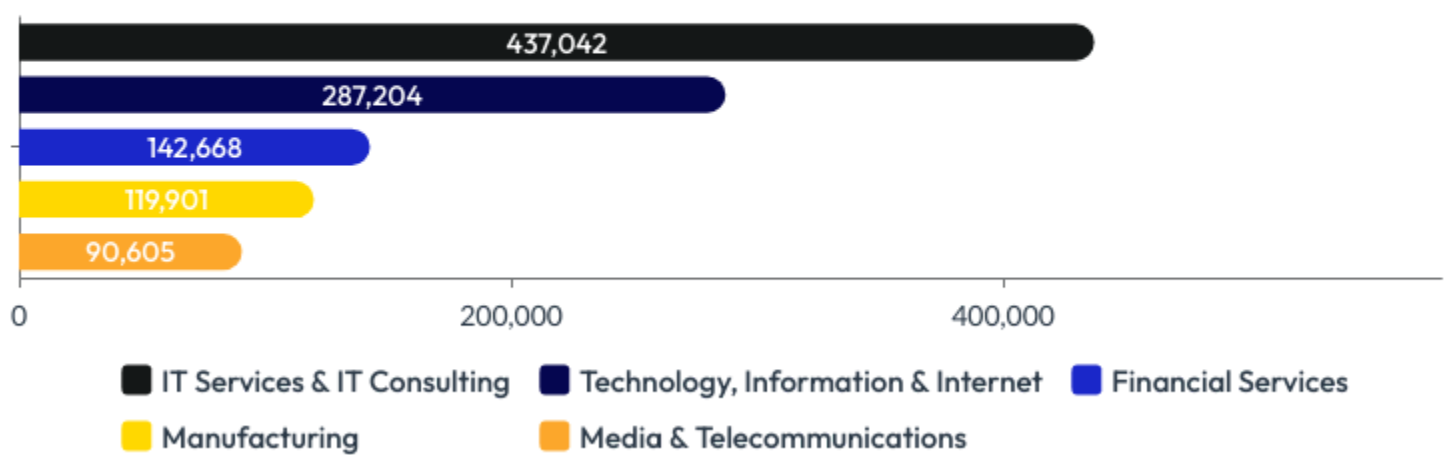# Lighthouse Labs
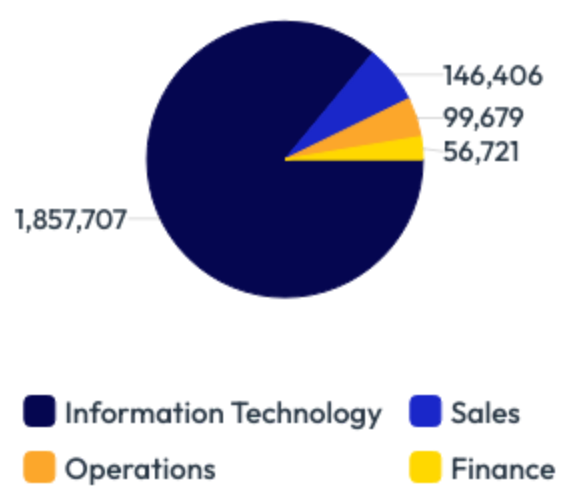## CyberSecurity Software Trends
July 2024

Overview

As the cybersecurity landscape continues to evolve, Lighthouse Labs have analyzed down funnel content consumption and engagements relating to security software and solutions. Summarized below is the basic categorization data collected about engagements to enable filtering and analysis of the data.
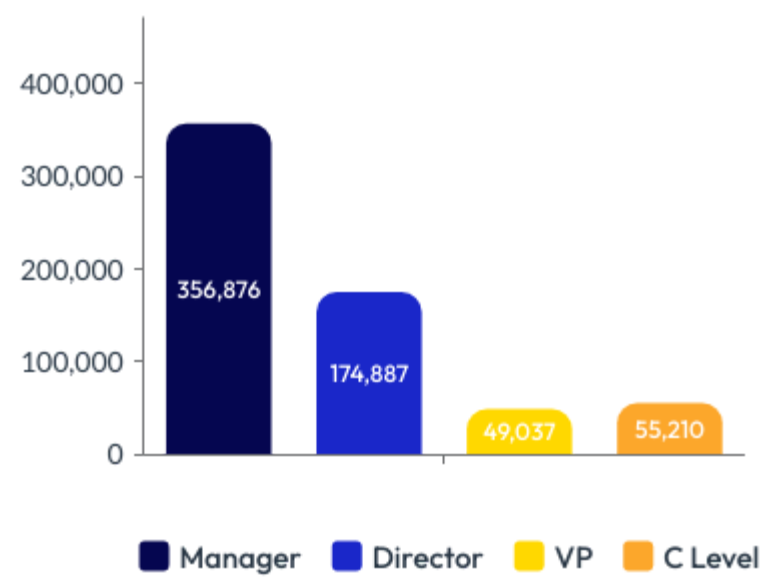
Industry Engagement
Cybersecurity Engagement By Industry

- IT Services & IT Consulting: 437,042
- Technology, Information & Internet: 287,204
- Financial Services: 142,668
- Manufacturing: 119,901
- Media & Telecommunications: 90,605

Functional Engagement
Cybersecurity Engagement By Function

- Information Technology: 1,857,707
- Sales: 146,406
- Operations: 99,679
- Finance: 56,721

Seniority Engagement
Cybersecurity Engagement By Seniority Level

- Manager: 356,876
- Director: 174,887
- VP: 49,037
- C Level: 55,210

Leveraging atlasIQ, this trend report utilizes these data-backed insights to identify crucial advancements in four strategic areas driving cybersecurity solutions: artificial intelligence, identity and access management, continuous threat management and, privacy-driven application decoupling.

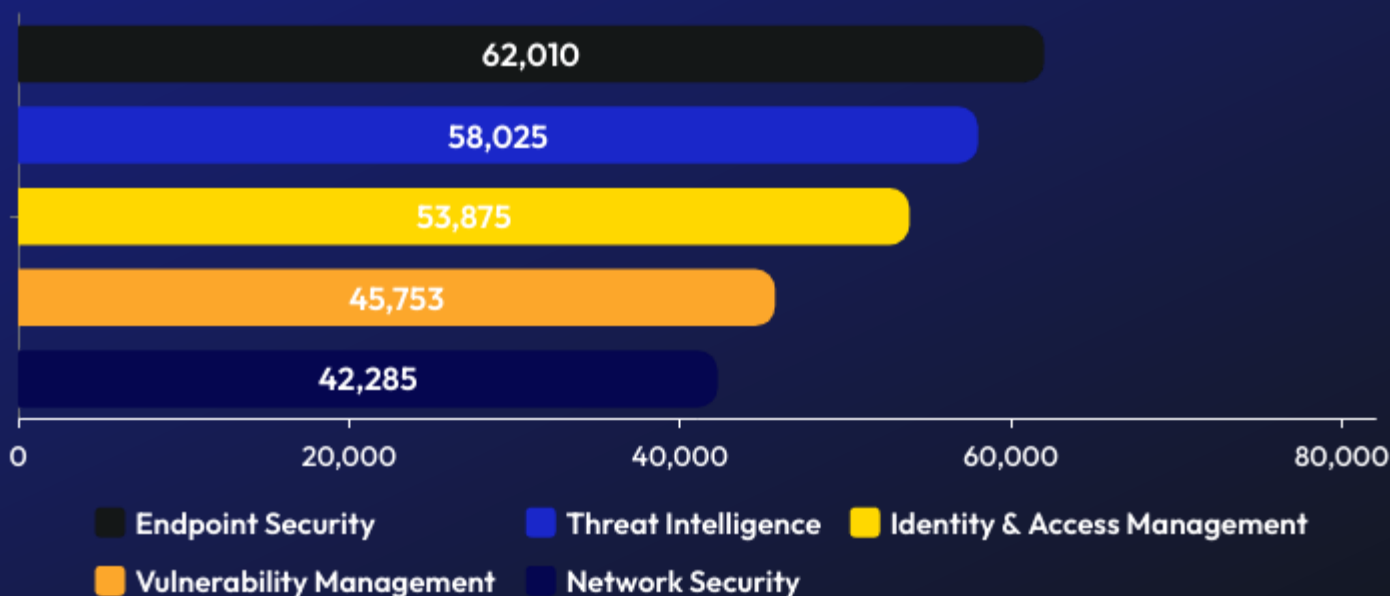pharosIQ

Cybersecurity and AI

Enabling security while managing risk.

AI is revolutionizing cybersecurity by improving threat detection, automating security operations, enhancing user authentication and providing advanced analytics capabilities. According to a survey by Darktrace, nearly 53% of organizations are in the early stages of AI adoption, while 18% are at advanced stages.

Our analysis reports over 385,000 engagements with research reports and case studies related to AI-driven technologies within cybersecurity over the last 6 months. Key themes from the most popular research formats suggest cybersecurity leaders are preparing for swift AI adoption and evolution within the business, resulting in a surge in engagement within the following areas of focus:

Engagement by Area of Focus
Top Areas of Engagement Across Last 6 Months

Area	Engagement
Endpoint Security	62,010
Threat Intelligence	58,025
Identity & Access Management	53,875
Vulnerability Management	45,753
Network Security	42,285

Legend:
- Endpoint Security
- Threat Intelligence
- Identity & Access Management
- Vulnerability Management
- Network Security
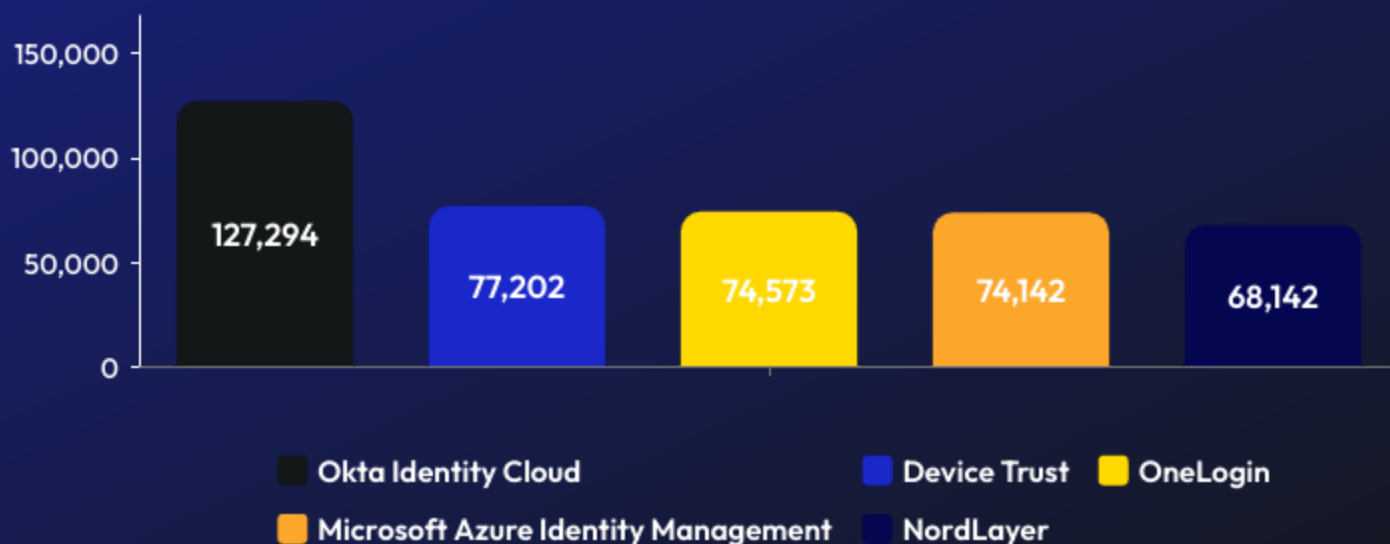
Identity & Access Management (IAM)

Evolving identity and access management.

Attacks targeting identity infrastructure are increasingly common, making identity-first security a critical focus for cyber teams. Consequently, cybersecurity leaders are shifting their emphasis from traditional network security to identity and access management (IAM). This shift necessitates evolving organizational practices to enhance identity hygiene, and developing the identity infrastructure towards a more integrated identity fabric architecture.

Our analysis reports over 400,000 bottom of funnel engagements with research reports and case studies relating exclusively to identity and access management over the last 6 months.s This engagement has also been supported by the consumption of peer review and price comparison guides related to the following products:

Performance by Product

Top Vendor/Products Generating Engagement Across Last 6 Months

Product	Engagement
Okta Identity Cloud	127,294
Device Trust	77,202
OneLogin	74,573
Microsoft Azure Identity Management	74,142
NordLayer	68,142

Legend:
- ■ Okta Identity Cloud
- ■ Device Trust
- ■ OneLogin
- ■ Microsoft Azure Identity Management
- ■ NordLayer

Risk-Based Approach to Threat Management

Continuous threat exposure management.

The expansion of digital attack surfaces has increased potential exposures from both self-managed technology vulnerabilities and cloud-driven applications. Traditional cybersecurity models that focus on patching and securing physical and self-managed software systems are no longer sufficient in today's complex environment.

In response, security and risk teams are now adopting continuous threat exposure management (CTEM), focused on prioritizing and continuously improving the organization's security posture. Our analysis reports over 500,000 engagements with case studies and peer review guides related to the following threat exposure management products:

Performance by Product
Top Vendor/Products Generating Engagement Across Last 6 Months

Product	Engagement
Cisco Umbrella	152,764
CrowdStrike Falcon® Exposure Management	135,843
Tenable One Exposure Management Platform	123,158
SonicWall Capture ATP	92,883
Fortinet FortiGuard	83,082

**Lighthouse Labs: Cybersecurity Trends,
July 2024 Edition**

Privacy-Driven Application & Data Decoupling

Enhancing organizational resilience amid growing risk.

Security and risk management leaders are now responsible for enhancing organizational resilience amid growing risks. With increasing global enforcement of privacy, data protection, and localization requirements, forward-thinking organizations must prioritize investments in resilience. This involves rethinking compliance processes, data migration and integration practices, and data architecture and storage to adapt to evolving regulatory landscapes.

Driven by increasing data protection and localization requirements, key themes from our most popular research formats within the last 6 months have demonstrated over 100,000 bottom of funnel engagements relative to restructuring enterprise application architectures and data architecture:

Key Themes
Engagement By Themes From High Performing Content

Theme	Engagement
Enterprise Application Restructuring	102,761
IT Operating Model Update	42,274
Modernize Legacy Systems	24,262
Application Data Transformation	20,309
Application Modernization,	16,899

Legend:
- Enterprise Application Restructuring
- IT Operating Model Update
- Modernize Legacy Systems
- Application Data Transformation
- Application Modernization,

Lighthouse Labs: Cybersecurity Trends, July 2024 Edition

This Lighthouse Labs Trends Report underscores the pivotal advancements and strategic areas that are shaping the future of cybersecurity. As the landscape continues to evolve, these trends provide a roadmap for organizations to balance the need to mitigate risk with the imperative to drive digital.

Digital technology initiatives remain at the top of the CEO's priority list, altering the operational landscape for cybersecurity leaders and driving investments to enhance security team resilience and performance. By adopting these trends, cybersecurity leaders can understand why the need for more agile and responsive cybersecurity programs is paramount. This approach allows them to better navigate the evolving challenges and demands of the cybersecurity landscape.

pharosIQ

Lighthouse Labs

Lighthouse Labs, powered by pharosIQ, is the definitive source for data-driven insights and industry trends. By analyzing down-funnel content consumption across multiple industries, we provide executives and senior managers in technology, financial services, manufacturing, marketing, and sales with actionable intelligence and comprehensive understanding of market dynamics.

pharosIQ

pharosIQ is a leading global provider of "intent-to-purchase" signal-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, driving global revenue efficiently. Powered by first-party audience engagement data, pharosIQ connects B2B software and services vendors with in-market buyers, transforming sales and marketing strategies worldwide.

For more information visit pharosIQ.com