OMDIA UNIVERSE

Publication date
July 11, 2023

Authors
Andrew Braunberg, Principal Analyst, Security Operations

Eric Parizo, Practice Leader, Cybersecurity

Omdia Universe: Risk-Based Vulnerability Management Solutions, 2023

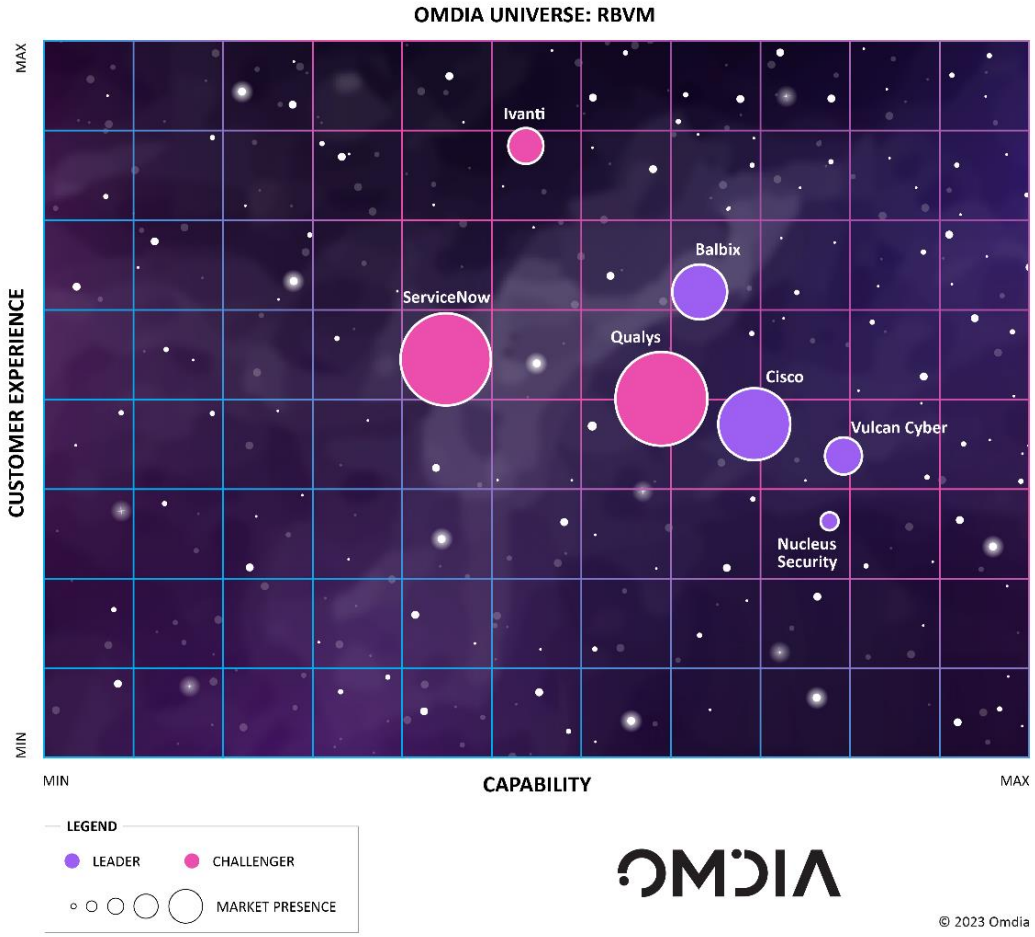
OMDIA
Brought to you by Informa Tech

Summary

Catalyst

The emergence of risk-based vulnerability management (RBVM) has been driven by several factors. Traditional vulnerability management tools that enable enterprises to identify, prioritize, and remediate software security vulnerabilities have increasingly struggled to meet the needs of organizations embracing digital transformation. The attack surface of the modern enterprise has both expanded and diversified in numerous ways, including the broad embrace of cloud services, the proliferation of IoT devices, and the acceleration of the application development lifecycle.

Figure 1: The Omdia Universe for RVBM



Source: Omdia

This Omdia Universe on RBVM aims to provide clarity into the key features of these evolving products.

Omdia view

The goal of better understanding and assessing risk is at the heart of RBVM and is the chief driver in the evolution of the legacy vulnerability management market. From an operational point of view, the scale of the vulnerability problem overwhelmed first-generation vulnerability management tools. (The US National Vulnerability Database catalogs more than 217,000 software vulnerabilities.) This growth led vendors to examine how a risk-based approach might inform better vulnerability prioritization and response. Instead of trying to figure out how to patch everything faster, RBVM tackles the scale problem by way of smarter, better-informed prioritization, helping enterprises calculate what to patch quickly and what to safely ignore.

Strategically, RBVM is part of a broader evolution within cybersecurity that Omdia refers to as proactive security. Defined as an overarching solution category that enables organizations to proactively seek out security issues—vulnerabilities, misconfigurations, and even poor policy and strategy—before an exploit ever takes place, proactive security solutions facilitate a comprehensive, proactive approach to risk reduction. With RBVM, the goal is to avoid breaches by proactively eliminating vulnerabilities and continuously reducing an organization's attack surface, thereby reducing cybersecurity risk. While legacy vulnerability management has had a proactive orientation as well, results have often been uneven. RBVM attempts to be both more efficient and effective.

Efficiency and effectiveness are chief selling points for RBVM products, which are marketed as providing prioritized risk rankings for vulnerabilities, with the goal of identifying the risk posed by each and determining the best response for optimal risk reduction. A chief benefit of this risk-based approach is a recognition of which actions can be delayed or ignored altogether. Yes, the most effective way to remediate a software vulnerability is through the patch management process, but because patching introduces its own set of operational costs (and concerns), knowing which patches *don't* need to be deployed can be as valuable as knowing those that do.

It is becoming commonplace among large enterprises to create dedicated cyber-risk management teams to handle cyber-risk, with proactive risk management serving as a particularly important component. For organizations of all sizes, Omdia recommends embracing a data-driven approach to risk reduction. Security operations (SecOps) teams will continue to inform many of these decisions, but increasingly cyber-risk needs to be understood as part of a broader enterprise risk management discussion.

Having a full and continuous understanding of the security posture of every asset within an organization will be a critical requirement for calculating enterprise-wide cybersecurity risk and accurately assessing it against other organizational risks. Omdia predicts that as RBVM products continue to mature, they will become foundational components of broader cyber-risk management solutions.

Key messages

- The most consistently mature capability across all the solutions evaluated was data collection. Omdia observed a strong ability to take in a variety of data from endpoints, networks, and cloud environments and to use this information effectively to assess cyber-risk associated with vulnerabilities across the entire digital domain.
- RBVM primarily solves a data problem. The analytics used in these solutions are generally mature and, in some cases, are beginning to commoditize. The ability to achieve up-to-the-minute visibility into the threat landscape, particularly emergent exploits, is an important differentiator for several leading vendors.
- Most vendors have, at best, a limited ability to take existing compensating controls into account when assessing actual risk and making mitigation recommendations. Most solutions simply allow asset owners to ask for exceptions to deploying patches based on their understanding of legacy protections. Omdia sees this as an important future opportunity for solution differentiation.
- RBVM vendors tend to offer annual (or longer) contracts, with pricing based on the number of assets managed. Most vendors have a complex set of SKUs based on the asset types, though some have employed a simpler tiered approach (e.g., standard, enterprise) to dictate their pricing. Application security capabilities are typically sold as separate SKUs or as premium functionality in higher-tier offerings. Omdia sees a trade-off in RBVM pricing: simpler models may be easy to understand but may not provide the best value, while more complex pricing methods can provide more value, but verifying that may take some work.
- Despite some separation in scoring, Omdia chose to rank ServiceNow as a Challenger, not a Prospect, due to the strength of its Vulnerability resolution features. Competing RBVM vendors have been able to focus heavily on risk-based features because they have been able to leverage legacy customer investments in ServiceNow's IT service management (ITSM) solution.

Analyzing the RVBM universe

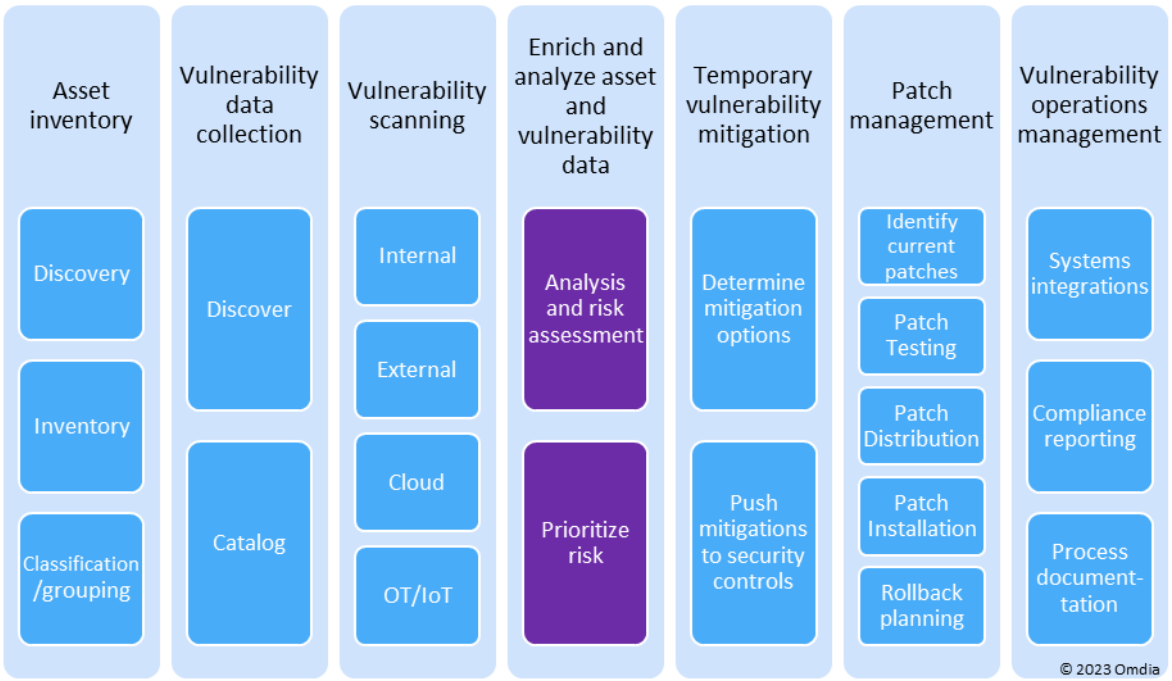
Market definition

The emergence of RBVM is another example of the periodic introductions of “next-generation” products seen in so many segments of the cybersecurity market. In other words, demand for the core functionality has not diminished, but evolving market requirements demanded that they be significantly augmented.

Therefore, an understanding of RBVM requires a baseline understanding of the key capabilities of what Omdia now refers to as legacy vulnerability management solutions. Omdia has broken down the functionality of these products into seven broad categories of capabilities:

- Asset inventory.
- Vulnerability data collection.
- Vulnerability scanning.
- Vulnerability assessment and prioritization.
- Temporary vulnerability mitigation.
- Patch management.
- Vulnerability operations management.

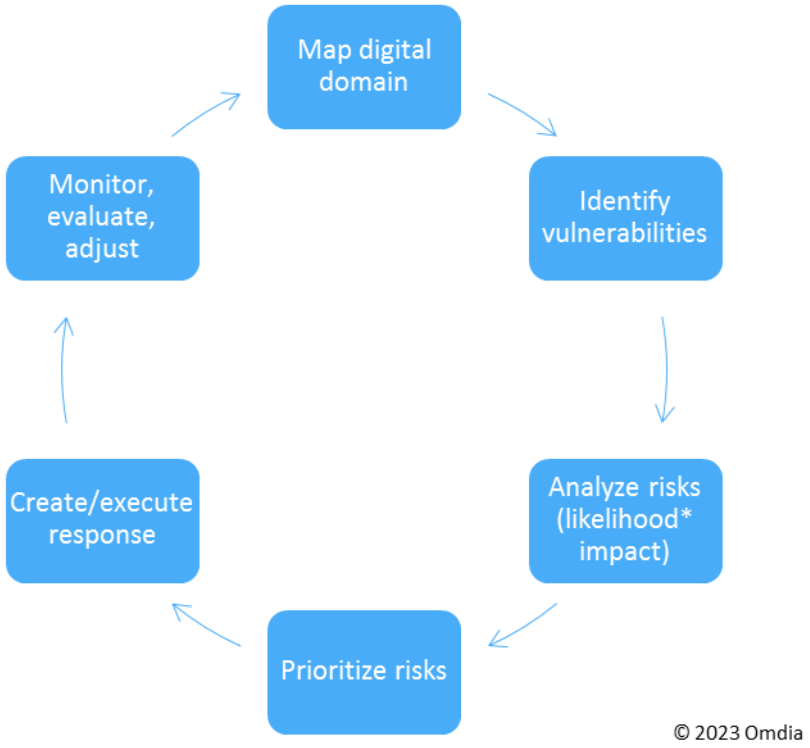
Figure 2: Vulnerability management functionality



Source: Omdia

The RBVM lifecycle expands on this, focusing on improving both the effectiveness and efficiency of traditional vulnerability management tasks. The three fundamental capabilities of an RBVM are complete asset visibility across the environment, accurate understanding of the risk associated with each vulnerability as it relates to each asset, and orchestration of mitigation and remediation recommendations. These capabilities are all required to achieve the goal of efficiently and proactively reducing cyber-risk.

Figure 3: Key RBVM functionality



Source: Omdia

Vendor focus

Most pure-play RBVM vendors have a primary focus on ensuring effective risk prioritization. Few of these vendors, for example, field their own scanners or ticketing tools. Rather they broadly integrate with any number of systems or tools that can provide visibility into corporate assets and fulfill remediation requests. This is an important market evolution. The (comparatively) simple days of setting up a few strategically placed network scanners and being able to create a (relatively) comprehensive view of corporate assets are long gone—as are the days of expecting security teams to be content with output in the form of a simple list of vulnerabilities sorted by common vulnerability scoring system (CVSS) scores.

Generally, Omdia sees RBVM vendors entering the market from three general directions.

- As noted, most pure plays initially focused on analytics and risk management. These tools were positioned primarily to augment existing vulnerability management tools.

- A second group consists of legacy vulnerability management vendors that are leveraging their strengths while addressing some of their limitations, often specific to risk-based features. These vendors are currently also very focused on analytics and risk management.

- The last set of vendors that have moved into the RBVM market is workflow and ticketing specialists seeking to increase their total addressable market (TAM) and see RBVM as an adjacent segment. These vendors, such as ServiceNow, highlight the strength of their orchestration and workflow capabilities.

This report provides a detailed analysis of product support for RBVM capabilities among leading RBVM solutions that Omdia has grouped into the following capabilities categories.

Solution capabilities

- **Data collection:** The foundation of RBVM solutions is a complete (as possible) view of an organization's assets across its entire digital domain. A full assessment of risk posture requires visibility into every asset that potentially creates an attack path into an organization.

- **Threat intelligence:** The ability to prioritize risk associated with software vulnerabilities and other security posture issues can benefit greatly from a near-real-time understanding of the current threat landscape. RBVM vendors are particularly focused on attacker activity related to the creation and deployment of new exploit code.

- **Telemetry and storage:** RBVM solutions need to collect, normalize, de-duplicate, enrich, store, and protect large volumes of sensitive data. The quality of this data will, in large, drive the quality of risk scoring and remediation recommendations.

- **Risk analytics:** RBVM solutions employ a host of analytic techniques to create risk scores and make remediation recommendations. Vendors need Security Operation Center (SOC) teams (and asset owners) to trust those scores and recommendations. This requires a level of transparency in how risk is assessed and a deep understanding of the criticality of each asset based on key criteria (e.g., asset type, location, user(s), etc.)

- **Vulnerability resolution:** Typically, a resolution will involve a software patch or patches. RBVM solutions often integrate with third-party patch management or ticketing systems. Other resolutions, particularly if no patch is yet available, could include temporary mitigation through existing security controls.

- **Deployment and management:** RBVM solution deployments typically take several months. Most of the back-end platforms run on one or more cloud service provider environments.

- **Pricing and licensing:** Solutions are typically sold through a mix of direct and channel. Pricing is often based on the number (and type) of assets monitored. Terms typically run annually or longer.

Market dynamics

The emergence of RBVM solutions has been driven by the same global trends that impact so many cybersecurity segments. Namely, the scale and velocity of activity across a highly dynamic threat landscape and the absolute digital chaos that results in security teams from enterprise-wide digital transformations.

These trends have had numerous negative effects on cybersecurity. The average organization's attack surface has expanded greatly, even as the number of security controls it deploys has expanded as well. As the number and types of digital assets have expanded within the average organization, the types of vulnerabilities that can be introduced into the digital domain have expanded as well. In addition to traditional software-related CVEs, for example, these broader "exposures" can include misconfigurations, weak credentials, and poorly coded software that is still in development, amongst other concerns.

These trends have led many RBVM vendors to considerably expand the types of assets they inventory and the types of vulnerabilities they look to remediate. With the goal of becoming a "single version of truth" regarding the security posture of an organization's entire attack surface, RBVM can inform much richer conversations around managing cyber-risk, which is an increasingly important component of overall enterprise risk.

Today's leading RBVM tools support an impressive ability to prioritize risk and make data-driven recommendations for remediation. This ability requires two important types of knowledge that relate back to the uber trends mentioned at the top of this section: a near-real-time understanding of the current threat landscape, particularly as it relates to active (or expected) exploits, and a detailed understanding of each customer's digital domain, particularly as relates to asset criticality and exposure.

At the time of this report's publication, the RBVM market includes several dozen vendors. Many are startups that have built RBVM capabilities organically. A few of these startups have been acquired over the last several years by larger players. For example, Cisco acquired Kenna Security, and Ivanti acquired RiskSense. Other market participants have augmented existing capabilities with tuck-in acquisitions. For example, Qualys acquired TotalCloud and Blue Hexagon.

Omdia, therefore, expects RBVM to eventually encompass the entire vulnerability management market. But that is only half the story. RBVM is already encroaching on the cloud security and application security markets by addressing "vulnerabilities" in cloud assets and application code still in development. The approach to finding vulnerabilities in code in development is distinct from production code because typically, application scanners, such as SAST and DAST, are not looking for specific CVEs but rather a code that is likely to be vulnerable to general types of attacks, such as buffer overflows, etc.

This expansive view of vulnerabilities (i.e., remediation beyond CVEs) will enable RBVM vendors to increase their TAM as RBVM tools become general exposure management solutions that provide a platform for risk-based proactive security operations. It should be noted that vendors in these adjacent markets are not standing still, and cloud security vendors, in particular, are well-funded, growing quickly, and see a similar end goal. Hence further market overlap is likely.

Differentiating evaluation criteria

Feature differentiation in the RBVM market can be traced back to the way in which vendors focus their product development investments. These decisions may reflect the primary market segment the vendor targets or may simply reflect how a vendor sees the market evolving. Often differentiation in approach is more about degree than kind, and occasionally more about product marketing than product development. Some points of differentiation to consider when evaluating RBVM solutions include:

- **Native scanners versus third-party integrations**: Most vendors argue that vulnerability scanning is unnecessary as a built-in feature because it has become commoditized and many customers already have scanners in place, while others assert that native scanners allow for superior granularity of metadata collection in support of risk-based prioritization. Omdia believes both positions are valid, but acknowledges that it is yet to be seen if the use of native scanners over a multiyear period can be iterated to the point where it provides a significant advantage over third-party scanning data.

- **Data collection versus model building:** Since RBVM tools emerged, there has been an ongoing debate regarding what is more important—data collection or proprietary model building. As open-source tools such as EPSS emerge and mature, several vendors are investing more in data collection capabilities. Omdia agrees that proprietary models will become a less important differentiator over time.

- **AI/(machine learning) ML versus other prioritization techniques:** The buzz around AI/ML in security use cases increased considerably during the first half of 2023. There is considerable disagreement among RBVM vendors, however, regarding the need for broad use of AI for RBVM use cases. There are also emerging techniques, particularly the use of decision trees, that can provide more transparent remediation recommendations. Omdia supports a multifaceted approach to prioritization, but regardless of approach, the quality of recommendations must be tested and measured carefully over time.

- **Temporal data versus environmental:** This is perhaps the area of focus that provides the sharpest distinction between vendors; all vendors evaluated in this research tend to favor one or the other of these philosophical approaches. Temporal data is primarily related to the current threat environments for software exploits—what are the *most critical vulnerabilities* likely to be exploited *right now*? Environmental data is primarily focused on the criticality and exposure of each asset—which assets are *most at risk*, and *pose the most risk* to the organization? Vendors focused more on environmental data tend to be moving more quickly to subsume cyber asset attack surface management (CAASM)-functionality because of the depth of asset data collected and retained. Vendors focused more on temporal data are hyper-focused on acquiring unique threat intelligence. Omdia believes both types of data are extremely important and should be combined to produce the best outcomes.

- **CVE versus non-CVE:** The definition of a vulnerability continues to expand as RBVM solutions evolve. Traditionally, the focus was almost exclusively on addressing CVEs; as discussed, this is in

and of itself a large and growing problem. But the real value in RBVM solutions will be in providing a single source of security truth for any type of asset and prioritizing risk regardless of the type of vulnerability associated with each asset. Omdia sees real value in taking a broader view of what constitutes a vulnerability.

- **AppSec bundling and pricing:** Many RBVM vendors have already moved to add traditional AppSec capabilities into an RBVM suite. Some vendors price these capabilities based on the type of asset (e.g., dynamic/static application security testing (D/SAST), while others roll these features up into an "enterprise" version of their solutions. Omdia would like to see this functionality quickly become standard in RBVM solutions.

- **Attack path management and compensating controls:** Not all vendors are actively working to ingest attack path scanning results (e.g., simulation and pen testing tools) or to support the mapping of legacy security controls to each asset to enable adjustments to risk estimates. Omdia strongly believes that an understanding of attack paths and compensating controls allows much more flexibility in remediation recommendations from RBVM solutions and facilitates faster execution of remediation actions.

- **Prioritization versus workflow:** Vendors tend to approach vulnerability management as primarily a prioritization problem or a workflow problem. The fact that some vendors believe the prioritization problem has been (mostly) solved perhaps speaks to a level of market maturity, suggesting that the core tenets of traditional vulnerability management are well established. Omdia is not as sanguine regarding prioritization and believes significant investment in enhancement and extension is warranted. That said, the end goal of RBVM is risk reduction, and that requires strong workflow capabilities. But workflows alone cannot build trust in recommendations; only strong, transparent prioritization techniques can do that.

Figure 4: Vendor rankings in the RVBM universe

Vendor	Product(s) evaluated
Leaders	
Balbix	Balbix Security Cloud: Risk Based Vulnerability Management
Cisco (Kenna)	Cisco Vulnerability Management (formerly Kenna.VM)
Nucleus Security	Nucleus Security
Vulcan Cyber	Vulcan Enterprise
Challengers	
Ivanti	Ivanti Neurons for RBVM
Qualys	Qualys Vulnerability Management, Detection & Response (VMDR)
ServiceNow	ServiceNow Vulnerability Response

Source: Omdia

Market leaders

Market leaders understand the current threat landscape as well as the criticality of assets within each customer's digital domain. This internal and external visibility is a key requirement in enabling risk assessment. These solutions also present a list of prioritized remediation suggestions and an orchestrated workflow for getting recommendations to appropriate asset owners. Leaders need to demonstrate the ability to marshal the right set of data to create actionable risk assessments for every asset and to push those recommendations with appropriate service level agreements (SLAs) in place to fully manage the entire lifecycle.

Market challengers

Challengers typically have good breadth in their solutions but not always a depth of features in every area. This shows up most noticeably in risk analytics, where leading vendors tend to have more innovative approaches to quickly and accurately assessing risk.

Market prospects

Prospects tend to be newer to the market and typically show real strength in only a few of Omdia's solution capabilities categories. These vendors tend to enter the RBVM market through an adjacent market or with a pivot in focus. There are several dozen vendors in the RBVM market, and most would fall into the prospects tier.

Opportunities

Omdia expects that all legacy vulnerability management asset visibility tools will eventually be augmented by RBVM. Detection tools are already viewed, mostly by RBVM vendors, as commodities, and few vendors currently offer native scanning capabilities beyond cloud assets. Visibility into and analysis of the threat landscape will, however, remain important differentiators for market leaders.

Baking risk management into broader exposure management represents a large and growing market opportunity. RBVM solutions are well positioned to land and then expand into this broader market. RBVM solutions are also well positioned to add the capability to quantify cyber-risk and thereby add use cases such as determining overall cyber-risk scores and enabling the comparison of cyber-risk with other enterprise risks.

Threats

RBVM solutions sit at the nexus of a dynamic, expanding, and rapidly evolving set of customer requirements. Several vendors in the broader proactive security space are already moving to consolidate capabilities into platforms that roll up currently disparate technology to deliver a holistic view of enterprise-wide cyber-risk. These include attack path management vendors, security posture management vendors, and attack surface management vendors, among others. All these solutions could eventually compete with RBVM solutions.

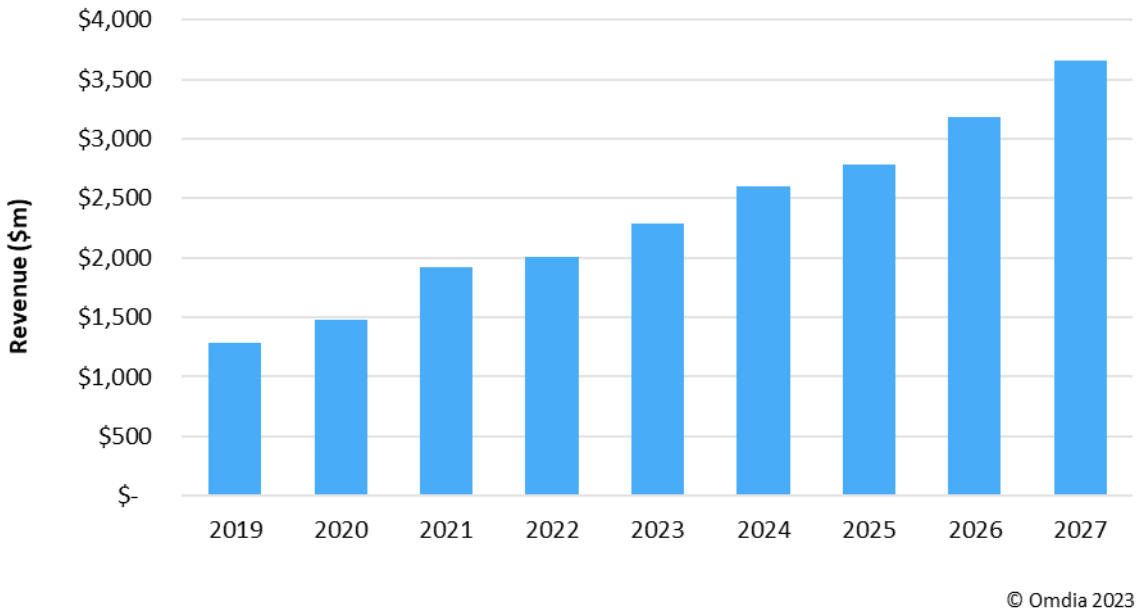
And, as previously discussed, RBVM tools are increasingly overlapping with other established markets. Many of these vendors also recognize the value of integrating risk management into their solutions. There are, in fact, vendors in multiple spaces that are looking to understand and manage the overall risk posture of organizations. Omdia expects these market dynamics to drive consolidation in the RBVM and related markets.

Market outlook

Omdia is generally bullish regarding the growth of the vulnerability management market. While some components of legacy vulnerability management solutions will increasingly become commoditized, over the coming years, RBVM adoption will become mainstream as an augment (or replacement) for legacy vulnerability management solutions. Customers are currently buying products based primarily on the strength of features and functions.

Omdia does not currently break RBVM out as a separate component of its overall vulnerability market tracker. Omdia estimates the overall vulnerability management market will be just under $2.3bn in global revenue in 2023. Omdia predicts the market will grow to just over $3.6bn by the end of our forecast period in 2027. Vulnerability management will remain a foundational component of proactive approaches to cyber-risk reduction.

Figure 5: Vulnerability management market size, 2019–27 ($m)



Source: Omdia

Both the legacy vulnerability management and RBVM markets remain fragmented. For example, revenue from the traditional big three legacy vulnerability management vendors combine to represent approximately a third of that market. Similarly, no vendor in the RBVM market is widely outpacing its competitors from a revenue perspective.

As discussed previously, Omdia strongly believes that RBVM solutions will continue to expand in functionality and use cases, which will further expand the total addressable market for these solutions and provide significant additional opportunities for leading RBVM vendors.

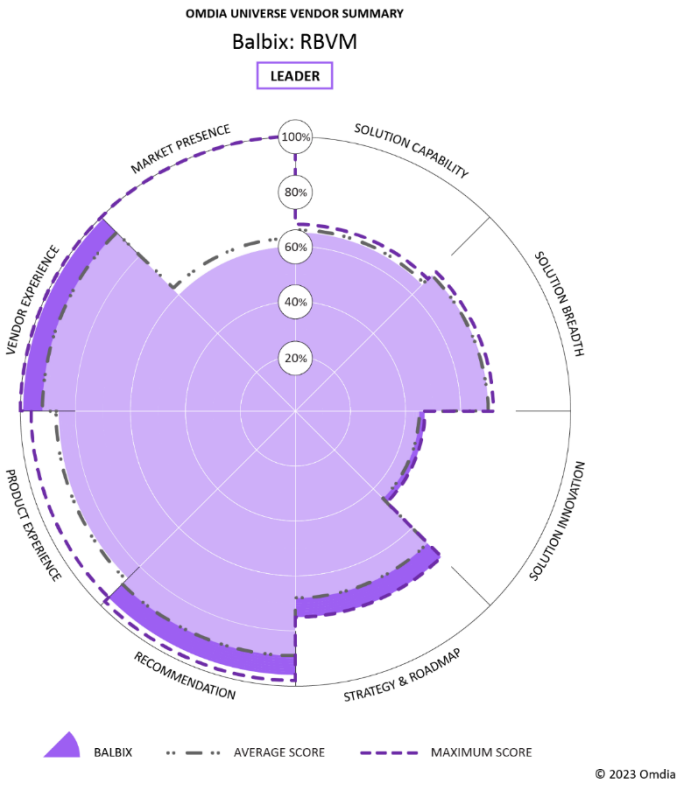
Vendor analysis

Balbix (Omdia recommendation: Leader)

Table 1: Balbix solution profile

Product	Balbix Security Cloud: Risk Based Vulnerability Management
Target markets	Mid-market, enterprise
No. of customers	Dozens (declined to provide exact number)
Key customers	Greenhill & Co., Oerlikon

Figure 6: Omdia Universe ratings—Balbix



Source: Omdia

Balbix should appear on your shortlist if:

- A solution for the mid-market and enterprise that has strong core functionality across all capabilities categories is important to you.
- You are looking for a solution that broadly addresses vulnerabilities beyond traditional Common Vulnerabilities and Exposures (CVEs) (e.g., misconfigurations, weak credentials).
- The ability to leverage existing security controls when formulating risk scores and implementing temporary mitigations is considered critical to your overall remediation strategy.

Market position overview

Balbix, ranked as a "leader" in this report, offers its RBVM product globally, targeting customers from medium-sized businesses up through enterprises. The company was founded in 2015 by Gaurav Banga, who was previously the co-founder & CEO of Bromium, an early application isolation vendor.

Balbix has raised more than $100m in total funding, including a $70m Series C round in March 2022. Balbix positions its product as a *Cybersecurity Posture Automation* platform, of which RBVM is a major component. The broader focus on "posture" speaks to the company's desire to advance beyond traditional software vulnerabilities to address cyber-risk. And "automation" addresses the need to reduce the operational burden of delivering improvements to an organization's overall cybersecurity posture. This is particularly important in the areas of prioritization and remediation. Omdia believes Balbix is well positioned in a growing market, with a solid strategy to expand its total addressable market.

Technology details

Balbix scored consistently well across all solution capability categories. The company was an early entrant into the RBVM market and has steadily enhanced its product to meet the needs of its customers.

Data collection: Balbix supports an extremely rich set of asset details, supporting more than 400 data attributes. This includes a runtime Software Bill of Materials (SBOM) to enable full dependency analysis. Balbix collects scanning data for software vulnerabilities, weak/missing encryption, misconfigurations, and password issues.

Threat intelligence: Balbix ingests data from the National Vulnerability Database; commercial threat intelligence services such as government agency feeds, including CISA KEV; open source and vendor feeds, including nearly a hundred parsers, to continually scan thousands of vendor/product combinations for vulnerability information.

Telemetry and storage: The Balbix Security Cloud platform, which is hosted on AWS, can scale to millions of assets and terabytes of data. Balbix considers RBVM to be largely a data problem, and its approach is to deliver a telemetry- and data-driven, near-real-time, asset-by-asset risk model.

Risk analytics: Balbix provides a customized, real-time Balbix Score and Balbix Rank for each vulnerability. The analysis considers the combination of vulnerability-specific parameters (e.g., accessibility, ease of attack, exploit consequence), threat level (e.g., exploit maturity, adversary activity), exposure (e.g., vulnerability exposure, vulnerability age), and available controls (e.g., mitigations detected).

Vulnerability resolution: The solution includes fully customizable asset inventory, vulnerability, and risk assessment dashboards, supported by role-based access control. On top of remediation workflows, users can filter assets by almost any attribute and tag assets based on individual compliance regimes. Balbix supports vulnerability management performance metrics to better incentivize asset owners to reduce their risk exposure.

Strategy and roadmap

Balbix is taking an expansive view of the types of vulnerabilities that RBVM solutions can address and is putting forth a clear vision of where it sees RBVM heading. It has developed its own CAASM, which creates a rich asset inventory for its RBVM solution. (Other vendors are moving in this direction, but Balbix made it an early part of its strategy.)

In addition to RBVM and CAASM, the solution supports Cyber-risk Quantification. A dashboarding, reporting, and compliance automation suite operates across all three products, which are hosted on the Balbix Security Cloud. While the market for quantified risk assessment is currently distinct from operational risk products such as RBVM, Omdia predicts that these markets will converge and that RBVM vendors, including Balbix, will be well-positioned in that evolved market.

Opportunities

Balbix fields a relatively mature RBVM product, but Omdia's customer experience scores show some concerns regarding ease of deployment. While the vendor would assert that its scanner allows for the richest visibility into assets, its early entrance into the space arguably led it to spend too much time and effort building out its own scanner, which later entrants clearly understood were becoming commodities.

Generally, Balbix delivers solid functionality across the breadth of Omdia's solution capabilities matrix, but it is not always on the bleeding edge with respect to introducing new features to the market. Anecdotally, Balbix may not get as much market buzz as some of its competitors, but its customers are very likely to recommend the product, based particularly on strengths in prioritization and remediation recommendations.

Omdia analysis

Balbix Security Cloud: Risk Based Vulnerability Management is finding traction both in the mid-market and enterprise. The company keeps its pricing model relatively simple, with licensing via annual subscription based on the number of monitored assets. Base pricing includes support and maintenance. Balbix's channel program includes dozens of partners that range from global systems integrators to VARs and other regional partners.

As mentioned, Balbix thinks deeply about the attack surface and attack paths through an enterprise. It is one of the few vendors that is really trying to map attack paths and leverage them into conversations about actual risk and the effect of existing security controls on assessing that risk. As

proactive functionality consolidates further onto cyber-risk management platforms, this will be an increasingly important differentiator.

All RBVM solutions need to address both the threat landscape and the asset landscape, but most vendors tend to emphasize visibility into the threat landscape when describing their products. In balance, Balbix spends more time talking about assets than exploitability; its product development, particularly its full embrace of CAASM functionality, reflects this orientation. Indeed, in Omdia's evaluation, the solution scored strongest in telemetry and vulnerability remediation features.

Overall, Balbix Security Cloud: Risk Based Vulnerability Management is a strong RBVM option for a broad swatch of both midsize and large organizations. It may not be flashy, but it has no glaring weaknesses, and its forward-leaning approach to risk is a good match for security programs seeking to tie cyber-risk to broader business risk initiatives.

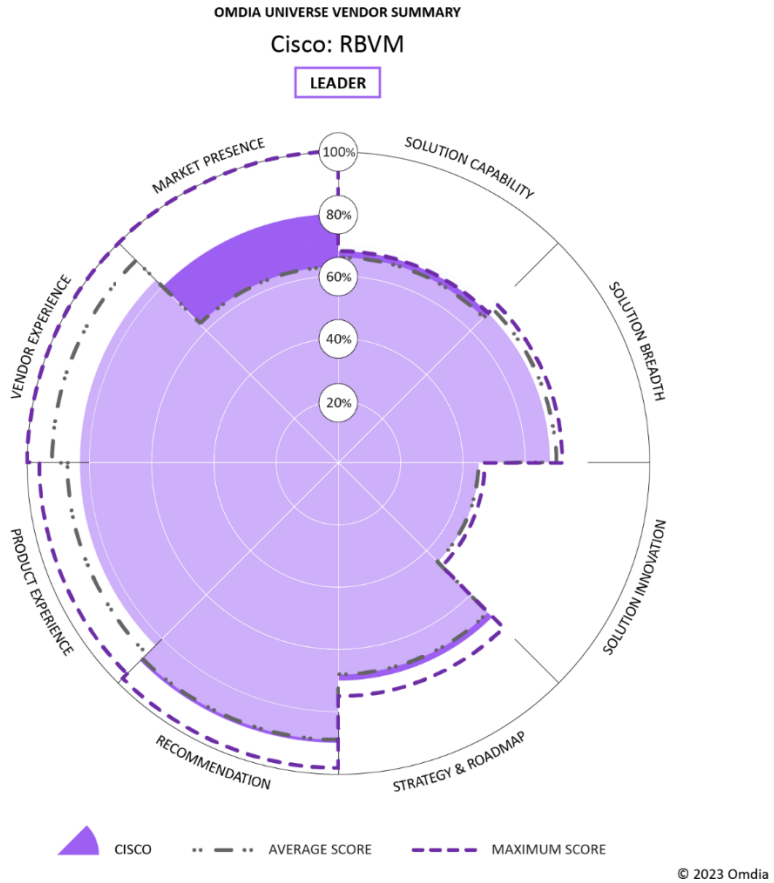
Cisco Vulnerability Management (formerly Kenna.VM) (Omdia recommendation: Leader)

Table 2: Cisco solution profile

Product	Cisco Vulnerability Management (formerly Kenna.VM)
Target markets	SMB, large enterprises
No. of customers	More than 400
Key customers	Not available

Source: Omdia

Figure 7: Omdia Universe ratings—Cisco Vulnerability Management



Source: Omdia

Cisco Vulnerability Management should appear on your shortlist if:

- You are currently a Cisco security customer, particularly if you are already leveraging Cisco Talos threat intelligence.
- An understanding of the current (and predicted future) landscape of software exploits is your most important determinant of risk associated with vulnerabilities.
- Flexibility in the customization of the analytic and reporting engine, as well as in the presentation of findings and recommendations, is a key requirement.

Market position overview

Cisco, ranked as a "Leader" in this report, entered the RBVM market through the acquisition of Kenna Security in 2021. Kenna was founded in 2010 by Ed Bellis and Jeff Heuer. The company had raised just under $100m in total funding before being acquired. Kenna has done as much as any vendor to build the market for RBVM.

Long before Kenna was acquired, Cisco was producing detailed and data-driven reports that made a strong case for RBVM. One of the most interesting findings from Kenna is that almost no organizations, regardless of size, remediate more than 10–15% of observed vulnerabilities in any given month. This finding succinctly captures the primary driver for RBVM solutions: organizations routinely fail to keep up with the ever-growing volume of vulnerabilities in their digital environments.

Technology details

Cisco fields one of the most mature RBVM products in the market. Historically, Cisco Vulnerability Management has had a relentless focus on traditional software vulnerabilities in production environments. Cisco has expanded its focus to address vulnerabilities in custom application development.

Data collection: As is common with RBVM vendors, Cisco does not have its own vulnerability scanners. Rather, data from telemetry sources are acquired from partners via script and file/XML-based uploads. Data elements are pulled into cloud-based services, and de-duplication logic is applied.

Threat intelligence: This is a key area of differentiation for Cisco, which collects an impressive level of threat landscape information. Cisco Vulnerability Management pulls data from 19 threat intel sources, OEMs, and its own Cisco Talos dataset to build vulnerability risk models.

Telemetry and storage: Cisco applies a zero-trust philosophy to its security products. Cisco uses a wide range of technologies—such as multi-factor authentication, threat analytics, and anomaly detection—in its zero-trust model to ensure proper access control. Cisco also enforces governance policies that support least-privilege access.

Risk analytics: Cisco is a strong proponent of the use of AI/ML for RBVM modeling. The product employs four distinct ML models for the product's core risk scoring. It also deploys innovative analytics for exploit prediction.

Vulnerability resolution: Users can create service tickets directly from the Cisco Vulnerability Management user interface or via API. Cisco Vulnerability Management APIs can be used in conjunction with leading orchestration or patch automation tools. Additionally, Cisco Vulnerability Management offers the capability to create risk-based SLAs tailored to the risk tolerance of the organization. These SLAs assist in tracking remediation progress.

Strategy and roadmap

Cisco acquired Kenna with the goal of integrating the Kenna technology into the broad Cisco Secure product portfolio. The Kenna Product Suite currently includes:

- Cisco Vulnerability Management: The flagship RBVM solution.
- Cisco Vulnerability Management Premier: Adds additional features to the base Kenna.VM offerings, such as Remediation Scoring and Zero-Day Intel powered by Cisco Talos.
- Cisco Kenna.AppSec: An application Security product.

Analytics have always been a core strength of the Kenna product, and that remains true under Cisco. Where Cisco looked to immediately augment the product was in threat intelligence. Cisco Talos threat intelligence can now be used as an additional input for building ML models for vulnerability risk.

The risk model is further informed with environmental considerations, such as asset criticality (from a business perspective), asset exposure (from an attack path perspective), and the patch level aggregation (patch risk supersedence) to provide recommendations, risk assessments, and measure risk over time on the vulnerability, asset, and asset group levels. Cisco's broader portfolio can help feed environmental data into the RBVM; eventually, Cisco security controls could be widely used to enforce temporary mitigations recommended by the RBVM.

Cisco Vulnerability Management has several features on its roadmap to further improve remediation management. For example, it recently launched a model for assessing vulnerability management performance and has built a model to predict ease of remediation based on past remediation data for each vulnerability. These features are market-leading and enablers to the mainstream adoption of these tools.

Opportunities

Cisco has not put as much effort as some of its competitors in expanding its definition of vulnerability and addressing non-CVE posture issues. While the primary expectation for these tools remains the prioritization of CVEs, the market is moving to manage a broader set of vulnerabilities.

Cisco's customer experience scores were mostly positive, although the product scored relatively poorly in its ability to integrate with other systems. An additional concern is that compared to its

peers, Cisco's RBVM pricing schedule is relatively complex (each product has its own set of volume pricing tiers).

Omdia analysis

Cisco fields a well-known and well-regarded RBVM portfolio based on the Kenna Security acquisition. The networking giant believes that its deep visibility into and understanding of the threat landscape is an important competitive differentiator. As important as analytics have been to Kenna's growth, it really sees RBVM as solving a data problem.

Cisco is focused on larger, more mature customers, and the features included in its premier offering (e.g., additional remediation analytics and richer threat intelligence) strongly hint at where it sees the RBVM value proposition moving. Cisco is working to get ahead of the attack curve with knowledge of predicted exploits and is building an early-warning system regarding zero-day vulnerabilities.

Kenna Security was a major contributor to the creation of the Exploit Prediction Scoring System (EPSS), which predicts the likelihood of an exploit being created for each CVE. While Cisco sees value in EPSS, it believes that it can provide more actionable insight into current risk with its deep understanding of the global landscape of active exploits. Cisco monitors active exploits via three main sources: IDS alerts, malware analysis, and malicious email. The company's global visibility into threat activity helps determine the range and velocity of each exploit.

Overall, Cisco Vulnerability Management is a strong RBVM option, particularly for large organizations. The product supports some of the most advanced analytics in the space, and it leverages leading threat intelligence feeds to provide near-real-time assessments of the threat landscape. Cisco's focus on enterprise customers is also driving it to develop very sophisticated tools for measuring and managing remediation success. The sum total of its capabilities and their quality more than justifies its Leader position.

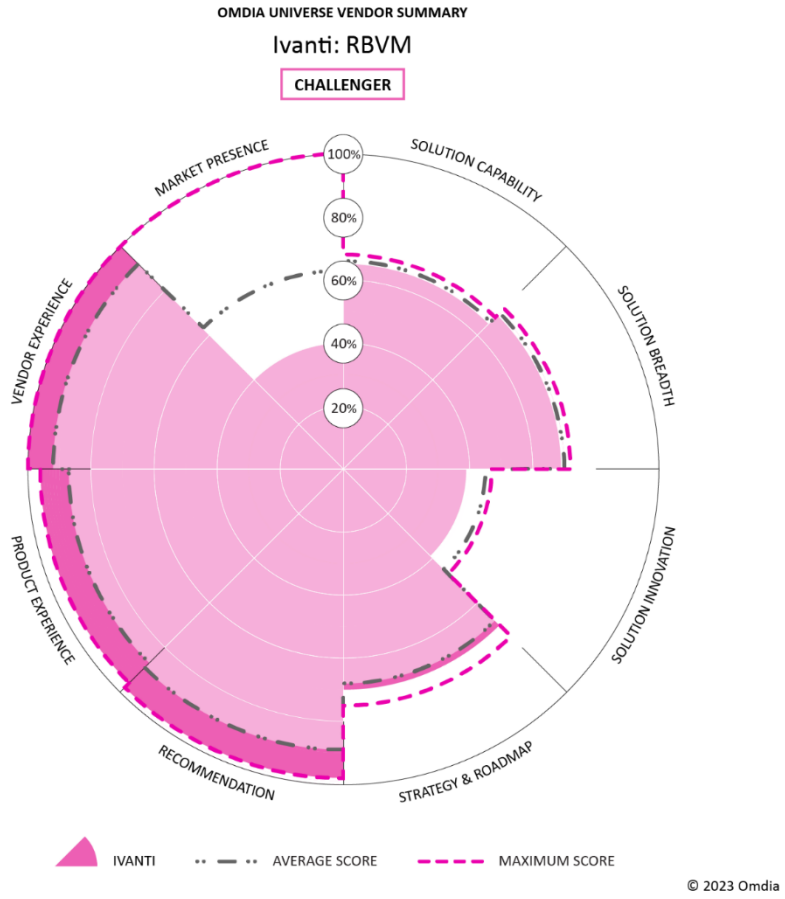
Ivanti (Omdia recommendation: Challenger)

Table 3: Ivanti solution profile

Product name	Ivanti Neurons for RBVM
Target markets	SMB, mid-market, enterprise
No. of customers	More than 100 (declined to provide exact figure)
Key customers	Declined to provide

Source: Omdia

Figure 8: Omdia Universe ratings—Ivanti



Source: Omdia

Ivanti should appear on your shortlist if:

- You are a current customer of the broader Ivanti Neurons Service and Asset Management solution, or other complementary Ivanti Neurons offerings, including UEM, patch, ITSM, or ZTA.
- Specific data sovereignty requirements are a requirement (Ivanti RBVM is delivered through partnership with AWS).
- Ease of deployment is an important consideration; Ivanti supports a relatively simple deployment model.

Market position overview

Ivanti, ranked as a "Challenger" in this report, is an amalgam of technology companies (LANDESK, HEAT, AppSense, Shavlik, Wavelink) that were combined and rebranded as Ivanti in 2017. Ivanti has three product pillars: IT service management (ITSM), unified endpoint management (UEM), and security. The company reported total FY22 revenue of approximately $1bn and more than 40,000 customers, including almost 90% of the Fortune 100 and almost 50% of the Global 2000. Ivanti has a network of 7,000 channel partners operating in 149 countries. The company is headquartered in South Jordan, Utah.

Over the years, Ivanti has acquired a host of security technologies, which now sit under the Ivanti Neurons brand. In addition to RBVM, Ivanti security offerings address zero trust access, application security, patch management, NAC, VPN, SSO, and mobile threat defense.

The company continues to expand its portfolio. It entered the RBVM market in 2021 with the acquisition of RiskSense. That technology has since been rebranded as Ivanti Neurons for Risk-Based Vulnerability Management (Ivanti Neurons for RBVM). The product is typically sold as part of a broader solution, however, that includes a vulnerability and threat intelligence product, Ivanti Neurons for Vulnerability Knowledge Base (Vuln KB), and an RBVM solution for applications, Ivanti Neurons for App Security Orchestration & Correlation (ASOC). Ivanti Neurons for ASOC consolidates application scan data and assesses vulnerabilities and weaknesses in code before it is deployed in production environments.

Technology details

It is early days in Ivanti's efforts to integrate RBVM broadly into its Neurons portfolio, and, in fact, even the RBVM portfolio is a collection of separate products. This is not surprising, given that the company acquired key pieces of RBVM technology.

Data collection: Ivanti Neurons for RBVM supports several methods of data ingestion depending on whether an API is available. If an API is available, it is simply configured to pull data from third-party products. If no API is available from the data source, customers can manually (or with scripts using the Ivanti API) update data to the product. Customers can also perform custom uploads.

Threat intelligence: Threat and vulnerability intelligence are provided via a proprietary database called Ivanti Neurons for VULN KB. VULN KB ingests vulnerability findings from 100+ independent

sources to provide detailed information on known vulnerabilities, threats (e.g., ransomware), level of exploitation, and trending.

Telemetry and storage: Storage can be restricted to specified geographic areas to support data export restrictions and sovereignty requirements. Indefinite data storage is standard in the per-asset licensing fee (unless deleted by the users), but access to reports and dashboards is restricted to last 365 days in most cases.

Risk analytics: The solution has two proprietary risk-scoring methodologies: Ivanti RS^3 and VRR. The VRR score assesses the risk from a particular vulnerability. It chiefly considers threat landscape factors in the risk calculation. Ivanti's RS^3 score is designed to provide an overall assessment of risk for an asset, group of assets, or the entire organization. It is calculated using a wide set of environmental and temporal factors.

Vulnerability resolution: Ivanti Neurons for RBVM allows bidirectional integration with Ivanti Neurons for ITSM, and third-party ticketing systems, including BMC Incident, Jira, and ServiceNow. When a ticket is updated with successful remediation in an integrated ticketing system, that status syncs to Ivanti Neurons for RBVM.

Strategy and roadmap

The three distinct groups of functionalities supported by Neurons are UEM, Service & Asset Management, and Network & Endpoint Security. Increasingly, security is becoming the glue that binds the suite together. While it is still early days in Ivanti's efforts to build a fully integrated product suite, RBVM will eventually become tightly integrated with its ITSM and UEM products. It wants to enable, for example, one-click integration into the Ivanti ticketing system. This is an area where the company sees an ability to differentiate in increasingly competitive markets.

Ivanti agrees with the assumption that the core analytics in RBVM tools are beginning to commoditize (driven in part by the availability of the open-source EPSS tool) and that, increasingly, RBVM leadership will be driven by automation and workflow features. This will require Ivanti to continue to enhance the asset management features in its RBVM product, which will put it more directly in competition with CAASM solutions.

Opportunities

A chief strength of Ivanti is that it has acquired numerous complementary technologies that can deliver magnified customer value when fully integrated. A chief concern with Ivanti is that it has acquired numerous complementary technologies that will take some effort to fully integrate. (Ivanti's roadmap is heavily focused on the development of out-of-the-box integrations between the products in its Neurons portfolio.)

This contributes to the related problem that Ivanti's price sheet can get complicated. There are multiple SKUs for VULN KB, based on the size of the organization, and multiple SKUs for assets, based on type (e.g., DAST, SAST, Container).

Ivanti also faces stiff competition across its portfolio, particularly in the ITSM market. And while many of the company's assets are quite mature, a corporate rebranding always diminishes name recognition, which is certainly the case for Ivanti itself as a security vendor, and its Neurons offering in the RBVM market.

Omdia analysis

The sweet spot for Ivanti Neurons for RBVM will be with customers of the larger Neurons portfolio. Ivanti has invested heavily in its presentation layer, particularly with the flexibility of its dashboard. One area where this is particularly important for the company is meeting the needs of its MSSP partners. For example, the solution supports the creation of per-client dashboards to ease management tasks for channel partners.

Ivanti's customer experience scores were impressive. The solution even scored well in areas where many of its competitors stumbled, such as integration with other systems and ease of deployment. RBVM is an important component of Ivanti's broader portfolio, and it is investing accordingly.

The company must continue to support ServiceNow and other third-party ITSM and patch management integrations and will officially remain agnostic regarding ticketing systems. But the hope will certainly be that customers standardize on the Ivanti Neurons platform.

Overall, Ivanti Neurons for RBVM is seeing good market success, with more than 100 current customers. The RBVM business benefits from the company's diverse, global channel of MSSPs, resellers, VARS, and distributors in place selling the entire Neurons portfolio. Its technology, strategy, and roadmap are all sound. Though it ranks as a challenger in this report, Omdia believes that could change, especially if the vendor can accelerate its efforts to fully integrate its broad portfolio with the acquired RiskSense technology.

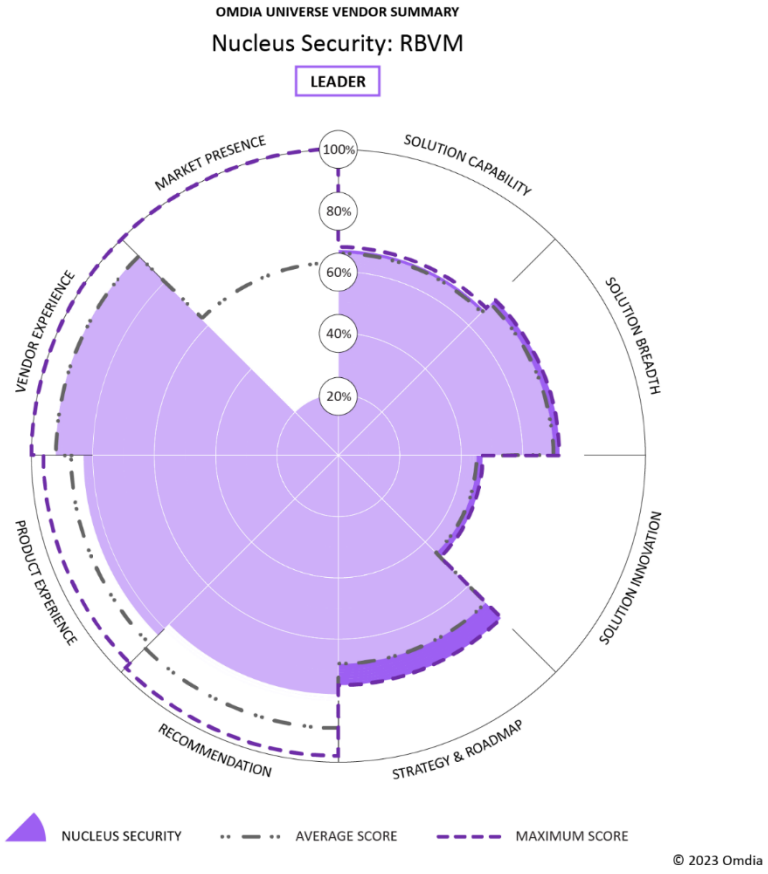
Nucleus Security (Omdia recommendation: Leader)

Table 4: Nucleus Security solution profile

Product	Nucleus Security
Target markets	Global 2,000, federal government
No. of customers	Several hundred
Key customers	Motorola, Canva, National Bank of Australia, Equinor

Source: Omdia

Figure 9: Omdia Universe ratings—Nucleus Security



Source: Omdia

Nucleus Security should appear on your shortlist if:

- The broadest flexibility of prioritization approaches, with full transparency into recommended remediations, is a key buying criterion.
- A solution that broadly addresses vulnerabilities beyond traditional CVEs (e.g., CWEs, misconfigurations, penetration testing results, compliance findings) is required.
- Decision-makers favor a solution currently deployed globally at large enterprises.

Market position overview

Nucleus Security is ranked as a "Leader" in this report and has seen good market traction, particularly among the Global 2000. The Nucleus product is particularly strong in features related to data telemetry and automation of remediation workflow.

Nucleus was founded in 2018, although the principals began research on a prototype with US government funding in 2016. The company has developed one product and is solely focused on the RBVM market. Nucleus currently employs 75 people and is headquartered in Sarasota, Florida. The company's latest funding round was a $21m Series B in 2022. In early 2022, Nucleus announced a strategic partnership with Mandiant, now a part of Google Cloud. Other go-to-market partners include Optiv, Orange Cyberdefense, Carahsoft, and GuidePoint Security.

Technology details

Nucleus has done a solid job building out RBVM functionality internally but relies on partner Mandiant for much of its threat intelligence capabilities and has been less aggressive in adopting AI/ML capabilities than some other vendors in the space.

Data collection: The solution supports more than 100 native integrations, with most being manageable through a GUI-based configuration. These include leading endpoint security products, network scanners, ASM products, and cloud scanners. Nucleus does not currently support formal integrations with IoT-focused scanners, although the vendor asserts traditional network scanners often detect these assets.

Threat intelligence: The primary threat intelligence feed for Nucleus Security is Mandiant's vulnerability threat intelligence, which is natively embedded as a feature within the Nucleus platform. (It is included without requiring a separate Mandiant license.)

Telemetry and storage: Nucleus views the collection, processing, de-duplication, and storage of asset and vulnerability data as foundational capabilities for its risk-based management platform. Nucleus is hosted on AWS and is "in process" for FedRAMP authorization.

Risk analytics: Nucleus believes that AI is currently overhyped in RBVM use cases but agrees that there is an important value in using AI/ML for prioritizing vulnerabilities. The solution supports the Exploit Prediction Scoring System (EPSS). Nucleus takes a diversified approach to prioritization

methodologies, also supporting Stakeholder Specific Vulnerability Categorization (SSVC) methodology.

Vulnerability resolution: Nucleus has invested heavily in building bi-directional integrations with ticketing and notification systems so that remediation workflows can be automatically pushed out to application owners. The Nucleus automation framework allows remediation recommendations to be addressed without asset owners needing to ever log into Nucleus.

Strategy and roadmap

Nucleus has a straightforward view of its functional goals: drive down risk and simplify remediation. Because the company sees the bottleneck of complexity in remediating vulnerabilities as a major inhibitor to risk reduction, it has invested heavily in workflow automation. Nucleus currently supports the broad use of automated workflows through its automation framework. These include asset inventory synchronization, vulnerability scan data ingestion, asset data processing, vulnerability enrichment, vulnerability prioritization, exception handling, vulnerability assignment, and remediation ticket tracking.

Nucleus ingests data from a diverse set of sources to give it visibility into vulnerabilities well beyond traditional CVEs. Nucleus imports data from network scans, application scans (SCA, SAST/DAST), asset inventories, CMDBs, compliance scans, Penetration tests (Pen Tests), and bug bounty programs, among other sources.

This approach results in Nucleus' functionality overlapping with several historically adjacent security markets. For example, the solution can assess application security business logic vulnerabilities inside of code in development environments. Pen test findings can provide visibility into attack path security. And visibility into cloud assets allows a level of cloud security posture management that can address misconfigurations. Nucleus is, of course, not alone in this strategy and roadmap but is particularly aggressive in its implementation.

One of the results of this expansion in footprint is that it is increasingly pushing Nucleus (and other RBVM vendors) to take on much of the asset management functionality traditionally seen in CAASM products. The breadth of Nucleus' visibility into the global vulnerability landscape has also convinced the company that it can sell its vulnerability intelligence platform as a standalone service for some customers. This service is on the company's roadmap for release in 2H23.

Opportunities

Nucleus suffers some of the same weaknesses as other startups in the space, including limited name recognition. And despite the heavy emphasis on integration with third-party systems, it still scored lower on that metric than others in our customer experience survey.

As noted, Nucleus has not put the same level of focus into advanced analytics as some of its competitors. The company sees the biggest pain points in vulnerability management today as data integration, workflow automation, and data visibility, none of which, it asserts, require AI/ML to address effectively. While there is merit in these arguments, given the level of hype in security markets around AI/ML, a lack of perceived focus on innovation in AI/ML may be seen as a negative.

As is true of several of its competitors, Nucleus has limited capability to take compensating controls into account when assessing the actual risk associated with a vulnerability and in recommending temporary mitigations based on available security controls.

Omdia analysis

Nucleus Security is well positioned, particularly at the higher end of the RBVM market, where it competes directly with Cisco Kenna and others. Nucleus arguably supports the broadest flexibility of prioritization approaches, and its support for full transparency into recommended remediations is a key product strength.

As discussed, Nucleus sees a long-term opportunity in addressing an expansive view of vulnerability management, which will continue to grow the company's total addressable market. It sees its "sweet spot" as delivering a single governance structure that encompasses cloud security, application security, and network security. Overall, Nucleus Security is a strong RBVM option, particularly for large enterprises, and is enjoying strong uptake among enterprise customers globally.

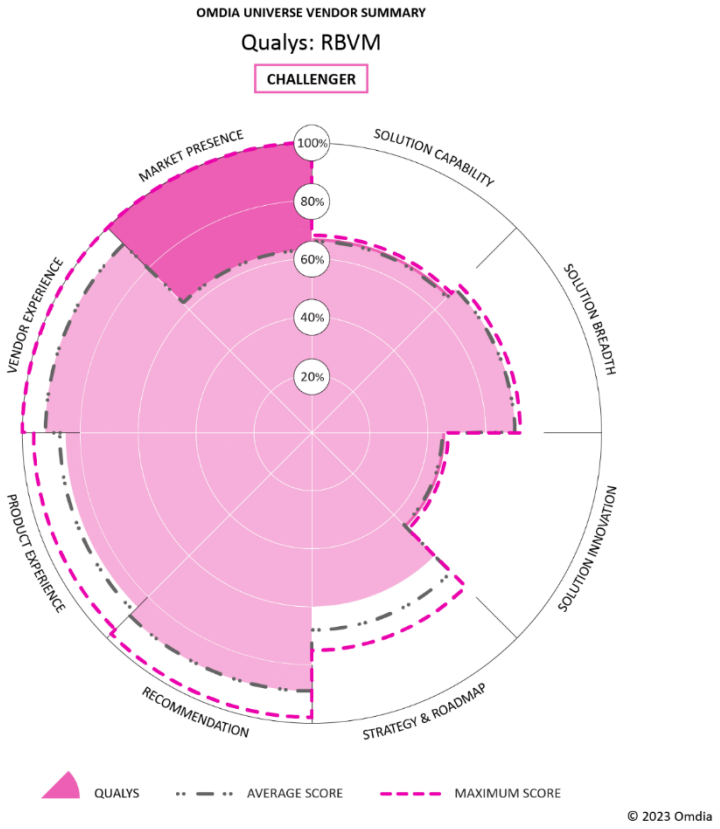
Qualys (Omdia recommendation: Challenger)

Table 5: Qualys solution profile

Product	Qualys Vulnerability Management, Detection & Response (VMDR)
Target markets	SMB, mid-market, enterprise
No. of customers	Vendor declined to provide
Key customers	Aflac, HCA Healthcare, Elevance, Cembra, CargoTech, Syntax, University of Westminster

Source: Omdia

Figure 10: Omdia Universe ratings—Qualys



Source: Omdia

Qualys should appear on your shortlist if:

- You are a Qualys shop for traditional vulnerability management, patch management, external attack surface management, web application scanning, or policy compliance tools.
- Credentialed scans of your assets are a requirement; Qualys support numerous scans with administrative privileges.
- Advanced reporting capabilities and preconfigured templates for regulatory compliance are important features.

Market position overview

Qualys, ranked as a "Challenger" in this report, was one of the earliest entrants into the traditional vulnerability management market. The company was founded in 1999 and went public on the Nasdaq under the stock ticker QLYS in 2012. In FY22, Qualys reported $489.7m in total revenue and claims 10,000 total customers. Qualys has built out a broad portfolio that includes asset management, IT security, compliance, cloud-native security, and web app security applications.

The company introduced Vulnerability Management, Detection and Response (VMDR) V2.0 in June 2022. That release supported RBVM capabilities through its TruRisk features, which debuted new capabilities, such as richer prioritization features, enabling a comprehensive assessment of the risk associated with vulnerabilities and assets. VMDR is sold through its direct sales team for enterprises, SMEs, and SMBs, and also by a large network of MSSPs and more than 1,000 channel partners.

VMDR builds on Qualys' expertise in the traditional vulnerability management market. The product enables organizations to automatically discover internal and externally facing assets, inventory all hardware and software, and classify and tag assets based on criticality. The product monitors assets for vulnerabilities and prioritizes them based on up-to-date threat intelligence and the risk posed by those vulnerabilities to the organization. Recommendations are made for remediation based on an automated assessment of the latest superseding patch for the vulnerable asset. And its integration with its own patch management solution also allows organizations to deploy patches to reduce risk.

Technology details

Obviously, some components of Qualys' RBVM solution are highly mature, for example, the On-premises Device Inventory capabilities. As mentioned, TruRisk scores and automated remediation workflows are newer features. Qualys VMDR 2.0 is hosted on the Qualys Cloud Platform, which combines the Qualys Cloud Agent, virtual scanners, and network analysis (passive scanning) capabilities. The complete bundle bundles asset management, vulnerability management, threat detection & prioritization, and response tools.

Data collection: Data is collected through Qualys agents, Qualys virtual scanner appliances, physical scanner appliances, external scanner appliances deployed by Qualys, cloud connectors, and passive sensors.

Threat intelligence: Qualys subscribes to 25+ sources of threat and exploit intelligence feeds to gather vulnerability-related threats. Some key sources included Exploit DB, Metasploit, multiple OEM threat feeds, Reversing Labs, Canvas, and CISA Known exploited vulnerabilities.

Telemetry and storage: Data is hosted on the Qualys Cloud Platform, which stores the data in the Oracle Database & Elastic Search. Expanding the data model to import data from third-party sources is done by building custom connectors to ingest the data and then transforming it to fit into the Qualys schema.

Risk analytics: Risk scores are created with a combination of external threat data and asset intelligence, such as the location of the asset (internal vs exposed to the internet) and the business criticality of the asset. Qualys positions this as TruRisk (as opposed to theoretical risk) that would result from simply relying on the technical severity of the vulnerability as indicated by its CVSS score.

Vulnerability resolution: VMDR leverages Qualys Sensor for Patch Management. Qualys Zero-Touch Patch identifies and deploys the proper patches and configuration changes required for remediating vulnerabilities automatically. Qualys has developed integrations with ServiceNow and Jira that support orchestration rules for tracking open vulnerabilities and mapping remediation tickets to respective asset owners.

Strategy and roadmap

With more than 20 years of experience in the vulnerability management market, Qualys positions its ability to provide mature data collection tools as a strong solution differentiator. That said, the company fully, if somewhat belatedly, understands that it needs to support asset and vulnerability data from any source, even from the tools of traditional competitors. This work is ongoing.

Qualys also understands the need to deliver recommendations that IT teams can understand and act on. A key strategy for the company is to further close the gap between security and IT teams by fully integrating VMDR with its own and third-party remediation tools.

Qualys is building a unified solution that spans asset management as well as vulnerability detection, prioritization, and remediation. For example, Qualys has integrated its patch management product with VMDR. (The company will continue to support third-party remediation tools.)

Qualys believes that a deep and current understanding of the threat landscape is critical to effective risk scoring. Qualys has also embraced exploit prediction, currently supporting Exploit Prediction Scoring System (EPSS, but aims to augment it in the future. The company is not convinced EPSS considers enough context to be fully predictive. But Qualys is taking a “big tent” approach to prioritization schemes, as demonstrated by its support for the CISA Stakeholder-Specific Vulnerability Categorization (SSVC) guidelines as well.

Qualys’ roadmap is rich with integrations. Omdia expects to see Qualys continue to integrate VMDR with its broader security and compliance suites, as well as integrate with a broader set of proactive tools (e.g., attack path management and attack simulation). Planned feature enhancements include risk reduction benchmarking and risk score customization.

Opportunities

The widespread adoption of heterogeneous digital assets across the enterprise has created multiple concerns for security teams, but one of the benefits has been the deployment of numerous new security controls. Those controls have, in turn, created a wide variety of new telemetry data (e.g., endpoint detection and response (EDR) EDR, cloud detection and response (CDR)) that is useful for asset and vulnerability management. Over the last several years, in particular, the problem has shifted from not always having enough visibility to being able to make sense of overlapping visibility telemetry from numerous sources.

This has accelerated the commoditization of detection data generally and network scanners in particular. Traditional vulnerability management vendors, such as Qualys, have had to make hard choices regarding product development and integration investments. Qualys was arguably slower to initiate these efforts than were some of its traditional competitors but is quickly being remedied and should not be an issue thereafter.

Omdia analysis

From a ranking standpoint, Qualys was the closest call in this report. It has an established track record of success in the traditional vulnerability management segment and is ably making the transition to RBVM, as demonstrated by its introduction of TruRisk last year. The solution balances customer needs well in several areas. For example, it does a good job of collecting and analyzing both environmental and temporal data. And more broadly, it has become good at not only collecting data but also analyzing it.

On the other hand, Omdia would like to see Qualys further open its solutions to third-party integrations and would like to see it expand its efforts to provide a broader “exposure” management capability. That said, Qualys is well-positioned in several market segments and is seeing traction from SMB up through enterprise.

Qualys has introduced several interesting product bundles: VMDR TruRisk FixIT bundles RBVM with patch management and VMDR TruRisk ProtectIT bundles RBVM with EDR. Qualys is also working on a premium solution that includes EASM capabilities as a native component of the RBVM product. The company also sells into the large enterprise market, where its scalability and advanced features are important buying considerations.

Qualys is well-positioned to expand sales of VMDR across its installed base. It’s an obvious update for vulnerability management refreshes, but as the company’s bundling suggests, VMDR provides a means of leveraging risk management across the Qualys portfolio.

Qualys has been busy adding the risk management features that make RBVM exciting and truly differentiating. The company has already made significant enhancements to its analytics and threat intelligence capabilities, demonstrating its understanding that risk models are only as good as the data that feeds them.

Qualys’ large installed base is the obvious target audience for VMDR. The company is being innovative with its bundling to deliver an attractive mix of capabilities to customers ranging from SMBs to enterprises.

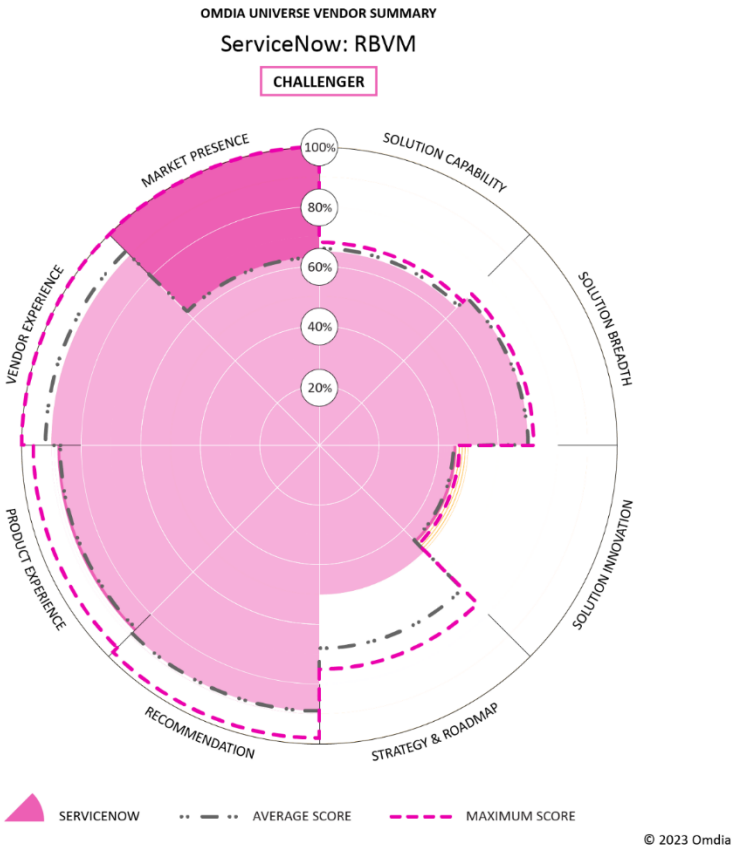
ServiceNow (Omdia recommendation: Challenger)

Table 6: ServiceNow solution profile

Product	ServiceNow Vulnerability Response
Target market	Enterprise
No. of customers	Vendor declined to provide
Key customers	Wellstar Health System, City of Raleigh, Latitude Financial

Source: Omdia

Figure 11: Omdia Universe ratings—ServiceNow



Source: Omdia

ServiceNow should appear on your shortlist if:

- You want to consolidate technology vendors and are currently a ServiceNow shop.
- Specific data sovereignty mandates or US FedRAMP certification is a requirement.
- Sophisticated orchestration of remediation workflow and availability of tools that are accessible to security and non-security teams is important.

Market position overview

ServiceNow, rated a “Challenger” in this report, has undeniable strengths in several solution categories, most notably vulnerability remediation. This is not surprising, given the company’s heritage as a pioneer in IT service management (ITSM). Indeed, ServiceNow is an undeniable leader in delivering effective IT workflows in a wide variety of contexts. And the company rightly sees its ability to garner trust in its workflows as a potent differentiator in the RBVM segment.

ServiceNow, by revenue, is the largest vendor reviewed in this report. The company reported FY22 revenue of $6.94bn, with 22% year-over-year growth. The company is relatively new to the security segment, but revenue in its SecOps solution portfolio exceeded $200m for the first time in FY21. Omdia expects ServiceNow to grow its security business significantly. At the end of FY22, ServiceNow had approximately 7,400 customers, and at least 1,600 of them were spending more than $1m in annual contract value.

ServiceNow’s portfolio includes ITSM, IT Operations Management, Observability, IT Asset Management, Security Operations, Integrated Risk Management, and Strategic Portfolio Management. These products are designed to enable network management, identification, and remediation of security vulnerabilities and threats, visibility of IT resources, and understanding of asset lifecycles.

Along with Vulnerability Response, the other main product in ServiceNow's SecOps portfolio is Security Incident Response (SIR), a Security Orchestration, Automation, and Response (SOAR) tool. SIR supports playbooks, dashboards, and a common data model for enterprise case management. The tool is designed to expedite investigation, response, and remediation actions across IT, security, and risk teams.

Technology details

ServiceNow leverages several mature technologies, such as the CMDB, in this solution. The company is also one of the few vendors in this comparative that has built integrations with IoT and operational technology (OT) scanning products.

Data collection: ServiceNow centralizes and combines the findings of third-party scanners, such as Qualys, Tanium, Tenable, Microsoft, Rapid7, Wiz, Tenable OT, Nozomi, Microsoft Defender for IoT, Armis, Dragos, and Claroty CTD to drive remediation by IT infrastructure, application, and SRE teams. Moreover, ServiceNow’s native cloud discovery agents enable the scanning of cloud resources.

Threat intelligence: The solution imports the CISA KEV catalog and automatically enriches the risk scores of vulnerability records with the newly added CVEs from CISA. The solution also supports integration with third-party vendors, such as Shodan and RecordedFuture, to correlate exploits and related intelligence with vulnerabilities.

Telemetry and storage: All asset information is stored in a central CMDB, consisting of a hierarchical tree structure of asset classes, with relationship records capturing asset interactions. ServiceNow supports a single-tenant, multi-instance architecture and operates mirrored data centers in every continent and regulatory region, with FedRAMP-certified environments for federal customers and contractors.

Risk analytics: ServiceNow prioritizes vulnerabilities based on enriched data such as asset criticality, business services criticality, and other vulnerability and threat intelligence sources. As a result of integration with components of its GRC suite, ServiceNow can enable tracking and reporting on risk management (and configuration compliance) activities and to set and monitor risk thresholds.

Vulnerability resolution: Integrations with patch management tools automate the process of remediation workflow and manage the lifecycle of the vulnerabilities. All remediation and mitigation automation is fully customizable.

Strategy and roadmap

ServiceNow is taking a broad view of the types of vulnerabilities that can be addressed with its RBVM solution. ServiceNow Application Vulnerability Response is a component of the product that is included with some license levels. It assesses DAST and SAST results to identify vulnerable applications based on Common Weakness Enumeration (CWE) and orchestrates remediations. ServiceNow can manage vulnerabilities across the entire attack surface of infrastructure, cloud, apps, OT/IoT, and supply chain.

The ServiceNow RBVM roadmap is working toward an enterprise view of cybersecurity posture. This will include SBOM support, and CSPM features, such as out-of-the-box, policy-based configuration scanning of cloud resources.

Opportunities

ServiceNow is a relatively new entrant into the RBVM market. While the company is leveraging its world-class workflow tools, other components of its RBVM solution are less mature. For example, the product does not support any form of exploit prediction (although it is on the roadmap) and ingests a relatively modest amount of third-party threat intelligence as compared to its competitors.

A difficulty for ServiceNow to differentiate in this market is that every other vendor in the space is working to enable its customers to leverage existing investments in the ServiceNow platform. In fact, every vendor in this comparative research supports some degree of interoperability with ServiceNow. To an extent, ServiceNow is a victim of its own success as it seeks to differentiate in RBVM.

Omdia analysis

ServiceNow Vulnerability Response is a natural extension to the company's existing portfolio, and Vulnerability Response will become an increasingly important product within the company's SecOps portfolio as the product continues to expand and mature.

While not the most complete RBVM product on the market, ServiceNow does support strong capabilities in several categories, notably vulnerability remediation. The company is also working hard to keep the product easy to license and to deliver value quickly. ServiceNow has a simple per-device per-month licensing model for the product, which supports three license levels: Standard, Professional, and Enterprise. The opportunity to upsell RBVM into this existing customer base is particularly attractive, given the natural synergies between RBVM and ticketing systems.

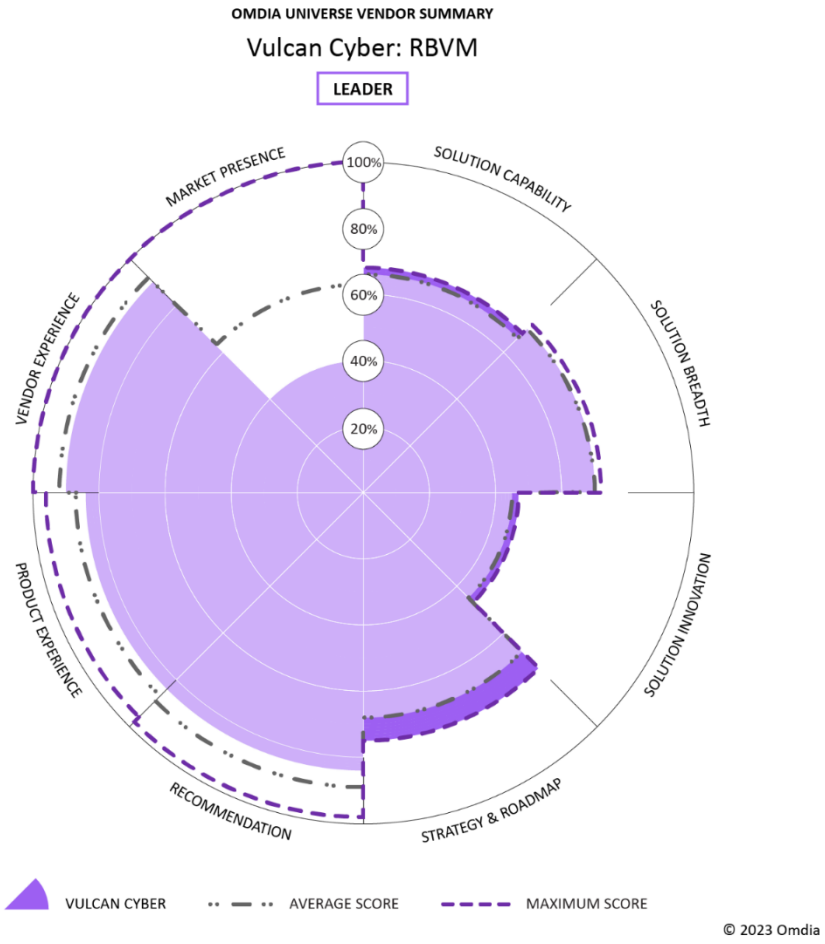
Vulcan Cyber (Omdia recommendation: Leader)

Table 7: Vulcan Cyber solution profile

Product name	Vulcan Enterprise
Target markets	Mid-market, enterprise
No. of customers	100
Key customers	Verana Health, Blackhawk Network, AAA, Snowflake, Mandiant

Source: Omdia

Figure 12: Omdia Universe ratings—Vulcan



Source: Omdia

Vulcan Cyber should appear on your shortlist if:

- Your organization values strong customization capabilities with respect to threat intelligence, risk scoring, and analytic and reporting dashboards.
- A solution that broadly addresses vulnerabilities beyond traditional CVEs (e.g., misconfigurations, weak credentials) is a key requirement.
- Flexibility in pricing and channel options is important.

Market position overview

Vulcan Cyber, ranked as a "Leader" in this report, has quickly established itself in the RBVM market. The company, founded in 2018 and headquartered in Tel Aviv, Israel, has received approximately $35m in funding, including a $21m Series B in March 2021. Vulcan Cyber sells a cyber-risk management platform that addresses three main use cases for vulnerability management: RBVM, application vulnerability management, and cloud vulnerability management.

The company licenses several versions of its product, spanning the market from SMB to enterprise. It is the only RBVM vendor to offer a freemium vulnerability prioritization tool for small businesses. Vulcan Standard is packaged for the needs of mid-sized teams, and Vulcan Enterprise provides full access to all Vulcan Cyber capabilities and functionality and is designed for large organizations. The startup reports approximately 100 customers. The Vulcan Cyber solution is sold globally, both directly and through channel partners. Vulcan Cyber channel partners include global systems integrators and regional resellers such as GuidePoint, Optiv, Herjavec, and Softcat. MSSP partners include Wipro, Kudelski, PurpleSec, TCS, and Deepwatch.

The solution supports tools that are available as free services. These include a tool (MITRE Mapper) that maps CVEs to their relevant MITRE ATT&CK tactics and techniques, and VulnRX, which is a library of thousands of curated vulnerability fixes.

Technology details

Vulcan Cyber leans more toward a focus on environmental factors (e.g., asset criticality, compensating controls) than temporal (e.g., current exploit landscape). As a result, the company supports almost all the functionality typically found in a CAASM, and prebuilt connectors for a rich set of telemetry are key features of the solution.

Data collection: Support for 100+ pre-built, API-based integrations, dubbed Vulcan Connectors. There is no current support for IoT assets, but Vulcan ConnectX can ingest data from any additional unsupported integrations.

Threat intelligence: Vulcan Cyber supports a host of open-source and commercial threat intelligence sources, including 0day.today, Alien Labs OTX, CISA, CVSS Vector, Exploit DB, Exploit Pack, GitHub, Metasploit, Microsoft CVRF, Mitre CVE, NVD, Packet Storm, SAINTexploit, seebug.org, Source Incite, Vulnerability-Lab, and Zero Science Lab.

Telemetry and storage: Vulcan Cyber stores customer data in an Amazon Relation Database Service (RDS) encrypted database. Each customer has its own schema, and backup is kept for 14 days. Vulcan Analytics is built on the Snowflake data lake combined with Microsoft PowerBI on Azure.

Risk analytics: Vulcan Cyber leverages three main parameters for risk calculations: technical severity (CVSS), vulnerability intelligence, and asset context set by the organization. Vulcan Cyber can leverage compensating controls and mitigation factors in risk calculation.

Vulnerability resolution: The Vulcan Cyber platform can create remediation tickets manually or automatically (using Vulcan Playbooks) in Jira or ServiceNow. Vulcan Cyber users can follow remediation progress using Vulcan Campaigns, which can track the status of remediation activity across groups of assets or by other classifiers, such as asset owners.

Strategy and roadmap

Vulcan Cyber likes to describe enterprise digital transformation as resulting in distributed chaos for security teams. This is a useful way to think about how the evolving IT landscape has upended the vulnerability management market. Vulcan Cyber sees its chief function as collecting, organizing, analyzing, and distributing the massive amount of data required to manage and secure digital assets.

Vulcan Cyber recognizes that a key potential inhibitor to the broad adoption of proactive tools, such as RBVM, is that they require collaboration and coordination beyond the SOC. Asset owners are equal partners who must buy into recommendation remediations. And that requires trust. Vulcan's solution is to create one system of record of all asset types. (The Vulcan cyber-risk management platform currently supports identifying and remediating vulnerabilities across infrastructure, cloud, and applications.)

Given this goal, it is not surprising that Vulcan Cyber takes an expansive view when defining vulnerabilities, which includes misconfigurations, IDs, open APIs, badly implemented SaaS apps, and other potential exposures. With respect to remediation, the company's product roadmap currently includes adding further attack path management capabilities to augment its visibility and understanding of the effectiveness of compensating controls.

Opportunities

Most RBVM vendors are cautious regarding the degree to which they will enable automated end-to-end remediation, such as the application of a patch or the deployment of a configuration change, and Vulcan Cyber is no different. Similarly, while support for visibility into OT/IoT assets is not a huge priority for most RBVM vendors, Vulcan has no pre-built support for OT/IoT-focused scanners.

Vulcan Cyber brings an impressive collection of capabilities to market with the Vulcan platform, and in several respects, the solution delivers a more mature set of capabilities than those of its competitors. But the company continues to suffer from relatively poor name recognition, particularly when compared to larger rivals.

Omdia analysis

Vulcan Cyber scored remarkably well in this report, especially given its relatively short time in the market. The company is building an RBVM solution that provides one system of record for any asset type, and that can address a broad spectrum of compliance and exposure management concerns.

Vulcan Cyber has invested heavily in usability and customization features, particularly in its risk analysis and vulnerability remediation capabilities. The Vulcan cyber-risk scoring model is fully customizable to capture unique business contexts. Customers can even use their own scoring models if desired. And Vulcan Cyber supports role-based, access-controlled risk analytics dashboards for risk, SLA, and remediation tracking.

Overall, Vulcan Enterprise is an attractive RBVM option that targets customers from small through large enterprises. The free and standard versions of the product provide smaller-sized organizations with no- and low-cost options for deploying the solution. Vulcan Cyber's focus on addressing the complexity of modern IT infrastructure and creating tools that can build trust between security and IT teams justifies its "Leader" position.

Appendix

Methodology

Omdia Universe

Omdia's rigorous methodology for the Universe product involves the following steps:

- Omdia analysts perform an in-depth review of the market using Omdia's market forecasting data and Omdia's enterprise insights survey data.
- Omdia creates a matrix of capabilities, attributes, and features that it considers to be important now and in the next 12–18 months for the market.
- Vendors are interviewed and provide in-depth briefings on the current solutions and future plans.
- Analysts supplement these briefings with other information obtained from industry events and user conferences.
- The Universe is peer-reviewed by other Omdia analysts before being proofread by a team of dedicated editors.

Inclusion criteria

Participants needed to meet the following inclusion criteria:

- RBVM solution is designed and sold to discover, assess, prioritize, and remediate software vulnerabilities for enterprise customers.
- RBVM solution is sold as an on-prem product or cloud-based SaaS service, and that it addresses the full vulnerability management lifecycle.
- RBVM solution incorporates analytics or other metrics for the purpose of assessing and prioritizing risk associated with known software vulnerabilities.
- RBVM solution must assess vulnerabilities using a risk-based model that incorporates internal and external factors such as asset criticality, vulnerability severity, and existing compensating controls.

- RBVM solution provides recommendations for remediation, prioritization, and mitigation actions for each vulnerability.
- RBVM solution is generally available for purchase as of January 1, 2023.

Further reading

2023 Trends to Watch: Cybersecurity Operations, November 2022

Fundamentals of Risk-based Vulnerability Management, November 2022

RSA Conference 2023 Analysis: Key Trends and Takeaways, May 2023

Authors

Andrew Braunberg, Principal Analyst, Security Operations

Eric Parizo, Practice Leader, Cybersecurity

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") and represent data, research, opinions or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness or correctness of the information, opinions and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees and agents, disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial or other decisions based on or made in reliance of the Omdia Materials.

CONTACT US

omdia.com

askananalyst@omdia.com