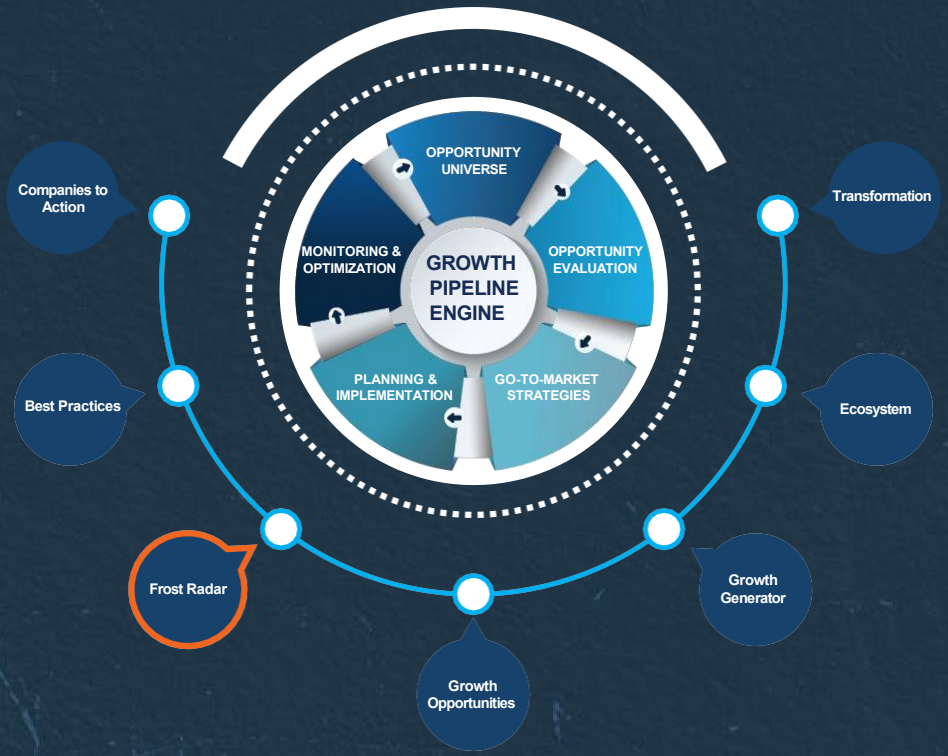
FROST & SULLIVAN

Frost Radar™: Enterprise Risk Mitigation and Management Platforms, 2026

A Benchmarking System to Spark Companies to Action - Innovation That Fuels New Deal Flow and Growth Pipelines



Global Security Research Team at Frost & Sullivan

Authored by: Danielle VanZandt

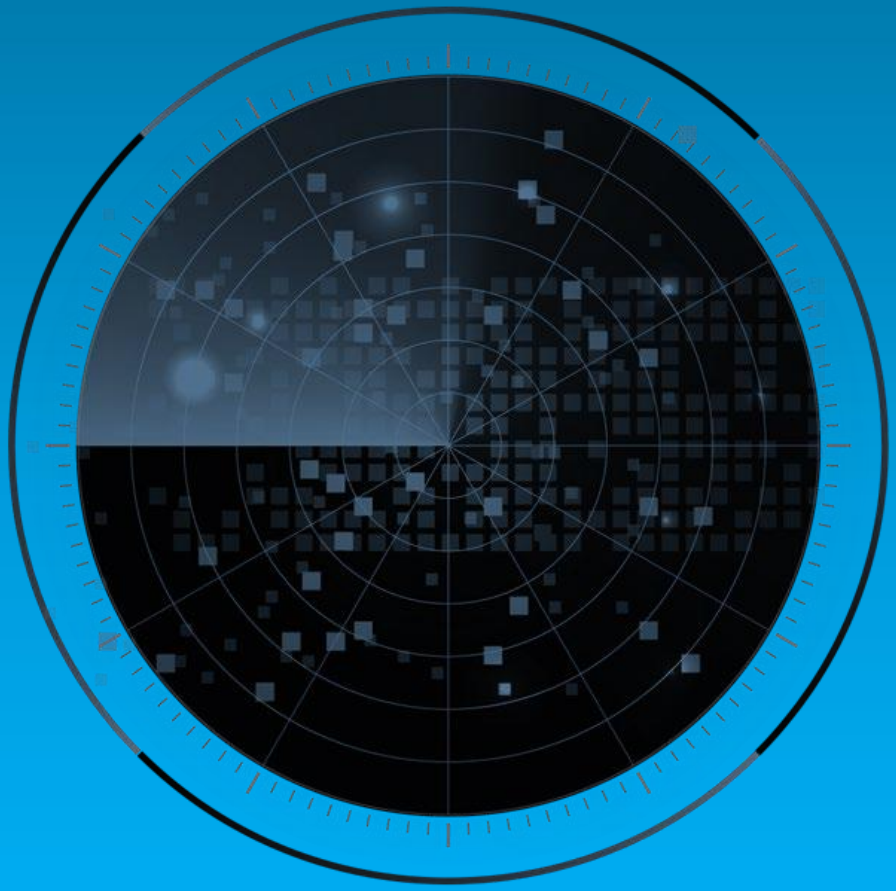
Contributors: Jarad Carleton

KC3B-74

July 2026

FROST & SULLIVAN

Strategic Imperative and Growth Environment



Source: Frost & Sullivan

Strategic Imperative

- Today's risk landscape has moved beyond isolated domains as physical, digital, operational, financial, and geopolitical risk factors merge into more complex, multidomain threats targeting businesses. The complexity is rendering point-solution risk management systems obsolete, necessitating that businesses adopt a more cross-functional, integrated resiliency strategy.
- With many businesses managing complex, multisite physical infrastructure networks as well as more complex digital architectures, obtaining full visibility into the architectural landscape is simply not possible without cross-domain platforms that can monitor and manage assets across converged physical-digital domains. By going beyond traditionally cyber-focused risk frameworks, enterprise risk platforms can correlate digital threat indicators with physical security signals to detect, model, and mitigate more complex risk scenarios.
- Two key vectors that are gaining prominence are geopolitical risk and third-party supply chain risk intelligence. Both impact an organization’s security posture as well as its operational risk landscape. Successful enterprise risk management programs now gain visibility across the entire enterprise architecture, even as that perimeter expands beyond the traditional organizational attack surface.
- Another operational risk consideration is the number of regulatory mandates influencing how enterprise risk and security operations are prioritized. A key facet of any enterprise risk resiliency program is compliance with regulations.
- The industry is not immune to the impacts of AI and automation. Security operations teams fighting a more robust threat landscape that includes AI-powered threat vectors are also deploying AI functionality in their enterprise risk platforms as a force multiplier. A platform-native response function that allows for automated detection, mitigation, and response while maintaining human-in-the-loop operational control is preferable to enterprises across industries.

Growth Environment

- Enterprise risk resiliency operations can now support strategic, risk-informed decision-making at the executive and board levels. Security teams must demonstrate the value of their operations in simple, understandable terms to executive stakeholders. As such, an in-demand platform function is the ability to offer quantifiable risk management and mitigation metrics that directly tie to operational goals, requirements, or business strategies.
- Rather than rely upon multiple disparate systems and manual threat correlation, a new category of security platforms has emerged. Enterprise risk mitigation and management (ERMM) solutions combine threat intelligence, attack surface management (ASM), and digital risk protection (DRP) in a comprehensive software platform to deliver a holistic view of enterprise risk across domains. True ERMM platforms also provide outside-in and inside-out perspectives of the potential threat vectors.
- A best-of-breed ERMM platform offers the following functions:
  - Comprehensive asset discovery to automate identification of websites, cloud services, APIs, and third-party hosted assets to eliminate blind spots and ensure complete inventory of external exposure
  - Risk prioritization and vulnerability insights to contextualize weaknesses against threat intelligence to help enterprises prioritize what attackers are most likely to exploit and remediate faster
  - Threat intelligence integration to enrich findings with real-world intelligence so security teams understand where exposures exist and how they tie into active cybercriminal campaigns or known threat actors
  - Security orchestration and automation capabilities either done natively or via integration with security information and event management (SIEM) and security orchestration, automation, and response (SOAR) solutions for risk and threat intelligence correlation and responses across the enterprise

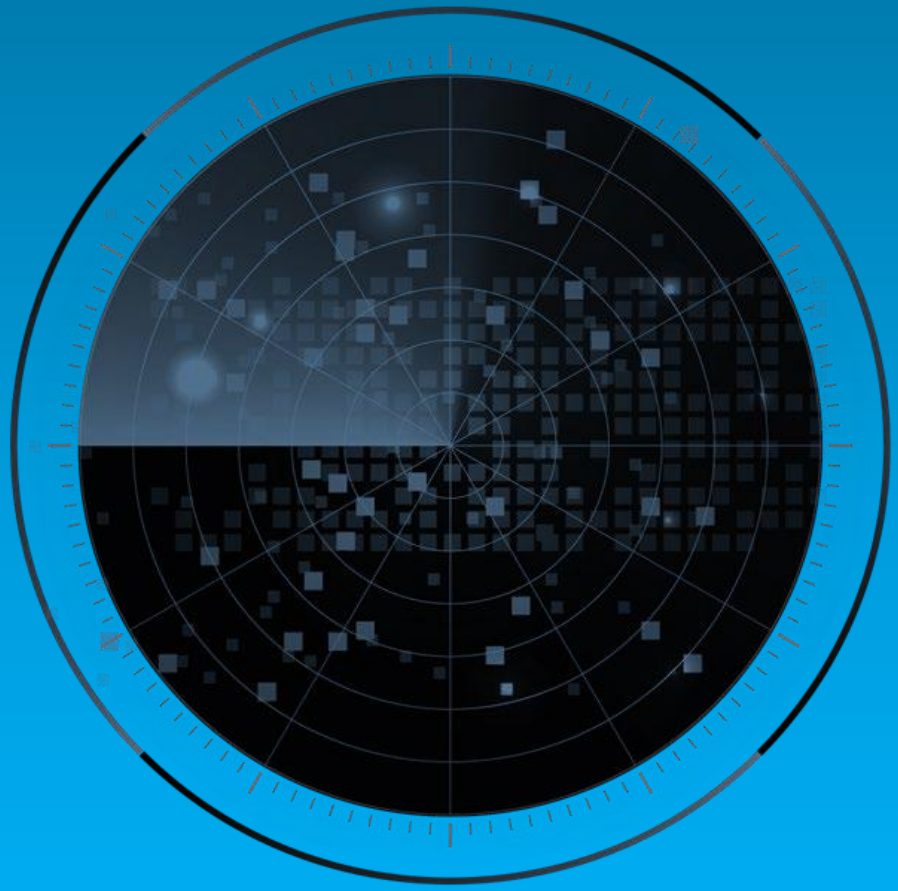
Growth Environment (continued)

- Multirisk domain dashboarding to provide board-level and C-suite visibility across cyber, financial, operational, physical, and geopolitical risk in a single-pane-of-glass view

- A Frost & Sullivan study related to this independent analysis:
  - External Risk Mitigation and Management Solutions, Global, 2025–2030

FROST & SULLIVAN

Frost Radar™: Enterprise Risk Mitigation and Management Platforms



Source: Frost & Sullivan

Frost Radar™: Enterprise Risk Mitigation and Management Platforms

Source: Frost & Sullivan

In a rapidly evolving market with more than 30 qualified participants meeting the core technical capabilities and global customer reach, Frost & Sullivan independently evaluated the landscape and selected just 15 companies to be benchmarked in this Frost Radar™. This small, carefully chosen group represents organizations that rise above the broader market; demonstrating not only strong growth, but a clear capacity to innovate and lead. Inclusion is not simply recognition; it signals that a company is operating at the forefront of its industry.

This evaluation is led by Frost & Sullivan's experienced global analyst team, combining deep domain expertise with a rigorous, fact-based approach. Using our proprietary, multi-dimensional benchmarking methodology, applied consistently and validated by analysts. Frost & Sullivan ensures a fair, globally comparable, and defensible assessment of true market leadership.

Frost Radar™: Competitor Categories

GROWTH CHAMPIONS

- Achieve significant market growth through effective execution.
- Leverage proven technologies and scalable business models.
- Maintain competitiveness via operational efficiency and customer focus.
- Require increased innovation investment for sustained leadership.

VISIONARY LEADERS

- Market leaders with a strong balance of innovation and growth.
- Deliver transformative technologies, business models, and processes.
- Influence industry direction and set new benchmarks.
- Combine strategic vision with operational excellence for market dominance.

CONTENDERS

- Emerging players with a modest market presence and cautious strategies.
- Often new entrants or niche participants establishing their positions.
- Emphasizes continuous improvement and ensures operational reliability.
- Hold potential for growth through innovation, alliances, and market expansion.

INNOVATORS

- Drive technological advancement with disruptive ideas and solutions.
- Prioritize R&D, IP development, and pioneering concepts
- Strong innovation foundation with opportunities to accelerate commercialization and scale
- Benefit from strategic partnerships and targeted go-to-market strategies

Source: Frost & Sullivan

Frost Radar™ Competitive Environment

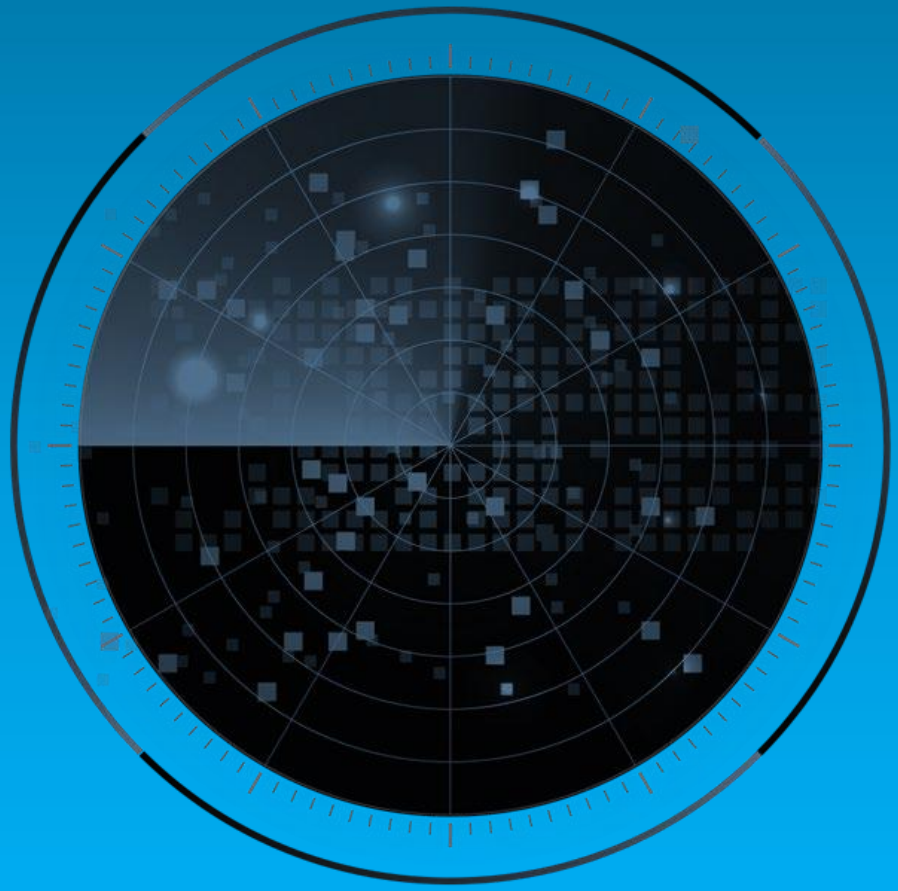
- Beginning with a list of more than 30 companies that identified themselves as ERMM vendors, Frost & Sullivan followed strict definitions of a true ERMM platform when determining the final group of vendors for inclusion in this Frost Radar™ analysis: vendors must offer ASM, cyber threat intelligence (CTI), and DRP functionality in a unified offering. Vendors that did not natively offer these three core functionality sets were excluded from consideration.
- To further differentiate ERMM platforms from the emerging continuous threat exposure management (CTEM) and exposure management industries, ERMM platforms must provide the visibility, prioritization, and intelligence behind the risks to a customer's environment and be capable of carrying out remediation actions natively. Solutions that required integration with external remediation or threat mitigation offerings were also excluded.
- Another core capability of an ERMM platform is the ability to view a customer environment from an outside-in perspective (the view of an outside attacker looking into the organizational infrastructure) as well as from an inside-out perspective (monitoring and visualization of the internal risk landscape and how it connects outside the organization). Platforms that did not offer both perspectives were also removed from consideration, resulting in the final group of 15.
- Vendors earning Visionary Leader distinction are Group-IB, Recorded Future, Check Point, Fortinet, and Rapid7, all of whom provide comprehensive ERMM platforms across security, governance, and operational management use cases for customers. These companies have leveraged considerable R&D, regular capability and functionality improvements, and an AI enablement strategy to bring new technical capabilities into use to solve myriad operational and security risk challenges that organizations face.

Frost Radar™ Competitive Environment (continued)

- Vendors earning Innovator distinction continue to match leading competitors in terms of solution development, scalable platform design and functionality, and leverage of prevalent megatrends, such as AI integration and holistic, cross-domain threat visibility. For BlueVoyant, ReliaQuest, Bitsight, Palo Alto Networks, and CrowdStrike, the ability to translate these platform development visions into tangible growth returns will shift their competitive positioning toward the Visionary Leaders category.
- Vendors earning Contender distinction are either start-ups or specialty players that have expanded their capabilities beyond more niche technologies to be newly classified as a more robust ERMM platform. The vendors in this category—Resecurity, CloudSEK, RiskProfiler, UpGuard, and CYFIRMA—show distinct potential for disruptive innovation as their offerings mature.

FROST & SULLIVAN

Frost Radar™: Companies to Action



Source: Frost & Sullivan

Check Point

VISIONARY LEADER

INNOVATION SCORE **4.30**

GROWTH SCORE **4.05**

INNOVATION

- By combining threat intelligence, ASM, digital risk monitoring, and automated mitigation capabilities, Check Point has developed an operationally focused ERMM framework designed to support continuous risk reduction. The company prioritizes translating intelligence insights into measurable remediation outcomes rather than limiting ERMM to visibility and alerting functions alone.
- Leveraging ThreatCloud intelligence, large-scale telemetry, and evidence-driven analytics, the company strengthens intelligence-based prioritization by correlating external threats, organizational exposures, security control weaknesses, and real-world adversary behavior into contextualized operational insights. This approach improves customers' ability to identify critical risks and accelerate mitigation activities.
- Through continued investment in AI-assisted analytics, adaptive prioritization, continuous exposure validation, and control-aware remediation workflows, Check Point enhances operational scalability and automation maturity. The addition of Veriti's remediation technology expands the company's ability to automate mitigation safely across enterprise security environments without disrupting day-to-day operations.
- With the development and integrations with SIEM, SOAR, ticketing platforms, and AI-enabled operational workflows, Check Point delivers strong platform interoperability across enterprise security ecosystems. Its combination of exposure management, intelligence-driven analytics, remediation orchestration, and executive-level risk visualization positions the company well among organizations seeking mature and operationally integrated ERMM capabilities.

Check Point (continued)

VISIONARY LEADER

INNOVATION SCORE **4.30**

GROWTH SCORE **4.05**

GROWTH

- Rather than focusing solely on enterprise risk visibility, Check Point's growth strategy emphasizes measurable risk reduction and operational execution through continuous, intelligence-driven ERMM. The company positions ERMM as an integrated process to unify exposure identification, prioritization, and remediation in a centralized operational framework.
- Leveraging its extensive global customer base, established channel ecosystem, and broad enterprise footprint, Check Point is well positioned to accelerate adoption of its ERMM capabilities. Continued investments in platform integration, strategic acquisitions, and AI-driven innovation should further strengthen cross-selling opportunities, expand recurring revenue potential, and enhance the company's competitive position as organizations adopt integrated exposure management and CTEM-driven security strategies.
- By building out its ERMM capabilities through strategic acquisitions and platform enhancements, Check Point continues to strengthen its market position. The acquisitions of Cyberint and Veriti significantly expanded its threat intelligence, exposure management, and automated remediation capabilities while also increasing ecosystem integration opportunities and enterprise market reach. More recently, the acquisition of Cyclops enhanced cyber asset ASM capabilities, improving asset visibility, security control validation, and exposure contextualization across increasingly complex enterprise environments.
- Through its platform-centric strategy, Check Point continues to capitalize on enterprise demand for integrated cybersecurity solutions that reduce complexity and maximize the value of security investments. Its ability to embed ERMM capabilities in a broader security architecture supports customer expansion opportunities, strengthens long-term platform adoption, and reinforces its position as a strategic cybersecurity partner for organizations seeking consolidated risk management capabilities.

Check Point (continued)

VISIONARY LEADER

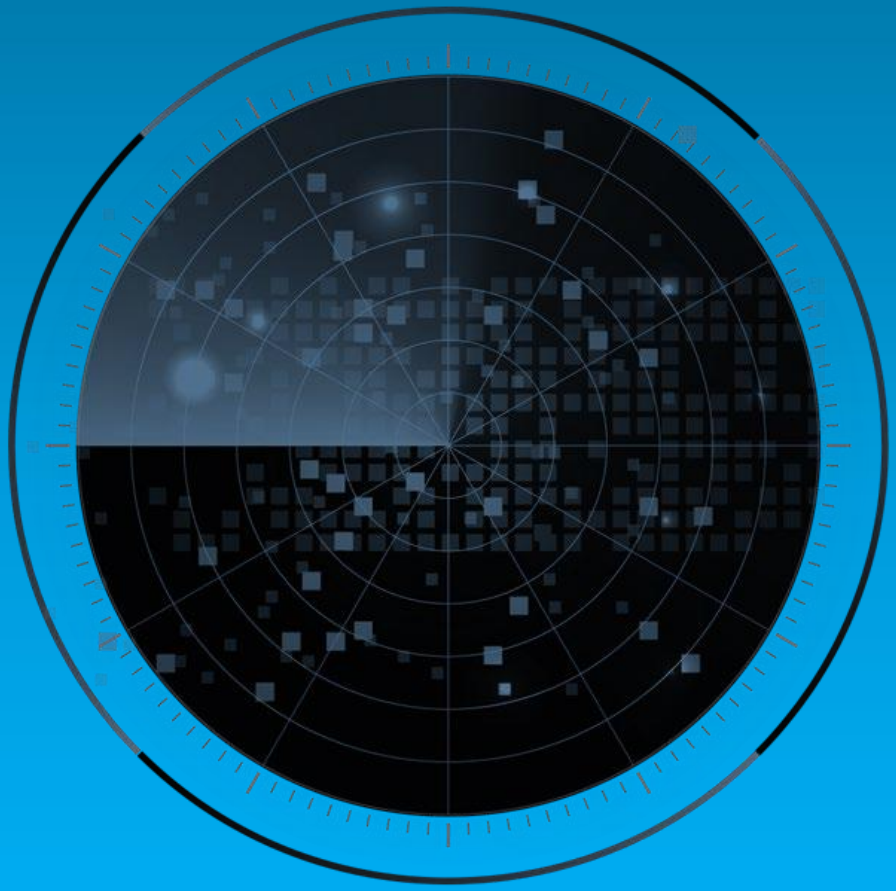
INNOVATION SCORE **4.30**

GROWTH SCORE **4.05**

FROST PERSPECTIVE

- Despite differentiation in remediation, orchestration, and operational execution, Check Point could strengthen its ERMM positioning through more streamlined workflow management across its growing portfolio of intelligence, exposure management, and mitigation capabilities. These user experience functions would particularly appeal to non-technical teams that would also benefit from ERMM platforms for operational visibility and management across additional business areas.
- With enterprises prioritizing centralized cyber risk intelligence platforms, the company would benefit from expanding governance-focused reporting, business-oriented risk measurement, and executive communication tools designed for boards, regulators, and cyber insurance stakeholders. These capabilities would help customers prove the true return on investment for specific risk management or cybersecurity investments.
- Given the company's advanced automation and AI-assisted remediation functionality, ongoing investment in AI explainability, operational transparency, and human oversight mechanisms remains important to addressing enterprise concerns about autonomous mitigation and trust in AI-driven workflows. Trust and transparency behind AI usage remains top of mind for enterprise customers, so emphasizing the explainability of its AI systems will help to gain customer buy-in.

Best Practices & Growth Opportunities



Source: Frost & Sullivan

Best Practices

1. Classification as an ERMM platform requires the consolidation of ASM, DRP, CTI, and third-party risk monitoring into a single, unified solution. Through this holistic visibility, enterprise security teams can break down operational silos, improve contextual risk prioritization, and enable more direct correlation of exposure risks across external assets, vendors, identities, and cloud environments more efficiently.

2. ERMM strategies should prioritize operationalization over passive monitoring by integrating automation, AI-assisted triage, and remediation workflows into daily security operations. Organizations that embed ERMM findings into SIEM, SOAR, ITSM, and governance processes can significantly reduce alert fatigue, improve remediation speed, and demonstrate measurable business outcomes.

3. Organizations should treat identity exposure, shadow AI usage, and non-human identities as core components of external risk management. As attackers increasingly target credentials, APIs, and machine identities, ERMM programs must extend beyond infrastructure scanning to include continuous monitoring of human and identity-related attack surfaces.

Growth Opportunities

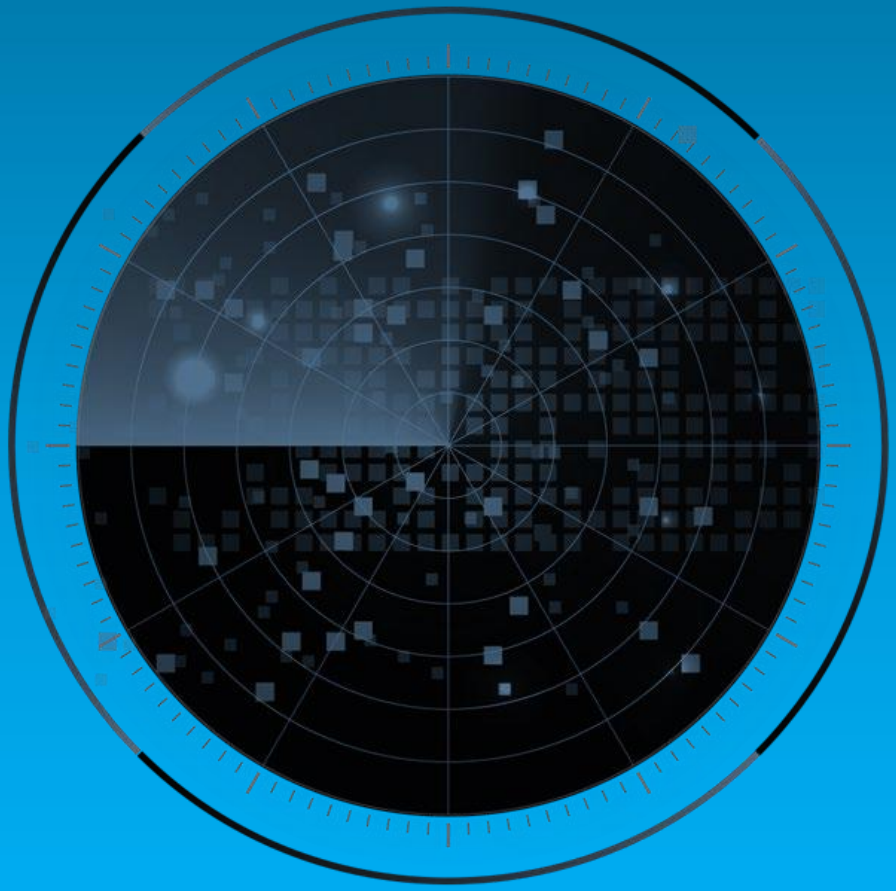
1. Demand for unified cyber risk visibility is creating opportunities for ERMM vendors that can consolidate EASM, DRP, CTI, third-party risk management, and identity exposure management into integrated platforms. Organizations increasingly seek fewer point solutions and more centralized risk orchestration capabilities aligned with CTEM strategies.

2. The rapid expansion of cloud services, remote work, shadow AI, APIs, and non-human identities is significantly increasing organizations' overall attack surface. ERMM vendors that provide visibility into machine identities, AI-related risks, cloud exposures, and human-centric vulnerabilities are well positioned to capture emerging enterprise security spending.

3. Enterprises are prioritizing automation, AI-assisted remediation, and measurable operational outcomes because of security staffing shortages and alert fatigue. ERMM vendors that deliver workflow automation, executive-level risk reporting, and faster remediation capabilities can differentiate themselves by improving operational efficiency and demonstrating clear business value.

FROST & SULLIVAN

Frost Radar™ Analytics



Source: Frost & Sullivan

Frost Radar™: Benchmarking Future Growth Potential 2 Major Indices, 10 Analytical Ingredients, 1 Platform

Growth Index

Growth Index (GI) is a measure of a company's growth performance and track record, along with its ability to develop and execute a fully aligned growth strategy and vision; a robust growth pipeline system; and effective market, competitor, and end-user focused sales and marketing strategies.

GI1

MARKET SHARE (PREVIOUS 3 YEARS)
This is a comparison of a company's market share relative to its competitors in a given market space for the previous 3 years.

GI2

REVENUE GROWTH (PREVIOUS 3 YEARS)
This is a look at a company's revenue growth rate for the previous 3 years in the market/industry/category that forms the context for the given Frost Radar™.

GI3

GROWTH PIPELINE
This is an evaluation of the strength and leverage of a company's growth pipeline system to continuously capture, analyze, and prioritize its universe of growth opportunities.

GI4

VISION AND STRATEGY
This is an assessment of how well a company's growth strategy is aligned with its vision. Are the investments that a company is making in new products and markets consistent with the stated vision?

GI5

SALES AND MARKETING
This is a measure of the effectiveness of a company's sales and marketing efforts in helping it drive demand and achieve its growth objectives.

Source: Frost & Sullivan

Frost Radar™: Benchmarking Future Growth Potential 2 Major Indices, 10 Analytical Ingredients, 1 Platform (continued)

Innovation Index

Innovation Index (II) is a measure of a company's ability to develop products/ services/ solutions (with a clear understanding of disruptive megatrends) that are globally applicable, are able to evolve and expand to serve multiple markets and are aligned to customers' changing needs.

II1

INNOVATION SCALABILITY
This determines whether an organization's innovations are globally scalable and applicable in both developing and mature markets, and also in adjacent and non-adjacent industry verticals.

II2

RESEARCH AND DEVELOPMENT
This is a measure of the efficacy of a company's R&D strategy, as determined by the size of its R&D investment and how it feeds the innovation pipeline.

II3

PRODUCT PORTFOLIO
This is a measure of a company's product portfolio, focusing on the relative contribution of new products to its annual revenue.

II4

MEGATRENDS LEVERAGE
This is an assessment of a company's proactive leverage of evolving, long-term opportunities and new business models, as the foundation of its innovation pipeline. An explanation of megatrends can be found here.

II5

CUSTOMER ALIGNMENT
This evaluates the applicability of a company's products/services/solutions to current and potential customers, as well as how its innovation strategy is influenced by evolving customer needs.

Next Steps

JOIN:
Growth Council

APPLY:
Companies to Action

ENGAGE:
Growth Dialog

PARTICIPATE:
Growth Council Think Tank

Does your current system support rapid adaptation to emerging opportunities?

Source: Frost & Sullivan

Legal Disclaimer

Frost & Sullivan is not responsible for any incorrect information supplied by companies or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan research services are limited publications containing valuable market information provided to a select group of customers. Customers acknowledge, when ordering or downloading, that Frost & Sullivan research services are for internal use and not for general publication or disclosure to third parties. No part of this research service may be given, lent, resold, or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without the permission of the publisher.

For information regarding permission, write to: permission@frost.com