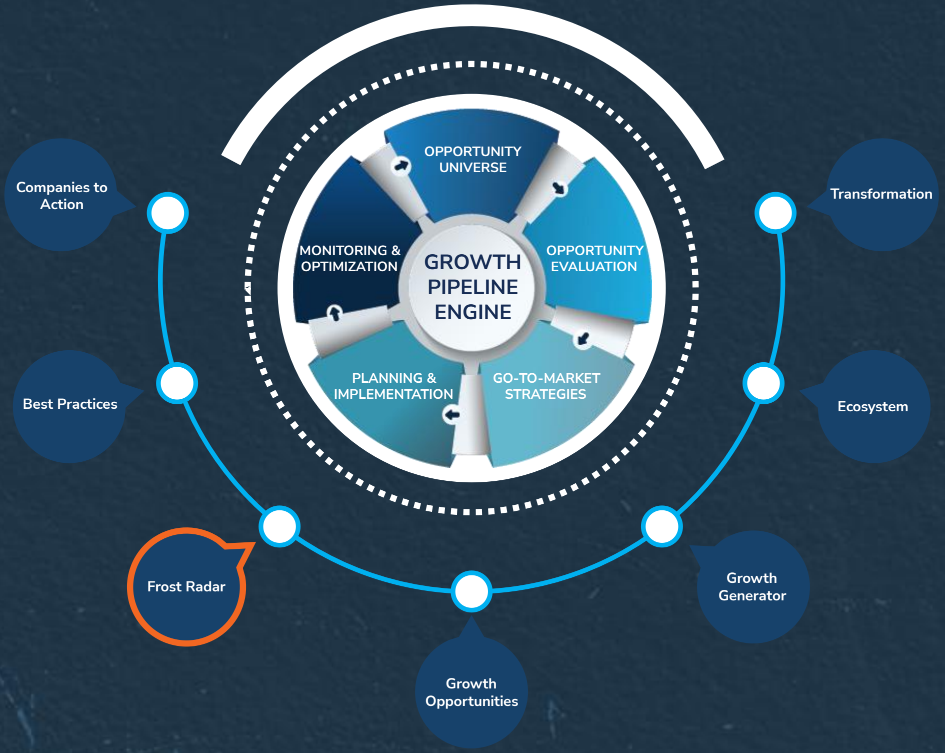
FROST & SULLIVAN

Frost Radar: Human Risk Management, 2024

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



MH62-74
December 2024

Strategic Imperative and Growth Environment

Strategic Imperative

- The human risk management (HRM) landscape is evolving rapidly as organizations face unprecedented challenges, including cybersecurity threats, remote work adaptation, and increasing employee well-being demands. This Frost Radar^{TM} is an essential benchmarking tool, identifying the industry's most innovative and impactful participants, highlighting what successful companies do to thrive in this dynamic environment, and offering insights into best practices.
- The industry is shifting from reactive risk management to proactive, employee-centric strategies. Disruptions, such as cyberattacks and hybrid work models, have pushed vendors to expand their offerings. Leaders now integrate advanced technologies, such as AI, for predictive analytics, automation for efficiency, and scalable platforms to meet diverse needs.
- To demonstrate leadership, companies must go beyond traditional solutions. This includes offering adaptive training modules, robust post-incident support, seamless integration with existing systems, and localized services to meet client-specific challenges and safeguard organizations’ most valuable asset: their people.
- By understanding the industry’s current state and the technologies shaping its future, readers will gain actionable insights into navigating and capitalizing on growth opportunities.

Source: Frost & Sullivan

Growth Environment

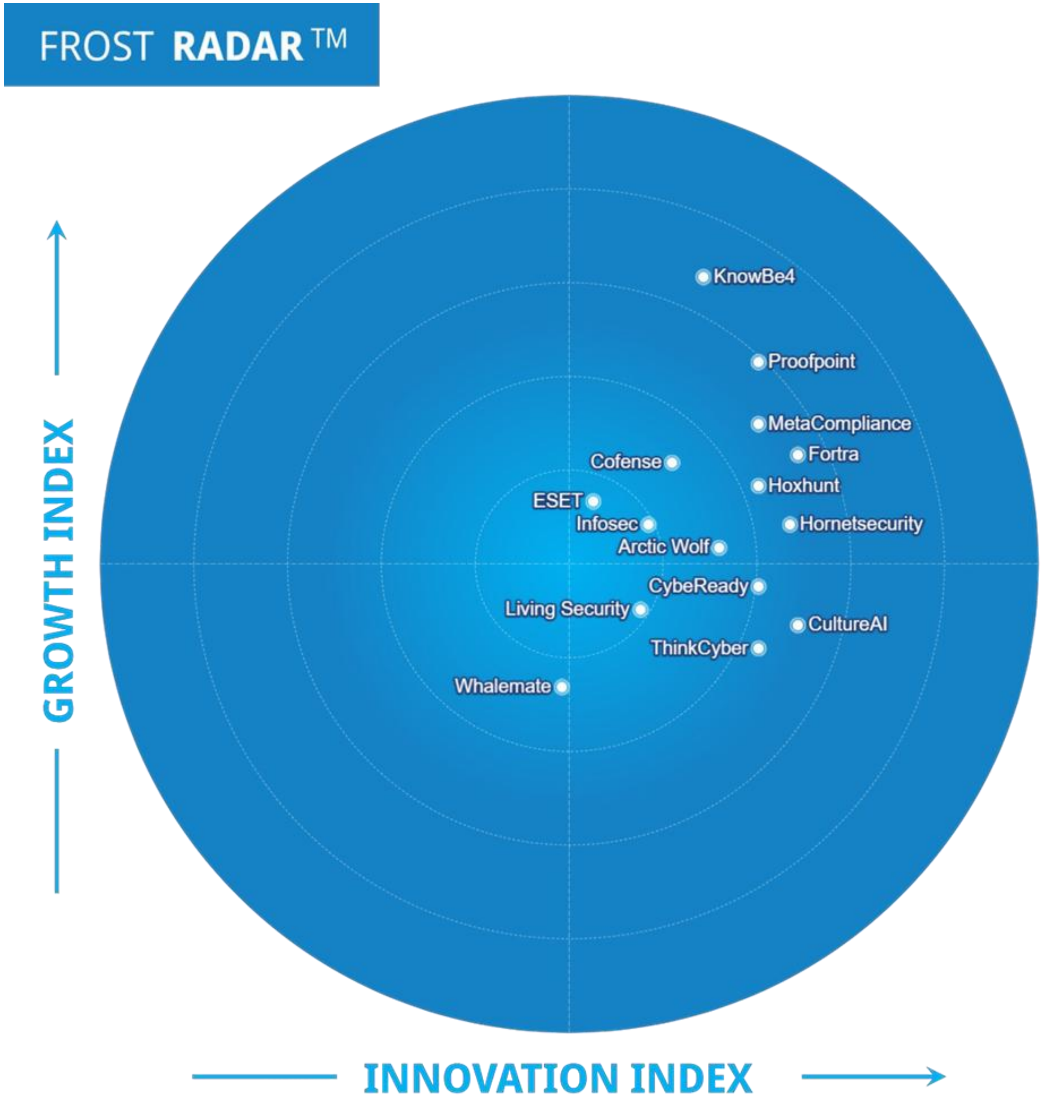
- The HRM market is growing rapidly, driven by the need to address cybersecurity threats, employee well-being, and compliance with complex regulations. With global revenues in the billions of dollars, the market is in a growth phase characterized by innovation and consolidation. Key offerings include training platforms, post-incident support, and AI-driven predictive analytics.
- The market is expected to grow significantly over the next few years due to the rise of hybrid work, increasing cyber threats, and heightened focus on employee engagement. Vendors are evolving from traditional risk management tools to holistic, scalable, and adaptive solutions.
- Vendors are developing diverse solutions to cater to varied client needs, emphasizing flexibility as a key success factor. Even small players are achieving remarkable innovation, challenging incumbents by offering tailored, niche solutions that resonate with specific market segments.
- Emerging technologies, such as machine learning, behavioral analytics, and advanced automation, disrupt the space, enabling proactive risk identification and response. These advancements redefine HRM by integrating seamless user experiences with predictive capabilities, shifting from reactive solutions to anticipatory strategies.
- Key trends include a focus on small and midsize business (SMB)-targeted solutions, integration of AI to improve training relevance and scalability, and investments in localized support. These developments are setting new benchmarks in addressing both technical and human aspects of risk, reshaping how organizations protect and empower their workforce.

Source: Frost & Sullivan

Frost Radar

Human Risk Management, 2024

Frost Radar: Human Risk Management, 2024



Source: Frost & Sullivan

Frost Radar Competitive Environment

- In a field of more than 80 industry participants globally, Frost & Sullivan selected, based on their performance and innovation, 15 players to benchmark in this Frost Radar™ analysis. With the growing demand for holistic HRM solutions, the industry has seen an influx of new entrants, offering diverse innovations to address evolving workplace needs and risks.
- Mergers and acquisitions have reshaped the HRM landscape over the past two to three years, driving consolidation and fostering strategic partnerships. These developments have accelerated the integration of advanced technologies, enhancing both the scalability and relevance of HRM platforms across diverse industries.
- The HRM industry has embraced significant innovation, focusing on user-centric design, behavioral insights, and automation to maximize employee engagement and risk mitigation. Vendors are expanding training coverage beyond traditional compliance to address emerging challenges, such as cybersecurity, mental health, and remote work adaptability. Higher investments in R&D and regional expansion enable vendors to provide tailored solutions that meet the needs of diverse organizational profiles and market dynamics.
- Arctic Wolf combines its expertise in managed detection and response (MDR) and HRM, leveraging tools, such as TruClick, for phishing defense and regional scalability to deliver highly relevant, real-time, and threat-aligned training solutions.
- Cofense leads the industry with its global phishing defense network, using adaptive simulations and the PhishMe Reporter to deliver behavior-driven, real-time threat intelligence tailored to customer needs.
- Culture AI pioneers real-time, AI-powered coaching that integrates with enterprise tools, such as Teams and Slack, using gamification and behavioral insights to redefine HRM in dynamic workplaces.

Source: Frost & Sullivan

Frost Radar Competitive Environment (continued)

- CybeReady focuses on localization and compliance training, offering adaptive modules in more than 40 languages and using data-driven insights to deliver targeted risk management for diverse employee profiles.
- ESET emphasizes phishing detection and compliance with gamified training solutions, providing role-based, accessible content designed to meet the needs of geographically dispersed organizations.
- Fortra combines predictive analytics with risk-based compliance training, creating a scalable HRM solution that integrates seamlessly into its broader cybersecurity suite for maximum impact.
- Hornetsecurity stands out with AI-driven user profiling, event-based training modules, and a robust phishing simulation framework, offering dynamic and seasonal relevance to meet evolving organizational threats.
- Hoxhunt differentiates itself with gamified phishing simulations and customizable learning paths, creating an engaging and effective training experience tailored to evolving threat landscapes.
- Infosec blends behavior-driven nudging with role-specific training to deliver dynamic, compliance-focused HRM solutions, integrating seamlessly with security operations center (SOC) tools to address real-time risks.
- KnowBe4 retains its leadership position with a diverse content library and a focus on human behavior and psychology, investing heavily to redefine adaptive training and cybersecurity awareness.
- Living Security transforms traditional HRM with gamified escape-room training and the Human Risk Index, combining AI-driven insights with integration across more than 50 platforms to deliver personalized, adaptive solutions.

Source: Frost & Sullivan

Frost Radar Competitive Environment (continued)

- MetaCompliance excels in compliance with its modular nano-video content, providing a scalable, highly accessible training solution tailored to regulatory requirements and role-specific needs.
- Proofpoint remains a leader in HRM by integrating adaptive learning paths and the DICE (Detect, Intervene, Change Behavior, and Evaluate) methodology, leveraging behavioral analytics to create highly aligned, real-world threat management solutions.
- ThinkCyber (Redflags) disrupts HRM training stereotypes by focusing on real-time, behavior-specific nudges, using contextual interventions to deliver practical and meaningful risk mitigation.
- Whalemate targets small-scale organizations with essential HRM tools, providing straightforward, no-frills training solutions for environments requiring minimal complexity and low investment.

Source: Frost & Sullivan

Frost Radar

Companies to Action

Hornetsecurity

INNOVATION

- Hornetsecurity is recognized as a leader in HRM. It delivers an AI-powered Security Awareness Service that provides automated, continuous training covering all types of attacks tailored to individual user behavior.
- Key innovations include sophisticated phishing simulations and targeted, on-demand micro-training sessions that elevate user engagement and real-world preparedness. Through the Employee Security Index (ESI), Hornetsecurity tracks and evaluates user progress, enabling dynamic adjustments to training intensity and content based on individual performance and evolving threat landscapes.
- Key innovations include:
  - **AI-driven user profiling:** Hornetsecurity's AI engine personalizes the learning experience, adjusting content, frequency, and difficulty to match each employee's needs and risk profile. This approach addresses user fatigue while enhancing engagement, ultimately improving learning outcomes.
  - **Realistic phishing simulations:** Using current events, Hornetsecurity's phishing simulations replicate genuine threats. By mirroring real-world attack vectors, such as seasonal scams or high-profile events, simulations are both timely and relevant, making users more adept at identifying and mitigating actual attacks.
  - **Dual layer of e-learning:** Hornetsecurity offers training on the fly when the user faces the threat. A user who succumbs to the simulation is then immediately taught at the "most teachable moment," which provides step-by-step training on how to better identify this kind of attack. This is in addition to the recurring and wide-ranging training delivered through videos and questionnaires.

Source: Frost & Sullivan

Hornetsecurity (continued)

INNOVATION

- **Event-based training:** Automated, event-specific training campaigns are initiated before critical periods (e.g., tax season, Black Friday), equipping employees with relevant skills to handle anticipated threats.
- **Integrated Security Hub:** The Security Hub centralizes all learning content, providing employees with convenient access to phishing simulations, e-learning modules, and security awareness resources. This centralized approach enhances both user experience and content accessibility.

Source: Frost & Sullivan

Hornetsecurity (continued)

GROWTH

- Hornetsecurity’s growth in the HRM market is driven by its comprehensive Security Awareness Service, which integrates with its broader cybersecurity suite. The solution’s adaptability to SMB and enterprise requirements has attracted a diverse client base, including organizations in highly regulated sectors, such as government and healthcare.
- Key growth drivers include:
  - **Bundled cybersecurity solutions:** Hornetsecurity’s suite includes email security, data loss prevention, backup solutions, and GRC, allowing clients to implement a layered defense strategy. Integration across solutions enhances HRM by providing contextual data that enriches training content and improves threat detection.
  - **Global expansion and channel partnerships:** Hornetsecurity leverages its worldwide partner network to extend its global reach into new markets, such as Latin America. By collaborating with managed service providers and channel partners, Hornetsecurity has amplified its market penetration, particularly in the SMB segment.
  - **Dedicated R&D for adaptive training:** With a commitment to research and development, Hornetsecurity continuously refines its AI engine to better detect, analyze, and respond to user behavior patterns, ensuring the training content remains relevant and effective. The training content is generated from real-life samples and scenarios, and the difficulty level is continuously fine-tuned always to prepare users for the future.

Source: Frost & Sullivan

Hornetsecurity (continued)

FROST PERSPECTIVE

- Hornetsecurity's HRM solution stands out with its combination of AI-driven automation, real-time training customization, and an integrated platform that simplifies deployment across various security functions.
- To further capitalize on its strengths, Frost & Sullivan suggests the following enhancements to maintain Hornetsecurity's leadership in the HRM space:
    - **Deeper integration of the ESI across the suite:** Expanding the use of ESI beyond security awareness to include interactions within email security, permission management, and DLP would enable more comprehensive risk scoring. This integration could provide administrators with a unified risk profile for each employee, drawing from a range of user actions and behavioral patterns.
    - **Event-specific, predictive training modules:** Hornetsecurity could build upon its event-based training by adding predictive modules that anticipate risks based on market trends. For instance, providing tailored training in response to new phishing tactics linked to major international events or emerging cyber trends would ensure timely user preparedness.
    - **Enhanced dashboard for visibility into user engagement:** Expanding the administrator dashboard to offer a more granular view of user engagement by content type, including drill-downs into specific phishing simulation types and training modules, would allow companies to better tailor their cybersecurity training strategies. This visibility could be precious for highly targeted departments, such as finance or HR, where a single breach has higher risk implications.

Source: Frost & Sullivan

Hornetsecurity (continued)

FROST PERSPECTIVE

- **Extended API support for cross-platform integration:** Given Hornetsecurity's commitment to a fully integrated platform, enhancing API support to facilitate data sharing with other security tools, such as SIEM or endpoint detection systems, would create a more holistic security posture. This would allow organizations to pull HRM data into broader risk management frameworks and receive a more unified view of threats.
- **Localization for emerging markets:** The solution is currently localized in 26 languages. To meet the demands of Hornetsecurity's expanding footprint in Latin America and APAC, prioritizing localized content in additional languages and adapting simulations and training materials to reflect region-specific threats would make the platform more impactful across diverse global teams.

Source: Frost & Sullivan

Best Practices & Growth Opportunities

Best Practices

1

Successful organizations prioritize their workforce's well-being, growth, and satisfaction. This includes offering tailored training programs, fostering inclusivity, and creating robust support systems to ensure that employees feel valued and empowered. Companies can cultivate a motivated and engaged workforce by aligning professional development opportunities with individual roles and aspirations.

2

Organizations must embed a culture of cybersecurity awareness to mitigate risks, especially as digital threats continue to evolve. Regular training and education programs should help employees recognize and respond to dangers like phishing and insider threats. A vigilant and informed workforce is imperative in safeguarding company assets and data.

3

Providing personalized development opportunities for employees while maintaining cost and operational efficiency is a persistent challenge. Companies must adopt innovative approaches to deliver tailored training and support systems that cater to diverse needs without overburdening HR teams or exceeding budgets.

Source: Frost & Sullivan

Growth Opportunities

1 Market leaders focus on post-incident training to help organizations recover and adapt after security breaches. Custom recovery plans, simulation exercises, and tailored support enhance resilience. They build trust and establish leadership in a competitive HRM landscape by providing continuous improvement programs and detailed documentation.

2 Companies leverage AI and machine learning to predict threats and automate responses. They invest in AI research and offer scalable, ethical solutions to stay ahead of technological shifts. By offering user-friendly, proactive risk management tools, they align with evolving customer needs and strengthen their market position.

3 Leaders provide SMBs with affordable, scalable HRM platforms tailored to their needs. Flexible pricing, bundled tools, and targeted training address SMB-specific threats. Collaborations for grants and subsidies make solutions accessible, empowering SMBs while bolstering trust and leadership in the global market.

Source: Frost & Sullivan

Frost Radar Analytics

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

Innovation Index

Innovation Index (II) is a measure of a company's ability to develop products/ services/ solutions (with a clear understanding of disruptive Mega Trends) 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

MEGA TRENDS 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 Mega Trends 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.

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

Source: Frost & Sullivan