pharosIQ

Cybersecurity Software Market Trends Report 2025

pharosIQ

Table of Contents

About Us

pharosIQ's industry insight reports are the definitive source for data-driven buyer intelligence and market trends. Analyzing down-funnel content consumption across multiple industries through our signals engine, we provide executives and senior managers in technology, financial services, manufacturing, marketing, and sales with actionable intelligence and comprehensive understanding of market and buyer dynamics.

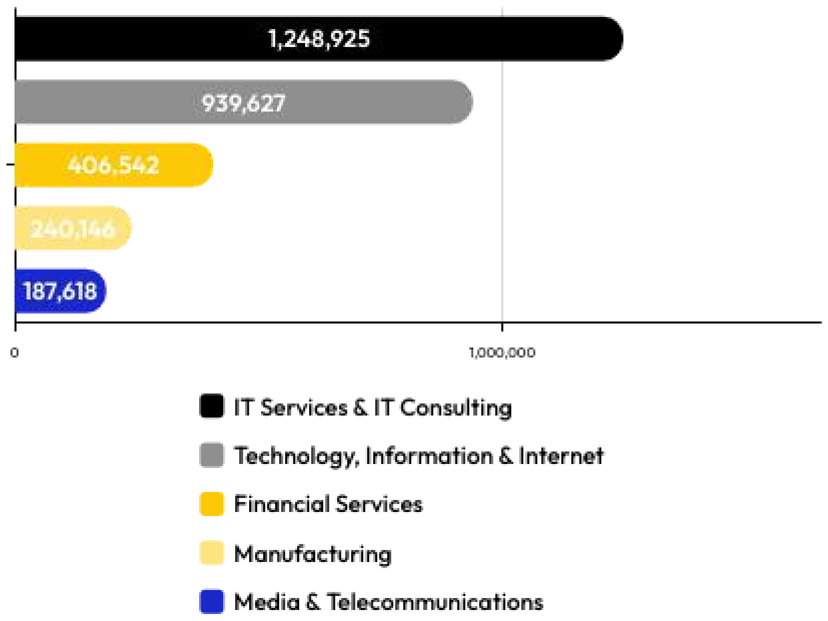
pharosIQ is a leading global provider of first-party engagement-driven lead generation solutions, delivering essential insights and demand for B2B organizations' sales and marketing success. With over four decades of expertise, pharosIQ converts proprietary intelligence into impactful engagements, connecting B2B software and services vendors with in-market buyers, transforming sales and marketing strategies worldwide.

Introduction

At pharosIQ, we don't make predictions—we track real buyer behavior to understand where the market is headed. Instead of speculation, we analyze content consumption patterns and engagement data to identify cybersecurity solutions buyers are actively researching. By examining over 21 million real-time interactions with cybersecurity software and solutions across the last 12 months, we provide a data-driven forecast of where organizations are looking to make investments. Below is a summary of key engagement categories, enabling further filtering and analysis of market demand.

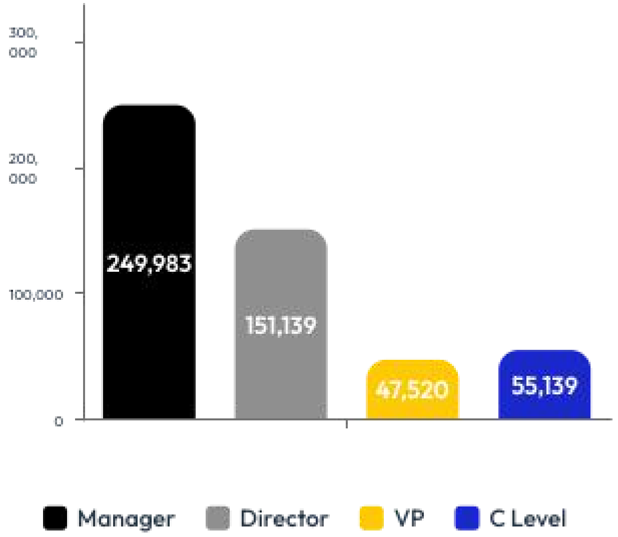
Industry Engagement

Cybersecurity Topical Engagement By Industry



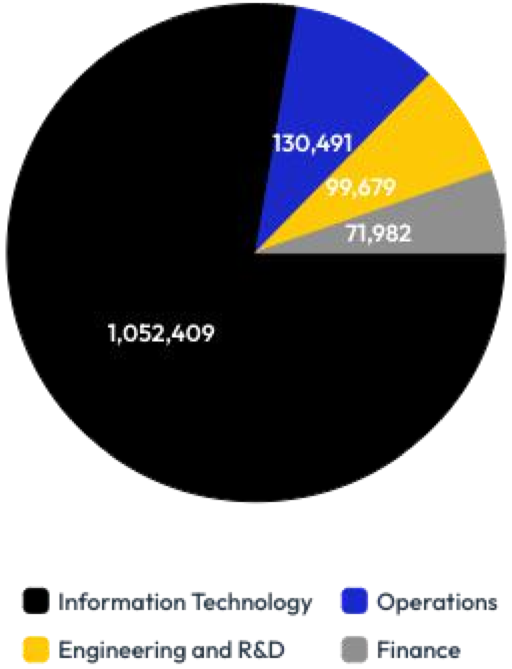
Seniority Engagement

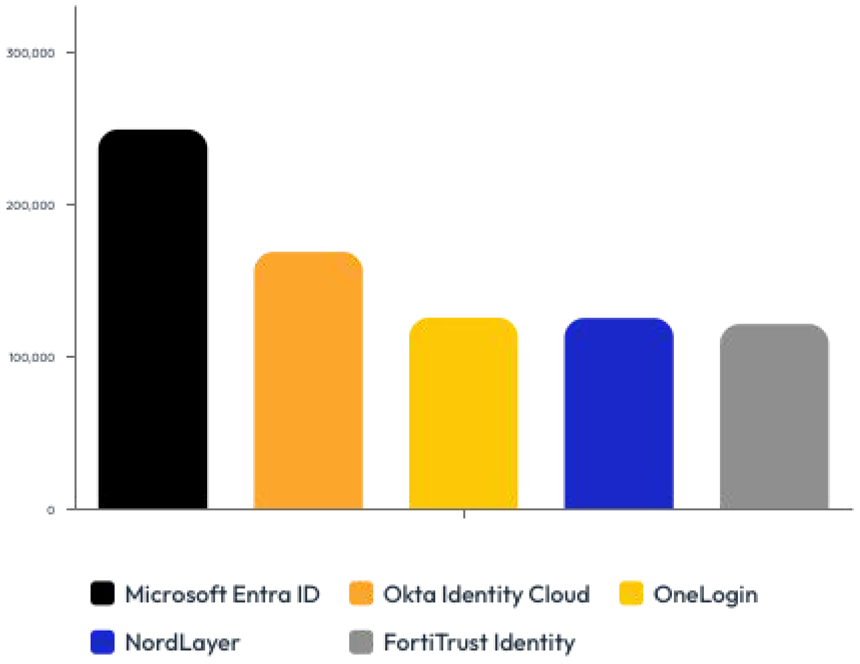
Cybersecurity Engagement By Seniority Level



Functional Engagement

Cybersecurity Engagement By Job Function





Performance by Product

Top Vendor/Products Generating Engagement Across Last 12 Months

Market Demand for Multi-Cloud Identity Management Solutions Surges

The importance of robust identity management has never been clearer. Despite economic pressures, only 11% of organizations are considering reducing their identity management budgets next year. With identity sprawl, the number of identities organizations manage continues to grow. Phishing attempts account for almost two-thirds of identity-related incidents. According to the Identity Defined Security Alliance (IDSA), an astonishing 84% of identity stakeholders said identity-related incidents directly impacted their business this year, up from 68% in 2023, and security outcomes remain a work in progress.

This trend of increasing priority is a positive recognition of the importance of identity. Our analysis reports over 800,000 bottom of funnel engagements with identity management research reports and case studies in the last 12 months, further supported by the consumption of peer review and price comparison guides related to the products in the chart opposite.

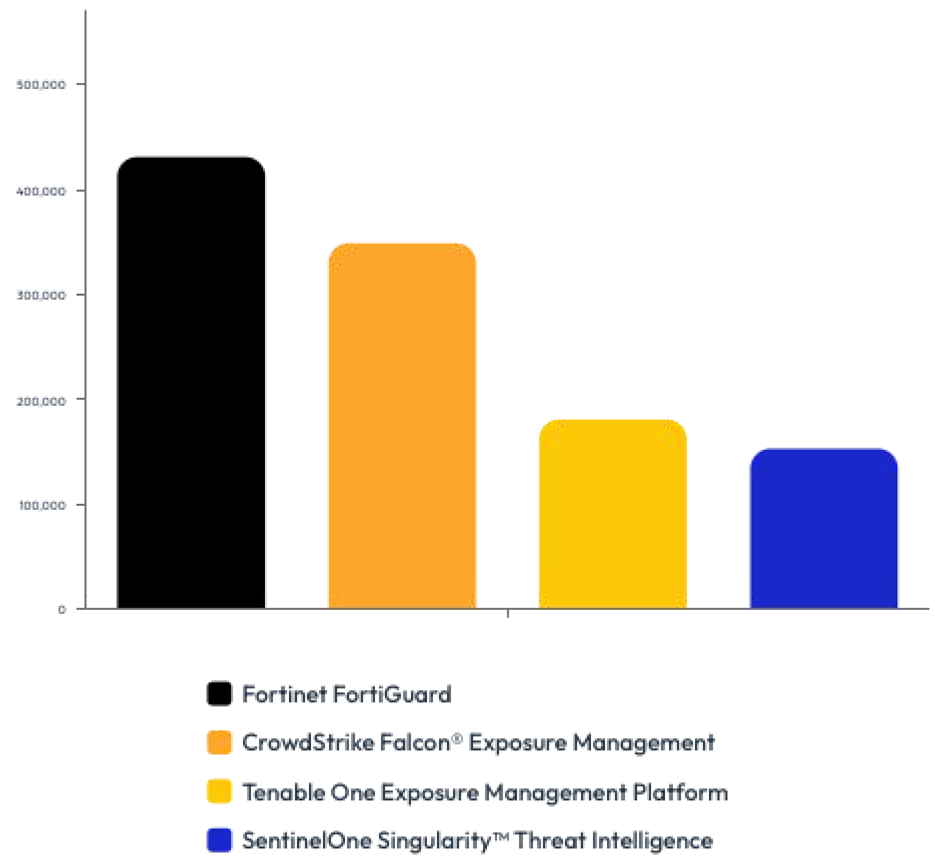
CTEM Gains Momentum as the Future of Cybersecurity

As cyberattacks grow more sophisticated and frequent, the need for real-time threat detection and response has never been more urgent. Organizations face a critical challenge: they cannot patch every exposure and often struggle to prioritize the most critical vulnerabilities despite having well-curated issue lists. This has created a pressing need for a paradigm shift in how cybersecurity is approached—moving from reactive measures to proactive, continuous assessment.

In 2024, CTEM has emerged as a critical cybersecurity trend, empowering organizations to stay ahead of attackers by continuously assessing, monitoring, and managing threats in real time. Our analysis reports over 1.1 million bottom of funnel engagements with CTEM research reports and case studies in the last 12 months, further supported by the consumption of peer review and price comparison guides related to the products in the chart opposite.

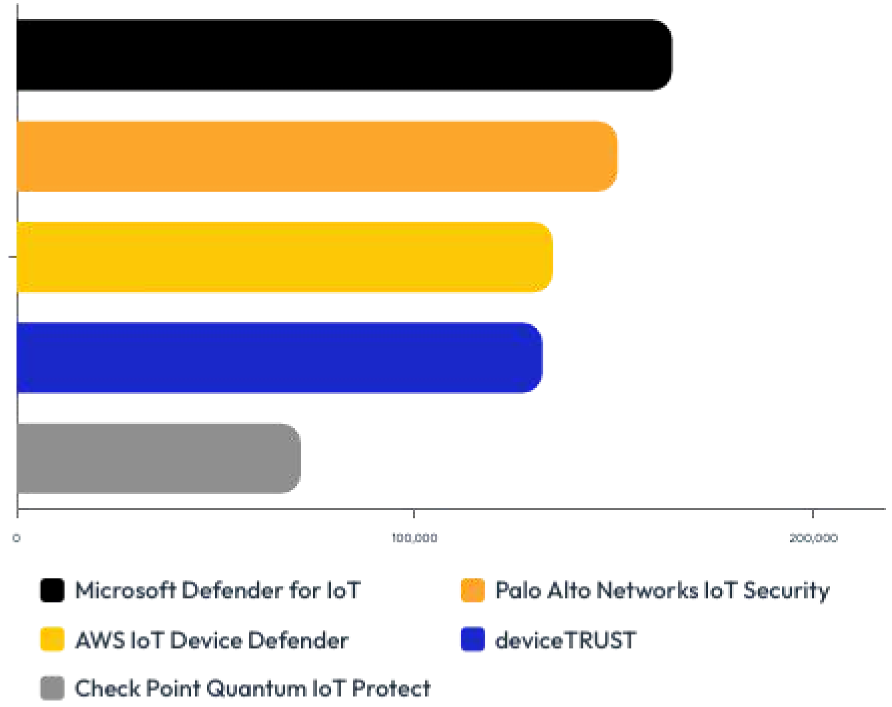
Performance by Product

Top Vendor/Products Generating Engagement Across Last 12 Months



Performance by Product

Top Vendor/Products Generating Engagement Across Last 12 Months



Industry Shifts Toward Securing the IoT Ecosystem

The rapid adoption of IoT has revolutionized enterprise operations, serving as a critical business enabler. However, it has also introduced unprecedented security challenges. With IoT devices now accounting for over 30% of all network-connected enterprise endpoints—and global IoT devices projected to exceed 30 billion by 2025—traditional network defenses and legacy processes are no longer sufficient. As enterprises increasingly migrate to multi-cloud environments, security leaders must adopt a comprehensive IoT lifecycle approach to address these risks. This strategy combines scalable, secure cloud storage with advanced tools to monitor, configure, and protect IoT ecosystems.

Recent research reveals a significant shift toward this holistic approach, with our analysis reporting over 650,000 bottom of funnel engagements with IoT security solution guides and case studies in the last 12 months, further supported by the consumption of peer review and industry reports related to the products in the chart opposite.

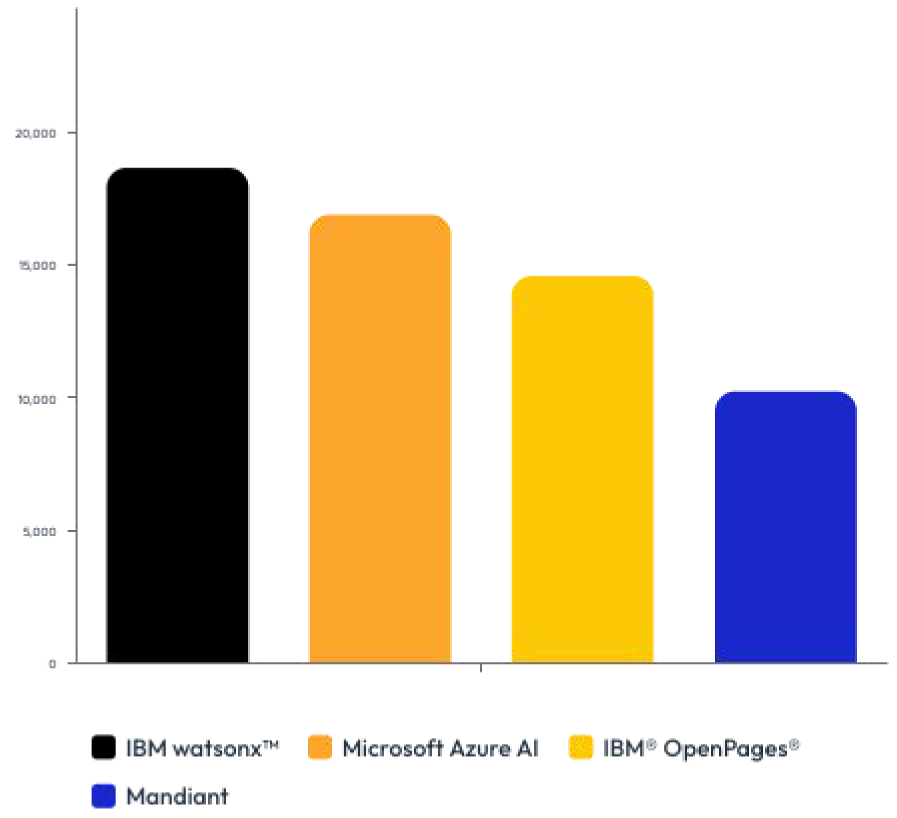
Rising AI Misuse Drives Market Concern Over Data Breach Risks

AI continues to transform the threat landscape, enabling highly sophisticated and scalable attacks. Advanced AI tools will allow malicious actors to generate complex malware from a single prompt, lowering barriers to entry and creating threats that outpace traditional defenses. Simultaneously, improper use of AI tools within organizations continues to increase risks, as employees inadvertently expose sensitive data through platforms like ChatGPT or Google Gemini. To address these challenges, organizations must implement stricter controls on AI usage, balancing productivity with robust data protection and privacy measures.

In response to these challenges, 2025 will also see the rise of AI governance platforms designed to ensure transparency, trust, and regulatory compliance. As new AI regulations come into effect, enterprises will be pushed to adopt frameworks that provide oversight and accountability for their AI tools and processes. Our analysis reports over 60,000 bottom of funnel engagements with AI governance research reports and case studies in the last 12 months, further supported by the consumption of peer review and price comparison guides related to the products in the chart opposite.

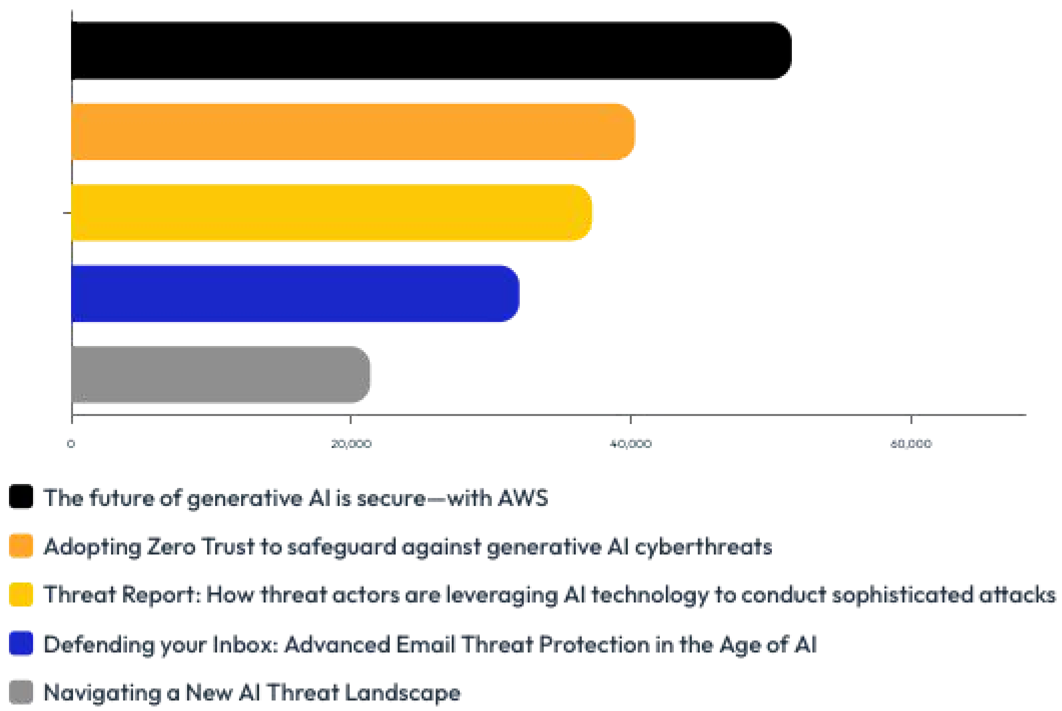
Performance by Product

Top Vendor/Products Generating Engagement Across Last 12 Months



Performance by Asset

Top Assets Generating Engagement Across Last 12 Months



CIOs Face Growing Pressure to Lead AI Integration Efforts

The role of the Chief Information Security Officer (CISO) will face increasing challenges driven by rapid AI adoption, hybrid-cloud environments, and heightened regulatory demands. CISOs will need to balance innovation with secure-by-design implementations, often navigating tensions between speed and security, particularly as AI-related data breaches become more prevalent. They must also translate complex technological risks into business terms for leadership while managing security across hybrid-cloud infrastructures. To address evolving threats, CISOs and CIOs must align priorities, integrating security objectives into every stage of technology deployment, from IT and IoT to AI.

This trend of adapting priorities is a positive recognition of the importance of identity. Our analysis reports over 180,000 CISO and CIO engagements with bottom of funnel reports and case studies in the last 6 months, further supported by the consumption of best practice guides related to proactively addressing potential vulnerabilities, and implementing security measures relating to AI technologies.

Conclusion

The evolving threat landscape underscores the critical importance of robust identity management, proactive cybersecurity strategies, and comprehensive governance frameworks. As organizations face increasing challenges from identity sprawl, sophisticated phishing attacks, AI-enabled cyber threats, and the rapid adoption of IoT and hybrid-cloud environments, the need for innovation in security practices has never been greater.

This reflects a growing recognition among security leaders that reactive approaches are no longer sufficient. Instead, enterprises are shifting toward proactive, continuous assessment and alignment of security objectives across all levels of technology deployment. As 2025 approaches, the rise of AI governance platforms, secure-by-design strategies, and a holistic approach to managing IoT and hybrid-cloud environments will become essential. By prioritizing real-time threat detection, robust data privacy measures, and cross-functional collaboration, organizations can navigate these challenges effectively, ensuring resilience and readiness in an increasingly complex digital landscape.

Distinctly Different. Strategically Smarter.

We're more than intent data. Or leads. B2B marketing that actually engages the way buyers want.

www.pharosIQ.com/

www.linkedin.com/company/pharosiq/

marketing@pharosIQ.com