于其 Intelligence Graph，它从比大多数供应商更多的来源收集和分析威胁数

据，因此在数据源多样性方面表现出色。这推动了其在安全性能分析和基于标准的调整方面的同等功能，其中包括人工智能见解，用于总结信息并为每个发现提供建议。然而，该产品的评级方法较弱，因为供应商没有进行评级相关性测试，使用相对简单的重要性权重，并且争议处理流程不太严谨。它还缺乏对安全调查问卷的本地支持，而是使用合作伙伴的解决方案。相关客户青睐其集成，但希望有更统一的模块来支持研究需求。Recorded Future 非常适合需要针对多个用例的全面威胁情报的安全团队。

竞争者

- **UpGuard 满足了核心用例，但在复杂需求方面缺乏差异化。**UpGuard 着重于攻击面管理和第三方风险管理，旨在为不断成熟的安全团队提供集成的 CRR 平台。该公司的采用策略处于市场领先地位，提供了一种全面的方法来提高客户成熟度，并有大量的教育和客户成功举措作为支持。一位相关客户指出：“UpGuard 的支持和解决问题的速度令人惊叹，产品开发速度非常快。”其创新战略和路线图与市场保持一致，重点关注人工智能主导的增强功能，以消除手动工作、自动化安全调查问卷并改进新兴威胁预警。然而，其合作伙伴生态系统和支持服务策略不及行业需求，主要关注个别客户需求而非全行业需求。

  UpGuard 的资产发现和归因功能与市场上大多数供应商相当，这有助于它与面向企业的供应商竞争。它还提供了可比较的第三方问卷管理支持、平台内协作工具和安全性能分析，以推动决策。UpGuard 为客户提供了一种独特的能力，可以立即重新扫描其环境，以验证问题是否已得到解决。然而，其供应商发现和映射功能不如其他供应商那样自动化，并且它主要根据严重性而非资产价值来优先考虑风险发现，这是不足之处。相关客户一致表示对 UpGuard 提高风险可视化的能力感到满意，但要求更先进的自动化和风险评估工作流程改进。UpGuard 非常适合小型企业和早期的第三方风险管理项目。

- **Prevalent 在第三方风险管理方面进行了创新，但在 CRR 方面进展缓慢。**Prevalent 旨在帮助客户管理整个第三方生命周期的风险，与大多数 CRR 供应商相比，其重点和功能更符合第三方风险管理和 GRC 用例。它通过支持性服务脱颖而出，包括评估（例如，尽职调查收集、SOC 2 审查和分析师主导的问卷跟踪）和管理服务（例如，分析师主导的整改、策划事件审查和事件响应）。它拥有与合作伙伴生态系统和采用策略相符的能力，有助于用户扩展规模。其将网络风险情报纳入第三方风险管理计划的愿景与市场一致，但其路线图和创新战略与 CRR 市场对更多第一方安全用例的需求不太一致。

Prevalent 的 CRR 解决方案侧重于风险评估、风险监察和共享供应商风险数据。它在供应商发现和映射方面功能强大，支持第四方和第 n 方的发现，并且由于其平台上的工作流能力，它在安全问卷管理方面表现出色。它包含有关供应商的网络和其他类型的风险数据，使其具备与风险优先级和整改相符的功能。此外，它还提供了一套可靠的集成，有助于将 Prevalent 打造成第三方风险管理的单一数据源。然而，其资产发现和评级方法以及流程的整体方法对于大多数安全团队来说过于简单，缺乏数据源多样性、评级模型与违规原因的相关性测试以及评级模型透明度。Prevalent 非常适合初创的第三方风险管理和以合规为重点的计划。Prevalent 拒绝参与完整的 Forrester Wave™ 评估过程。

挑战者

- **ISS Corporate Solutions 提供了高质量的评级，但其解决方案仍在迎头赶上。**2020 年，ISS Corporate Solutions 推出了网络风险评级解决方案，以增强其面向机构投资者和企业客户的治理、风险和环境、社会和治理（ESG）服务。它的愿景是让企业能够通过与投资者和其他利益相关者相同的视角来看待自己，这说明了它对治理和预测风险洞察的关注。然而，由于其战术重点，它在战略上的表现不佳。其简化的定价模型使客户在成熟时可以轻松扩展他们的供应商监控。但它在合作伙伴关系、社区和采用支持等对 CRR 客户至关重要的关键领域落后。ISS Corporate Solutions 将需要加强其创新和路线图承诺，以提高长期竞争力。

ISS Corporate Solutions 的优势在于评级透明度。在这次评估中，它是少数几个不在客户和其第三方之间共享风险暴露信号数据的供应商之一，这为那些不愿分享风险暴露细节的客户增加了额外的信任层。相关客户也赞扬了评级模型的相关性方法。然而，虽然其资产发现和归因流程具有强大的质量控制，但它们依赖于手动管理，这使得它们难以扩展，相关客户表示发现能力有限。该供应商在风险优先级和修复功能方面与其他供应商持平，但它缺乏平台协作、安全问卷管理和对于平台解决方案至关重要的合作伙伴集成的能力。ISS Corporate Solutions 主要适合没有扩展安全或第三方支持的治理和监察用例。

评估概述

Forrester 将评估标准分为三个类别：

- **当前产品。**每个供应商在 Forrester Wave™图形纵轴上的位置，代表了其当前产品的实力。
- **战略。**每个供应商在 Forrester Wave™图形横轴上的位置，代表了其战略的实力，包括愿景和创新等要素。
- **市场占有率。**在 Forrester Wave™图形上，每个供应商标记的圆圈大小，代表了其市场占有率。

供应商纳入标准

在此评估中，每个供应商应具备以下条件：

- **企业级平台产品。**Forrester 纳入的供应商拥有全面的企业级 CRR 平台，该平台提供公共评级，支持各种第三方网络风险管理、外部攻击面管理和暴露管理用例。
- **客户关注度和市场相关性。**Forrester 的客户在咨询和访谈中询问纳入的供应商，或提出这些供应商非常适合支持的用例。被纳入此评估意味着这些供应商在 CRR 市场上积极竞争，并出现在 Forrester 客户之间的讨论中。
- **产品收入达到 1,000 万美元或更多。**Forrester 纳入的供应商直接从其 CRR 产品中获得了 1,000 万美元或更多的全球收入。

补充内容

Forrester Wave™ 方法论

Forrester Wave™ 是一份为购买者在技术市场上考虑购买选项的指南。为了向所有参与者提供公平的流程，Forrester 遵循 Forrester Wave™方法论来评估参与的供应商。

在审查中，Forrester 进行了初步研究，以制定一份要考虑评估的供应商名单。从最初的供应商库中，根据纳入标准缩小了最终名单。然后，通过问卷、演示、简报和对相关客户调研访谈来收集产品与战略的详细信息。Forrester 使用这些输入以及分析师在市场上的经验和专业知识来对供应商进行评分，并使用相对评级系统将每个供应商与评估中的其他供应商进行比较。

每份 Forrester Wave™报告的标题都清楚地标明了发布日期。根据供应商于 2024 年 3 月 20 日之前提供的材料进行了本次评估，供应商此后不能再提供更多材料。Forrester 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 的供应商审查政策，要求供应商在报告发布之前审查 Forrester 的调查结果，以检查其准确性。Forrester Wave™ 图表中标记为【非参与供应商】的供应商是符合纳入标准的，但拒绝参与评估，或仅对评估做出部分贡献。根据 Forrester 的供应商参与政策，对这些供应商进行评分，并将其排名与参与供应商的排名一起发布。