FROST & SULLIVAN

2024 COMPANY OF THE YEAR

IN THE DACH MANAGED SECURITY SERVICES INDUSTRY

T-SECURITY

FROST & SULLIVAN

2024 BEST PRACTICES AWARD

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. Deutsche Telekom excels in many of the criteria in the managed security services space.

Visibility is the First Step Towards Better Cybersecurity.

In today's cybersecurity landscape where threats are becoming even more sophisticated and diverse, enterprises increasingly resort to managed security services to improve their cybersecurity stance.

> *"Deutsche Telekom's MDR service portfolio offers holistic security by covering all potential entry points, ensuring no part of the organization is unprotected. It can detect and respond to threats quickly and effectively by leveraging multi-source telemetry and advanced analytics. Integrating various security tools and data sources into a single platform reduces complexity and inefficiencies."*
>
> ***- Claudio Stahnke***
> ***Industry Analyst***

Deutsche Telekom represents one of the most prominent players in the space, especially in the DACH region. Its robust economic performance is evidenced by revenue exceeding €400 million from its security offerings. This impressive financial achievement is derived from various sources - including infrastructure, network security, cyber defense, identity and access management, and consulting services. These revenue streams highlight the company's diversified portfolio and strong market position, reinforcing its leadership in the cybersecurity sector.

Deutsche Telekom's initiative to offer multi-source Extended Detection and Response (XDR) telemetry is a significant advancement. This approach integrates investigation, orchestration, and automation across five critical pillars: endpoints, identities, connectivity, cloud, and Operational Technology (OT).

Endpoints, including computers, mobile devices, and IoT devices, are common cyber-attack targets. Deutsche Telekom's MDR service portfolio enhances security by monitoring and analyzing endpoint activities to detect threats in real-time, isolate infected devices, limit the spread of malware, and initiate remediation processes. This comprehensive visibility into endpoint security postures and vulnerabilities enables proactive threat management.

Identity theft and misuse of credentials are significant concerns in cybersecurity. Focusing on identities, the MDR solution ensures secure authentication through multi-factor and continuous methods, protecting user identities. It monitors user activities to detect unusual access patterns and potential compromises while managing and controlling access to critical resources, ensuring that users have the appropriate level of access.

Secure Access Service Edge (SASE) combines networking and security functions to protect data in transit. Deutsche Telekom's MDR service portfolio leverages SASE to provide secure and efficient connectivity for remote employees, reducing risks associated with remote access. It applies consistent security policies across all network edges, ensuring a holistic defense strategy and optimizing network performance while maintaining security.

As organizations increasingly migrate to cloud environments, securing cloud infrastructure becomes crucial. The XDR approach provides visibility across public, private, and hybrid clouds to ensure comprehensive security. It detects and responds to threats unique to cloud environments, such as misconfigurations and unauthorized access, ensuring that cloud deployments meet regulatory and compliance requirements and reducing the risk of non-compliance.

Operational Technology (OT) systems, such as those used in industrial control systems (ICS), are critical to infrastructure, but often lack modern security measures. Deutsche Telekom's MDR services monitor and secure OT environments, preventing disruptions to essential services. It offers a unified view of IT and OT security, enables coordinated defense strategies, and implements security measures for legacy OT systems that cannot be easily updated or replaced.

Deutsche Telekom's MDR service portfolio offers holistic security by covering all potential entry points, ensuring no part of the organization is unprotected. It can detect and respond to threats both quickly and effectively by leveraging multi-source telemetry and advanced analytics. Integrating various security tools and data sources into a single platform reduces complexity and inefficiencies. Scalable and flexible, the solution adapts to new threats and changing business needs. Enhanced automation of routine security tasks frees up security teams to focus on strategic initiatives, reducing the potential for human error.

Automation is a Necessity, not a Luxury

Frost & Sullivan believes that Deutsche Telekom's commitment to implementing best practices is quite evident in its strategic use of Artificial Intelligence (AI) and Machine Learning (ML) for threat analysis. The company's approach is particularly relevant in today's cybersecurity landscape, where the volume and complexity of threats are continuously increasing.

Deutsche Telekom's strategy goes beyond continuous anomaly detection, focusing on decision augmentation and automation to optimize human resources and improve response times and accuracy.

AI and ML play a pivotal role in this framework, significantly enhancing the company's ability to detect and respond to threats swiftly and accurately. This integration is part of their broader strategy to transcend traditional methods, adopting advanced techniques that provide superior protection for their clients.

In the current cybersecurity environment, many organizations struggle with an overwhelming amount of data and the speed at which threats evolve. Traditional security measures often fail to address these challenges effectively. By leveraging AI and ML, Deutsche Telekom can analyze vast amounts of data in real-time, identify patterns, and detect anomalies that might indicate a security threat. Frost & Sullivan recognizes how this capability is crucial for staying ahead of increasingly sophisticated cyber threats.

Furthermore, Deutsche Telekom's decision augmentation and automation approach aims to optimize human resources by automating routine tasks, allowing cybersecurity professionals to focus on more complex and strategic issues. This improves response times and enhances the accuracy of threat detection and mitigation efforts. Automating mundane and repetitive tasks reduces the potential for human error. It ensures that security teams can concentrate on tasks that require human intelligence and creativity - such as threat hunting and strategic planning.

"In the current cybersecurity environment, many organizations struggle with an overwhelming amount of data and the speed at which threats evolve. Traditional security measures often fail to address these challenges effectively. By leveraging AI and ML, Deutsche Telekom can analyze vast amounts of data in real-time, identify patterns, and detect anomalies that might indicate a security threat. This capability is crucial for staying ahead of increasingly sophisticated cyber threats."

- Claudio Stahnke
Industry Analyst

Finally, this strategy exemplifies the shift towards more intelligent, automated security solutions. As cyber threats become more advanced, integrating AI and ML into cybersecurity frameworks is increasingly seen as a necessity rather than a luxury. This approach aligns with industry trends where organizations seek to enhance their security posture through advanced technologies that provide real-time insights and proactive defense mechanisms.

Streamlined Portfolios and Processes Help Stabilize SMEs get on the Cybersecurity Ladder

The company's efforts to simplify pricing structures and improve scalability aim to make it easier for businesses to adopt their security solutions. By streamlining these processes, Deutsche Telekom ensures that new clients can be onboarded within 30 days on average, providing quick access to robust security measures. Deutsche Telekom's efforts to cater to clients ranging from small and medium enterprises (SMEs) to large global enterprises across diverse verticals are quite commendable. The company's tailored solutions and consulting services address the unique needs of SMEs, providing them with robust protection against cyber threats despite budget constraints and technological disparities.

Properly recognizing the specific needs of SMEs, Deutsche Telekom has developed scalable and cost-effective solutions to provide robust cybersecurity protection. By leveraging strategic partnerships and offering tailored expertise, the company addresses SMEs' budget constraints and technological disparities, ensuring they receive the necessary protection against cyber threats. Deutsche Telekom's future strategy includes expanding its AI capabilities to offer standardized and highly automated solution

packages. This will enable the company to develop scale and offer a lower entry point to SMEs with more constrained budgets - or those that do not yet consider cybersecurity a high priority. This strategic move will ensure that all businesses, regardless of size, have access to top-tier security solutions.

Conclusion

Deutsche Telekom has established itself as a leader in today's rapidly evolving cybersecurity landscape, particularly in the DACH region. The company's multi-source MDR service portfolio integrates endpoint, identity, connectivity, cloud, and OT security, providing holistic protection against sophisticated cyber threats. By leveraging AI and ML, Deutsche Telekom enhances threat detection and response, ensuring both timely and accurate mitigation. The company's streamlined pricing and scalable solutions make advanced cybersecurity accessible to SMEs, addressing their unique needs and budget constraints.

Deutsche Telekom's forward-looking strategy, including expanding AI capabilities and automating security processes, positions it to continue leading the industry. This comprehensive approach safeguards enterprises of all sizes. It sets a benchmark for excellence in managed security services, reinforcing Deutsche Telekom's role as a pivotal player in global cybersecurity.

With its strong overall performance, Deutsche Telekom earns the 2024 Frost & Sullivan DACH Company of the Year Award in the Managed Security Services industry.

What You Need to Know about the Company of the Year Recognition

Frost & Sullivan's Company of the Year Award is its top honor and recognizes the market participant that exemplifies visionary innovation, market-leading performance, and unmatched customer care.

Best Practices Award Analysis

For the Company of the Year Award, Frost & Sullivan analysts independently evaluated the criteria listed below.

Visionary Innovation & Performance

Addressing Unmet Needs: Customers' unmet or under-served needs are unearthed and addressed by a robust solution development process

Visionary Scenarios Through Mega Trends: Long-range, macro-level scenarios are incorporated into the innovation strategy through the use of Mega Trends, thereby enabling first-to-market solutions and new growth opportunities

Leadership Focus: Company focuses on building a leadership position in core markets and on creating stiff barriers to entry for new competitors

Best Practices Implementation: Best-in-class implementation is characterized by processes, tools, or activities that generate a consistent and repeatable level of success

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

Customer Impact

Price/Performance Value: Products or services provide the best value for the price compared to similar market offerings

Customer Purchase Experience: Quality of the purchase experience assures customers that they are buying the optimal solution for addressing their unique needs and constraints

Customer Ownership Experience: Customers proudly own the company's product or service and have a positive experience throughout the life of the product or service

Customer Service Experience: Customer service is accessible, fast, stress-free, and high quality

Brand Equity: Customers perceive the brand positively and exhibit high brand loyalty

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™

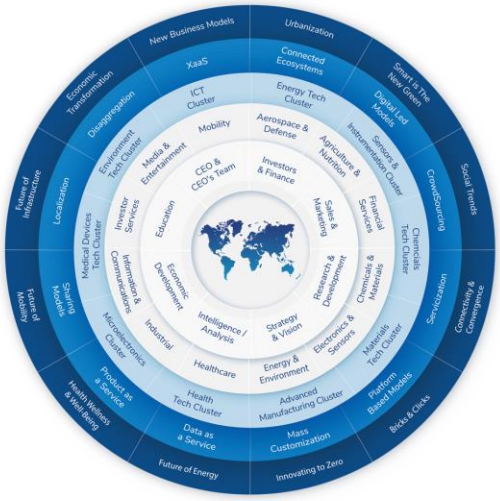
Frost & Sullivan's proprietary model to systematically create ongoing growth opportunities and strategies for our clients is fuelled by the Innovation Generator™.
Learn more.

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)