FROST & SULLIVAN

BEST PRACTICES

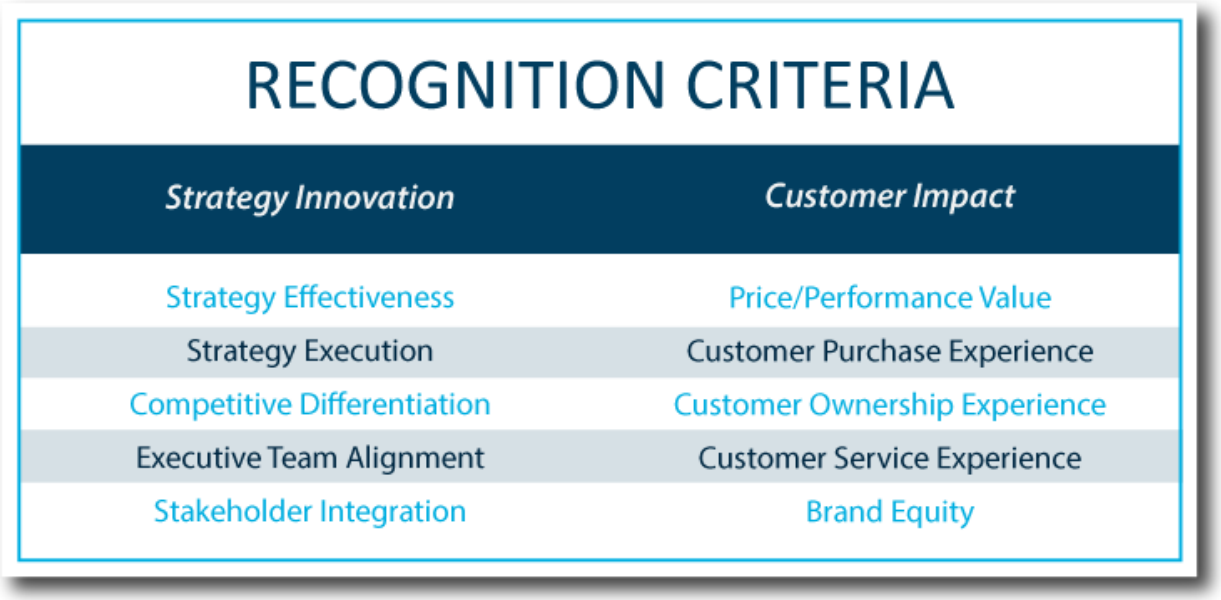
2026 GLOBAL IDENTITY THREAT DETECTION AND RESPONSE COMPETITIVE STRATEGY LEADERSHIP

Microsoft

Table of Contents

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. Microsoft excels in many of the criteria in the ITDR space.



The Transformation of the ITDR Industry

The transformation of the global ITDR industry is being driven by the emergence of identity as a primary attack vector in an increasingly digitized and hybrid enterprise landscape. Organizations must manage the rise in identity-driven threats across cloud, on premises, and SaaS ecosystems, where adversaries exploit fragmented identity estates, misconfigurations, credential compromise, and token abuse to login rather than 'break in' through traditional perimeter defenses. Additionally, security teams must now secure a complex mix of human identities, non-human identities (NHIs), service accounts, workloads, and emerging agentic identities, increasing both the scale and complexity of identity risk management. These shifts have resulted in ITDR evolving from a niche discipline into a foundational security capability. Demand is growing for integrated threat intelligence, identity posture management, cross domain correlation, real time adaptive access, and automated attack disruption.

> *"Microsoft is enabling adopters to enhance operational identity security by scaling from legacy Active Directory estates to cloud, SaaS, and emerging agentic identities through integrated, enterprise-wide security workflows."*
>
> ***- Deepali Sathe***
> ***Industry Principal***

Microsoft has emerged as a strong contender in the market by connecting IAM and SOC workflows through integrated identity security capabilities across Entra and Defender so that detection and response actions can feed back into preventive controls. Microsoft's security operations at hyperscale reference

over 100 trillion security signals informing its security systems and protects one billion monthly active users in Entra, reflecting the scale and urgency of the modern identity threat landscape.,

Managing identity security for a hybrid, multi-cloud infrastructure

Organizations worldwide face the critical challenge of securing identities across hybrid, multi-cloud environments that include legacy Active Directory, cloud directories, SaaS platforms, and third party identity providers. Microsoft addresses this challenge through a unified identity security architecture that interconnects IAM and XDR capabilities across Microsoft Entra ID and Microsoft Defender. This approach strengthens visibility, threat intelligence, and enforcement by operationalizing Zero Trust principles across identity, workload, application, and network boundaries. Microsoft emphasizes that Conditional Access functions as a Zero Trust policy enforcement engine, helping organizations enforce risk-based policies at scale. Microsoft's ITDR strategy reflects visionary innovation by re-architecting identity security around continuous risk evaluation and closed-loop prevention where intelligence from trillions of signals is translated into real-time policy enforcement, disruption, and posture improvement rather than static detection alone.

> *"Microsoft's ITDR strategy reflects visionary innovation by re-architecting identity security around continuous risk evaluation and closed-loop prevention where intelligence from trillions of signals is translated into real-time policy enforcement, disruption, and posture improvement - rather than static detection alone."*
>
> ***- Deepali Sathe***
> ***Industry Principal***

Integrated identity risk engines evaluate user, workload, and sign-in risks using signals such as anomalous sign-in patterns and token theft indicators, enabling risk driven enforcement that can reduce identity compromise by applying stronger controls when risk rises. A key differentiator is Microsoft's 'any identity / any environment / any component' framing for coverage, including hybrid identity components and expanding protections across NHI and agentic identities. The platform supports heterogeneous environments by utilizing sensors and connectors, enabling integration with other cloud identity providers such as Okta. The platform also offers ecosystem connectivity with PAM/IGA components, such as CyberArk.

With integrated attack path mapping, posture recommendations, and cross domain correlation across hybrid and cloud identity layers, Microsoft positions ITDR as a core pillar of enterprise Zero Trust programs linking prevention, detection, investigation, and response into an operational loop shared by identity and SOC teams. An example of consolidation is evident in ElringKlinger, one of the world's leading automotive industry system partners, where it is reinforcing identity security with Entra ID and Entra ID Protection to enhance visibility by consolidating multiple security tools into Microsoft Security.

Microsoft's AI-driven defense is rooted in intelligence at unprecedented scale

The rapid increase in attack volume and velocity places sustained operational strain on identity administrators and SOC teams. Microsoft addresses this challenge by applying AI across identity security workflows, spanning risk-based access enforcement, posture analysis, investigation support, and response prioritization. Its security platforms ingest and correlate security signals at hyperscale, enabling

machine learning models to surface anomalies, identify posture gaps, and generate contextual recommendations that support timely risk-based decisions.

The Conditional Access Optimization Agent illustrates Microsoft's execution focus. The capability analyzes Conditional Access configurations, highlights policy gaps introduced by new users, devices, applications, or configuration drift, and provides guided recommendations that help administrators strengthen enforcement. By emphasizing actionable recommendations rather than static insight, Microsoft reduces administrative friction and accelerates posture improvement while allowing organizations to retain control over policy changes.

Microsoft's generative AI investments further strengthen execution by augmenting, rather than replacing, human decision making. Identity-focused Copilot experiences provide contextual explanations of identity risk signals, assist with investigation workflows, and support remediation actions such as guided credential resets or access enforcement. The ability to tailor recommendations to organizational policy, such as restricting high-risk sign-ins, demonstrates Microsoft's emphasis on scalable, AI assisted operational efficiency. Across identity and SOC workflows, these AI-enabled capabilities help accelerate triage, enrich investigations, and reduce manual effort, which is increasingly critical for global enterprises confronting credential abuse, identity-led lateral movement, and human-operated ransomware.

Unifying IAM and SOC operations into an interconnected security model

Microsoft's operating model emphasizes that modern identity security requires a partnership between identity administrators and SOC teams; a 'team sport' in which each persona retains context specific workflows while sharing data and actions through an interconnected loop. In this model, identity posture signals, risky user alerts, sign-in anomalies, and policy outcomes can inform SOC investigations, while SOC actions, such as disabling accounts or marking users compromised, can feed back into identity controls to tighten enforcement.

Microsoft supports a layered identity security approach that includes IAM foundations, posture, threat protection, and GenAI augmentation, with the goal of enabling faster containment and disruption of multistage attacks. Interconnected portal experiences reduce client concerns about replacing systems by building solutions with existing assets. The growing trend of governance becoming more dynamic is reflected in identity protection risk scores triggering access reviews. This benefits clients by managing review fatigue and reducing rigid, and calendar-based review cycles.

Stakeholder informed innovation and customer centric evolution

The ITDR market is shaped by diverse stakeholders including identity administrators, SOC analysts, cloud architects, compliance teams, threat researchers, and executive leaders. Microsoft integrates these perspectives through telemetry feedback loops, customer engagements, standards partnerships, and incident response learnings, so that ITDR capabilities evolve in line with real-world identity threats and operational requirements. From a customer ownership standpoint, Microsoft's Customer and Partner Experience (CPE) framework gathers insights from usability studies and feedback mechanisms that influence roadmaps, feature prioritization, and improvements to security quality and user experience.

Customer service excellence is reinforced through FastTrack onboarding teams, Customer Success Units, and Customer Experience Engineering (CxE), which work to accelerate deployment, resolve challenges, and translate feedback into engineering priorities. Microsoft emphasizes simplification initiatives intended to reduce adoption friction. Microsoft conducts biannual Customer and Partner Satisfaction surveys to gain actionable feedback for improvement. Over 60 teams worldwide develop CPE plans under a unified strategy, supported by 300+ professionals. Security offerings are customized for core personas including identity administrators and SOC teams, delivering benefits such as faster protection, lower operational costs, and clear ROI for CISOs. Microsoft positions its AI-driven, unified security platform as adaptable and future-ready, giving customers and partners confidence in ITDR and ongoing satisfaction.

Delivering high value through consolidation, automation and operational efficiency

Enterprises face increasing pressure to reduce tool sprawl, consolidate vendors, and achieve more with constrained budgets. Microsoft positions value through consolidation by packaging identity and security capabilities in suites such as Microsoft 365 E5, reducing procurement and integration overhead for organizations standardizing on the Microsoft security stack. This consolidation can reduce operational complexity by streamlining onboarding, enabling policy templates, and accelerating the path to risk-based access and continuous posture improvement. With its top-tier solutions and expertise in both IAM and XDR, Microsoft seamlessly integrates its identity platform with Microsoft Security, processing over 100 trillion security signals daily. This vast data supports AI-powered threat detection and proactive response across endpoints, documents, emails, and cloud setups. With this intelligence, the Zero Trust architecture efficiently detects and addresses identity-based attacks, including those from nation-state actors, with exceptional accuracy and speed.

Microsoft also emphasizes automated response and disruption where security systems can take containment actions based on observed signals, supporting a shift from reactive response toward proactive risk prevention. An example of this is the replacement of fragmented, siloed operations by Heineken, a multinational brewing company, which adopted Microsoft Sentinel and Microsoft 365 Defender, to strengthen identity controls with Entra Conditional Access and Defender for Identity supporting the ‘consolidation + agility’ value claim. Microsoft is enabling adopters to enhance operational identity security by scaling from legacy Active Directory estates to cloud, SaaS, and emerging agentic identities through integrated, enterprise-wide security workflows.

Conclusion

Microsoft's contribution to shaping the future of global ITDR is reflected in its interconnected architecture across identity and security operations, AI assisted workflows, continuous posture improvement, and reinforced collaboration between IAM and SOC teams. By combining risk-based Zero Trust enforcement at scale with detection, investigation, and disruption capabilities across Entra and Defender, Microsoft positions ITDR as a backbone capability for enterprises managing identity risk across hybrid, multi-cloud, and SaaS ecosystems.

Microsoft earns the 2026 Frost & Sullivan Global Competitive Strategy Leadership Recognition in the ITDR industry for its sustained innovation, execution focus, and its ability to drive customer value through integrated identity security outcomes that respond to evolving identity threats across modern enterprise environments.

What You Need to Know about the Competitive Strategy Leadership Recognition

Frost & Sullivan's Competitive Strategy Leadership Recognition identifies the company with a standout approach to achieving top-line growth and a superior customer experience.

Best Practices Recognition Analysis

For the Competitive Strategy Leadership Recognition, Frost & Sullivan analysts independently evaluated the criteria listed below.

Strategy Innovation

Strategy Effectiveness: Effective strategy balances short-term performance needs with long-term aspirations and overall company vision

Strategy Execution: Company strategy utilizes best practices to support consistent and efficient processes

Competitive Differentiation: Solutions or products articulate and display unique competitive advantages

Executive Team Alignment: Executive team focuses on staying ahead of key competitors via a unified execution of its organization's mission, vision, and strategy

Stakeholder Integration: Company strategy reflects the needs or circumstances of all industry stakeholders, including competitors, customers, investors, and employees

Customer Impact

Price/Performance Value: Products or services offer the best ROI and superior value compared to similar market offerings

Customer Purchase Experience: Purchase experience with minimal friction and high transparency assures customers that they are buying the optimal solution to address both their needs and constraints

Customer Ownership Excellence: Products and solutions evolve continuously in sync with the customers' own growth journeys, engendering pride of ownership and enhanced customer experience

Customer Service Experience: Customer service is readily accessible and stress-free, and delivered with high quality, high availability, and fast response time

Brand Equity: Customers perceive the brand positively and exhibit high brand loyalty, which is regularly measured and confirmed through a high Net Promoter Score®

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 fueled 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)