

2025 TECHNOLOGY INNOVATION LEADER

Enhancing Customer Impact Through Powerful Technology Integration

RECOGNIZED FOR BEST PRACTICES IN THE NORTH AMERICAN SOCIAL MEDIA INTELLIGENCE SOLUTIONS INDUSTRY

FROST & SULLIVAN

Table of Contents

Best Practices Criteria for World-class Performance 2

The Transformation of the Social Media Intelligence Solutions Industry 3

Technology Leadership 4

Flexibility Aligned with Sector-Specific Needs 5

Customer-Specific Value Creation 7

Ongoing Commitment to Technology Innovation to Combat Emerging Threats 7

Conclusion 8

What You Need to Know about the Technology Innovation Leadership Recognition 9

Best Practices Recognition Analysis 9

Technology Leverage 9

Business Impact 9

Best Practices Recognition Analytics Methodology 10

Inspire the World to Support True Leaders 10

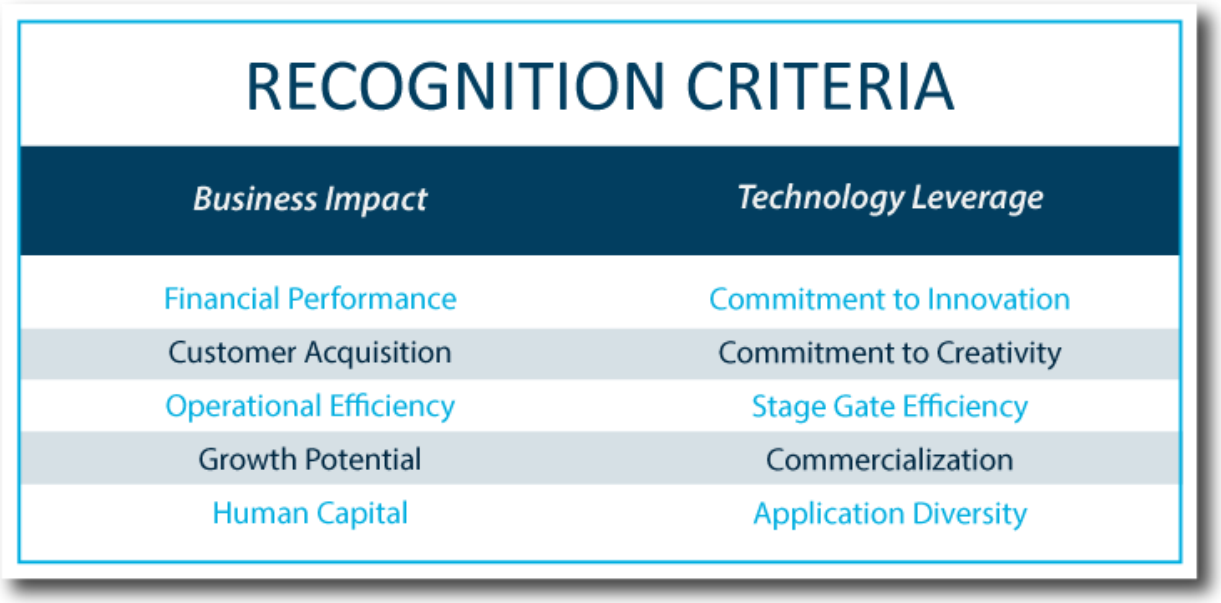
About Frost & Sullivan 10

The Growth Pipeline Generator™ 11

The Innovation Generator™ 11

Best Practices Criteria for World-class Performance

Frost & Sullivan applies a rigorous analytical process to evaluate multiple nominees for each recognition category before determining the final recognition recipient. The process involves a detailed evaluation of best practices criteria across two dimensions for each nominated company. Cyabra excels in many of the criteria in the social media intelligence solutions space.



RECOGNITION CRITERIA	
Business Impact	*Technology Leverage*
Financial Performance	Commitment to Innovation
Customer Acquisition	Commitment to Creativity
Operational Efficiency	Stage Gate Efficiency
Growth Potential	Commercialization
Human Capital	Application Diversity

The Transformation of the Social Media Intelligence Solutions Industry

With the growing variety of social media platforms, businesses and governments need advanced capabilities to proactively identify, track, and react to conversations on social media to prevent potentially dangerous or inaccurate information (mis/disinformation) before it impacts a company's brand, influences community opinion, or leads to physical harm. As a result, social media intelligence (SOCMINT) solutions have gone from a want-to-have to an absolute need for businesses, communities, and governments to understand shifting sentiment and arising crises in real-time.

SOCMINT solutions have evolved to enable enhanced conversation tracking, including identifying and following the information origin and social virality, and validating threats as authentic or fake. Furthermore, SOCMINT allows operators to find the jumps between social media sites to identify how the conversations move between those sources or social sites. With the increased use of artificial intelligence (AI), Frost & Sullivan appreciates how SOCMINT solutions can provide greater insights on narrative authenticity, modeling the threat types and combatting deepfake threats and those derived from bot campaigns.

Despite significant advancements in SOCMINT capabilities, adoption remains hindered by customers' lack of trust in a solution's ability to accurately determine whether threats are real and require remediation. Furthermore, even when mis/disinformation is identified as dangerous, SOCMINT solutions often lack the necessary integrations to recommend or execute the most effective next steps for mitigating the threat's impact.

Further complicating SOCMINT needs, AI technology is being exploited by bad actors to automate the creation of thousands of fake social media accounts, amplify false narratives, and manipulate public opinion on a massive scale. AI-driven tools and techniques that were once heralded for their ability to filter and flag false content are now being exploited by threat actors to create and spread disinformation at an unprecedented scale. Moreover, the rise of GenAI enables the creation of highly convincing fake accounts and content, making it harder for manual detection methods to identify them as fake and harmful. These AI-generated bots and deepfakes can mimic human behavior with remarkable accuracy, flooding social media platforms with misleading information and eroding public trust.

> *"Cyabra's advanced platform goes beyond traditional SOCMINT capabilities, empowering clients to understand what is being said and by whom, and whether it is an organized social campaign. The platform also identifies any malicious patterns or threat actions within social metadata, while analyzing user behaviors to identify commonalities."*
>
> ***- Danielle VanZandt***
> ***Research Manager,***
> ***Commercial & Public Security***

Cyabra, a leader in SOCMINT, provides solutions tailored to customers specific audience base or business goals, including public relations (PR) and marketing, the public sector, and cybersecurity. Its leading capabilities (including authenticity analysis, disinformation detection, and sentiment analysis), detect and track dangerous mis/disinformation, and identify potential threats enabling operators to proactively act to mitigate negative impacts on a brand or potential physical harm. Moreover, Cyabra leverages advanced AI and machine learning (ML) technologies to monitor and analyze online conversations in real-time, identifying and mitigating disinformation. Its platform collects publicly available data from various sources, including social media and news sites, and applies proprietary algorithms to assess authenticity and sentiment. By uncovering fake accounts and tracking disinformation waves, Cyabra empowers organizations to protect their brand reputation and ensure the authenticity of online discourse. Its solutions leverage AI-powered deep insights into operator-specific intelligence streams, offering impactful deep analysis guiding relevant mitigation steps and empowering informed decision-making.

As a result, Cyabra is a unique leader within the SOCMINT solutions market, working with 19 democracies worldwide in 2024 alone to monitor and protect elections and currently partnering with some of the largest brands and PR/Marketing agencies globally.

Technology Leadership

Cyabra's advanced platform goes beyond traditional SOCMINT capabilities, empowering clients to understand what is being said and by whom, and whether it is an organized social campaign. Its key differentiation stems from its ability to identify fake accounts on social media and include them within its wider SOCMINT capabilities.

Cyabra's proprietary algorithms assess authenticity, enabling the company to identify fake accounts (such as sock puppets, avatars, and bots) and filter between real and fake authors. It does this by analyzing patterns typical of fake profiles spreading harmful narratives, tracking the source and spread of information to measure its reach and impact.

Cyabra's technology is built on semi-supervised ML algorithms to determine the authenticity of a social media account in real-time. Cyabra's proprietary algorithm examines hundreds of behavioral parameters and then presents its analysis as a binary answer with a confidence score to show how the platform determined whether an account was authentic or inauthentic.

The platform also identifies any malicious patterns or threat actions within social metadata, while analyzing user behaviors to identify commonalities. Beyond basic social media listening, the company provides sentiment analysis, user profiling, and proactive, contextual insights to offer a deep dive into emerging trends. Cyabra pairs information gathered with common threat signals to verify the authenticity of a detected threat, ensuring that reported intelligence is credible and potentially harmful. This accuracy allows security operators to efficiently assess threats, optimizing response time and minimizing wasted resources to non-threatening mis/disinformation. Moreover, the platform provides customers with proposed mitigation steps that they can enact, in addition to pattern and tactic identification. The platform also enacts proactive monitoring to track specific threat vectors, enabling future and real-time awareness for subsequent threats. Moreover, with narrative detection becoming an increasingly sought after request from SOCMINT tools, Cyabra's unique approach with authenticity capabilities empowers its narrative analysis to be also mapped by the authenticity of profiles and communities.

Cyabra offers native and audience-based translations for its social monitoring capabilities integrated directly into its platform, ensuring full visibility into potential social traffic. The company also monitors alternative media, including non-English platforms, allowing for enhanced capture understanding of where harmful campaigns and traffic span from, particularly beneficial when tracking foreign interference and mis/disinformation spread. This inclusive span of SOCMINT and open-source intelligence (OSINT) technologies enables Cyabra to capture a deep understanding of sentiment and metadata highlighting threats that emerge from both authentic actors, as well as those originating from coordinated mis/disinformation campaigns which often contain higher elements of inauthentic activity

Flexibility Aligned with Sector-Specific Needs

Cyabra's extensive product line is tailored to customers' specific needs, whether it be for business in PR and marketing management, security for the public sector, or enhanced cybersecurity applications. The company's portfolio is General Data Protection Regulation compliant, and it designs capabilities directly to clients' needs, ensuring relevant risk identification to enable increased security.

PR/Marketing

Cyabra's PR and marketing solutions have two key focuses: brand protection and customer expansion. Its brand protection offerings track brand mentions, narratives, and sentiments to detect changes in emotion or conversations and potential risks to the brand. The company's AI solutions uncover fake accounts, generative AI (GenAI) content, bot networks, and disinformation campaigns that can impact a client's brand. Cyabra provides proactive, real-time risk alerts that enable clients to defend against potential reputation crises before they arise. Moreover, the company's brand protection solutions include crisis prevention and management, giving clients support across the complete brand protection journey.

Cyabra's PR and marketing brand expansion solutions track and analyze consumer behavior, improving decision-making with actionable insights about customers' feelings to enhance brand loyalty.

Furthermore, the company identifies authentic, relevant trends and finds potential new customers (including leaders, communities, or influencers) enabling clients to expand their audience and increase revenues. Finally, it empowers competitor benchmarking, allowing clients to compare online conversations and social performance with competitors to better understand how to enhance brand loyalty. Cyabra's PR and marketing solutions can be delivered as a Software-as-a-Service (Saas), Application Programming Interface (API), alerts, or managed services, tailoring delivery directly to a customer's needs and budget.

Public Sector

Cyabra's public sector solutions provide governments and communities with online monitoring to protect against risks to public safety (including election interference, foreign influence, protection from mis/disinformation, and inciting civil unrest). The company's OSINT platform detects influence operations and social engineering attacks in real-time across the internet, while its SOCMINT solutions uncover threats on social media. Its vast array of solutions detects risks at the individual level and can identify and map emerging narratives and large-scale unrest, giving communities a complete breadth of monitoring to empower public safety.

Cyabra's software identifies bot networks, disinformation campaigns, and influential and malicious actors (whether local or foreign) that are sowing mistrust, manipulating conversations, or inciting public unrest. It monitors harmful or illegal online activity (such as gun violence threats, gang activity, illegal drug trades, and cyber predators) by conducting psychological operations analysis, enabling the company to identify potential threats to communities proactively. On a large-scale, Cyabra maps communities and identifies emerging narratives, empowering real-time tracking of online protests as they escalate and uncovering the leaders fueling online civil unrest to help law enforcement manage arising situations more effectively.

Its public sector solutions are delivered as SaaS, API, or on-premises, providing flexible options meeting customer's budget and security needs.

Cyber and Security

Cyabra's cyber and security solutions defend against impersonation, phishing attacks, and executive threats arising on social media. The company's 24/7 intelligence feed identifies, tracks, and monitors harmful sentiments from inauthentic, GenAI, deepfakes, or bot campaigns impersonating a brand or employee that is attempting to harm a company or brand by spreading mis/disinformation. By contextualizing the proliferation, Cyabra identifies and monitors groups and places of interest to enable long-term security and proactive harmful sentiment detection. Moreover, the company provides enhanced monitoring for digital threats, including social threat detection, and monitors physical assets to identify dangers arising from online conversations. As such, it provides comprehensive protection for executives from emerging threats, online hate, or exposure to sensitive data.

Delivered as an application programming interface, SaaS, or alerts, Cyabra delivers full-scale and broad-spectrum online protection of physical assets, brand reputation, and executives.

"Cyabra pairs information gathered with common threat signals to verify the authenticity of a detected threat, ensuring that reported intelligence is credible and potentially harmful. This accuracy allows security operators to efficiently assess threats, optimizing response time and minimizing wasted resources to non-threatening mis/disinformation. Moreover, the platform provides customers with proposed mitigation steps that they can enact, in addition to pattern and tactic identification."

- Danielle VanZandt
Research Manager,
Commercial & Public Security

Customer-Specific Value Creation

Cyabra's vision is to understand the authenticity of social media data and combat damaging mis/disinformation. The company has an actor-behavior-content methodology focus, showing the complete picture of the metadata and SOCMINT intelligence to understand what is real or false. Cyabra educates customers proactively on tactics being deployed, helping them to understand how to identify and react to disinformation tactics. Its clients experience high value on tracking due to the capabilities being tailored to their specific applications. For example, the company's government clients mainly track for threats around specific events or major foreign or domestic priorities through coordinated activity, allowing for more efficient and effective actions by law enforcement. Its private brand clients track potential crises that could affect consumers or impact brand reputation, leveraging Cyabra's solutions to identify potential issues and conduct crisis planning, minimizing potential damage to their brand that can lead to lost customers or decreased revenues.

By empowering value creation tied to a client's specific application, Frost & Sullivan believes Cyabra is a leader within the SOCMINT industry, poised to experience high brand loyalty and overall growth as it extends its value creation through innovation.

Ongoing Commitment to Technology Innovation to Combat Emerging Threats

Cyabra's focus on authenticity is a central tenant of its research and development pipeline. It continuously enhances its detection and monitoring to evolve with advancing technologies and thereby threats. As a result of an inbound customer request, the company is expanding its authenticity capabilities for applicability for GenAI threats. It is also developing ongoing, automated analysis and alerting, building cases and timelines for greater threat monitoring and enhanced visibility. Finally, Cyabra is creating remediation solutions for customers, providing them with enhanced next steps for proper threat mitigation.

In addition to its innovation roadmap directly aligned with customer feedback and emerging needs, Cyabra continuously invests in leading expertise, ensuring that it remains on the knowledge forefront and can infuse this proficiency into its innovations. For example, Mike Pompeo, former Secretary of State and previous director of the CIA, joined Cyabra's board in January 2024, bringing it a firsthand perspective of leading threats and emerging needs within social media intelligence solutions.

Cyabra expects to be listed on the Nasdaq in May 2025, becoming the first publicly traded company solely dedicated to fighting disinformation.

Frost & Sullivan believes Cyabra's ongoing investment in technology innovation empowers true visibility for customers, offering a better possibility for successful outcomes.

Conclusion

With the growing variety of social media platforms, businesses and governments need advanced capabilities to proactively identify, track, and react to conversations on social media to combat potentially dangerous or disinformation. Social media intelligence (SOCMINT) solutions enable the identification and monitoring of both potentially dangerous authentic actors and mis/disinformation for various applications, including the public sector and businesses, allowing operators to act to mitigate damage (whether physical threats or to a brand's reputation) proactively.

A leader in SOCMINT, Cyabra's SOCMINT portfolio enables identification and tracking of mis/disinformation and harmful narratives derived from various avenues, including inauthentic, generative artificial intelligence (GenAI), deepfakes, or bot campaigns. The company's advanced features empower full-spectrum threat monitoring, such as authenticity investigation, disinformation and harmful narrative detection, and sentiment analysis, to detect and track dangerous mis/disinformation. Its solutions also enable monitoring for potential threats, allowing operators to proactively mitigate negative impacts on a brand or stop potential physical harm.

Cyabra's inclusive span of SOCMINT and open-source intelligence (OSINT) technologies enables Cyabra to capture a deep understanding of sentiment and metadata highlighting threats that emerge from both authentic actors, as well as those originating from coordinated mis/disinformation campaigns which often contain higher elements of inauthentic activity. Moreover, the company's solutions drive AI-powered insights into operator-specific intelligence streams, offering impactful deep analysis guiding relevant mitigation steps. As a result of its commitment to remaining on the forefront of threat detection, Cyabra invests heavily in technology innovation and focuses on expanding its authenticity capabilities to be relevant for GenAI campaigns and enhance automated analysis and alerting.

With its strong overall performance, Cyabra earns Frost & Sullivan's 2025 North American Technology Innovation Leadership Recognition for its strong overall performance in the social media intelligence solutions Industry

What You Need to Know about the Technology Innovation Leadership Recognition

Frost & Sullivan's Technology Innovation Leadership Recognition is its top honor and recognizes the market participant that exemplifies visionary innovation, market-leading performance, and unmatched customer care.

Best Practices Recognition Analysis

For the Technology Innovation Leadership Recognition, Frost & Sullivan analysts independently evaluated the criteria listed below.

Technology Leverage

Commitment to Innovation: Continuous emerging technology adoption and creation enables new product development and enhances product performance

Commitment to Creativity: Company leverages technology advancements to push the limits of form and function in the pursuit of white space innovation

Stage Gate Efficiency: Technology adoption enhances the stage gate process for launching new products and solutions

Commercialization: Company displays a proven track record of taking new technologies to market with a high success rate

Application Diversity: Company develops and/or integrates technology that serves multiple applications and multiple environments

Business Impact

Financial Performance: Strong overall business performance is achieved in terms of revenue, revenue growth, operating margin, and other key financial metrics

Customer Acquisition: Customer-facing processes support efficient and consistent new customer acquisition while enhancing customer retention

Operational Efficiency: Company staff performs assigned tasks productively, quickly, and to a high-quality standard

Growth Potential: Growth is fostered by a strong customer focus that strengthens the brand and reinforces customer loyalty

Human Capital: Leveraging innovative technology characterizes the company culture, which enhances employee morale and retention

Best Practices Recognition Analytics Methodology

Inspire the World to Support True Leaders

This long-term process spans 12 months, beginning with the prioritization of the sector. It involves a rigorous approach that includes comprehensive scanning and analytics to identify key best practice trends. A dedicated team of analysts, advisors, coaches, and experts collaborates closely, ensuring thorough review and input. The goal is to maximize the company's long-term value by leveraging unique perspectives to support each Best Practice Recognition and identify meaningful transformation and impact.

		VALUE IMPACT	
STEP		WHAT	WHY
1	**Opportunity Universe**	Identify Sectors with the Greatest Impact on the Global Economy	Value to Economic Development
2	**Transformational Model**	Analyze Strategic Imperatives That Drive Transformation	Understand and Create a Winning Strategy
3	**Ecosystem**	Map Critical Value Chains	Comprehensive Community that Shapes the Sector
4	**Growth Generator**	Data Foundation That Provides Decision Support System	Spark Opportunities and Accelerate Decision-making
5	**Growth Opportunities**	Identify Opportunities Generated by Companies	Drive the Transformation of the Industry
6	**Frost Radar**	Benchmark Companies on Future Growth Potential	Identify Most Powerful Companies to Action
7	**Best Practices**	Identify Companies Achieving Best Practices in All Critical Perspectives	Inspire the World
8	**Companies to Action**	Tell Your Story to the World (BICEP*)	Ecosystem Community Supporting Future Success

*Board of Directors, Investors, Customers, Employees, Partners

About Frost & Sullivan

Frost & Sullivan is the Growth Pipeline Company™. We power our clients to a future shaped by growth. Our Growth Pipeline as a Service™ provides the CEO and the CEO's growth team with a continuous and rigorous platform of growth opportunities, ensuring long-term success. To achieve positive outcomes, our team leverages over 60 years of experience, coaching organizations of all types and sizes across 6 continents with our proven best practices. To power your Growth Pipeline future, visit Frost & Sullivan at http://www.frost.com.

The Growth Pipeline Generator™

Frost & Sullivan's proprietary model to systematically create ongoing growth opportunities and strategies for our clients is fuelled by the Innovation Generator™.

Learn more.

Key Impacts:

- **Growth Pipeline:** *Continuous Flow of Growth Opportunities*
- **Growth Strategies:** *Proven Best Practices*
- **Innovation Culture:** *Optimized Customer Experience*
- **ROI & Margin:** *Implementation Excellence*
- **Transformational Growth:** *Industry Leadership*



The Innovation Generator™

Our 6 analytical perspectives are crucial in capturing the broadest range of innovative growth opportunities, most of which occur at the points of these perspectives.

Analytical Perspectives:

- Megatrend (MT)
- Business Model (BM)
- Technology (TE)
- Industries (IN)
- Customer (CU)
- Geographies (GE)

