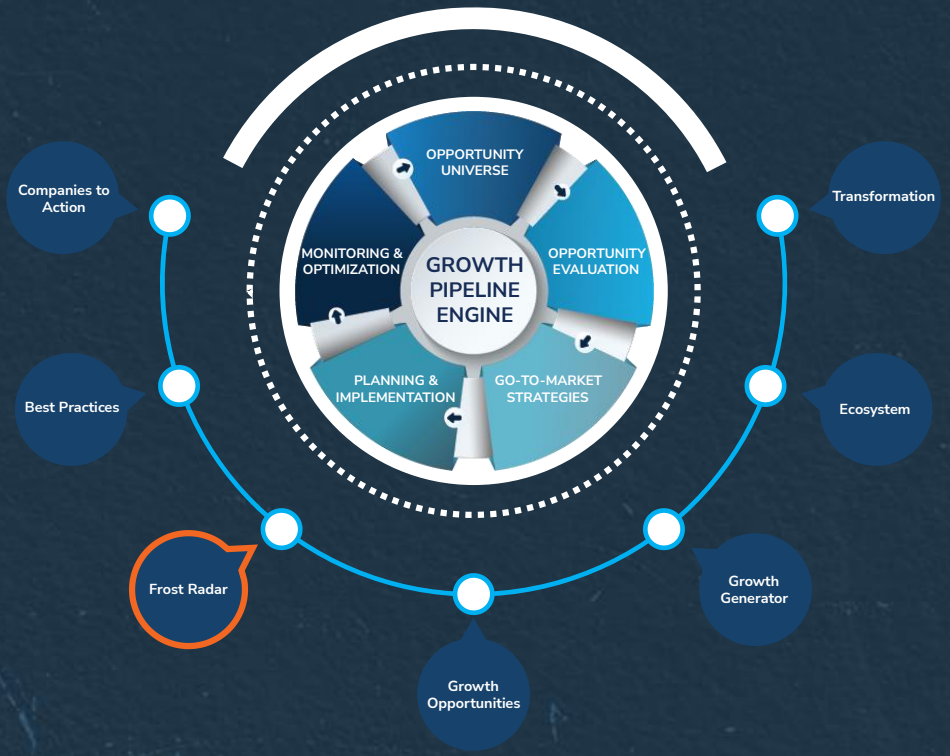
FROST & SULLIVAN

Frost Radar™: Network Detection and Response, 2026

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



Authored by: Keith Beizer
Contributor: Jarad Carleton

KCCD-74
October 2026

© 2026 Frost & Sullivan. All rights reserved. This document contains highly confidential information and is the sole property of Frost & Sullivan. No part of it may be circulated, quoted, copied, or otherwise reproduced without the written approval of Frost & Sullivan.

FROST & SULLIVAN

Strategic Imperative and Growth Environment



Strategic Imperative

- In an increasingly complex operating environment shaped by the adoption of artificial intelligence (AI) and lowered barriers to entry for threat actors, legacy cybersecurity infrastructure, including firewalls and intrusion detection systems (IDS), are unable to keep pace. While convenient with respect to costs and logistics, the proliferation of cloud and hybrid security stacks lengthens the exposure chain that enterprise security teams manage. Indeed, teams that lack full-spectrum visibility into their operating environment often fall short when threat actors use machine speed-enabled tools to move laterally within a network, exfiltrate data, and disrupt operations. This exemplifies the importance of network detection and response (NDR) solutions as the linchpin of security operations in the modern era, where most threats can be first detected along the network and empower security professionals to respond to alerts before they can erupt as an existential crisis.
- NDR solutions monitor network traffic across on-premises, cloud, and hybrid environments, using deep packet inspection, behavioral analytics, and machine learning to detect threats that evade traditional controls and accelerate investigation and response. By centering the network, NDR solutions can identify threats that evade traditional endpoint detection and response (EDR) and perimeter security solutions. As security teams around the world grapple with increasingly sophisticated threat actors, CISOs and key decision-makers have come to view NDR as the intelligence backbone of the security stack.
- The NDR industry continues to experience rapid evolution around the globe, typified by rigorous data security compliance standards, third-party supply chain risks, geopolitical upheaval, and increasing IT complexity. Diverse NDR solution providers have entered the market, ranging from pure-play vendors to AI security operations center (SOC) vendors that leverage NDR as an intelligence layer. The providers aim to empower organizations all along the maturity spectrum to proactively identify threats, address visibility gaps, and manage disparate, complex environments.

Source: Frost & Sullivan

Strategic Imperative (continued)

- To remain competitive and avoid being absorbed into larger, full-spectrum security solutions, pure-play NDR vendors must differentiate themselves based on unique use cases, such as historical data retention, deep visibility, encrypted traffic analysis, native integrations, investigations support, and automated response.
- At the same time, competition among pure-play vendors continues to intensify as tools such as Zeek, Suricata, VPC flow logs, and TLS fingerprinting enable upstarts in the market to bypass traditional approaches to data management and telemetry analysis. Taken together with AI-enhanced solutions, NDR market players are differentiating based on innovation and product efficiency as organizations look to combat tool sprawl while remaining as lean as possible.
- Regulatory frameworks, such as the European Union's NIS2 directive and revisions to China's Cybersecurity Law, delineate explicit data retention and information flow obligations that require deep visibility into the network—mandates that NDR solutions are uniquely capable of addressing. According to IBM's 2026 Cost of a Data Breach Report, the average cost of a data breach over the past year was $4.99 million, underscoring the need for proactive network monitoring and security solutions as the scope, speed, and scale of threats continue to escalate.
- Based on the current state of the NDR market and its anticipated trajectory, NDR solutions regardless of delivery model form an essential intelligence layer that drives effective threat identification, analysis, and response. NDR is a must-have security solution for organizations looking to remain competitively viable as AI democratizes cybersecurity threats and unlocks new nodes along the threat spectrum.

Source: Frost & Sullivan

Growth Environment

- NDR revenue globally for 2025 was approximately $3.66 billion and is projected to increase to $9.96 billion by 2030 at a compound annual growth rate of 22.2%. Contributing factors include an expanding attack surface, the growing sophistication of AI-powered threats, regulatory demands for proactive and comprehensive security measures, and third-party supply chain risks. Security solutions with limited visibility are proving insufficient as organizations continue investing in cloud and hybrid technologies, underscoring the need for solutions that center deep visibility and complex metadata analysis as part of their value proposition.
- North America is the largest and most mature market for NDR vendors because of the preponderance of large organizations with high security maturity and robust cybersecurity budgeting. However, as NDR continues to mature, North America's revenue percentage will decrease as adoption trends filter out around the world because of rising security maturity and the emergence of strict regulatory frameworks that NDR is uniquely capable of addressing. The region encompassing Europe, the Middle East, and Africa (EMEA) is the second-largest NDR market and Asia-Pacific is in third place. Latin America remains the smallest market by revenue, yet the region is expected to exhibit significant growth rates as businesses seek to nearshore supply chains away from challenging jurisdictions elsewhere in the world and minimize costs while maintaining a competitive advantage.
- Financial services, government, and healthcare are expected to remain among the most profitable verticals. Frost & Sullivan expects manufacturing, oil and gas, mining, retail, professional services, and education to experience significant growth, driven by the prevalence of advanced threats, such as targeted phishing campaigns, supply chain attacks, and vulnerabilities associated with the internet of things (IoT) and the increasing number of deployed IoT devices in end-user environments.

Source: Frost & Sullivan

Growth Environment (continued)

- To remain competitively viable, vendors must balance two existential points:
  - The NDR market is trending away from stand-alone offerings in favor of integrated platform approaches that bundle NDR with EDR, XDR, and SASE capabilities. As costs continue to rise, CISOs and other security officials responsible for budget oversight find it increasingly difficult to justify separate NDR line items when platforms offer consolidated solutions that lower costs.
  - Small and medium-sized businesses (SMBs) and specialized end users that are sensitive to ecosystem lock-in want flexible solutions that champion open integrations.
- Another distinction that vendors should be mindful of is whether NDR solutions can maintain visibility over unmanaged agents as AI continues to permeate through the market. NDR vendors that win the most business point to how their solutions enable high visibility into OT, medical devices, IoT, and agentic traffic. However, rapid advancements in AI have made full visibility increasingly difficult to achieve. Vendors that balance full visibility while keeping costs as low as possible will be best positioned to win new business and make their solutions integral components of daily workflows.
- Large organizations will continue to experience significant growth and remain the primary NDR customer base because of elevated risk profiles for cyber attacks, larger IT/security budgets, sensitive operations, and higher security maturity. In tandem with the democratization of cyber crime via AI, however, AI has also enabled NDR providers to market their solutions to SMBs via direct sales and indirect channel partners, including managed security service providers (MSSPs). A hybrid approach enables vendors to engage the full organizational size spectrum, marshal financial and human resources through a targeted lens, and democratize access to NDR in underserved markets.

Source: Frost & Sullivan

Growth Environment (continued)

- As globalization continues to drive NDR expansion, China-based vendors have looked to Latin America to drive overall revenue growth. The vendors employ a combination of direct sales, MSSP partnerships, and market education to build relationships and diversify revenue.
- Frost & Sullivan studies related to this independent analysis:
  - Global Network Detection and Response, 2026-2030 (KCCC, to be published soon)
  - Global AI Security Operations Centers, 2025-2028 (KC99, to be published soon)
  - Extended Detection and Response, Global, 2024–2027
  - Frost Radar™: Extended Detection and Response, 2024
  - Managed Detection and Response, Global, 2025–2028
  - Frost Radar™: Managed Detection and Response, 2025

Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™: Network Detection and Response



Frost Radar™: Network Detection and Response



About 35
qualified participants

18
selected

- **Inclusion Criteria:** Deep hybrid network visibility, AI-enabled product features, such as behavioral detection, encrypted-traffic analysis, open integration and telemetry correlation, and investigation and response enablement.
- **Exclusion Criteria:** Insufficient scale, weak differentiation, limited data transparency, limited evidence of growth potential, and insufficient innovation potential.
- **Evaluation Approach:** Global analysts; rigorous, fact-based methodology.
- **Benchmarking Methodology:** Proprietary framework delivering fair, consistent, global comparison.

Source: Frost & Sullivan

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 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 modest market presence and cautious strategies.
- Often new entrants or niche participants establishing their position.
- 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

- The global NDR market features a diverse array of vendors that each have different strategies, capabilities, approaches to innovation, and positioning. NDR solution providers have allocated an average of 32% of revenue to research and development (R&D) and 30% to marketing. The vendors featured in this Frost Radar™ analysis continue to leverage traditional tools, including security information and event management (SIEM); security orchestration, automation, and response (SOAR); endpoint detection and response (EDR); and extended detection and response (XDR), alongside innovations in AI to offer solutions capable of identifying and interdicting threats at machine speed.
- ThreatBook is on of our Frost Radar™ Visionary Leaders because of strong revenue streams, enterprise relationships in multiple industry verticals, and diverse product portfolios, all of which support NDR growth.

Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™: Companies to Action



VISIONARY LEADER

ThreatBook

INNOVATION

- Implemented via the Threat Detection Platform (TDP), ThreatBook's NDR solution features five primary layers: traffic ingestion and visibility, decryption, behavioral machine learning, intelligence correlation, and automated response. This structure enables full capture of north-south and east-west traffic; TLS fingerprinting to bypass network encryption; intelligence correlation via Advanced Threat Intelligence (ATI); implementation of automated response actions, such as TCP resets; and integration into an end user's existing SOC. ThreatBook can deploy TDP across on-premises, cloud, and hybrid environments, in addition to deployment as part of Managed NDR.
- ThreatBook's innovation process is driven by evolving threat intelligence and customer needs. The company continuously tracks emerging attack techniques, maps them to real-world customer environments, and develops AI-assisted minimal viable product (MVP) rollouts to address identified security gaps. ThreatBook validates new product features with customers through iterative feedback and implements them once the proposed features demonstrate a clear value proposition. By partnering closely with security-mature customers and prioritizing customer-centric validation, ThreatBook ensures that innovations deliver practical, measurable outcomes at scale. The company's R&D investments reflect its approach to continuous improvement and native product development.
- Product developments and system improvements from the past year reflect this approach to innovation. ThreatBook has introduced an early-stage AI governance feature, AI agents, integrations with AWS and other cloud platforms, and dynamic cloud asset identification, all of which is intended to help customers gain insight into their AI ecosystem and mitigate operational risks as AI and agentic workflows occupy a larger percentage of daily operations.

Source: Frost & Sullivan

VISIONARY LEADER

ThreatBook (continued)

GROWTH

- ThreatBook maintains robust revenue growth and pipeline alignment, scoring well on both metrics. The vendor's focus on large enterprises corresponds with its strengths with customers in energy and manufacturing. Typical customers have advanced security maturity, generous cybersecurity budgets, and complex network security environments.
- ThreatBook continues to do most of its business in Asia-Pacific, yet the vendor has made efforts to expand operations in EMEA and North America. It leverages strategic alliances with local partners, participation in industry events, and targeted outreach via social media and industry publications to initiate sales leads. For customers lacking a SIEM or SOAR, ThreatBook offers TDP to help build out the security operations, providing an additional growth driver.
- The messaging that underpins ThreatBook's growth strategy stresses a shift toward an agentic-first security approach that enables a fusion of the vendor's NDR solution and its threat intelligence platform. Such an approach facilitates customer base consolidation and unlocks lucrative cross-selling opportunities, especially with OT customers.

Source: Frost & Sullivan

VISIONARY LEADER

ThreatBook (continued)

FROST PERSPECTIVE

- ThreatBook's NDR thesis emphasizes the flexibility of TDP and its position as a functional intelligence layer for the vendor's push toward a unified, AI-driven agentic product ecosystem. TDP's strengths in hybrid deployment and open integration allow ThreatBook to innovate its own ecosystem and its growing list of strategic alliances.
- ThreatBook can improve its standing on the Frost Radar™ Innovation Index if it increases its R&D investment to support efforts to integrate AI into product workflows. The vendor's incorporation of advanced UEBA can strengthen native detection and behavioral baselining, especially as it seeks to become an agentic security operations platform.
- Despite expanding its presence in Asia-Pacific through new offices in Singapore and Hong Kong, limited expansion into North America, Latin America, and EMEA precludes a higher standing on the Growth Index. To achieve success in Latin America, where the customer base has a lower average security maturity than a typical ThreatBook customer, the vendor should simplify its product offerings. At the same time, Latin America and EMEA pose fewer geopolitical challenges for ThreatBook than North America. GTM efforts in these regions should stress local partnerships and leverage distributors to ensure solid customer footing before expanding direct sales.

Source: Frost & Sullivan

FROST & SULLIVAN

Best Practices & Growth Opportunities



Best Practices

1. Strengthen cloud-native deployments to support an increasingly diverse group of end users that want visibility into OT and IoT operating environments. Third-party interoperability is also important to end users that want unified telemetry while reducing their dependency on physical systems. Doing so enables enhanced alignment with NDR market trends and a stronger innovation scalability proposition.

2. Expand beyond the traditional cybersecurity revenue centers of North America and EMEA to target underserved regions, and prioritize high-growth verticals, such as energy and manufacturing. Resilient product portfolios support medium- and long-term growth while insulating vendors from vertical-specific demand shocks. Such a framework strengthens market share, bolsters revenue growth, and demonstrates a long-term revenue generation strategy.

3. Increase R&D investment and align product development with a clearly defined roadmap. Vendors should prioritize open integrations, cloud-native capabilities, AI automation, identity security, and OT/IoT visibility. Operationalizing these priorities can strengthen innovation scalability and customer alignment.

Source: Frost & Sullivan

Growth Opportunities

1. Channel-friendly NDR offerings can help vendors address customer pain points, such as deployment complexity and trust, while strengthening the NDR value proposition. NDR vendors can help the channel-led ecosystem provide technical training and sales support so that business development professionals can effectively communicate the merits of NDR to new customers, enabling sustained competitive viability in an increasingly crowded market.

2. Stand-alone NDR vendors can mitigate commoditization risks by prioritizing investment in use cases where NDR addresses the unique visibility, compliance, and threat detection requirements of highly regulated verticals, such as healthcare and financial services. NDR providers must expand the ability to cover emerging attack surfaces associated with cloud adoption, digital transformation, OT, and distributed environments.

3. Effective investment in AI-powered NDR solutions can provide organizations with a more complete understanding of their network activity and reduce blind spots that attackers may exploit. NDR vendors must close the maturity gap by demonstrating clear business outcomes, including accelerated threat remediation and improved cyber resilience.

Source: Frost & Sullivan

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 (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.

Source: Frost & Sullivan

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

© 2026 Frost & Sullivan. All rights reserved. This document contains highly confidential information and is the sole property of Frost & Sullivan. No part of it may be circulated, quoted, copied, or otherwise reproduced without the written approval of Frost & Sullivan.