使用許諾対象：個人使用のみ

The Forrester New Wave™：サイバーセキュリティリスクレーティングプラットフォーム、2021年第1四半期

主要プロバイダ7社とその状況

執筆者：Paul McKay、Alla Valente

2021年2月25日

レポートの趣旨

サイバーセキュリティリスクレーティングの新興市場に関するForresterの調査では、同カテゴリから主たる7社（BitSight、Black Kite（旧Normshield）、Panorays、Prevalent、RiskRecon、SecurityScorecard、UpGuard）を選定し、評価を行いました。本レポートでは、10項目で各ベンダーを採点し、各社の相対的な位置付けを明らかにしています。セキュリティとリスク管理の担当者はこのレポートを活用することで、サイバーセキュリティリスクレーティングのニーズに対処するうえで適切なパートナーを選定できます。

重要ポイント

SecurityScorecardとBitSightが市場をリード

Forresterの調査の結果、SecurityScorecard、BitSightがリーダー、Panorays、RiskReconが優良ベンダー、Prevalent、UpGuard、Black Kiteが有望ベンダーと認定されました。

レーティングモデルの精度、透明性、連携が主な差別化要因

サイバーセキュリティリスクレーティング市場は信用格付の影響を受けており、両者の性質は類似しています。モデルの精度（アトリビューションの精度だけでなく）の信頼性、オープンで透明性の高い手法を確立することが、その他のあらゆることの基礎となります。サードパーティリスク管理や全社的リスク管理のプロセスにおいてCISOがサイバーセキュリティリスクレーティングソリューションを活用するためには、その他のリスク管理およびコンプライアンス管理テクノロジとの高品質な連携によりユビキタスな導入を実現することがきわめて重要です。セキュリティポータルや一元管理ソリューションを新たに導入することは求められていないのです。

このPDFはforrester.comまたはreprints.forrester.comからダウンロードして個人で使用することのみが認められています。それ以外のあらゆる配布は禁止されています。

The Forrester New Wave™：サイバーセキュリティリスクレーティングプラットフォーム、2021年第1四半期

主要プロバイダ7社とその状況

執筆者：Paul McKay、Alla Valente
共同執筆者：Joseph Blankenship、Shannon Fish、Peggy Dostie
2021年2月25日

目次

2 **サイバーセキュリティレーティングは成熟の途上にある**

3 **サイバーセキュリティリスクレーティング評価の概要**

6 **ベンダークイックカード**

14 **補足資料**

関連する調査ドキュメント

Cybersecurity Risk Ratings Market Outlook, 2020 And Beyond（2020年以降のサイバーセキュリティリスクレーティング市場の展望）

The Forrester New Wave™: Cybersecurity Risk Rating Solutions, Q4 2018（The Forrester New Wave™：サイバーセキュリティリスクレーティングソリューション、2018年第4四半期）

レポートを同僚と共有しましょう。
調査共有を使用してメンバーシップを有効活用しましょう。

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

© 2021 Forrester Research, Inc. 提案内容はその時点での判断に基づくものであり、変更される可能性があります。Forrester®、Technographics®、Forrester Wave、TechRadar、およびTotal Economic Impactは、Forrester Research, Inc.の商標です。その他すべての商標は所有各社に帰属します。不正なコピーまたは配布は、著作権法に違反します。Citations@forrester.comまたは+1 866-367-7378

サイバーセキュリティレーティングは成熟の途上にある

サイバーセキュリティリスクレーティング（CSR）市場は、信用格付の市場から影響を受けています。CSR市場のソリューションは、企業のオンラインにおける対外的プレゼンスについての社外調査によるデータに基づき、複数のセキュリティリスク要素にまたがる企業のサイバーセキュリティのあり方を一元的に集約して評価します。プラットフォームが収集したデータは、企業のセキュリティへの取り組み姿勢と実際の調査結果の比較について、サードパーティや社内関係者が申告した内容を企業が検証するために活用できる点に価値があります。こうしたソリューションが活用される最も一般的なユースケースとして、サイバーセキュリティの信用度調査やサードパーティリスク管理（TPRM）の継続的モニタリング、全社的セキュリティリスク管理とベンチマーキング、M&A適正評価、経営幹部層のコミュニケーション、サイバー保険契約の引受などがあります。

2018年に発行された前回のForrester New Wave™以降、CSRの多数のプラットフォームによりレーティング精度、アセットアトリビューション、ワークフローなどさまざまな改善が見られました[1]。しかし、市場はまだ成熟したとは言えません。市場が成熟し企業が採用するに足るセキュリティソリューションとして完成を見るためには、なおもいくつかの課題が残っています。今回の調査では、以下のようなことが明らかになりました。

- **CSRプラットフォームの精度の評価は、必ずしも企業のサイバーリスクを反映していない。**今回の調査対象となったベンダーの多くは、アセットアトリビューションに特化した精度評価を行っています。すなわち、アセットを適切な組織に正しく紐付けられているか、という観点です。ベンダーはモデルのレビューを外部機関に委託し、外からの視点で評価を行っています。ただし正確なアセットアトリビューションは重要ではあるものの、そうしたレーティングそのものが企業の現在のセキュリティのあり方を正しく反映していると統計的に確信できるわけではありません。レーティングベンダーは、モデルに使用されるセキュリティデータポイント、変数の重み付け、分析の種類、機械学習モデルの訓練と検証の方法についても、真のリスクを正しく想定したものであるかをさらに詳細に検証する必要があるのです。
また、自社のモデルについて内部でレビューするだけでなく外部の検証も受けることで、レーティング市場が提供する価値に対し、さらなる自信を持つことができるようになります。

- **ベンダーのモデルやアルゴリズムの透明性の水準がまちまちである。**透明性については前回のForrester New Waveより改善されたものの、CSR企業が解決すべき課題はまだ多くあります。顧客にのみ開示するために多くの情報を秘匿し、他社に比べて詳細情報を公開しない企業もあれば、誰でも確認できるよう自社の手法をホワイトペーパーやポータルで詳細に開示する企業もあります。過誤検知の申告のプロセスに関する透明性が、改善の鍵となる領域です。こうした領域は主にCSR企業が自社内で対処しますが、こうした対応はセキュリティ業界の他企業からCSR企業が「神のように振る舞っている」と批判される事態にもつながります。CSRレーティング企業は自社の過誤検知の申告手順に関する透明性の水準を改善し、企業間の紛争を独立した立場から公平的に見ることのできる業界のオンブズマンを導入し、紛争の結果を公開する努力をする必要があります。

- **ベンダーは関連性の高いセキュリティソリューションとの連携を進める必要がある。**CSRソリューションは主に2つのユースケースに利用されています。CSRソリューションの提供するさらなるデータと継続的な監視機能により、企業が自社のセキュリティのあり方と、サードパーティのエコシステムのセキュリティのあり方の両者の評価を実施できるのです。ベンダーの連携へのアプローチは各社で異なっています。自社のワークフローエンジンやクエスチョネアモジュールを構築している場合もあれば、主要なGRCやTPRMプラットフォーム（また、Splunkなどのセキュリティアナリティクスプラットフォームとも）とネイティブに連携するよう構築されている場合もあります。なかには、十分と言えない品質での連携により、低品質なデータダンプの提供に留まり、サードパーティによるセキュリティレビューや全社的リスク管理といったより幅広いビジネスプロセスの観点でデータのさらなるコンテキストやインサイトを実現する機会を逸しているベンダーもいます。

© 2021 Forrester Research, Inc. 不正なコピーまたは配布は、著作権法に違反します。
Citations@forrester.comまたは+1 866-367-7378

- **リスクをコンテキスト化する機能が限定的なため、レーティングの運用のしやすさが制限されている。**この市場のベンダーは、アラートや通知、サードパーティについて収集するデータポイントをあまりに大量に提供するため、顧客は圧倒されてしまい、こうした情報に基づく対処を取るうえでかえって妨げになっています。こうした「多ければ多いほど良い」というアプローチは、収集したりモデルにインプットしたりするデータが多ければ多いほど、レーティングが正確になるというベンダーの誤ったメッセージにもつながります。CSRベンダーは、ユーザーに大量のデータを送りつけるのではなく、レーティングにおけるリスクの状況をより正確に伝えるよう注力することで、セキュリティやリスクの担当者がどの取り組みを優先すべきかを判断し、リスクに基づく意思決定を行い、情報に基づき行動できるよう支援すべきなのです。さらに、データ主導型の取り組みや意向に対応するため、この分野の顧客は、CSRプラットフォームを利用するのか、自社で選択したセキュリティプラットフォーム経由でソリューションを利用して独自のシナリオやアルゴリズムを実行するのかを、自社で自由に決定できるようにすべきです。

サイバーセキュリティリスクレーティング評価の概要

Forrester New Waveは、従来のForrester Wave™とは異なります。Forrester New Waveでは、新興のテクノロジのみを評価対象とします。10項目の評価基準について調査し、評価対象の各ベンダーと2時間の面談を行います。これら10項目は「現在の製品」と「戦略」に分類されます（図1参照）。また、市場プレゼンスについてもレビューを実施します。

今回の評価で調査対象とした7社のベンダーは、BitSight、Black Kite（旧Normshield）、Panorays、Prevalent、RiskRecon、SecurityScorecard、UpGuardです（図2、図3を参照）[2]。本調査を開始した頃、FICOのサイバーセキュリティリスクレーティング事業はISSに買収されました。この事業は2社の間の移行期にあったため、今回の調査には同2社を加えないこととしました。これらの各ベンダーは以下の特徴を備えています。

- **サイバーセキュリティリスクレーティング製品で100万ドルの収益を達成している。**サイバーセキュリティリスクレーティング製品での収益が100万ドルに達しないと報告している企業については、今回の調査から除外しました。
- **高い知名度と市場におけるプレゼンス。**CSR製品の導入数ではなくアクティブな顧客のロゴの数が75社以上いるベンダーで、Forresterのクライアントが関心を持つベンダーのみを対象としました。

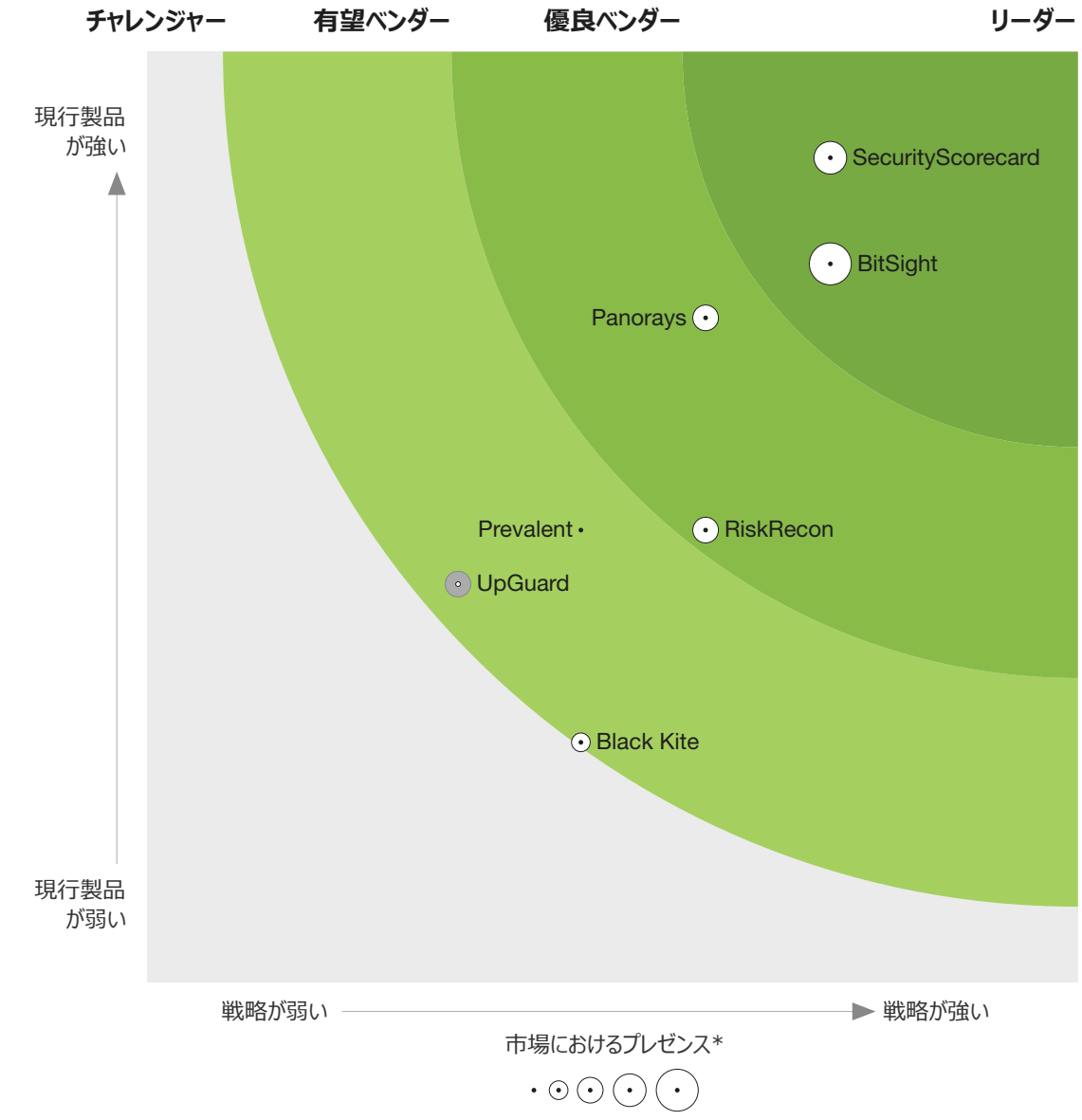
© 2021 Forrester Research, Inc. 不正なコピーまたは配布は、著作権法に違反します。
Citations@forrester.comまたは+1 866-367-7378

図1 評価基準：サイバーセキュリティリスクレーティング、2021年第1四半期

基準	プラットフォーム評価の詳細
データ精度	サイバーセキュリティレーティングを行うための情報として、どのような種類のデータをベンダーが収集しているか、またどのような収集方法を採用しているか。ベンダーはどのようにしてデータをレーティング対象の企業と正しく関連付けているか。ベンダーはどのようなチェック方法でレーティングモデルを更新しているか、その頻度はどの程度か。
レーティングプロセスの透明性	ベンダーはレーティング対象の企業に対し、レーティング方法についての透明性をどのように確保しているか。レーティングを決定する手法やプロセスについて、レーティング対象の企業（顧客ではなく）にはどのような情報が公開されているか。
過誤検知の申告	企業のレーティングについての過誤検知の申告に対処するベンダーのプロセスはどのようなものか。ベンダーは過誤検知の申告プロセスについてどのように公開し、アクセスのしやすさを確保しているか。レーティングの修正を承諾した場合、修正は現在のレーティングと過去のレーティングにどのように反映されるか。
連携と相互運用性	他のリスク管理プラットフォームとのテクノロジ連携に対するベンダーのアプローチはどのようなものか（GRCやサードパーティリスク管理など）。こうした連携により、顧客が他の企業のテクノロジを利用してレーティングを運用できるか。ベンダーはどの言語をサポートしているか。
ユースケースの幅広さ	セキュリティレーティングの閲覧やインタラクションを行うためのダッシュボードやレポート機能はどのようなものか。ベンダーのプラットフォームは、サードパーティのセキュリティ管理や社内のセキュリティリスク管理ユースケースおよびワークフローに対応しているか。
リスクコンテキスト	ベンダーはサイバーセキュリティやその他のリスク要素をどのようにコンテキスト化してレーティングを運用しているか。コンプライアンス基準やフレームワークに対するプラットフォームのマップリスクの問題をどのように特定するか。エンドユーザーはベンダーのプラットフォームにより、リスク軽減の進捗をどのように把握するか。
問題と改善措置の管理	ユーザーはソリューションにより、全体的なレーティングスコアを改善するために自社が解決すべき課題をどのように把握するか。ベンダーのソリューションにより、ユーザーは特定された問題のリスクや重大性に紐付く改善措置の計画をどのように策定するか。
市場のビジョンと製品ロードマップ	今後12ヵ月～18ヵ月のベンダーの製品ロードマップはどのような内容か。今後12ヵ月～18ヵ月のサイバーセキュリティリスクレーティング市場の成長についてのベンダーの見立てはどのようなものか。
グローバルでの市場展開とパートナー戦略	今後12ヵ月～18ヵ月で、ベンダーの市場開拓戦略はどのように進化するか。今後12ヵ月～18ヵ月で、ベンダーの戦略的パートナーシップやアライアンスのアプローチはどのように変化するか。ベンダーは海外の対象顧客に対しどのように製品の市場展開を行うか。
コマーシャル戦略と価格のイノベーション	今後12ヵ月～18ヵ月で、ベンダーのコマーシャル戦略と価格に対するアプローチを、どのように進化させる計画か。

© 2021 Forrester Research, Inc. 不正なコピーまたは配布は、著作権法に違反します。
Citations@forrester.comまたは+1 866-367-7378

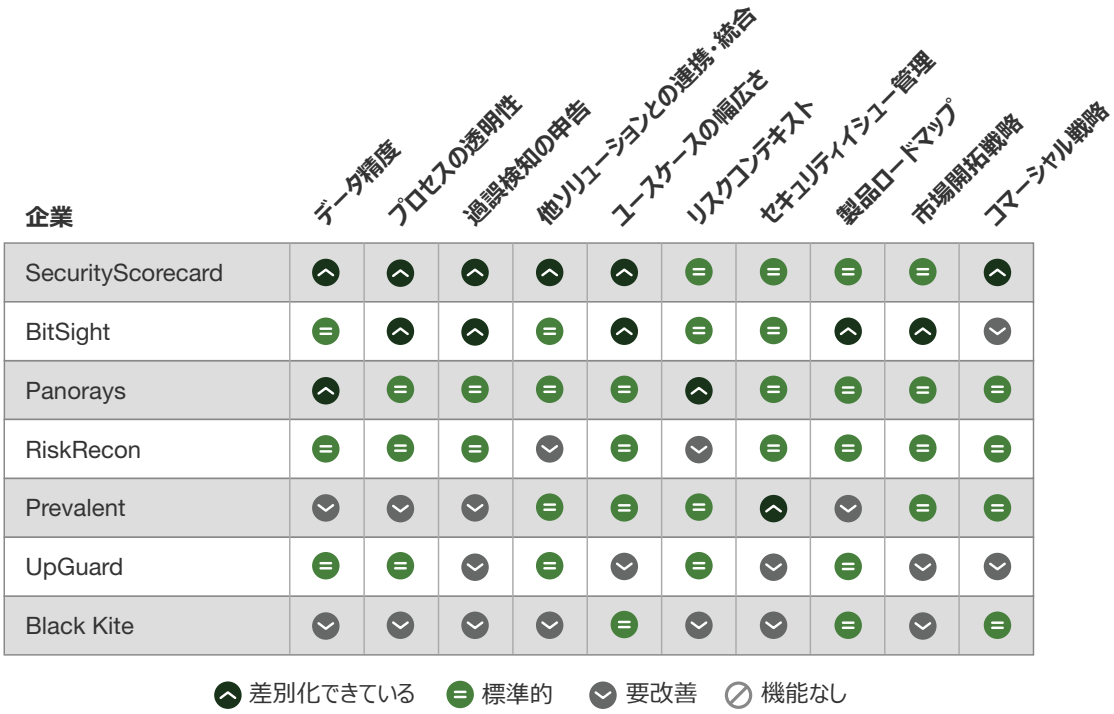
図2 Forrester New Wave™：サイバーセキュリティリスクレーティング、2021年第1四半期



*グレーの円は、評価に参加しなかったベンダーを表しています。

© 2021 Forrester Research, Inc. 不正なコピーまたは配布は、著作権法に違反します。
Citations@forrester.comまたは+1 866-367-7378

図3 Forrester New Wave™：サイバーセキュリティリスクレーティングのスコアカード、2021年第1四半期



ベンダークイックカード

Forresterは7社のベンダーを評価し、10項目の評価基準に関してランク付けしました。各社に対するForresterの見解は以下のとおりです。

© 2021 Forrester Research, Inc. 不正なコピーまたは配布は、著作権法に違反します。
Citations@forrester.comまたは+1 866-367-7378

SecurityScorecard：Forresterの見解

ForresterはSecurityScorecardを次のとおり評価しました（図4参照）。

- **確立されたプロセスの透明性とワークフロー機能が群を抜いている。**SecurityScorecardは、非常に詳細なレーティングモデルのホワイトペーパーを提供し、同社のTrust Portalを通じて情報を公開しています。Atlasモジュールがレーティングデータとベンダーのクエスチョネアをマッチングすることで、ワークフローのプロセスの詳細さを大幅に向上させます。
- **セキュリティイシュー管理とサードパーティの連携品質には改善の余地がある。**問題やその改善措置の管理機能については、問題の詳細や改善措置の優先順位付け機能を追加することで改善できるでしょう。サードパーティとの連携については、GRCとTPRMプラットフォームで不整合が見られます。
- **調査機能を備えたGRC/TPRMプラットフォームを持たない顧客に最適。**レーティングにおける確固たる透明性と評価調査により得られる完全な客観性を必要とし、分かりやすい価格構造を求める顧客には、SecurityScorecardは最適です。

SecurityScorecardユーザーの声（要約）

リファレンス顧客は、SecurityScorecardの使いやすさ、プラットフォームの可視性、UXを高く評価しています。一方で、カスタムレポートオプションは限定的であると指摘しており、手順の改善も要望しています。

図4 SecurityScorecardのクイックカード

SecurityScorecard

Waveでの位置付け
リーダー

↗ **データ精度**	= **リスクコンテキスト**
↗ **プロセスの透明性**	= **セキュリティイシュー管理**
↗ **過誤検知の申告**	= **製品ロードマップ**
↗ **他ソリューションとの連携・統合**	= **市場開拓戦略**
↗ **ユースケースの幅広さ**	↗ **コマーシャル戦略**

↗ 差別化できている	↘ 要改善
= 標準的	⊘ 機能なし

評価対象製品
SecurityScorecard Ratings Platform

ユーザーの声

「サードパーティに対し、サイバーセキュリティへの取り組み姿勢を改善してもらうよう説得するために活用している」

「対応済みのセキュリティイシューの申請への対応が傑出している」

「使いやすく、取引先とのコミュニケーションを担当している他のチームへのデモも非常に実施しやすい」

© 2021 Forrester Research, Inc. 不正なコピーまたは配布は、著作権法に違反します。
Citations@forrester.comまたは+1 866-367-7378

BitSight：Forresterの見解

ForresterはBitSightを次のとおり評価しました（図5参照）。

- **レーティングプロセスの透明性と高品質な連携による差別化。**BitSightは過誤検知の申告の評価に対する堅牢なプロセスを開発し、自社の手法について詳細な情報を多数提供しています。ベンチマークとアセットエンティティマッピングは、評価対象の企業の構造を明らかにします。BitSightは、高品質なサードパーティ連携に強みを持ちます。
- **分かりにくいパッケージ提供による価格体系を簡素化する必要がある。**BitSightのサードパーティのパッケージ価格は、最近ますます複雑になりました。このため、顧客は適切なパッケージを確定することがさらに困難になっています。またBitSightは、顧客のセキュリティの問題のためにITサービスプロバイダのレーティングが低くなっている点についても改善の余地があるでしょう。
- **幅広いユースケースやレポートの要件に対処する必要のある企業に最適。**BitSightは、幅広いユースケースに対応でき、定評のあるレーティング企業を活用して、高品質なベンチマーキングを行いたいと考える、CSR予算を専用で確保した企業に最適です。

BitSightユーザーの声（要約）

BitSightのリファレンス顧客は、同社の精度やレーティングプロセスの透明性には非常に満足しています。一方、経営幹部へのレポートは改善すべき領域であると指摘しています。

図5 BitSightのクイックカード

BitSight

Waveでの位置付け
リーダー

データ精度	**リスクコンテキスト**
プロセスの透明性	**セキュリティイシュー管理**
過誤検知の申告	**製品ロードマップ**
他ソリューションとの連携・統合	**市場開拓戦略**
ユースケースの幅広さ	**コマーシャル戦略**

差別化できている　要改善
標準的　機能なし

評価対象製品
BitSight Security Ratings Platform

ユーザーの声

「第三の防御系統として、レーダーが探知できない領域についてのさらなるインサイトを提供してくれる」

「使いやすく分かりやすい。誰でも活用できる」

「企業のツリー図とシンプルなレーティングの凡例こそが最も価値のある特徴だ」

© 2021 Forrester Research, Inc. 不正なコピーまたは配布は、著作権法に違反します。
Citations@forrester.comまたは+1 866-367-7378

Panorays：Forresterの見解

ForresterはPanoraysを次のとおり評価しました（図6参照）。

- **ワークフロー機能、精度、リスクコンテキストの性能が傑出。**Panoraysはクエスチョネア機能、精度、ワークフローにおいて他社との差別化を実現しています。Panoraysの提供するリスクコンテキストは、人的要素、サードパーティ向けのクエスチョネア管理、使いやすいフォースパーティ機能などと組み合わせることができます。
- **レーティング手法やレポートの文書化は改善が必要。**一方、レーティング手法の文書化については、内容の充実や明確化の観点で改善が必要です。レポートは表形式で多くの情報を提示していますが、中にはより視覚的で見やすくする必要があるものもあります。
- **TPRMワークフローと組み合わせることのできるレーティングプラットフォームを求める顧客に最適。**Panoraysは、これまでGRCやTPRMテクノロジに投資しておらず、クエスチョネアワークフローとレーティングデータを組み合わせるソリューションを必要としている組織に特に適しています。

Panoraysユーザーの声（要約）

Panoraysのリファレンス顧客は、プラットフォームの精度、高品質なレーティングレポート、誤検知率の低さを高く評価しています。一方、コンプライアンスクエスチョネアをロードマップ機能としてオンラインで編集できるようにしてほしいという要望を持っています。

図6 Panoraysのクイックカード

Panorays

Waveでの位置付け
優良ベンダー

データ精度	**リスクコンテキスト**
プロセスの透明性	**セキュリティイシュー管理**
過誤検知の申告	**製品ロードマップ**
他ソリューションとの連携・統合	**市場開拓戦略**
ユースケースの幅広さ	**コマーシャル戦略**

差別化できている　要改善
標準的　機能なし

評価対象製品
Panorays

ユーザーの声

「Panoraysを選んだのは、レポートの透明性が理由だ」

「Panoraysは、自社の情報セキュリティチームがより詳細なレベルのサイバーアセスメントについて意思決定する際の鍵となる」

「これまで利用したどの企業よりも優れたカスタマサービスを提供してくれる」

© 2021 Forrester Research, Inc. 不正なコピーまたは配布は、著作権法に違反します。
Citations@forrester.comまたは+1 866-367-7378

RiskRecon：Forresterの見解

ForresterはRiskReconを次のとおり評価しました（図7参照）。

- **詳細なレーティングデータを提供し、価格体系も明確。**RiskReconは、幅広いデータポイントを提供し、詳細な調査で顧客をサポートします。リスクプライオリティマトリックスは、発見事項の視覚化に役立ちます。また、パッケージの価格体系も顧客に分かりやすい設定です。
- **サードパーティ連携や経営幹部層へのレポート機能に改善の必要がある。**RiskReconは、サードパーティ連携の提供の多様性と品質において、他社の後塵を拝しています。経営幹部層へのレポート機能の一部は、過度に詳細であるため経営陣が使うには適していません。
- **レーティングデータの詳細を把握したい顧客に最適。**RiskReconの詳細なデータやダウンロードオプションは、アタックサーフェス監視用途にレーティングデータを活用したいと考える顧客に最適です。

RiskReconユーザーの声（要約）

RiskReconのリファレンス顧客は、フィードバックに対する適切な対処や収集データの詳細さが同社の強みであると評価しています。また、コンプライアンスフレームワークの改善されたマッピングについても言及しています。一方、ユーザーインターフェースについては強い不満を表明しており、メール通知も実用性に欠けると指摘しています。

図7 RiskReconのクイックカード

RiskRecon

Waveでの位置付け
優良ベンダー

データ精度	**リスクコンテキスト**
プロセスの透明性	**セキュリティイシュー管理**
過誤検知の申告	**製品ロードマップ**
他ソリューションとの連携・統合	**市場開拓戦略**
ユースケースの幅広さ	**コマーシャル戦略**

差別化できている　要改善
標準的　機能なし

評価対象製品
RiskRecon

ユーザーの声

「RiskReconは広範な査定対象項目を備え、最も高度なリスク管理機能を有している」

「フィードバックに対して非常にオープンで、製品品質の向上に役立ててくれている」

「経時的に顧客のセキュリティに対する姿勢が変化した場合に、アラートを発出する機能を評価している」

© 2021 Forrester Research, Inc. 不正なコピーまたは配布は、著作権法に違反します。
Citations@forrester.comまたは+1 866-367-7378

Prevalent：Forresterの見解

ForresterはPrevalentを次のとおり評価しました（図8参照）。

- **TPRM製品との強力な連携と幅広い非サイバーデータ。**Prevalentは、標準的なセキュリティ中心のレーティングデータを広範な財務リスクやビジネスデータで補完します。同社のプラットフォームの機能性やワークフローは傑出しています。
- **VTM製品によりサイバーセキュリティレーティング市場における差別化を実現しようと苦戦。**Prevalentはレーティング市場の他社と提携し、基礎となるデータを提供しています。Prevalentは、レーティング市場で他社と差別化を図る独自の強みを明確に打ち出そうと苦戦しています。そのため、同社のセキュリティレーティングのロードマップやビジョンは、CSRの顧客のニーズと整合していません。
- **Prevalent TPRMのアドオンとしてレーティングを求める顧客に適している。**Prevalent VTM製品は、多様なPrevalent TPRM製品の購入とあわせて導入するのが良いでしょう。マネージドサービスのサポートを求める企業は、Prevalentを検討されることをお勧めします。

Prevalentユーザーの声（要約）

リファレンス顧客は、ビジネスおよびサイバーに関するリスクレポートを提供する点を評価しています。また同社のマネージドサービスも好評です。一方、ライセンス構造の改善について指摘されており、一部サプライヤのセキュリティ違反がPrevalentのサイバーリスクインテリジェントソースによって検出されなかった点にも言及されています。

図8 Prevalentのクイックカード

Prevalent

Waveでの位置付け
有望ベンダー

データ精度	**リスクコンテキスト**
プロセスの透明性	**セキュリティイシュー管理**
過誤検知の申告	**製品ロードマップ**
他ソリューションとの連携・統合	**市場開拓戦略**
ユースケースの幅広さ	**コマーシャル戦略**

差別化できている　要改善
標準的　機能なし

評価対象製品
Prevalent Vendor Threat Monitor

ユーザーの声

「ベンダーのサイバーリスクに加え、ビジネスリスクを評価してくれる点が優れている」

「すべてのサードパーティサプライヤについて、概して正確な評価を行っている」

「サプライヤのリスクレポートと、企業プロフィールの概要ページを評価している」

© 2021 Forrester Research, Inc. 不正なコピーまたは配布は、著作権法に違反します。
Citations@forrester.comまたは+1 866-367-7378

UpGuard：Forresterの見解

ForresterはUpGuardを次のとおり評価しました（図9参照）。

- **詳細なデータの収集と調査を提供。**UpGuardは脅威インテリジェンスの一連の詳細な指標や組織のアタックサーフェスについての情報を収集しています。同社の注力領域である、サードパーティやフォースパーティのリスクの集中は、顧客にとって有益な機能です。
- **過誤検知の申告手順における透明性への対処が必要。**UpGuardはプロセスの一部について、競合他社と比較して限られた文書しか公開していません。手法や過誤検知の申告の手順のさらなる公開を進めることで、このサービスを用いてレーティングされた非クライアントの要求に応える必要があります。
- **アタックサーフェス監視での利用を検討する顧客に最適。**UpGuardは、自社のアタックサーフェスについて詳細な情報に基づき把握したいと考える顧客に最適です。また、自社のサプライチェーンにおける特定の脆弱性に対する危険性の把握など、脆弱性の検出を実行したいと考える企業向けだと言えるでしょう。

UpGuardユーザーの声（要約）

UpGuardは当社の調査に参加しなかったため、ユーザーの声についての情報はありません。

図9 UpGuardのクイックカード

UpGuard

Waveでの位置付け
有望ベンダー

データ精度	**リスクコンテキスト**
プロセスの透明性	**セキュリティイシュー管理**
過誤検知の申告	**製品ロードマップ**
他ソリューションとの連携・統合	**市場開拓戦略**
ユースケースの幅広さ	**コマーシャル戦略**

ユーザーの声

Forresterは、今回の評価調査ではUpGuardユーザーの声を集めることができませんでした。

差別化できている　要改善
標準的　機能なし

評価対象製品
UpGuard Vendor Risk

© 2021 Forrester Research, Inc. 不正なコピーまたは配布は、著作権法に違反します。
Citations@forrester.comまたは+1 866-367-7378

Black Kite（旧Normshield）：Forresterの見解

ForresterはBlack Kiteを次のとおり評価しました（図10参照）。

- **レーティングモデルに広範なデータポイントを統合。**Black Kiteは、同社のモデルにおいて、レーティング対象企業の広範なデータポイントを追跡および収集しています。顧客が利用できるよう、コンプライアンスや財務に関する定量化データも追加しており、製品価格も高い競争力を誇ります。
- **プラットフォームや過後検知の申告プロセスの各要素を大幅に改善する必要がある。**Black Kiteのレポート機能や可視化機能は標準的なものに留まり、操作性は高くありません。OpenFAIRを用いた財務の定量化指標はあまりに広範なものであるため、意思決定を行ううえで実用的ではありません。レーティング対象の事業体が自社のレーティングを変更できるため、独立性やレーティングの完全性が損なわれます。
- **高度なデータ分析を求める企業に最適。**Black Kiteは、レーティングデータについて詳細な情報を求める顧客に適しています。また、予算の制約がある顧客にも最適です。

Black Kiteユーザーの声（要約）

Black Kiteの顧客は、提供されるデータの詳細さを評価しています。一方、サードパーティのセキュリティリスククエスチョネア機能とプラットフォームとの高度な連携を実現することで、レーティングデータを既存のTPRMプログラムセキュリティクエスチョネアと組み合わせられるようにしてほしいと考えています。

Black Kite

Waveでの位置付け
有望ベンダー

データ精度	**リスクコンテキスト**
プロセスの透明性	**セキュリティイシュー管理**
過誤検知の申告	**製品ロードマップ**
他ソリューションとの連携・統合	**市場開拓戦略**
ユースケースの幅広さ	**コマーシャル戦略**

差別化できている　要改善
標準的　機能なし

ユーザーの声

「ツールが非常に使いやすいため、ユーザー向けのプラットフォームの導入は迅速かつ簡単に実施できる」

「Black Kiteのスキャン対象のデータカテゴリが幅広いという点が気に入っている」

評価対象製品
Cyber Risk Ratings Platform, 4.9

© 2021 Forrester Research, Inc. 不正なコピーまたは配布は、著作権法に違反します。
Citations@forrester.comまたは+1 866-367-7378

アナリストにご相談ください

Forresterの専門家にご相談ください。お客様のビジネスおよびテクノロジ施策とForresterの調査結果を照らし合わせ、自信を持って意思決定できるようサポートいたします。

アナリストへの問い合わせ

調査結果を実践に活かせるように、アナリストが30分間の電話セッションで質問にお答えします。メールでの回答も可能です。

詳細はこちら

アナリストによる助言

アナリストがカスタム戦略セッション、ワークショップ、講演会などを通じて、具体的な取り組みを支援します。調査結果を行動につなげましょう。

詳細はこちら

Webセミナー

ビジネスを変える最新の調査結果に関するオンラインセッションにご参加ください。オンデマンドで利用可能な各セッションはスライドを使用し、アナリストによるQ&Aが含まれます。

詳細はこちら

iOSおよびAndroid向けのForrester調査アプリ：
どこにいても競合他社より早く情報を得られるアプリです。

図10 Black Kiteのクイックカード

補足資料

Forrester New Waveの調査手法

Forresterは一次調査を実施し、この新興市場の評価と定義に関する当社の評価基準を満たすベンダーリストを作成しました。10項目の評価基準でベンダーを評価しました。そのうち7項目は製品の機能に基づく基準、3項目は戦略に基づく基準です。また、市場プレゼンスもレビューしました。トップレベルの新興ベンダーを招待し、RFPスタイルのデモンストレーションに参加してもらい、インタビューを実施してユーザーの意見を求めました。その後、各基準に関してベンダーをランク付けしています。戦略スコアの合計値をX軸、現行製品のスコアの合計値をY軸とし、市場プレゼンスのスコアでマーカーのサイズを決定しました。高いスコアを獲得したベンダー数社をリーダーとして選出しています。

© 2021 Forrester Research, Inc. 不正なコピーまたは配布は、著作権法に違反します。
Citations@forrester.comまたは+1 866-367-7378

す。SecurityScorecard、BitSightがリーダーです。Panorays、RiskReconが優良ベンダーです。Prevalent、UpGuard、Black Kiteが有望ベンダーです。

巻末注釈

[1] Forresterのレポート「The Forrester New Wave™: Cybersecurity Risk Rating Solutions, Q4 2018（The Forrester New Wave™：サイバーセキュリティレーティングソリューション、2018年第4四半期）」を参照。

[2] 評価時点では、Normshieldは2021年1月初旬に行われたBlack Kiteへのブランド名称変更の過程にありました。基礎となる評価対象製品については、当該期間中の変更はありません。

© 2021 Forrester Research, Inc. 不正なコピーまたは配布は、著作権法に違反します。
Citations@forrester.comまたは+1 866-367-7378

FORRESTER®

当社はビジネスおよびテクノロジのリーダーと連携して、お客様を最も大切にし、成長を促進する戦略を策定します。

製品とサービス

- コア調査およびツール
- データと分析
- 対等な協力関係
- アナリストの積極的な協力
- コンサルティング
- イベント

Forresterは顧客の担当部門と重要なビジネスに特化した調査を行い、インサイトを提供します。

FORRESTERがサポートする職務

マーケティング戦略担当者
CMO
B2Bマーケティング
B2Cマーケティング
カスタマーエクスペリエンス
カスタマーインサイト
eビジネス／チャネル戦略

テクノロジ管理担当者
CIO
アプリケーションの開発／提供
エンタープライズアーキテクチャ
インフラストラクチャ／運用
- セキュリティ／リスク管理

外注／ベンダー管理

テクノロジ業界担当者
アナリストリレーション

クライアントサポート

印刷版または電子版をご希望の場合は、クライアントサポート（電話：+1 866-367-7378、+1 617-613-5730、電子メール：clientsupport@forrester.com）までご連絡ください。教育機関および非営利団体向けの数量割引や特別価格をご用意しています。

Forrester Research（NASDAQ：FORR）は、世界的に有力な調査/アドバイザリ企業です。当社はビジネスおよびテクノロジのリーダーと連携して、お客様を最も大切にし、成長を促進する戦略を策定します。Forresterは、独自の調査、データ、カスタムコンサルティング、専属のエグゼクティブピアグループ、イベントを通じ、お客様の考えを刺激してお客様の組織の変革につなげるという並外れた力強い目標を達成しようとしています。
詳細については、forrester.comをご覧ください。

161625