NETSCOUT

2025 TECHNOLOGY INNOVATION LEADER

Enhancing Customer Impact Through Powerful Technology Integration

RECOGNIZED FOR BEST PRACTICES IN THE MENA CYBERSECURITY INDUSTRY

FROST & SULLIVAN

Table of Contents

Best Practices Criteria for World-class Performance ***3***
NETSCOUT: Committed to Cybersecurity Innovation 3
AI/ML-Powered Defense: A Major Shift in Cybersecurity 3
Adaptive Threat Detection and Response 4
Commercializing DDoS Defense: NETSCOUT & Arelion's Strategy 5
NETSCOUT: Powering Resilient IT with Unified Visibility 5
Visibility Without Borders (VWB) for Seamless Integration 5
Integrating Analytics, Automation, and Security 6
Unified Data for Proactive Performance Management 6
Optimizing Network Performance to Drive Customer Acquisition 6
Growth Potential: NETSCOUT Strengthens Digital Security 7
Optimizing Operational Efficiency with End-to-End Network Visibility 8

Conclusion ***9***

What You Need to Know about the Technology Innovation Leadership Recognition ... ***10***

Best Practices Recognition Analysis **10**
Technology Leverage 10
Business Impact 10

Best Practices Recognition Analytics Methodology ***11***

Inspire the World to Support True Leaders **11**

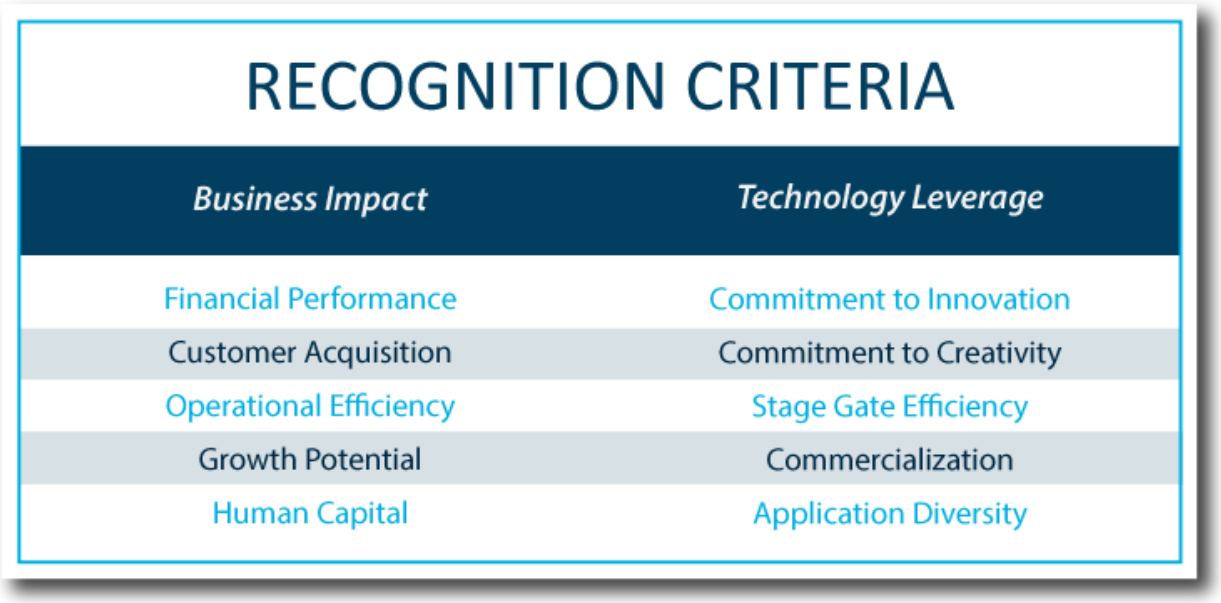
About Frost & Sullivan ***12***

The Growth Pipeline Generator™ **12**

The Innovation Generator™ **12**

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. NETSCOUT excels in many of the criteria in the Cybersecurity space.



NETSCOUT: Committed to Cybersecurity Innovation

In today's rapidly evolving digital ecosystem, enterprises are grappling with unprecedented cyber threats that endanger their critical IT infrastructure. Legacy security measures designed for a simpler era are no match for modern adversaries deploying DDoS attacks, ransomware, stealthy network intrusions and crippling data breaches. As organizations expand their digital footprints, network complexity surges, creating new vulnerabilities.

AI/ML-Powered Defense: A Major Shift in Cybersecurity

> *"NETSCOUT's AI/ML integration redefines cybersecurity by transforming reactive defenses into proactive shields. Its dynamic threat detection synchronizes network and security operations, enabling enterprises to preempt cyberattacks, secure infrastructure, and bolster robust digital trust amid evolving threats."*
>
> ***- Sapan Agarwal***
> ***SVP, Frost & Sullivan***

NETSCOUT has redefined cybersecurity by embedding artificial intelligence (AI) and machine learning (ML) into its core strategy. The company's AI-driven systems analyze vast streams of network traffic in real-time, identifying anomalies and triggering automated countermeasures. This approach transforms threat detection from reactive to predictive, enabling organizations to outpace adversaries. By leveraging historical patterns, the technology continuously enhances its algorithms, learning to spot even the faintest signals of malicious activity. It is a critical advantage in an era where threats evolve by the minute.

Adaptive Threat Detection and Response

Central to NETSCOUT's innovation is its ability to adapt. Contrasting static security tools, its AI/ML models evolve alongside emerging threats. For DDoS attack protection in particular, NETSCOUT leverages its ATLAS System which has a unique, global view into DDoS attack activity. Using AI/ML, vast amounts of DDoS attack information are transformed into actional intelligence that continuously arms all of their Arbor DDoS Protection solutions for automated DDoS attack mitigation. The solution autonomously adjusts to new attack patterns, minimizing reliance on manual intervention and shrinking the window of opportunity for cybercriminals. This dynamic defense mechanism is bolstered by the integration of NetOps and SecOps through NETSCOUT's unified platform, aligning network and security teams through a unified network data plane.

NETSCOUT nGenius® and Omnis Cyber Intelligence products exemplify NETSCOUT's innovative approach. It integrates these advanced technologies into a unified network data solution for network visibility, service assurance, and security, offering a comprehensive strategy to manage complex network environments. The company's integration of deep packet inspection with AI-driven analytics provides a more comprehensive view of network performance and security, setting it apart in the industry. NETSCOUT's emphasis on technological advancement and its focus on addressing critical customer needs to solidify its reputation as a pioneer in the industry. The company's commitment

to innovation and customer-centric solutions is evident in its ability to navigate the evolving needs of the network service assurance market.

Furthermore, the integration of the NetOps SecOps platform unifies network performance data with security analytics, offering a holistic view of network health. This unified approach enables proactive measures that pre-emptively address potential disruptions, thus minimizing downtime and financial losses. The commercial benefits of these proactive measures are significant: improved service availability, reduced costs associated with downtime and reinforced customer trust are among the key outcomes.

Securing Telecom Ecosystems: Cornerstone of Digital Trust

Acknowledging the critical role of telecommunications in global connectivity, NETSCOUT extends its expertise to safeguard mobile networks. Its Mobile Network Operator Security solutions are tailored to defend against sophisticated threats targeting 5G, IoT, and other next-gen infrastructures. By securing these systems, NETSCOUT ensures telecom providers maintain uptime, performance, and trust even as cyberattacks grow in scale and complexity.

Therefore, NETSCOUT's synergy of AI/ML, integrated operations and telecom security establishes a benchmark for defending intricate digital architectures. Its visionary approach not only tackles current weaknesses but anticipates emerging risks. Through sustained R&D investments, NETSCOUT drives innovation, enabling secure operations amid relentless technological change. As cyber dangers intensify, its progress heralds an era where smart, self-learning shields become vital protectors of worldwide systems.

Commercializing DDoS Defense: NETSCOUT & Arelion's Strategy

In a hyperconnected world, businesses confront relentless cyber risks, with Distributed Denial of Service (DDoS) attacks being a particularly disruptive challenge. These assaults can paralyze networks, causing costly outages and reputational damage. As attack methodologies grow more advanced, conventional reactive defenses fall short. Organizations now demand proactive, scalable solutions to shield infrastructure and sustain seamless operations.

In the world of sophisticated, modern-day DDoS attacks, Communication Service Providers (CSPs) play a major role in protection. For years, NETSCOUT's Arbor DDoS Attack protection solutions have enabled CSPs to not only protect their own infrastructure and services from DDoS attacks but also enable revenue via managed DDoS protection services for their customers. As an example, Arelion, a global Internet Services Provider, is partnering with NETSCOUT to offer a managed DDoS protection service to their enterprise customers. This strategic collaboration leverages NETSCOUT's advanced threat intelligence and real-time network monitoring integrated with Arelion's extensive global network infrastructure. The combined solution rapidly identifies abnormal traffic patterns and employs automated interventions to neutralize DDoS assaults before they impact essential services.

In conclusion, Arelion and NETSCOUT's expanded partnership signifies a strategic leap in DDoS defense commercialization. Blending cutting-edge security innovations with robust network scalability, the alliance equips enterprises to counter evolving threats while fostering long-term resilience. This model illustrates how preemptive security investments translate to tangible operational and financial returns. As cyber adversaries refine their tactics, adopting such forward-looking strategies becomes pivotal for maintaining service integrity and market competitiveness.

NETSCOUT: Powering Resilient IT with Unified Visibility

Modern organizations operate in increasingly complex IT environments where application performance directly impacts productivity and stability. Legacy systems and fragmented monitoring tools fail to provide a unified network view, leading to downtime and inefficiencies. The convergence of operational and cybersecurity challenges demands an integrated performance management solution.

> *"NETSCOUT's integrated performance management solutions deliver real-time analytics, proactive monitoring and cybersecurity within a unified platform. This approach mitigates inefficiencies, enhances collaboration and fortifies resilience, ensuring operational continuity and a competitive edge in today's digital landscape."*
>
> ***- Robin Joffe***
> ***Partner & MD, Frost & Sullivan***

Visibility Without Borders (VWB) for Seamless Integration

NETSCOUT's VWB platform tackles network complexity by merging performance management, cybersecurity, and availability into one solution. Powered by Adaptive Service Intelligence (ASI), it delivers real-time metadata from network traffic, ensuring consistent, actionable insights across IT infrastructures. Key components include Arbor DDoS Protection, which defends against cyber threats, and nGenius for Carrier Service Assurance, optimizing network performance across 4G/5G, IoT, cloud, and edge environments and Omnis Cyber Intelligence, an advanced deep-packet-inspection (DPI)-powered Network Detection

and Response solution. Its shared network data infrastructure fosters collaboration, enhancing operational efficiency for NetOp and SecOps teams.

Expanding Network Visibility with Edge Observability

NETSCOUT introduces the Business Edge Observability Suite to improve network visibility, featuring nGenius Edge Sensor and Remote InfiniStreamNG. These tools support retail, healthcare, and utilities, ensuring seamless monitoring and security for critical applications in remote locations. By integrating ASI technology, synthetic transaction testing, and automatic decryption, NETSCOUT delivers comprehensive observability, reducing risks and optimizing operations as edge computing expands.

Integrating Analytics, Automation, and Security

NETSCOUT has enhanced its performance management solution by incorporating advanced analytics, real-time monitoring, and automated problem resolution. Covering traditional data centers to modern cloud applications, this enriched platform improves visibility while embedding cybersecurity protections through Omnis Security, ensuring that security incidents don't disrupt operations.

Unified Data for Proactive Performance Management

The NetOps SecOps platform consolidates network operations and security analytics, offering a real-time IT infrastructure view. This correlation helps identify performance bottlenecks and security threats before they escalate, enabling proactive risk management, resource optimization, and increased productivity.

NETSCOUT's strategic integration of cybersecurity and performance management through Omnis Cyber Intelligence and NetOps SecOps represents a major step forward in handling IT complexities. This unified approach mitigates inefficiencies, enhances security, and ensures that performance optimization and cybersecurity work together to safeguard business continuity. As organizations navigate the digital era, NETSCOUT's solutions remain indispensable for ensuring resilience and efficiency.

According to Frost & Sullivan, NETSCOUT's integrated performance management solutions redefine IT operations by combining real-time analytics, proactive monitoring, and cybersecurity. The Visibility Without Borders platform, powered by nGenius, Arbor DDoS Protection, Omnis and Omnis Cyber Intelligence products, enables a NetOps SecOps framework that provides a unified IT view, enabling rapid threat detection and resolution. This approach enhances collaboration, optimizes resources, and boosts productivity. As digital landscapes evolve, NETSCOUT ensures resilience, continuity, and a competitive edge, making its solutions essential for long-term growth and future-ready IT progress.

Optimizing Network Performance to Drive Customer Acquisition

In the telecom ecosystem, seamless and secure connectivity is essential for attracting and retaining customers. Operators must deliver reliable network performance while proactively mitigating evolving cyber threats. The integration of performance monitoring with security has become crucial for real-time insights and threat detection.

NETSCOUT optimizes both cost and performance by minimizing infrastructure footprints and streamlining network operations. Its Omnis AI Streamer efficiently processes network data, eliminating redundancies

while ensuring high performance. A customer-centric approach ensures tailored solutions that build trust, transparency and long-term loyalty.

With a strong focus on end-to-end visibility, NETSCOUT enhances monitoring across radio access networks (RAN), a critical factor in telecom performance. Its involvement in open RAN (O-RAN) solutions, in collaboration with key partners like Mavenir, underscores its commitment to advancing telecommunications infrastructure and adapting to emerging industry standards.

The multi-year partnership between NETSCOUT and Vodafone exemplifies leadership in network monitoring. Vodafone leverages NETSCOUT's Mobile Network Operator Security suite to gain deeper visibility into network operations. By integrating NetOps and SecOps principles, the solution unifies performance metrics with security intelligence, enabling real-time issue detection and resolution.

This advanced monitoring approach strengthens both network reliability and cybersecurity defences, reducing disruptions and enhancing customer confidence. Real-time threat detection ensures secure, uninterrupted connectivity, improving service quality and minimizing downtime. The collaboration reinforces Vodafone's commitment to superior network performance while showcasing how intelligent monitoring solutions drive customer acquisition in a highly competitive market.

By combining cutting-edge monitoring with proactive security, the NETSCOUT-Vodafone partnership sets a new industry benchmark. As cyber threats evolve, strategic collaborations like this will be critical in ensuring secure, high-performance telecommunications—driving sustained growth, innovation, and market leadership.

Growth Potential: NETSCOUT Strengthens Digital Security

In the dynamic digital environment, organizations must continuously strengthen their digital resilience to safeguard critical assets and ensure operational continuity. The rapid evolution of cyber threats ranging from ransomware to advanced persistent threats demands a shift from reactive security measures to proactive, integrated defense systems. Enterprises now require solutions that not only detect threats in real-time but also fortify their overall security posture.

NETSCOUT meets this challenge by deploying a suite of integrated security solutions that enhance digital resilience. Central to this approach is the combination of AI/ML-driven threat detection, real-time monitoring, and automated incident response within the NetOps SecOps framework. This unified platform provides a single, coherent view of network performance and security, ensuring that vulnerabilities are identified and addressed promptly. The integration of Omnis Security further reinforces the defense by delivering comprehensive, multi-layered protection that spans across the entire IT infrastructure.

Additionally, NETSCOUT's Mobile Network Operator Security solutions offer specialized protection for mobile networks, addressing the unique vulnerabilities inherent in wireless communications. This ensures that both fixed and mobile infrastructures are secured against emerging cyber threats, thereby bolstering overall digital resilience. Continuous investments in research and development enable NETSCOUT to refine its technologies, ensuring that its solutions remain effective against future threats.

In conclusion, NETSCOUT's comprehensive approach to enhancing digital resilience and security posture represents a critical evolution in cybersecurity. The integration of advanced threat detection with unified

network and security analytics delivers robust protection that is essential in today's complex digital landscape. This multi-layered defense strategy not only mitigates current risks but also prepares organizations for future challenges, paving the way for sustainable growth. The ability to maintain a resilient security posture is vital for organizations aiming to innovate and expand in an increasingly interconnected world, ensuring long-term success and operational continuity.

Optimizing Operational Efficiency with End-to-End Network Visibility

Rural and independent network operators face unique challenges, including limited resources, dispersed infrastructures and heightened exposure to cyber threats. These challenges make it difficult to achieve robust, real-time visibility necessary for optimizing performance, reducing maintenance costs and ensuring secure connectivity. Comprehensive network monitoring that integrates cybersecurity measures is critical for addressing these issues.

NETSCOUT's innovative solution provides end-to-end visibility across rural networks by combining advanced analytics with real-time monitoring tools. The solution delivers a unified view of network performance, enabling operators to detect anomalies and address issues promptly. Enhanced cybersecurity capabilities, drawn from Mobile Network Operator Security and the NetOps SecOps platform, ensure that any detected performance irregularities are swiftly correlated with potential cyber threats. This integrated approach allows operators to take proactive measures, reducing downtime and optimizing resource allocation across geographically dispersed infrastructures.

The scalability and adaptability of NETSCOUT's solution make it especially valuable for rural operators. Its ability to integrate with diverse network components ensures that even remote areas benefit from comprehensive monitoring and robust security. Automated data collection and analysis provide actionable insights, empowering network managers to make informed decisions that improve overall efficiency. This fusion of performance monitoring with cybersecurity not only minimizes operational risks but also drives significant cost savings, ultimately enhancing service quality.

In conclusion, NETSCOUT's commitment to delivering end-to-end network visibility, enriched with advanced cybersecurity features, is transforming the operational landscape for rural and independent networks. The solution's comprehensive framework ensures that operators can continuously monitor, detect, and resolve issues in real time, bridging the digital divide and enhancing connectivity in underserved regions. This integrated strategy sets a new standard for network efficiency, driving operational excellence and fostering sustainable digital growth. With robust visibility and proactive cybersecurity, rural network operators are well-positioned to deliver reliable, cost-effective services in an increasingly competitive market.

Conclusion

NETSCOUT's end-to-end network visibility and AI-driven cybersecurity enhance operational efficiency for rural and independent network operators. By integrating real-time monitoring with proactive threat detection, operators can minimize downtime, optimize resources and ensure secure connectivity.

The scalable solution seamlessly integrates with diverse network components, providing actionable insights for better decision-making. Automated analysis reduces risks and operational costs while strengthening network resilience against evolving threats.

By unifying performance monitoring and cybersecurity, NETSCOUT future-proofs global to rural networks, enabling cost-effective and high-quality services. As demand for secure, high-speed connectivity grows, NETSCOUT's innovative approach ensures sustained efficiency, reliability, and digital transformation. This sets a new benchmark for network resilience and operational excellence in underserved regions. With its strong overall performance, NETSCOUT earns Frost & Sullivan's 2025 MENA Technology Innovation Leadership Recognition in the Cybersecurity industry.

© Frost & Sullivan 2025

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)

