FROST & SULLIVAN

BEST PRACTICES

2026

# INDIA BREACH AND ATTACK SIMULATION

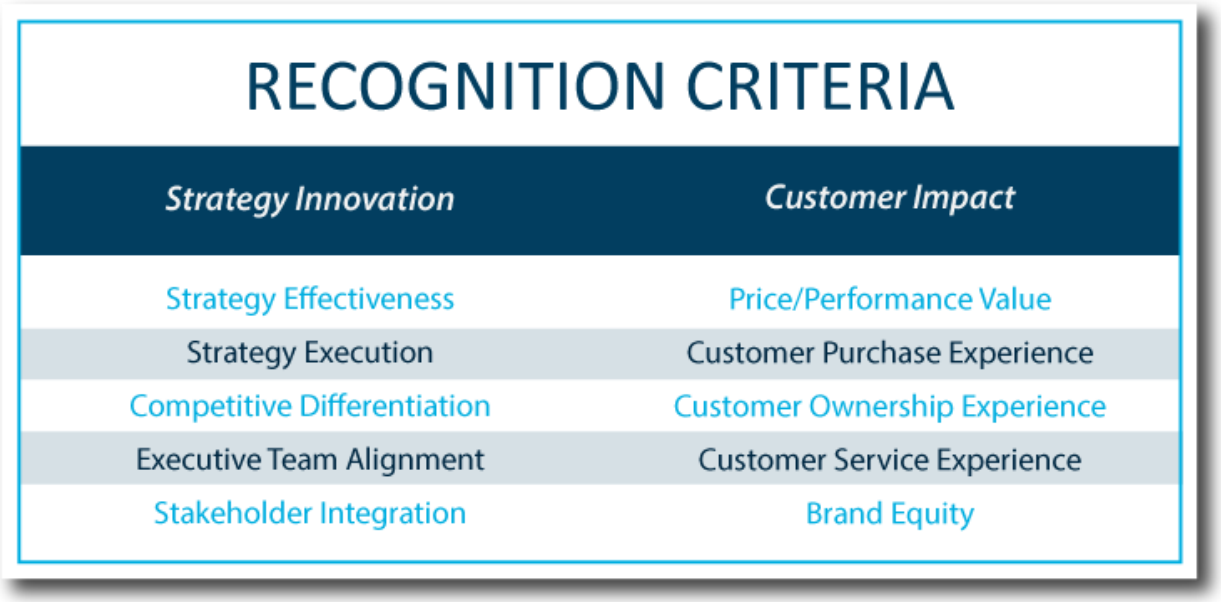
# COMPETITIVE STRATEGY LEADERSHIP

cymulate

# 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. Cymulate excels in many of the criteria in the breach and attack simulation space.




## The Transformation of the Breach and Attack Simulation Industry

The global breach and attack simulation (BAS) market is evolving as organizations seek more proactive approaches to cybersecurity amid increasingly complex and expanding attack surfaces. Enterprises operate across hybrid environments that include on-premises infrastructure, multi-cloud platforms, operational technology (OT), legacy systems, and emerging artificial intelligence (AI) services, creating new security challenges that traditional approaches cannot address. Organizations require greater visibility across interconnected environments, with actionable insights that reduce alert fatigue and help prioritize risks based on business impact and exploitability. The growing number of fragmented security tools has also increased demand for integrated platforms that consolidate capabilities, enable seamless workflows, and provide a unified view of cyber exposure.

At the same time, organizations are shifting from reactive vulnerability management toward continuous exposure management and risk-based security strategies. BAS solutions are gaining importance as enterprises seek to validate whether security controls operate effectively against real-world attack techniques. The market is moving toward more comprehensive attack path analysis, enabling organizations to understand how individual vulnerabilities and misconfigurations can combine into realistic attack scenarios. Cloud-native architectures, AI-driven exposure detection, and multi-agent AI technologies are becoming key areas of innovation as vendors enhance their ability to simulate sophisticated adversary behavior and evaluate emerging threats.

The increasing adoption of AI services is creating additional opportunities for BAS providers, as organizations need to identify and secure new exposure points such as unauthorized AI usage, credential theft, and vulnerabilities within AI-managed applications. Vendors are expanding beyond traditional simulation capabilities by incorporating attack graph analytics, offensive security testing, and integrations with vulnerability management, external attack surface management, governance, risk, and compliance, extended detection and response, and security orchestration, automation, and response platforms. These developments reflect a broader industry transition toward platform-based security models that combine prevention, validation, and continuous improvement.

Over the 2026-2031 period, Frost & Sullivan expects BAS adoption to accelerate as enterprises prioritize cyber resilience and business-aligned risk management.[1] Vendors are increasingly integrating proactive defense mechanisms (e.g., deception technologies, honeypots, and automated attack simulations) with AI-driven analytics to identify advanced attack strategies, detect lateral movement, and reduce attacker dwell time. Strategic partnerships, mergers, and acquisitions are also expected to increase as cybersecurity providers seek to consolidate exposure management, validation, and security operations capabilities into comprehensive platforms that address the growing complexity of modern cyber threats.[2]

### Cymulate: Advancing Continuous Security Validation for Enterprise Cyber Resilience

Founded in 2016 by a team of former Israeli intelligence officers and cybersecurity researchers, and headquartered in Tel Aviv, Israel, Cymulate is a cybersecurity company that provides BAS and a threat exposure validation platform that continuously assesses and improves organizations' security posture. The company allows enterprises to simulate real-world cyberattacks, validate the effectiveness of security controls, identify vulnerabilities, and prioritize remediation efforts. It serves organizations worldwide across highly regulated industries, including financial services, healthcare, government, and critical infrastructure, helping security teams transition from periodic assessments to continuous cyber resilience programs.

Cymulate pioneered the BAS market in India by introducing continuous security validation at a time when organizations primarily relied on penetration testing and red teaming. In 2019, the company invested in educating enterprises about the value of continuous attack simulation, explaining how it differs from traditional assessment methods and why it plays a critical role in modern cybersecurity. This effort helped establish BAS as an essential component of enterprise cyber resilience.

During the early stages of market adoption, Cymulate overcame skepticism by supporting every simulated attack with technical evidence, demonstrating that security gaps often resulted from misconfigurations or incomplete optimization instead of shortcomings in the underlying technologies. This evidence-based approach increased customer confidence and reinforced the importance of continuously validating deployed security controls.

Cymulate positions threat exposure validation as the foundation of modern offensive security by enabling organizations to continuously assess the effectiveness of security controls against real-world attack techniques. While the market uses terms such as adversarial exposure validation and continuous threat

[1] *Automated Security Validation (ASV) Market, Global, 2025–2030* (Frost & Sullivan, February 2026)
[2] Ibid.

exposure management (CTEM), the company's approach centers on comprehensive attack simulations that provide objective evidence of cyber resilience.

The Cymulate platform differentiates itself through one of the industry's broadest attack libraries, covering a wide range of tactics, techniques, and procedures across email security, endpoint security, data protection, cloud environments, and other critical domains. Rapid deployment permits organizations to begin simulations quickly and evaluate major security controls within the first day, accelerating time to value and enabling security teams to prioritize remediation without lengthy implementation cycles.

Unlike periodic penetration testing, red teaming, and vulnerability assessments that provide only point-in-time visibility, Cymulate verifies whether existing security controls detect and prevent newly disclosed attack techniques.

Cymulate also addresses operational challenges by providing objective evidence of control effectiveness. Organizations can verify that security technologies remain properly configured, and strengthen visibility across hybrid environments (e.g., cloud services, application programming interfaces, and distributed infrastructure).

The platform also extends threat exposure validation to OT environments where cybersecurity controls have been deployed. As information technology (IT) and OT environments increasingly converge, Cymulate allows organizations to validate controls (e.g., next-generation firewalls, endpoint protection, data protection technologies, and system hardening measures) within production environments where they can conduct simulations safely.

> *"The Cymulate platform differentiates itself through one of the industry's broadest attack libraries, covering a wide range of tactics, techniques, and procedures across email security, endpoint security, data protection, cloud environments, and other critical domains. Rapid deployment permits organizations to begin simulations quickly and evaluate major security controls within the first day, accelerating time to value and enabling security teams to identify configuration weaknesses and prioritize remediation without lengthy implementation cycles."*
>
> ***- Marcos Ainchil***
> ***Best Practices Research Analyst***

The company recognizes that OT environments require a measured validation approach because many industrial systems support critical infrastructure and production processes. Cymulate assesses the suitability of each environment before conducting production-safe simulations, enabling organizations to extend threat exposure validation across eligible OT environments.

The platform validates security controls across both north-south and east-west traffic, allowing organizations to assess their ability to detect attacks throughout the enterprise, including lateral movement that occurs after initial compromise. Cymulate also distinguishes threat exposure validation from cyber range platforms, which focus on training security operations center (SOC) personnel to respond to cyber incidents. Rather than replacing cyber range capabilities, Cymulate provides independent validation of deployed security controls by executing realistic attack scenarios against production environments. This objective assessment complements defensive training by measuring whether existing controls detect, prevent, and respond effectively to simulated attacks.

Many organizations also use the platform to evaluate SOC performance through operational metrics such as mean time to detect and mean time to respond. Cymulate simulates attacks that abuse legitimate administrative tools and protocols, including remote desktop protocol, secure shell, windows management instrumentation, and server message block, enabling organizations to verify that monitoring tools generate appropriate alerts and that security teams respond reliably. Security teams can use validated findings to improve product configurations, optimize security controls, and prioritize remediation activities, enabling organizations to maximize the value of existing cybersecurity investments rather than replacing deployed technologies.

The platform integrates with enterprise cybersecurity ecosystems, including vulnerability management platforms, endpoint detection and response solutions, security information and event management platforms, secure web gateways, and IT service management tools. These integrations allow validated attack data to flow directly into operational workflows, while embedded analytics correlate findings across multiple security controls to prioritize remediation based on validated risk and support informed security decisions.

The company operates in a market where organizations evaluate BAS, automated penetration testing, CTEM, and other offensive security solutions against the same cybersecurity budget. The company views CTEM as a strategic cybersecurity program instead of a standalone technology.

Cymulate differentiates its platform through comprehensive attack coverage, rapid deployment, continuous innovation, and a strong customer support organization. As opposed to competing primarily on price, Cymulate emphasizes long-term operational outcomes, encouraging organizations to evaluate offensive security platforms based on technical effectiveness, scalability, implementation maturity, and the ability to sustain continuous validation as cyber threats evolve. This approach has supported broad adoption among organizations operating critical infrastructure and highly regulated environments across both the public and private sectors.

Cymulate attributes its market position to sustained platform innovation and the continuous introduction of new capabilities that address evolving cybersecurity challenges. Recent enhancements include AI capabilities that generate advanced attack scenarios, create realistic attack chains, and automate testing processes. The platform's modular architecture allows organizations to progressively expand validation coverage, automate remediation workflows, and strengthen cyber resilience without replacing existing security infrastructure.

The company also maintains a clear separation between independent security validation and the implementation of defensive technologies. Many customers procure and deploy security products through systems integrators or resellers, while Cymulate independently validates the effectiveness of those controls. This separation reinforces the objectivity of validation results and supports customers in using evidence-based findings when working with implementation partners and technology vendors to resolve configuration issues and strengthen security controls.

Customers typically establish a foundational deployment and subsequently add new functional modules that address evolving security priorities, automation requirements, and validation use cases. This modular

architecture aligns technology adoption with organizational maturity while enabling enterprises to expand platform capabilities over time without replacing their existing deployment.

### Expanding Market Adoption and Strengthening Industry Trust

Highly regulated financial institutions led the adoption of Cymulate's platform in India, with implementation expanding from private sector banks to insurance providers, mutual fund companies, housing finance organizations, and stockbroking firms. The company subsequently broadened its presence across information technology services, aviation, manufacturing, shipping, pharmaceuticals, government, and regulatory organizations. Regulatory bodies also incorporated lessons from continuous security validation into cybersecurity policies and best practices that promote stronger cyber hygiene across Indian enterprises.

Independent industry recognition and broad enterprise adoption reinforce Cymulate's market position. The platform supports many of India's leading private and public sector banks, major technology companies, aviation organizations, financial market infrastructure providers, and other critical infrastructure operators, demonstrating its ability to address complex cybersecurity environments at enterprise scale.

Cymulate has also observed a broader shift from compliance-driven cybersecurity toward outcome-based cyber resilience, driven by increasing regulatory oversight and greater board-level accountability. In response, the platform provides data-driven insights that help chief information security officers (CISOs) present objective evidence of organizational cyber hygiene, support executive reporting, and guide technology investment decisions. Organizations also use Cymulate to evaluate prospective security technologies under realistic attack conditions, replacing feature-based proof-of-concept exercises with operational validation that compares products within production-like environments. This approach facilitates more informed procurement decisions while ensuring future security investments align with validated organizational needs.

Cymulate has established a predominantly partner-led go-to-market strategy in India that combines the scale of an expanding channel ecosystem with direct customer engagement for strategic accounts. During the early stages of market development, the company led customer acquisition directly because BAS represented a new category that required significant market education. As enterprise awareness increased and demand accelerated, a growing network of channel partners began investing in the capabilities required to deliver the platform.

Today, the company collaborates with systems integrators, managed security service providers (MSSPs), and specialized cybersecurity partners that extend its market reach while supporting customer adoption. These partners play an important role in expanding the availability of threat exposure validation across the Indian market, and several have developed dedicated offensive security expertise around the Cymulate platform to deliver implementation and managed services for customers with limited internal cybersecurity resources.

Alongside its partner ecosystem, Cymulate continues to maintain direct relationships with selected strategic customers that adopted the platform during its early market expansion. This hybrid engagement model enables the company to preserve close relationships with key enterprises.

## Delivering Long-Term Customer Success and Operational Value

Cymulate recommends a phased implementation strategy that prioritizes the highest-risk attack vectors before expanding validation across additional domains. Organizations typically begin by assessing internet-facing controls (e.g., email security, web gateways, and web application firewalls), then progressively extend validation to cloud environments, infrastructure, OT, and other specialized environments. Through implementation guidance, knowledge transfer, and operational enablement, Cymulate helps organizations transition from reactive incident response to a proactive security strategy that continuously tests defenses against evolving threats.

The platform allows organizations to validate newly disclosed vulnerabilities and emerging attack techniques without waiting for scheduled penetration tests or red team exercises. Security teams can verify that remediation activities consistently reduce exposure, monitor security maturity through trend analysis, and provide management with measurable evidence of improvements in cyber resilience.

The company complements its technology with a dedicated customer success organization that supports long-term operational maturity. Customer success teams conduct technical workshops, facilitate knowledge transfer, monitor platform utilization, and encourage customers to adopt new capabilities as their cybersecurity programs evolve.

> *"Cymulate differentiates its platform through comprehensive attack coverage, rapid deployment, continuous innovation, and a strong customer support organization. As opposed to competing primarily on price, Cymulate emphasizes long-term operational outcomes, encouraging organizations to evaluate offensive security platforms based on technical effectiveness, scalability, implementation maturity, and the ability to sustain continuous validation as cyber threats evolve."*
>
> ***- Rajarshi Dhar***
> ***Associate Director***

Cymulate supports its Indian customer base through a local organization that combines sales, technical support, customer success, and marketing functions. The team also monitors platform utilization, shares implementation best practices and cross-industry use cases and recommends additional capabilities that align with evolving customer requirements.

A complementary 24/7 technical support organization assists with platform operations, configuration, software updates, and technical issues, creating a two-tier engagement model that combines proactive customer enablement with responsive operational support. Cymulate further measures customer engagement through operational metrics that track platform utilization, attack simulations, validation results, security scores, and feature adoption, enabling customer success teams to maximize long-term customer value.

This customer-centric approach has contributed to customer retention exceeding 90% while supporting continued platform expansion through additional modules as organizations mature their threat exposure validation programs.

## Use Cases Demonstrating Technological Excellence

An India-based leading banking and financial services company with a three-person cybersecurity team relied heavily on MSSPs and external consultants to support security operations and offensive testing.

However, the organization needed greater confidence that its internal controls, outsourced security services, and consumer-facing applications could withstand real-world attacks. Traditional red team assessments were manual, time-consuming, and limited in scope, making it difficult to continuously validate security controls, measure MSSP detection capabilities, and assess protection against emerging threats.

The company selected Cymulate to replace manual validation processes with automated security assessments, continuous threat simulation, and actionable remediation guidance. The platform enabled the security team to continuously validate security controls, optimize MSSP performance, prioritize remediation activities, and test defenses against newly emerging attack techniques. Cymulate also helped automate red team activities, allowing the small security team to conduct broader assessments with reduced effort while improving collaboration between security operations, offensive teams, and managed service providers.

The implementation improved operational efficiency by 60%, strengthened validation of outsourced security services, and drove faster response to emerging threats.[3] Cymulate provided executive-level insights that helped the CISO communicate cybersecurity maturity and risk reduction strategies to leadership while giving technical teams clear guidance on remediation priorities.

*"Cymulate gives us a benchmark to work towards improvement. I can effectively plan my security roadmap by outlining the steps I need to achieve optimal cybersecurity maturity."* [4]

— Chief Information Security Officer

Persistent Systems (Persistent), a global digital engineering and enterprise modernization company, implemented Cymulate to establish continuous security validation and gain greater visibility into its cybersecurity posture. With a security environment spanning risk and governance, audit and compliance, and security operations, Persistent faced challenges with traditional quarterly penetration tests that provided only point-in-time assessments, manual vulnerability prioritization processes, and limited visibility into security control effectiveness. The company sought an automated approach that could continuously validate security policies, identify weaknesses, and assess exposure to emerging threats across its global operations.

Cymulate enabled Persistent to continuously test security controls, validate breach feasibility, assess lateral movement risks, and evaluate defenses against emerging threats. The platform helped the security team verify the effectiveness of email gateways, web gateways, web application firewalls, and network segmentation policies while providing actionable remediation guidance. Persistent also leveraged Cymulate for phishing assessments, vulnerability prioritization, security technology evaluations, and automated red team exercises, allowing the organization to improve collaboration across security functions and make more informed decisions based on measurable risk data.

The implementation delivered measurable improvements in Persistent's security operations, reducing critical vulnerabilities identified during third-party penetration testing by 70% and decreasing security

[3] Leading Finance Company Validates MSSP with Cymulate (Cymulate, 2026)
[4] Ibid.

analysis efforts from approximately one and a half days to one to three hours.[5] Cymulate also allowed the security team to demonstrate the relationship between cybersecurity investments and risk minimization through quantifiable insights shared with executive leadership.

*"With Cymulate, we can present quantifiable data to the board and show a direct correlation between investments and the reduction in risk."* [6]

*— Avinash Dharmadhikari, Chief Information Security Officer, Persistent Systems*

## Conclusion

Cymulate is a pioneer in the Indian breach and attack simulation market and advances the adoption of continuous security validation across enterprise environments. The company has enabled organizations to move beyond periodic assessments by continuously testing security controls against real-world attack techniques and providing measurable evidence of cyber resilience. Through broad attack coverage, rapid deployment, ecosystem integrations, and continuous innovation, Cymulate helps enterprises identify weaknesses, prioritize remediation, and maximize existing security investments. Its strong adoption among financial institutions, critical infrastructure operators, and highly regulated organizations demonstrates the platform's ability to address complex cybersecurity challenges at scale. Supported by a customer-centric operating model, local expertise, and a growing partner ecosystem, Cymulate continues to strengthen how organizations prepare for and respond to evolving cyber threats.

With its strong overall performance, Cymulate earns Frost & Sullivan's 2026 India Competitive Strategy Leadership Recognition in the breach and attack simulation industry.

[5] Persistent Systems Gains Visibility & Control of its Security Posture (Cymulate, 2026)
[6] Ibid.

# 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)