Darktrace Recognized for

2021

Technology Innovation Leadership

North American Industrial Cybersecurity AI Industry

Excellence in Best Practices

FROST & SULLIVAN

Best Practices Criteria for World-Class Performance

Frost & Sullivan applies a rigorous analytical process to evaluate multiple nominees for each award category before determining the final award recipient. The process involves a detailed evaluation of best practices criteria across two dimensions for each nominated company. Darktrace excels in many of the criteria in the industrial cybersecurity AI space.

AWARD CRITERIA

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

Commitment to Innovation and Creativity, and Application Diversity

Industrial cybersecurity focused on securing operational technology (OT) alone is not ideal because it is an inherently historical and retrospective approach in a constantly evolving threat landscape. A unified view and protection across interconnected OT and information technology (IT) is now more crucial than ever before. Just this year, for example:

- The Colonial Pipeline incident was not a targeted OT attack; ransomware compromised IT systems, and out of an abundance of caution the pipeline operator decided to shut down OT to avoid any safety issues.
- In the JBS Foods cyberattack, ransomware compromised IT yet indirectly affected OT.

  A static, siloed approach to security based on fixed lists/baselines or rules or signatures will not suffice as novel and zero-day attacks launched by unknown threat actors increasingly target industrial environments.

Darktrace, with its world-leading team of AI and cyber experts with industrial and government intelligence backgrounds (e.g., MI5, Government Communications Headquarters, FBI, and CIA), offers a self-learning artificial intelligence (AI) technology for autonomous threat detection, investigation, and response. Research and development is at the heart of Darktrace as it continually refines its product

offerings and technology for the industrial space. Frost & Sullivan found that Darktrace displays its technological leadership on several fronts.

While most cybersecurity AI offerings automate manually defined human processes or playbooks, or act based on predefined threats, Darktrace's self-learning AI uniquely identifies any unusual activities that may indicate an attack, even if it has never been seen before. The self-learning approach understands the normal patterns of life for each user, device, environment, and controller across the OT and IT landscape and immediately detects, contextualizes and reports on all indicators of threat, no matter how small.

Darktrace has an open and extensible architecture and can complement a variety of solutions due to its adaptive, fluid, and protocol-agnostic technology. The self-learning AI technology works seamlessly across both the IT and OT ecosystem, spanning on-premise, cloud and email environments as well as industrial control systems (ICS) on the factory floor.

Frost & Sullivan finds that Darktrace's holistic, dynamic, and adaptive approach to cybersecurity is an especially critical capability for diverse, bespoke ICS environments with a variety of industrial protocols and devices. Darktrace's self-learning AI autonomously adapts to learn a normal 'pattern of life' for each new individual device and plant, in addition to the enterprise environment as a whole, and then warns against atypical actions and behaviors that represent threats.

Many OT-focused security vendors are unaware of threats that originate in IT systems that can subsequently compromise OT systems, either directly or indirectly. However, because Darktrace technology extends across IT, cloud, SaaS, email, and OT environments, it is able to identify and stop threats wherever they originate. This holistic approach to identifying and thwarting threats provides unrivaled protection for mission-critical assets.

In addition to its trademark self-learning approach for cyber defense, Darktrace recently announced the release of new industrial security capabilities surrounding active device identification and vulnerability tracking. These provide Darktrace customers with information that enables their unique compliance with reference to cybersecurity frameworks, cyber hygiene best practices, and government regulations. Active device identification and vulnerability tracking are carried out in the narrowest way possible to mitigate the potential risk of disruption to sensitive OT systems.

Antigena, Darktrace's autonomous response solution, stops attacks at their earliest stages, and can mitigate the lateral spread of attacks to avoid compromising mission critical systems and assets. Antigena can be used in an active mode (where it autonomously takes action) or in a human confirmation mode (where it waits for a security analyst to approve an autonomous action). Antigena is thus customizable to each customer's individual needs, landscape, and risk appetite. Frost & Sullivan finds that the key advantage of Antigena is that the technology leverages advanced mathematical computations and AI learnings to respond with surgical precision, in order to maintain business continuity even as it takes decisive action. For instance, if a ransomware attack in a manufacturing plant has the potential to spread to multiple devices, Antigena can contain the threat to the point of origin, avoiding the spread of attack and protecting industrial manufacturing operations from costly downtime.

Darktrace also offers an investigation component for proactive threat hunting. Its Cyber AI Analyst

technology executes its own autonomous investigations. All unusual activity detected by the Industrial Immune System is automatically fed into Cyber Analyst AI, which comprehensively and automatically stitches together disparate data, rationalizes the findings, and reports actionable insights in a fraction of the time required by a cyber analyst. The average time savings with the Cyber AI Analyst is around 92%. Moreover, the issues are identified near real-time at the point of origin, escaping the costly cycle time delays associated with sending disparate data to a SIEM for secondary analysis.

Frost & Sullivan recognizes Darktrace for offering technology based on self-learning AI that provides autonomous detection, investigation, and response against novel attacks by unknown actors in the evolving cyber threat landscape.

Customer Acquisition, Financial Performance, and Growth Potential

Darktrace's first customer was one of the biggest power plants in the United Kingdom, and it has since expanded into other types of industrial environments including renewables and critical infrastructure. Today, Darktrace protects organizations across all 16 CISA critical infrastructure sectors. Customers find Darktrace appealing because it seamlessly protects IT, OT, email and cloud environments, regardless of the presence of bespoke systems and or protocols. Growth across the United States, Europe, and the Asia-Pacific regions is evidence that a rear-view approach to identifying and containing threats is no longer sufficient in this complex, ever-changing threat landscape.

> *"Customers find Darktrace appealing as it protects their existing systems and allows them to safely and securely transition into their future cyber-physical systems."*
>
> ***- Sankara Narayanan, Senior Industry Analyst***

New initiatives from the Biden administration to upgrade industrial cybersecurity in the United States should further heighten the need for technologies such as self-learning AI across the nation's critical infrastructure. Earlier this year, the Biden Administration published an Executive Order on improving the nation's cyber security, including ICS cyber security for electric utilities, and similar initiatives are planned for water and energy in the near future. The Department of Energy is advocating for threat detection and response for OT environments and for unified protection of IT and OT environments—all of which Darktrace can offer.

Conclusion

Industrial organizations need an advanced technology platform that can help detect and respond to novel attacks, even if they are waged by unknown threat actors. Darktrace's self-learning AI platform addresses this need. It's adaptive and interoperable technology dynamically and continuously learns normal patterns for all devices and controllers across an industrial environment, looking for subtle indicators of unusual and threatening activity rather than acting upon only predefined threats.

Companies can no longer rely on baselines or rules or signatures that fail to detect the 'unknown unknowns'. Darktrace has consistently proven its ability to catch novel and never-before-seen attacks across its customer base. The strength of its self-learning AI based approach to industrial cyber defense is underscored by the fact that all 16 CISA critical infrastructure sectors—among the most sensitive and vital cyber-ecosystems in the US—rely upon Darktrace's self-learning AI to defend their environments.

Frost & Sullivan advocates that a siloed OT-focused security approach is insufficient given the criticality of business continuity for mission critical assets and the ability for threats to span across IT and OT environments. Frost & Sullivan is impressed that Darktrace's self-learning AI technology provides unified protection across IT and OT and other complex cyber-physical ecosystems and stops attacks in IT before they spill over into other systems. Darktrace's Antigena and Cyber AI Analyst further enhance customer value by providing autonomous response and investigation capabilities.

For its strong overall performance, Darktrace earns Frost & Sullivan's 2021 North American Technology Innovation Leadership Award in the industrial cybersecurity AI market.

© Frost & Sullivan 2021

What You Need to Know about the Technology Innovation Leadership Recognition

Frost & Sullivan's Technology Innovation Leadership Award recognizes the company that has introduced the best underlying technology for achieving remarkable product and customer success while driving future business value.

Best Practices Award Analysis

For the Technology Innovation Leadership Award, 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 Success: 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 financial performance is achieved in terms of revenues, 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: Commitment to quality and to customers characterize the company culture, which in turn enhances employee morale and retention

© Frost & Sullivan 2021

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 Engine™

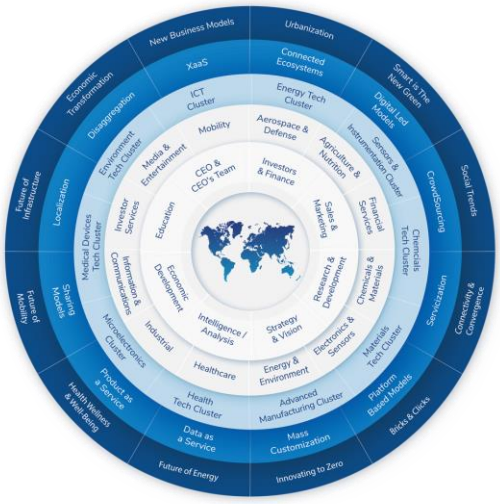
Frost & Sullivan's proprietary model to systematically create ongoing growth opportunities and strategies for our clients is fuelled by the Innovation Generator™.
Learn more.

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:

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