IDC MarketScape

IDC MarketScape: Worldwide Exposure Management 2025 Vendor Assessment

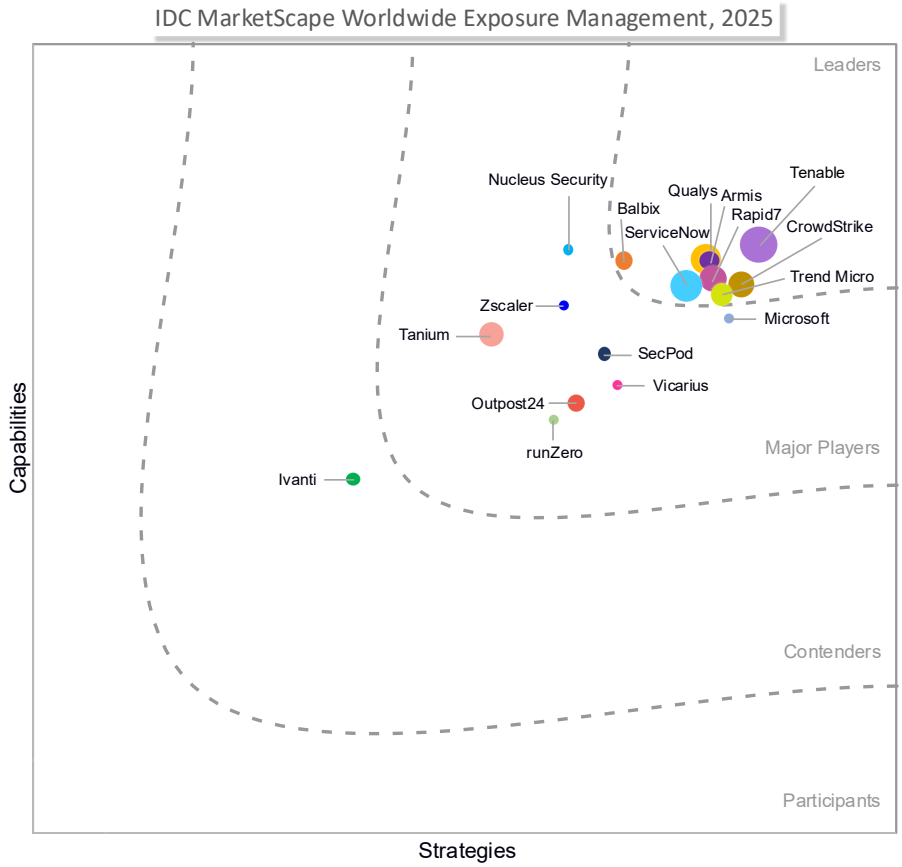
Michelle Abraham

THIS EXCERPT FEATURES TREND MICRO AS A LEADER

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Exposure Management Vendor Assessment



Source: IDC, 2025

August 2025, IDC #US52994525e

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

ABOUT THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Exposure Management 2025 Vendor Assessment (Doc # US52994525).

IDC OPINION

Traditional vulnerability management is slowly evolving to more holistic exposure management within security organizations. Those that are placing more emphasis on proactive cybersecurity can find solutions that help them evaluate their entire attack surface holistically, illuminate the exposures in their environment, prioritize their risks, and integrate with remediation workflows to close the gaps.

According to Verizon's 2025 *Data Breach Investigations Report (DBIR)*, the exploitation of vulnerabilities was the second most used initial access vector, just behind credential abuse. The 34% rise shows that organizations should not take exposure risk lightly, instead managing risks just as they do alerts from security tools. However, in the sea of threats, many security teams are more reactive than proactive — so all vendors are challenged by the need to convince organizations to invest in a proactive cybersecurity solution beyond the vulnerability scanner they likely use today.

There is also the problem of security silos. Since attack surfaces are expanding with AI being the latest surface, some organizations are using multiple security posture management tools, one for each attack surface. Security teams need to investigate solutions that unify exposures because each exposure does not exist in a vacuum. Exposures may be chained together for initial access or lateral movement; attack path analysis presents a visual communication of these issues.

Exposure management solutions still need to ensure the basics of vulnerability management. According to IDC's March 2025 *Exposure Management Survey,* the most important feature is vulnerability prioritization, with integration of real-time threat intelligence and attack path analysis next in order, respectively. The survey also showed that 53% of respondents prioritize their exposure workflow based on partial information such as CVSS score or vulnerability exploit lists instead of using prioritization algorithms that take into account exploitability of the vulnerability and asset context within their own environment, among other factors.

Managing exposures goes beyond investing in technology because doing it well often means changing people and processes, making sure they understand the impact these

risks have on the organization. Therefore, vendors need to help customers mature their vulnerability and exposure management programs. Visibility and prioritization are only part of the solution; remediation through mitigations and patching must also be part of the workflow with the ability to track progress.

IDC expects the following critical success factors for exposure management platforms:

- Out-of-the-box (OOTB) connectors to many sources of exposure data beyond traditional vulnerability scanners
- A view of risk across all the exposures with the ability of the user to customize the prioritization of the work
- Automation of the remediation workflow
- Easy to understand and predictable pricing with few add-ons
- Straightforward customer support plans that help customers receive more value from their exposure management solution over time
- Wide range of channel and MSSP partners

There should be continuous innovation and expansion in all the areas mentioned in the previous bullets.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

In determining the group of vendors for analysis in this IDC MarketScape, IDC considered the following set of inclusion criteria:

- The offering should be commercially available for use as an exposure management platform that is managed by the customer, not a vendor-managed device vulnerability management platform.
- The solution must have been generally available by December 31, 2024.
- The solution must have the ability to bring in at least two data sources besides the IT vulnerability scan data.
- The solution must have at least $10 million in revenue in CY24.
- The solution must be offered and available on a worldwide basis, with sales in a minimum of four regions.
- No single region or country can account for more than 92% of solution revenue.

ADVICE FOR TECHNOLOGY BUYERS

- Note that for those who are still prioritizing remediation work based on CVSS score or other single metrics, move to a solution with prioritization algorithms

that account for the specifics in your organization. Asset Graphs and attack path analysis offer important visualizations to see relationships between assets and exposures.

- Aggregate exposures into a solution that can unify them, so they are examined holistically and not in silos. Individual exposures may not be important issues when analyzed on their own; however, chaining them amplifies the priority of their remediation.
- Work with a vendor that will help your organization mature its proactive cybersecurity processes over time to cover additional attack surfaces and automate the workflow, so exposure management is less onerous.
- Look for a solution with reporting that can be used throughout the organization, not just in security, so others can easily understand the risk posture. Gamification of risk posture is one way to involve other parts of the organization outside of security.
- Consider solutions that include identities in Asset Graphs and attack paths to see exposures related to identity security posture in the holistic view.
- Investigate platforms that infer asset ownership because remediation requests often need to go to the owner. Even if incorrect, the inferred owner is a starting place for fixing the issue.

VENDOR SUMMARY PROFILES

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

Trend Micro

Trend Micro is positioned in the Leaders category in this 2025 IDC MarketScape for worldwide exposure management.

Trend Micro is a global cybersecurity provider with a significant presence across North America, Europe, and Asia/Pacific. The company's core exposure management solution is Trend Vision One Cyber Risk Exposure Management (CREM), generally available since 2023. CREM provides centralized visibility and continuous risk assessment across endpoints, servers, identities, data, cloud resources, AI models, networks, and APIs natively while supporting third-party integrations.

Flexible, credit-based licensing allows organizations to tailor their exposure management approach, allocating coverage across different modules and asset types.

Self-service purchasing options and marketplace availability support a range of deployment needs. Customers can expand beyond core discovery and prioritization with additional capabilities such as attack path prediction, compliance management, and security awareness training available through an enhanced package. For organizations operating in cloud-native or hybrid environments, dedicated cloud exposure management capabilities are also available under the CREM umbrella.

Users can see peer comparisons in CREM, which can help them justify additional investment if they are behind. Security teams can create training campaigns within the platform for risky users. Trend Micro introduced a digital twin model that will enable continuous red teaming against the digital twin of an organization's hybrid cloud and on-premises environment. Security teams can identify gaps before attackers and validate if their security controls are working as expected.

Strengths

- Trend Micro combines native security posture management tools with several third-party integrations to provide exposure telemetry to CREM, bringing many types of exposure, including those in identities, into a centralized platform. Users can also create Vision One playbooks for automated endpoint and account remediation tasks.
- Users may launch the Trend Companion GenAI assistant to ask natural language questions about the exposures in the platform as well as suggestions for making themselves more secure. Suggested prompts are available and depend on where the user is in the platform.

Challenges

- Some organizations still perceive Trend Micro primarily as an endpoint or network security vendor, potentially overlooking the breadth of its exposure management capabilities.
- While CREM supports a growing range of third-party integrations, some connectors are still under development.

Consider Trend Micro When

Trend Vision One Cyber Risk Exposure Management is particularly well suited for enterprises aiming to consolidate security tools and automate remediation, with the added ability to report on compliance requirements within the Trend Micro ecosystem. The solution is an optimal fit for buyers that value integrated asset discovery, predictive analytics, and automated response within a single platform, especially where reducing operational silos and achieving measurable risk reduction are strategic priorities.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

Exposure management solutions offer a different approach to managing device vulnerabilities, emphasizing the fusion of multiple exposure sources by bringing together CVEs, unknown assets, misconfigurations, and other types of exposure. Exposure management often encompasses standalone cybersecurity asset management and attack surface management tools, integrating data from diverse

sources for a comprehensive risk analysis. With holistic exposure management solutions, organizations can aggregate, deduplicate, and analyze data from a variety of sources to provide a more accurate assessment of an organization's risk posture.

For this analysis, exposure management must incorporate device vulnerability management scan results. Device vulnerability management involves network-based or host-based scanners/agents that scan servers, workstations, other devices, and applications to uncover security vulnerabilities in the form of known security holes (vulnerabilities) or configuration settings that can be exploited. They can have credentialed access (using usernames and passwords) into devices or provide an uncredentialed look at a device. The scan data may come from internal or third-party scanners.

Exposure management solutions may also integrate code scanning, container scanning, and runtime scanning of applications and cloud infrastructure. Devices may include IoT/OT systems in addition to IT devices.

LEARN MORE

Related Research

- *Concerns in Managing Vulnerabilities* (IDC #US53615025, June 2025)
- *Desired Features in Exposure Management, 2025* (IDC #US53637325, June 2025)
- *Challenges in Exposure/Vulnerability Management Platforms, 2025* (IDC #US53529425, June 2025)
- *Lack of Prioritization Demonstrates Inadequate Attention on Proactive Cybersecurity* (IDC #US53464025, May 2025)
- *Exposure Management: Security Team Monitoring of "All" Assets Is Improbable* (IDC #US53368225, May 2025)

Synopsis

This IDC study provides a vendor assessment of those offering exposure management platforms. Using the IDC MarketScape model, we considered exposure management vendors based on quantitative and qualitative criteria that is important to organizations selecting an exposure management solution. The assessment is based on a comprehensive and rigorous framework that includes vendor and customer interviews to evaluate how each vendor stacks up, and the framework highlights the key factors that are expected to be the most significant for achieving success in the exposure management market over the short term and long term.

The study highlights the importance of proactive cybersecurity solutions that provide comprehensive attack surface visibility, risk prioritization, and integration with remediation workflows. Key success factors include unified risk views, remediation automation, and straightforward pricing models. The study underscores the need for vendors to address security silos, expand third-party integrations, and innovate in areas like AI-driven analytics and attack path visualization. The assessment provides insights for organizations seeking solutions to manage exposures across IT, OT, IoT, and cloud environments, helping them prioritize risks and enhance their cybersecurity posture effectively.

"Proactive exposure management is the future as traditional vulnerability detection transforms into holistic risk management and remediation," says Michelle Abraham, senior research director, Security and Trust at IDC. "As attack surfaces expand, organizations must leverage advanced tools to illuminate hidden risks and close critical gaps before exploitation occurs."

ABOUT IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com