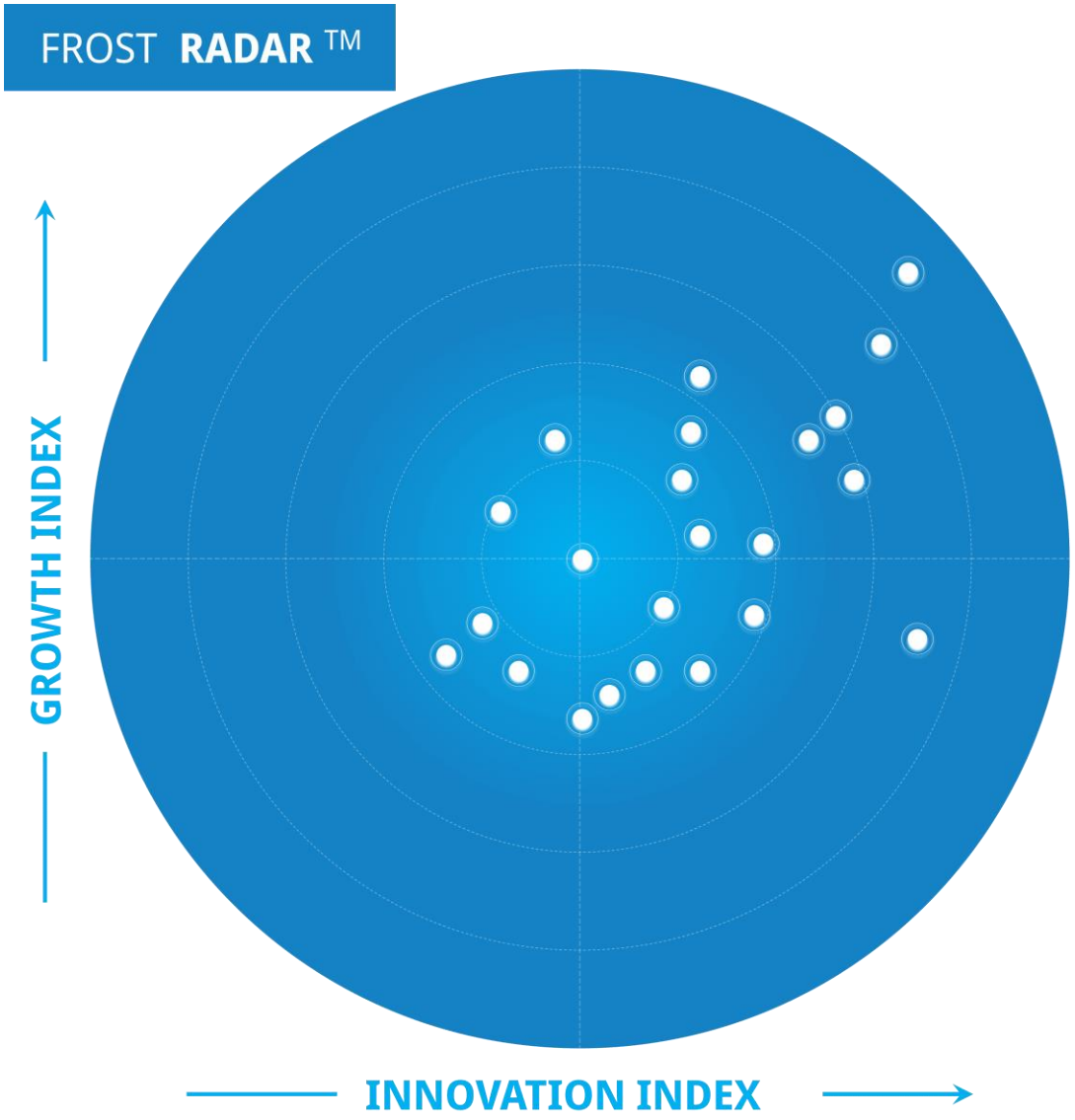
Frost Radar™

Cyber Threat Intelligence, 2024

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

Authored by
Martin Naydenov



KA5F-74
July 2024

Table of Contents

Frost Radar™ Summary

Market Phase	Base Year	Radar Type
Growth Phase	2023	Industry

Tags
cybersecurity, cyber threat intelligence, threat intelligence, Digital risk protection, ERMM, external attack surface management, CTI, DRP, easm

Market Analysis

Research Summary

The modern threat landscape has undergone a profound transformation, driven by the global push toward digitalization. This has led to expanded attack surfaces, heightened IT complexity, and increased risks in supply chains. Today, threat actors launch multivector attacks that target organizations' internal networks and their external digital assets, such as social media accounts and third-party applications. Consequently, organizations have ramped up their cybersecurity spending and adopted an array of tools to mitigate risks. The efficacy of these measures depends on whether organizations have a deep understanding of the modern threat landscape.

Actionable threat intelligence (TI) plays a pivotal role in cybersecurity, serving as the foundation for informed decisions and a robust security posture. In essence, TI encompasses actionable information about threats targeting an organization. The conventional TI ecosystem comprises 4 primary areas: cyber threat intelligence (CTI), threat intelligence platforms (TIP), external attack surface management (EASM), and digital risk protection (DRP), each serving distinct purposes.

CTI solutions gather data from diverse sources, such as open-source intelligence and the dark web, to provide insights into cyber threats. They offer commercial TI feeds containing indicators of compromise (IOCs) and comprehensive intelligence reports. Threat intelligence platforms (TIP) offer a collaborative interface to operationalize TI, streamlining data collection, aggregation, and organization. DRP solutions specialize in brand and phishing protection, identifying potential risks to an organization's external digital assets, and threat remediation. EASM solutions aid organizations in mapping their digital footprints, inventorying digital assets, and quantifying risk exposure to prioritize threats effectively.

As the cybersecurity landscape evolves and TI vendors try to remain competitive, traditional TI point solutions are consolidated into integrated security platforms. This convergence is giving rise to 2 main developments: the emergence of unified external risk mitigation and management (ERMM) platforms that include CTI, EASM, and DRP functionalities; and the transition of TIP providers into comprehensive security operations (SecOps) platforms that integrate security information and event management and security orchestration, automation, and response capabilities serving as centralized security control towers. Still, confusion persists because of overlapping capabilities and vendor terminologies.

Nonetheless, the TI market is poised for substantial growth, with North America and Europe, the Middle East, and Africa (EMEA) leading in terms of revenue size, driven by the presence of large enterprises with mature security postures and substantial cybersecurity budgets. Asia-Pacific and Latin America, though smaller markets, are expected to experience steady growth as investments in enterprise security reflect an overarching trend toward security maturity.

This Frost Radar™ focuses on the CTI industry, with separate studies available for other TI subdomains. Frost & Sullivan analyzes numerous companies in an industry. Those selected for further analysis based on their leadership or other distinctions are benchmarked across 10 Growth and Innovation criteria to reveal their position on the Frost Radar™. The publication presents competitive profiles of each company on the Frost Radar™, considering their strengths and the opportunities that best fit those strengths.

Strategic Imperative

The threat intelligence (TI) industry is growing steadily, fueled by low barriers to entry for start-ups due to venture capital injections, advancements in data scraping engines such as web crawlers, and the demand for proactive protection indirectly nudged by regulators and cyber-insurance firms. This has prompted nearly all cybersecurity vendors to offer some form of TI, ranging from basic telemetry data to comprehensive strategic threat reports. In response to this heightened demand and competition, more pure-play cyber threat intelligence (CTI) providers are integrating external attack surface management (EASM), and digital risk protection (DRP) capabilities, while cybersecurity platform providers are leveraging their economies of scale to enter the TI domain and get a piece of the pie.

As TI capabilities become commoditized, vendors must invest in research and development (R&D) to expand their use cases, integrating more DRP, EASM, and generative artificial intelligence (AI) functionalities. The rise of AI presents both opportunities and challenges: while it empowers organizations to proactively enhance security, bridge talent gaps, and gain a strategic advantage in cybersecurity, it also enables threat actors to exploit vulnerabilities more efficiently. The integration of AI throughout the TI lifecycle enhances detection, response, productivity, and threat reporting, driving demand for AI-enabled TI solutions across industries and regions. This trend is expected to surge in the next 5 years, reshaping the TI landscape and compelling non-AI-enabled providers to adapt to these changes to avoid becoming obsolete.

TI enhances security solutions by providing insights into emerging threats and attacker tactics, bolstering security ecosystems. However, practical implementation poses challenges, including quantifying TI's value and making compelling business cases. To navigate confusion and drive adoption effectively, vendors must focus on strategic marketing campaigns emphasizing outcomes and return on investment (ROI) rather than solely on capabilities.

Geopolitical tensions and conflicts, such as the Russo-Ukrainian War, have a dual impact on the TI industry. On the one hand, it increases demand for TI because of heightened threats from nation-state-sponsored hackers. On the other hand, sanctions and mistrust constrain the industry, hindering partnerships and global expansion for cybersecurity providers. This geopolitical turbulence affects the cybersecurity industry, shaping demand for TI and influencing vendors' go-to-market (GTM) strategies, especially for vendors based in Russia and China that are operating in the West.

Growth Environment

Advancements in AI, platform consolidation (such as the integration of external risk mitigation and management [ERMM] solutions), and the emphasis on proactive security measures will drive CTI industry revenue, with a compound annual growth rate of 33.5% projected from 2023 to 2028. On average, CTI participants included in this Frost Radar™ have seen revenue growth rates of 29% in the last 3 years, while marketing investments have averaged 17% of revenue.

Acquisitions such as that of Mandiant by Google are accelerating the growth of the CTI industry. Cybersecurity platform providers from adjacent industries also are propelling growth by developing proprietary solutions or acquiring smaller CTI vendors. North America and EMEA will remain focal points for vendors because of the prevalence of large enterprises with advanced security maturity and substantial IT/cybersecurity budgets, but slightly higher growth rates in APAC and Latin America will reflect an upward trajectory in security maturity in these regions. Latin America and APAC also offer significant opportunities for Russian and Chinese vendors that face challenges expanding in North America and Western Europe.

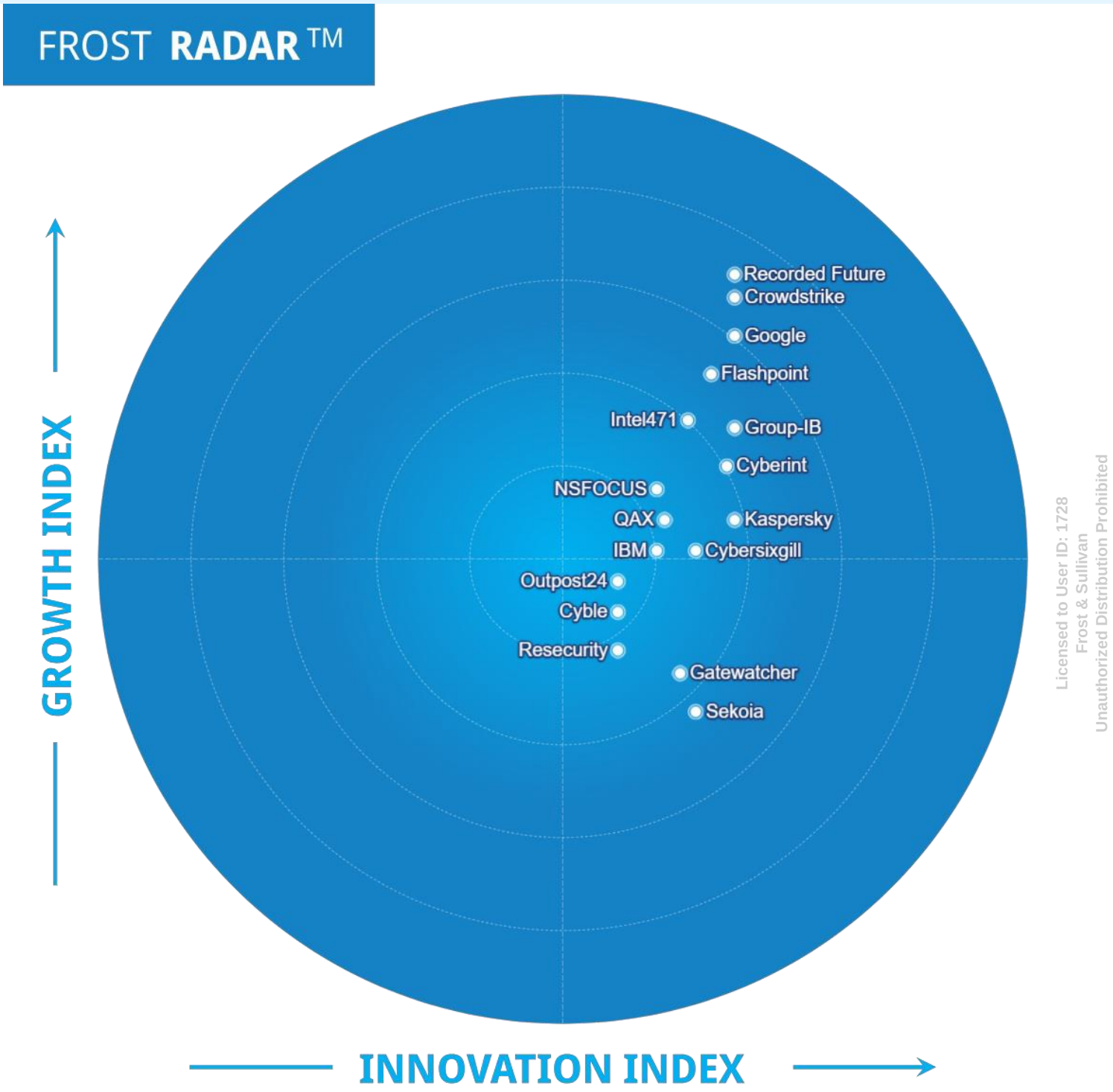
The technology, government, and financial verticals will continue to be the most profitable, with healthcare poised for significant expansion. This growth is driven by escalating threats from targeted phishing campaigns, supply chain attacks, and internet of things (IoT) vulnerabilities. Regulatory frameworks such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States also indirectly drive CTI adoption in healthcare, with organizations focusing on continuous risk assessments across their supply chains.

CTI solutions are best suited for organizations with advanced security maturity, elevated risk profiles for phishing attacks, large IT budgets, and low risk tolerance—criteria typically associated with large and mid-market companies that have strategic risk management capabilities and requirements. As a result, Frost & Sullivan expects large and mid-market organizations to remain the most significant growth areas. Still, small and medium-sized businesses (SMBs) are increasingly targeted by threat actors and need CTI solutions. Through managed TI services and managed security service providers (MSSPs), CTI vendors can expand their growth pipeline and serve this traditionally underserved segment.

Frost & Sullivan studies related to this independent analysis:

- Global Cyber Threat Intelligence and Threat Intelligence Platform Growth Opportunities
- Frost Radar™: Global Cyber Threat Intelligence, 2022
- Global External Risk Mitigation & Management Growth Opportunities

Frost Radar™



Source: Frost & Sullivan

Competitive Environment

The CTI industry has a wide variety of vendors with different profiles, value propositions, and use cases. On average, vendors invest 39% of their revenue in R&D. Recorded Future has the leading position on the Growth Index, holding a dominant global CTI revenue share with steady growth rates and strong execution of its vision. Recorded Future, Crowdstrike, Google, Group-IB, and Kaspersky lead on the Innovation Index because of comprehensive CTI capabilities, scalable innovations, high R&D investments, thought leadership in the CTI space, and robust innovation roadmaps.

Crowdstrike Flashpoint, Intel471, Cyberint, and Cybersixgill, hold significant market shares in the CTI space. They continue to enhance their value propositions in customer support, use cases, quality of intelligence sources, and other areas. Despite being longstanding industry participants, they remain committed to upgrading their offerings.

NSFOCUS, QAX, and IBM leverage their extensive security portfolios to create multiple revenue streams, capitalize on network effects, effectively cross-sell their products, and establish barriers to entry through vendor lock-in potential. However, they still lack some important use cases and R&D investments.

Niche players Outpost24, Cyble, Resecurity, Gatewatcher, and Sekoia have robust product portfolios but limited growth pipelines and global market shares. Notably, NSFOCUS, QAX, Kasperksy, and Resecurity offer both CTI and TIP solutions, enabling them to ingest third-party commercial CTI feeds from other vendors.

ZeroFox was considered for inclusion but chose not to participate in this analysis. Because of the lack of sufficient information for benchmarking, the vendor was not included on this Frost Radar™.

Companies to Action

Crowdstrike

Innovation

- Crowdstrike's extensive security portfolio encompasses a wide range of solutions from endpoint detection and response to TI, all integrated into a centralized ecosystem. Its Falcon platform supports various intelligence use cases, including DRP and EASM.
- The Adversary Intelligence module provides detailed insights into more than 230 threat actors, including e-criminals, nation-states, and hacktivists. It offers threat actor profiles and their tactics, techniques, and procedures (TTPs) mapped to the MITRE ATT&CK framework. It also includes Recon (the vendor's DRP solution), weekly threat summaries, an integrated sandbox, a vulnerability intelligence application, and a real-time indicator of compromise feed. The Premium edition adds thousands of finished intelligence reports (published each year), quarterly briefings, pre-built hunting libraries, and detection rules.
- With Falcon Adversary OverWatch, Crowdstrike combines a managed 24/7 threat-hunting service (spanning its endpoint, identity, and cloud solutions) and its baseline intelligence offering (integrated sandbox, vulnerability intelligence app, and IOC app).
- Despite below-average R&D investments, between the 40th and 60th percentiles, Crowdstrike has continuously enhanced its CTI offering, including adding generative AI features in 2024.

Growth

- With a dominant revenue share in the 80th to 100th percentiles, Crowdstrike serves a global customer base, primarily focusing on large and mid-market enterprises in North America.
- The vendor's above-average marketing investments, also in the 80th to 100th percentiles, have contributed to steady growth rates in the 40th to 60th percentiles over the past 3 years.
- Thanks to its diverse security portfolio, Crowdstrike benefits from numerous cross-selling and upselling opportunities, significantly amplifying its growth potential.

Frost Perspective

- Crowdstrike is one of the leading CTI vendors in terms of both innovation and growth. The vendor can access proprietary telemetry data from millions of endpoint devices thanks to its extensive security portfolio. To further improve its position on the Frost Radar™ Innovation Index, the vendor needs to increase its R&D investments to at least match the market average. The additional R&D capital should be allocated toward developing its CTI analyst teams in strategic locations globally to provide more contextual TI beyond its telemetry data.
- Crowdstrike already has strong footholds in North America and EMEA, but its customer base in APAC and Latin America is still minimal. To amplify its growth potential and accelerate its growth rates, the vendor should expand in these regions by partnering with more local MSSPs and launching targeted marketing campaigns.

Cyberint

Innovation

- Cyberint has a comprehensive ERMM platform combining CTI, DRP, and EASM solutions ranging from asset discovery to social media monitoring. Its CTI solution encompasses both targeted intelligence explicitly tailored to the organization (such as identifying phishing sites and data leaks) and global threat intelligence providing insights into general threat landscapes including vulnerabilities, IOCs, TTPs, and advanced persistent threats.
- Cyberint's centralized data lake aggregates billions of data points from various channels such as source code repositories, marketplaces, and forums. Through an intricate contextualization process with the help of human and machine learning analysis, these data points are refined, offering organizations custom intel, proactive threat hunting, and risk management capabilities.
- With R&D investments exceeding the industry average and ranking between the 60th and 80th percentiles, Cyberint continually enhances its security offerings. Recent advancements include the 2023 rollout of its malware and supply chain intelligence modules that provide further insights into malware families and third-party risks.

Growth

- Cyberint employs diverse distribution channels that encompass direct sales and partnerships with MSSPs, value-added resellers, and original equipment manufacturers. This strategic approach has facilitated the vendor's expansion, resulting in a diverse customer base that has enabled Cyberint to derive revenue from numerous industry verticals across North America, Latin America, EMEA, and APAC.
- Despite Cyberint's marketing investments falling below the industry average, ranking in the 20th percentile, the vendor has achieved remarkable growth rates, ranking between the 80th and 100th percentiles.

Frost Perspective

- Cyberint has a solid CTI offering and actively embraces global megatrends, such as connectivity and convergence, to build its innovation roadmap.
- To further improve its position on the Growth and Innovation indices, the vendor should consider expanding its product portfolio beyond its ERMM offering. For instance, it can consider allocating some of its R&D investments toward introducing complementary product lines such as managed detection and response and email protection or forging new integrations with other cybersecurity solutions. This strategic move would enable Cyberint to leverage additional cross-selling opportunities and extend its reach to a broader customer base.
- As part of its refined GTM strategy, Cyberint should boost its marketing investments to align with the industry average. Doing so will bring it closer to maximizing product adoption, enhancing visibility, and firmly establishing its presence as a comprehensive cybersecurity platform provider.

Cybersixgill

Innovation

- Cybersixgill monitors, collects, and curates data from a range of sources including open-source intelligence, closed forums on the deep web, the dark web, messaging apps, and X (formerly known as Twitter). This extensive data collection provides organizations with diverse intelligence use cases including third-party risk, vulnerability management, brand protection, identity fraud, and geopolitical intelligence.
- With investments in R&D ranking among the top, ranging between the 80th and 100th percentiles, Cybersixgill has continually enhanced its product suite. Over time, the company has introduced numerous capabilities and use cases, most recently its new third-party intelligence and identity intelligence modules, in addition to the EASM module in 2023. This evolution has transformed its CTI offering into a comprehensive ERMM platform.
- Recognizing the profound benefits of AI in SecOps, the vendor rolled out Cybersixgill IQ, a generative AI solution integrated into its security ecosystem. Cybersixgill has continued to innovate with IQ, most recently releasing a self-driven report generator. IQ is trained on real-time threat intelligence from Cybersixgill's large data lake. The AI engine enables end users, regardless of function or skill level, to extract actionable insights and generate custom reports, thereby streamlining SecOps.

Growth

- Cybersixgill has developed a diverse channel partner network with resellers, distributors, and MSSPs strategically positioned worldwide. This has facilitated the establishment of a global customer base and a varied sales pipeline. The bulk of its revenue comes from long-standing government engagements as well as from the largest global system integrators in the industry, with the remaining revenue derived from various entities.
- Cybersixgill has made substantial marketing investments, emerging as a leader in terms of the percentage of marketing expenditure. This strategic focus has yielded consistent growth rates since 2021, positioning it between the 40th and 60th percentiles.

Frost Perspective

- Cybersixgill's substantial investments in R&D and well-established technology roadmap for expanding its intelligence use cases, automation capabilities, and third-party integrations demonstrate its commitment to innovation.
- To further amplify its growth potential and improve its position on the Growth Index, the vendor should strengthen its footprint across additional industry verticals. While the vendor already serves organizations across a range of industries, it should reach across the finance, healthcare, and manufacturing verticals, where demand for CTI is rising.
- To achieve this, Cybersixgill should allocate some of its R&D to implementing industry-specific use cases such as dashboards and benchmarks to measure how the organization stands in comparison to its peers. In addition, it should allocate some of its marketing investments to launch targeted campaigns to solidify these sales pipelines.

Cyble

Innovation

- Cyble's security portfolio comprises 4 main products: Cyble Vision, Cyble Hawk, AmIBreached, and Cyber Odin. Its flagship product, Cyble Vision, seamlessly integrates CTI, EASM, and DRP solutions, establishing itself as a robust ERMM platform.
- Cyble Hawk, the vendor's custom CTI solution tailored for the public sector, offers specialized investigation capabilities for law enforcement, intelligence agencies, and governments.
- Despite introducing new solutions and products in recent years, including TheCyberExpress, a cybersecurity journal in 2022, and Cyble Odin, an internet scanning solution in 2023, Cyble has not yet achieved widespread global adoption of its offerings. This challenge is compounded by its R&D investments, which currently rank among the lowest percentiles, impeding its scalability and innovation potential.

Growth

- Cyble has achieved remarkable growth since 2021, acquiring 500 new customers and establishing itself as the frontrunner in revenue growth rates. However, the vendor's global market share remains between the 20th and 40th percentiles, and its marketing investments, which are in the 20th percentile, are among the lowest. Moreover, its growth pipeline predominantly revolves around APAC, particularly India.
- To bolster its global expansion and R&D initiatives, Cyble concluded a Series B funding round in 2023, securing more than $30 million in capital investment. Driven by its high revenue growth trajectory, the company is poised for further growth, with plans for a Series C funding round between January and April 2025.
- In 2023, Cyble launched its Cyble Partner Network (CPN), which now boasts over 200 partners across 25 countries and includes global system integrators, the Big4s, and top-tier cybersecurity MSSPs. The CPN encompasses various programs, including training, rewards, and certifications, aimed at aligning channel partners with Cyble's strategic expansion goals.

Frost Perspective

- While Cyble shows promising growth potential with the CPN initiative and industry-specific solutions such as Cyble Hawk, its CTI and broader ERMM offering have yet to gain significant global traction.
- To enhance its standing on the Innovation and Growth indices, Cyble should allocate a substantial portion of its recent Series B funding toward R&D and marketing efforts, aiming to at least match industry averages.
- R&D investments should prioritize new features such as generative AI and supply-chain risk management capabilities, ensuring that Cyble catches up with industry leaders in innovation.
- In parallel, new marketing investments should fund targeted campaigns highlighting the value propositions of Cyble's Vision and Hawk solutions, particularly in APAC and Latin America, where Cyble already has a foot in the door. This strategic approach would solidify its presence and capture a larger market share.

Flashpoint

Innovation

- Flashpoint has a comprehensive TI offering, including CTI, vulnerability intelligence, physical security intelligence, national security intelligence, managed intelligence, and professional services. Its Ignite platform integrates various use cases, such as fraud, brand protection, and ransomware defense, into a centralized ecosystem.
- Setting itself apart from the competition, Flashpoint is among the few CTI vendors offering managed attribution capabilities. This empowers organizations to conduct deep threat investigations and interact with threat actors anonymously and securely within a sophisticated virtual environment.
- Demonstrating a commitment to innovation, Flashpoint continually enhances its products. The company's highlights from 2023 include Ignite AI, an AI chatbot that leverages natural language processing and sources data points from Flashpoint's intelligence; Flashpoint Firehose, a data-as-a-service solution delivering enriched data streams; and Automated Source Discovery, an AI-based technology that rapidly identifies new high-fidelity sources relevant to priority intelligence requirements at scale.

Growth

- Holding a substantial market share ranking between the 80th and 100th percentiles, Flashpoint has maintained modest but steady growth rates since 2021, ranking in the 20th percentile.
- While boasting a global customer base, Flashpoint primarily derives its revenue from organizations in North America, particularly in the finance, government, technology, and healthcare sectors.

Frost Perspective

- Flashpoint is one of the leaders in communicating a solid vision and strategy and makes a conscious effort to convey its value proposition with practical use cases, such as fraud protection, brand protection, and account takeover prevention. This approach empowers organizations to gauge their ROI, fueling demand for Flashpoint's Ignite platform.
- To bolster its standing on the Growth Index and broaden its sales pipeline, Flashpoint should explore geographic expansion through partnerships with local resellers. EMEA presents a prime opportunity, being the second-largest CTI market by revenue and offering substantial growth prospects. Notably, the United Kingdom, DACH region, and Spain emerge as areas of focus because of the dense concentration of enterprises across the public and private sectors that demand advanced CTI solutions.
- While Flashpoint's R&D investments currently fall between the 40th and 60th percentiles, the vendor should intensify its commitment to R&D to align with innovation leaders and elevate its position on the Innovation Index. Flashpoint should focus its R&D funds on enhancing EASM capabilities with the introduction of supply chain risk assessment solutions.

Gatewatcher

Innovation

- Gatewatcher's product portfolio includes network detection and response (NDR), CTI, and network test access point devices, combining internal and external security risk exposure capabilities into a unified ecosystem. Its CTI offering includes identity, brand, exposure, SecOps, and vulnerability intelligence modules, which can be licensed as stand-alone solutions or as add-ons integrated via its NDR platform.
- With R&D investments between the 40th and 60th percentiles, Gatewatcher has continuously enhanced its product offering. Notably, in 2024, the vendor rolled out Gatewatcher AI Assistant (GAIA), a generative AI-based assistant integrated into the product ecosystem to combine technical and operational use cases such as best practices recommendations, operation enrichment, and report summaries.
- While Gatewatcher has begun rolling out some brand intelligence and attack surfacement capabilities, they are works in progress and have yet to match the scalability of the DRP and EASM solutions of other innovation leaders.

Growth

- Leveraging a combination of Tier 1 and Tier II distribution channels, including resellers and MSSPs, Gatewatcher maintains a global revenue share and growth trajectory positioned between the 20th and 40th percentiles.
- France-based Gatewatcher's customer base is predominantly concentrated in EMEA, with a growing presence in APAC. The company primarily serves large finance, education, and technology enterprises.
- In 2022, Gatewatcher secured €25 million in a Series A funding round. A significant portion of this capital infusion fueled the company's international expansion strategy, enabling Gatewatcher to establish additional offices in United Kingdom, Belgium, the Netherlands, Luxembourg (Benelux), Singapore, the Middle East, and North Africa.

Frost Perspective

- Gatewatcher is in the process of enhancing its TI offering by incorporating DRP and EASM capabilities. This will unlock new cross-selling and upselling opportunities. To improve its standing on the Innovation Index, the company should direct its R&D investments toward phishing protection, takedown services, and supply chain risk assessment, which are key DRP and EASM use cases increasingly prevalent among leading industry innovators.
- To enhance its position on the Growth Index and accelerate its global expansion endeavors, Gatewatcher must boost its marketing investments, currently situated in the 20th percentile, to align with the market average. The marketing capital should be directed toward targeted campaigns in APAC, where Gatewatcher already maintains a foothold. These initiatives must convey the value propositions of CTI and other pivotal DRP and EASM applications to maximize market penetration and foster sustainable growth.

Google

Innovation

- Google's security portfolio encompasses a diverse range of solutions, from cloud security to threat intelligence.
- Google Threat Intelligence leverages an extensive array of sources including open-source data, proprietary telemetry from billions of endpoints and emails, VirusTotal (one of the largest malware databases and communities in the world), and human-curated intelligence. The company's offerings are further enhanced with strategic security consulting and incident response services tailored to customer needs.
- Google Threat Intelligence is underpinned by Gemini, a sophisticated generative AI assistant that enables organizations to streamline SecOps such as malware analysis, data enrichment, and reporting.
- Google's R&D investments rank between the 20th and 40th percentiles. While it introduced DRP and EASM cases in 2022 with the acquisition of Mandiant, these are still being developed. The vendor still relies on third parties for its DRP takedown services.

Growth

- Since the acquisition of Mandiant, Google's CTI offerings have helped it achieve steady growth rates between the 40th and 60th percentiles.
- Google holds a significant market share, ranking between the 80th and 100th percentiles. The company serves a global customer base primarily composed of large and mid-market enterprises across various industries.
- The vendor provides customized threat intelligence subscriptions, from Standard to Enterprise+, to cater to organizations at various stages of security maturity.

Frost Perspective

- Similar to other leading vendors, Google has a strong presence in North America and EMEA, but its customer base in APAC and Latin America remains relatively small. To boost its growth potential and accelerate its expansion, Google should focus on these regions. Forming partnerships with local MSSPs and launching targeted marketing campaigns will help establish stronger footholds in APAC and Latin America.
- To improve its position on the Innovation Index, Google should increase its R&D investments to match those of the other innovation leaders and avoid the risk of falling behind. Additional R&D capital should be allocated to further develop its DRP use cases, such as managed takedown services.

Group-IB

Innovation

- Group-IB is a leader on the Frost Radar™ Innovation Index with its Unified Risk Platform (URP), which seamlessly integrates ERMM, extended detection and response (XDR), email protection, and fraud prevention. This centralized ecosystem empowers cross-functional teams to collaborate more effectively, leveraging synergies across various workflows, thereby enhancing the vendor's innovation scalability.
- Group-IB collaborates closely with its customers to gather TI requirements, delivering tailored, actionable intelligence such as custom reports, brand infringement alerts, and compromised account notifications. Leveraging a global team of analysts and web crawlers, Group-IB collects high-fidelity data from numerous sources including the dark web, marketplaces, and vulnerability repositories. Thanks to custom-configured threat-hunting rules, Group-IB's security teams can detect potential threats, such as suspicious infrastructure, even before they are used for attacks.
- With R&D investments between the 80th and 100th percentiles (one of the highest), Group-IB consistently enhances its products. In 2024, the vendor introduced new functionalities such as the Fraud Matrix framework, which enables organizations to contextualize fraud schemes more effectively. The vendor also launched a new AI assistant to streamline reporting processes, identify appropriate registrars, and automatically initiate malicious content takedown requests.

Growth

- Group-IB has a global customer base, with a concentration of clients in EMEA and APAC. It is also making incremental gains in North America and Latin America. The company predominantly serves large enterprise customers in finance, eCommerce and retail, technology, telecommunications, and government.
- To further expand its presence and support existing customers in the Americas, Group-IB has already hired local staff and is planning to launch its new Digital Crime Resistance Center (DCRC) in Chile in Q3 2024. The center will focus on researching local threats and providing incident response and other services, as well as threat intelligence, DRP, and fraud protection solutions, in key markets such as Chile, Brazil, Mexico, and Colombia.
- Despite its marketing investments being in the 40th to 60th percentiles, which is below the market average, Group-IB has achieved high growth rates, ranking between the 60th and 80th percentiles.

Frost Perspective

- Group-IB is a leading CTI vendor in terms of innovation and growth. To enhance its innovation scalability and improve its position on the Innovation Index, the company should consider expanding its reach to mid-market and SMB organizations. This can be achieved by offering tailored, cost-effective solutions or by partnering with additional MSSPs that can leverage economies of scale to better serve smaller organizations.
- To boost its growth in Latin America and the broader Americas, Group-IB should increase its marketing investments to at least the industry average. Additionally, launching targeted campaigns that address the specific challenges faced in these regions will help amplify its market presence.

IBM

Innovation

- IBM's comprehensive QRadar suite covers a wide range of security solutions from ASM to security orchestration, automation, and response. At the core of the QRadar suite is X-Force Threat Intelligence, which can be licensed as a stand-alone solution or as part of the broader QRadar offering.
- X-Force Threat Intelligence gathers and analyzes over a billion data points from both human and machine-generated sources. Leveraging its extensive security portfolio, IBM provides unique insights from more than 330 million proprietary endpoint devices, honeypots, and vulnerability repositories. Its partnership with Quad9, a domain name system (DNS) security provider with more than 200 points of presence, enriches IBM's threat intelligence with malicious domain information for proactive security measures such as early detection of phishing sites.
- IBM effectively leverages partnerships to gain broad visibility into global DNS traffic, develop insightful intelligence on emerging malicious domains, and rigorously test feeds to ensure an exceptionally low false-positive rate.
- QRadar portfolio enhancements include integrating ASM capabilities through acquiring Randori in 2022 and developing the Unified Analyst Experience (UAX), an intuitive user interface that integrates all QRadar modules to facilitate better collaboration among cross-functional teams. However, IBM's R&D investments remain in the 20th percentile, and the portfolio lacks DRP use cases such as brand protection, which limits its innovation scalability.

Growth

- IBM's sales and marketing investments are in the 60th and 80th percentiles, respectively. As an international conglomerate, IBM boasts a diverse growth pipeline, a global customer base, and a comprehensive security product portfolio, creating numerous cross-selling and upselling opportunities for its X-Force Threat Intelligence offering.
- IBM primarily serves large enterprises across industries including government, utilities, manufacturing, finance, and services. Unlike many CTI vendors, IBM has a strong presence in Latin America, specifically Brazil, Ecuador, and Bolivia. However, despite steady overall growth, IBM's CTI market share and revenue growth rates are between the 20th and 40th percentiles.
- In May 2024, IBM announced the sale of its QRadar suite to Palo Alto Networks (PAN) and a new consulting services partnership, but as of publication the transaction is not yet final because of SEC regulations. IBM and PAN will continue to operate as separate entities until the transaction officially closes, which is estimated to occur in September 2024. In the meantime, IBM remains committed to selling its entire QRadar product line, including the X-Force Intelligence offering, and actively supports all its QRadar suite customers through the transition period.

Frost Perspective

- IBM's sales and marketing investments are in the 60th and 80th percentiles, respectively. As an international conglomerate, IBM boasts a diverse growth pipeline, a global customer base, and a comprehensive security product portfolio, creating numerous cross-selling and upselling opportunities for its X-Force Threat Intelligence offering.
- IBM primarily serves large enterprises across industries including government, utilities, manufacturing, finance, and services. Unlike many CTI vendors, IBM has a strong presence in Latin America, specifically Brazil, Ecuador, and Bolivia. However, despite steady overall growth, IBM's CTI market share and revenue growth rates are between the 20th and 40th percentiles.
- In May 2024, IBM announced the sale of its QRadar suite to Palo Alto Networks (PAN) and a new consulting services partnership, but as of publication the transaction is not yet final because of SEC regulations. IBM and PAN will continue to operate as separate entities until the transaction officially closes, which is estimated to occur in September 2024. In the meantime, IBM remains committed to selling its entire QRadar product line, including the X-Force Intelligence offering, and actively supports all its QRadar suite customers through the transition period.

Intel471

Innovation

- Intel471's TITAN platform offers organizations highly contextualized and finished intelligence across 5 critical domains: adversary, malware, credentials, vulnerabilities, and marketplace intelligence, addressing more than 40 use cases.
- While many CTI vendors supplement their data with third-party intelligence and open-source intelligence, Intel471 distinguishes itself through its human-intelligence-centered approach and timely reports. Leveraging a global team of analysts, Intel471 extracts insights from threat actors and facilitates tailored research through requests for information, ensuring the relevance, timeliness, and uniqueness of its intel.
- In 2022, Intel471 bolstered its CTI capabilities by acquiring Spiderfoot, an EASM provider, enhancing its asset discovery and supply chain monitoring use cases. Over the years, Intel471 has improved its products, introducing mobile malware detection and image recognition capabilities in 2023.
- Despite regular enhancements, its R&D investments currently rank in the 20th percentile. Moreover, Intel471's TITAN still lacks generative AI features, which CTI vendors increasingly embrace. The company is adopting a "pause-and-see" approach to generative AI.

Growth

- Intel471 holds a substantial market share, positioning it between the 60th and 80th percentiles globally, with a predominant customer base in North America and EMEA.
- Primarily serving large organizations in the government, finance, retail, manufacturing, pharmaceuticals/biotech, technology, and services industries, Intel471 experienced steady growth rates in the past 3 years, ranking it between the 20th and 40th percentiles. However, its marketing investments, until recently and prior to its acquisitions, were more conservative (ranking in the 20th percentile), slowing its growth potential.
- In May 2024, Intel471 acquired Cyborg Security, setting a new standard in intelligence-led threat hunting that leverages CTI to streamline customers' hunt processes and help them stay ahead of emerging threats. With this strategic move, Intel471 has increased its customer base and further expanded its growth pipeline.

Frost Perspective

- Given the recent acquisition, Intel471 needs to ensure the seamless integration of Cyborg Security's threat-hunting solution into the TITAN ecosystem to prevent disjointed experiences and data silos. This will satisfy customers and enable upselling opportunities.
- Intel471 should increase R&D investments to align with market averages, enhancing its innovation scalability and position on the Frost Radar™ Innovation Index. The new R&D capital should be directed toward product integration and the implementation of generative AI and managed attribution features to elevate TITAN's threat-hunting capabilities.
- The vendor can expand its market share by either intensifying efforts in North America and EMEA or solidifying its presence in APAC and/or Latin America. To achieve this, Intel471 should boost marketing investments to match industry averages to reach target audiences effectively through targeted campaigns that highlight TITAN's value proposition to businesses and governments in these regions.

Kaspersky

Innovation

- Kaspersky's comprehensive cybersecurity suite encompasses a wide range of solutions including security information and event management, extended detection and response (XDR), managed detection and response, and network detection and response, underpinned by its TI offering. Its TI portfolio has 10 integrated modules spanning threat feeds and lookups to reporting and takedown services.
- Kaspersky is one of the few vendors that provide both CTI and TIP and can ingest third-party commercial data from other vendors. It has global customer support and a research team spread across strategic locations to scale its solutions in a range of segments and provide highly contextualized threat intelligence services.
- With R&D investments between the 60th to 80th percentiles, Kaspersky has made numerous enhancements in recent years. In 2023, it introduced new threat lookup features, such as timeline analysis of IOCs and similarity lookups for malicious files, supported by one of the largest repositories with more than 25 years of historical data.
- Kaspersky maintains a strong innovation roadmap and offers DRP and EASM use cases such as brand protection, social media monitoring, and asset management through its Digital Footprint Intelligence module. While it has yet to introduce generative AI capabilities to its customer base, they are on the roadmap for Q4 2024.

Growth

- Kaspersky has a global customer base with a market share between the 40th and 60th percentiles, primarily serving large and mid-market enterprises in the government, finance, and technology verticals.
- The vendor's extensive product portfolio presents numerous cross-selling and upselling opportunities. Its TI offering is highly customizable, with 5 pricing options and sets of capabilities tailored to the security maturity and budgets of various organizations.
- Most of Kaspersky's CTI revenue is generated through its distributor channel, achieving steady growth. However, its growth rates and marketing investments both rank in the 20th percentile.

Frost Perspective

- Kaspersky has an extensive product portfolio and comprehensive CTI capabilities, amplifying its innovation scalability. The vendor demonstrates a strong technology roadmap and is in the process of implementing generative AI capabilities, ensuring that it remains competitive with the other leading vendors.
- While Kaspersky has a global customer base, it is concentrated in Russia, Saudi Arabia, and the United Arab Emirates. Geopolitical conflicts and economic sanctions further restrict this Russia-based vendor's reach in North America and Western Europe. Kaspersky should expand its distribution channels and partner more with MSSPs to grow in Latin America and APAC, and increase its marketing investments to the industry average and launch targeted campaigns in these regions.

NSFOCUS

Innovation

- NSFOCUS's extensive product portfolio covers numerous aspects of the cybersecurity lifecycle, from proactive threat intelligence to reactive detection and response. The NTI line in the company's product suite integrates seamlessly into the broader NSFOCUS security ecosystem, offering modules such as NTI Cloud for threat intelligence queries, NTIP, advanced persistent threats group detection, threat advisory, audits, and Sandbox Cloud.
- Catering to a diverse range of organizations, NSFOCUS provides both CTI and TIP solutions that can be tailored to specific needs regardless of size or industry vertical. For instance, NTI Cloud accommodates SMBs and mid-market businesses with limited budgets seeking threat intelligence, while NTIP targets larger enterprises needing to bolster their TI capabilities.
- Despite product enhancements such as the introduction of the EASM module in 2023, NSFOCUS's R&D investments remain below the market average, positioning the company between the 20th and 40th percentiles in this area. While its CTI solutions have advanced, they still lack comprehensive DRP use cases and MITRE ATT&CK mapping capabilities, which are increasingly considered standard in TI offerings.

Growth

- Thanks to a diverse product portfolio, effective cross-selling strategies, and above-average marketing spending, NSFOCUS has experienced steady growth since 2021. However, its revenue growth rates remain in the 20th percentile.
- Although NSFOCUS maintains a global presence and serves industries including government, finance, technology, and services, its primary customer base is highly concentrated in APAC, particularly China, Singapore, and Malaysia. This geographical limitation restricts its global growth potential.

Frost Perspective

- Thanks to a diverse product portfolio, effective cross-selling strategies, and above-average marketing spending, NSFOCUS has experienced steady growth since 2021. However, its revenue growth rates remain in the 20th percentile.
- Although NSFOCUS maintains a global presence and serves industries including government, finance, technology, and services, its primary customer base is highly concentrated in APAC, particularly China, Singapore, and Malaysia. This geographical limitation restricts its global growth potential.

Outpost24

Innovation

- Outpost24 offers a large cybersecurity portfolio that includes CTI, EASM, vulnerability management, application security, and password security. The vendor's CTI solution, Threat Compass, combines CTI and DRP use cases such as domain protection, credit card fraud protection, dark web monitoring, and threat monitoring. Outpost24 follows a best-of-breed approach, acquiring different vendors to enhance its capabilities.
- Outpost24 has enhanced its exposure management capabilities by acquiring vendors including Blueliv in 2021 for CTI and DRP solutions, Specops Software in 2021 for password and user authentication, and Sweepatic in 2023 for EASM. In 2024, Outpost24 combined these solutions with existing pentest-as-a-service, dynamic application security testing, and vulnerability scanning to create an exposure management platform that provides a comprehensive view of the attack surface and critical applications.
- Outpost24's R&D investments are between the 20th and 40th percentiles. Recent product enhancements included the implementation of dynamic scoring in 2022 for real-time vulnerability assessments and the launch of Threat Explorer, which provides real-time alerts for vulnerabilities, in 2023.

Growth

- Outpost24's global market share is between the 20th and 40th percentiles, primarily serving organizations in EMEA and North America. By working closely with MSSPs, Outpost24 effectively scales its CTI offerings across businesses ranging from SMBs to large enterprises, primarily in the technology, finance, and media verticals.
- Despite below-average marketing investments between the 20th and 40th percentiles, the vendor has experienced steady growth, placing it between the 40th and 60th percentiles in terms of revenue growth.

Frost Perspective

- Outpost24 has a solid vision and roadmap, aiming to integrate all its acquired point solutions into a comprehensive ERMM platform for a unified user experience. To improve its position on the Frost Radar™ Innovation Index and facilitate this integration, the vendor needs to increase its R&D investments to match the industry average. A portion of the new R&D capital should be allocated toward developing generative AI and threat intelligence graph visualizations, the latter of which is already a standard among CTI vendors.
- To enhance its position on the Growth Index, Outpost24 should increase its marketing investments to at least match industry averages. These new investments should be focused on the regions where the vendor aims to expand.
- While Outpost24 has a strong presence in EMEA and North America, its customer base in Latin America and APAC remains small. To expand in these regions, the vendor should consider partnering with more local MSSPs.

QAX

Innovation

- QAX boasts a diverse product portfolio that includes CTI, TIP, security information and event management, network detection and response, endpoint detection and response, and security orchestration, automation, and response. QAX empowers organizations to operationalize QAX's CTI feed with its proprietary TIP platform or seamlessly integrate it into their existing security stack via REST API.
- With more than 150 threat analysts and 100 million endpoint devices, QAX monitors numerous sources and processes data with a unique mix of machine learning and human expert analysis to provide organizations with a holistic view of the threat landscape.
- With above-average R&D investments that rank between the 60th and 80th percentiles, QAX has introduced various product capabilities and solutions, such as a generative AI assistant, its Threat Intelligence Operation System (TIOS), and a multi-product solution for threat intelligence production, operation, and sharing.
- Despite regular new product enhancements, QAX is still catching up with the Frost Radar™ innovation leaders and has yet to introduce use cases and capabilities such as DRP and EASM.

Growth

- With a diverse product portfolio, QAX can capitalize on many cross-selling opportunities. However, its growth pipeline is still limited to mostly the government and media verticals in China and other countries in APAC.
- Leveraging its above-average marketing investments, QAX is pursuing strategies to expand its international footprint and enhance its growth prospects. The vendor's 2022 marketing campaign as the official cybersecurity sponsor for the 2022 Winter Olympics and Paralympics in Beijing was a great move to elevate its brand recognition beyond APAC.
- QAX has experienced consistent growth over the past 3 years, positioning it within the 60th to 80th percentiles for revenue growth and securing a market share within the 40th to 60th percentiles globally.

Frost Perspective

- QAX offers organizations a robust security suite, providing a centralized ecosystem for enhanced protection. However, to improve its standing on the Frost Radar™ Innovation Index and adapt to the evolving landscape where many CTI vendors are transitioning toward more comprehensive ERMM platforms, QAX must broaden its threat intelligence offerings. This entails incorporating additional DRP and EASM use cases such as brand protection, fraud prevention, remediation services, and third-party risk assessments.
- While QAX has maintained steady growth rates, primarily serving customers in China and adjacent locations, there is a clear imperative to maximize its growth potential and establish a firmer foothold globally. Latin America presents QAX with a great opportunity because it is still an underserved region and offers much room for growth.
- To achieve this growth, QAX should diversify its distribution channels (it is currently reliant on direct sales for the majority of its revenue). Partnering with additional resellers, distributors, and MSSPs would facilitate expansion into new regions.

Recorded Future

Innovation

- Recorded Future is one of the leaders on the Frost Radar™ Innovation Index thanks to its strong innovation roadmap and diverse intelligence portfolio scalable to various industries, locations, and user personas. Consisting of 9 integrated modules, a sandbox, and 5 solutions, Recorded Future's Intelligence Cloud is one of the largest threat data repositories in the world.
- The vendor's Collective Insights connects the dots between a customer's internal telemetry and external threat intelligence. It enables customers to understand what is happening in their environment and externally to others like them. It sheds light on blind spots caused by organizations using different security tools and dashboards.
- While Recorded Future's R&D investments remain below the industry average, the vendor has made significant enhancements in recent years. For instance, in 2023, it introduced Recorded Future AI, an AI engine that streamlines organizations' intelligence cycles by automating analysis and reporting processes, saving considerable time and resources.

Growth

- Thanks to its dominant market share, diverse channel partner network, and powerful brand equity in the CTI space, Recorded Future is a leader on the Frost Radar™ Growth Index. Recorded Future has an extensive sales pipeline, serving a global customer base in industry verticals including government, finance, and technology.
- Ranking between the 20th and 40th percentiles, Recorded Future's marketing investments cover diverse channels, including independent news sites, podcasts, newsletters, proprietary conferences, and a dedicated university program to raise the next generation of threat intelligence analysts.
- The company follows an innovative customer alignment strategy that includes low-friction selling with the help of free trials and tools. It simplifies the customer lifecycle with the help of free self-service onboarding guides and training sessions, accelerating the time to value for organizations. In parallel, Recorded Future offers custom bundles tailored to individual organizational needs, emphasizing effective security outcomes over disjointed tools. This strategic approach enables it to capture new customers and create upselling opportunities.

Frost Perspective

- Recorded Future's strategies are in alignment with its vision to be "building the most significant intelligence platform of our time." As an industry benchmark and thought leader in the CTI space, it boasts a strong innovation roadmap leveraging global megatrends and a strategic GTM approach encompassing targeted marketing campaigns and streamlined sales cycles.
- While Recorded Future is a leader on both the Innovation and Growth indices of the Frost Radar™, competitive intensity is increasing, with many TI use cases becoming commoditized. With a higher price point than other market participants, Recorded Future faces the risk of customer churn and missed opportunities in requests for proposals, where organizations may opt for lower-priced solutions offering similar capabilities. To maintain its leadership position, Recorded Future should increase its R&D investments to align with the industry average, ensuring that its capabilities are not easily replicated.

Resecurity

Innovation

- Resecurity's cybersecurity platform combines endpoint protection, ERMM, vulnerability assessment, and penetration testing capabilities into a unified experience powered by a sophisticated machine learning/AI data engine on the back end.
- Resecurity is one of the few vendors that offer both CTI and TIP solutions, being able to ingest third-party commercial feeds from other CTI vendors. Context, the vendor's CTI offering, covers a wide range of use cases, such as antipiracy, brand protection, data breaches, dark web monitoring, security intelligence, and threat response.
- Resecurity's R&D investments fall between the 20th and 40th percentiles. Recent advancements include the 2024 launch of Context AI, a generative AI feature trained on a combination of open-source and proprietary threat actor data to streamline analyst workflows.

Growth

- Resecurity's global market share is in the 20th percentile, serving primarily large enterprises in the finance, government, and technology sectors.
- North America makes up most of its customer base, which has experienced steady growth during the last 3 years, primarily through referrals and reseller sales channels. The vendor's marketing investments are among the highest, ranking between the 80th and 100th percentiles, amplifying its growth potential.

Frost Perspective

- Resecurity's robust product portfolio enables it to capitalize on cross-selling and upselling opportunities. To complement this strategy, Resecurity should invest some of its substantial marketing capital in highlighting its value proposition as a comprehensive platform provider for all threat intelligence needs. To further amplify its growth potential and capture a larger market share, Resecurity must expand its distribution channels through MSSPs and resellers.
- To improve its standing on the Frost Radar™ Innovation Index, Resecurity needs to increase its R&D investments to meet the market average. New product initiatives should focus on integrating Context AI across its entire product portfolio and building out its AI use cases, such as best practice recommendations and threat investigation automation.

Sekoia

Innovation

- Sekoia's cybersecurity portfolio includes Sekoia Defend and Sekoia Intelligence solutions integrated into a unified security operations center platform, which fills the gap between threat landscape evolution and detection capabilities.
- Sekoia Intelligence, the vendor's CTI offering, provides a range of capabilities and use cases, including interactive dashboards, threat actor tracking, selective intelligence feeds, reports, graph visualizations, AI assistants, and playbooks for proactive cybercrime protection and threat hunting.
- Sekoia has the highest R&D investments in the CTI industry, placing it in the top percentile. The vendor regularly introduces new product enhancements, such as graph investigations in 2022 and IOC retro hunt capabilities in 2023, but it still lacks EASM use cases such as supply chain risk assessments, which an increasing number of competitors have adopted.

Growth

- Sekoia's global market share is in the 20th percentile. It primarily serves large enterprises in the finance, government, media, and manufacturing industries in EMEA. In 2023, Sekoia raised $37 million in a Series A funding round to support its international expansion.
- Despite below-average marketing investments, Sekoia experienced rapid growth rates, placing it in the 80th and 100th percentiles, the second highest in the industry.
- The company operates through a diverse distribution network involving direct sales, distributors, and MSSPs. Strengthening its partnerships, Sekoia offers a flexible pricing model tailored to MSSPs, scaling according to the size of its customer base.

Frost Perspective

- Sekoia is the leader in R&D investments in terms of percentage of total revenue. To enhance its standing on the Frost Radar™ Innovation Index, it should allocate some of its capital to developing new DRP and EASM use cases, which will become essential for maintaining competitiveness.
- Sekoia boasts a robust product portfolio, offering various cross-selling and upselling opportunities. However, its growth pipeline is currently limited to EMEA, primarily France, Belgium, and the United Arab Emirates. To bolster its position on the Growth Index, the vendor must expand its market share and venture into new regions.
- The integrated portfolio offered by Sekoia is particularly well-suited for large enterprises. To capitalize on this strength, Sekoia should penetrate North America, which has a large concentration of enterprises with high-security maturity and budgets, presenting a compelling opportunity for expansion.
- The recent Series A capital injection will enable it to achieve this and pursue new opportunities. It should allocate some of this capital to increase its marketing investments to match the industry average. New marketing capital should be geared toward strategic marketing campaigns in the United States, Canada, and Mexico.

Strategic Insights

1. Cybersecurity vendors face significant challenges communicating their value propositions, especially for TI solutions. Many resort to fear-based marketing and gimmick capabilities, which lose effectiveness as organizations become desensitized to constant threats and dissatisfied with overpromises. Instead, vendors should highlight the unique benefits and positive ROI of their TI solutions. Vendors can present a more compelling business case as these solutions evolve into comprehensive ERMM and SecOps platforms.

2. Effective marketing campaigns should focus on tangible benefits, addressing pain points such as brand erosion, revenue loss, visibility constraints, and productivity limitations. Messaging must avoid overpromises and excessive buzzwords to prevent confusion. Implementing ROI metrics in product offerings, displayed in dashboards, is key to conveying value. For instance, CTI providers can showcase cost savings from identifying leaked credit card data, and TIP providers can highlight how eliminating redundant data reduces costs.

3. Latin America, though the smallest TI market by revenue, holds substantial growth potential driven by economic, regulatory, and technological advancements. The region remains underserved, with Brazil and Ecuador experiencing high phishing attack rates. Frost & Sullivan found in a recent survey that 50% of Brazilian organizations use DRP and EASM solutions, with 35% planning to implement them in 2024. This indicates the growing adoption of advanced security measures, presenting promising opportunities for TI vendors. In Brazil, more than 50% of security products are acquired through resellers and more than 40% via direct channels.

4. While significant opportunities exist in North America, EMEA, and APAC, competition is fierce. Expanding into Latin America offers TI vendors a chance to establish a strong presence. Success in Latin America requires a well-balanced GTM strategy, including partnerships with local channels, customized pricing, regional offices, and local talent. Brazil, Mexico, Colombia, and Chile are particularly promising because of their large enterprises and unmet TI needs.

5. Organizations struggle with visibility, limited resources, alert fatigue, and manual processes. AI technology complements TI solutions by enhancing security, visibility, and productivity. Full AI integration across TI ecosystems is ongoing, but current applications have already improved data analysis by providing historical context and identifying attack vectors. AI can also offer tailored reports, predictive risk analysis, workflow automation, and dynamic threat visualizations. To remain competitive, TI vendors must increase AI investment. Prioritizing R&D in AI empowers customers to fully leverage TI solutions. Partnering with AI providers to enhance and integrate AI capabilities is crucial, allowing vendors to address evolving customer challenges and boost growth prospects.

Legal Disclaimer