2025 NEW PRODUCT INNOVATOR

Pioneering New Features and Functionality to Exceed Customer Expectations

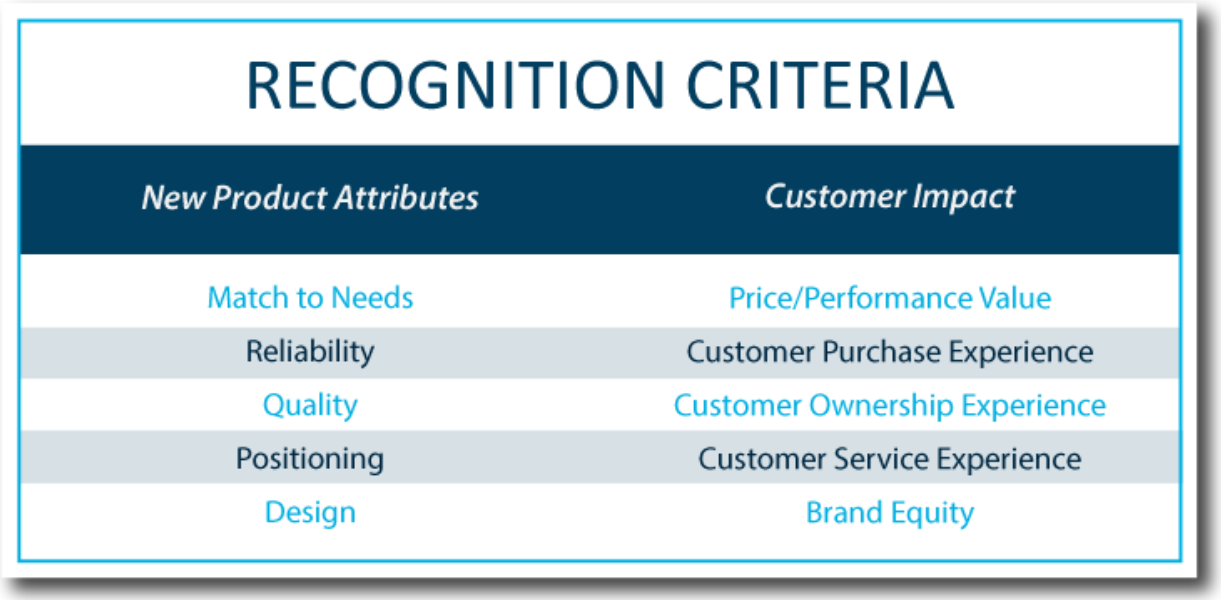
RECOGNIZED FOR BEST PRACTICES IN THE GLOBAL APPLICATION SECURITY INDUSTRY

FROST & SULLIVAN

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. Miggo excels in many of the criteria in the application security space.



RECOGNITION CRITERIA

New Product Attributes	*Customer Impact*
Match to Needs	Price/Performance Value
Reliability	Customer Purchase Experience
Quality	Customer Ownership Experience
Positioning	Customer Service Experience
Design	Brand Equity

The Transformation of the Application Security Industry

Over the past 5 years, applications have gone through a significant transformation, shifting from static, monolithic structures to dynamic cloud-native and artificial intelligence (AI)-native ecosystems. Each deployment now requires reconfiguration of business logic, creation of new containers, and modification of API pathways, resulting in an unprecedented threat landscape.

This complexity has made traditional application security (AppSec) tools, such as static application security testing (SAST), dynamic application security testing (DAST), and web application firewalls (WAFs), insufficient, as they were built for predictable codebases and rely on signature-based detection. These traditional AppSec testing tools are foundational tools that analyze source code for vulnerabilities during the development stage. They perform static, periodic, and point-in-time security checks during development or testing phases rather than offering continuous, real-time monitoring and detection. They fail to keep up with the dynamic nature of applications in production, where runtime conditions and function calls often differ from static analysis predictions, making it challenging for AppSec and security operations (SecOps) teams to prioritize and respond to genuine threats effectively.

These legacy solutions often fail to capture how applications behave in production under real-world conditions, generate a high number of false positives due to a lack of runtime context, and miss critical runtime threats, such as prompt injection, logic abuse, and behavioral drift, that only surface in live environments.

As attackers increasingly exploit these dynamic gaps using AI-driven techniques to target real-time application flows, organizations require a transformation in their AppSec strategy, moving beyond traditional capabilities of vulnerability and compliance management to focus more on active threat management. Application detection and response (ADR) is designed to help organizations address this evolution by providing continuous runtime observability, predictive threat intelligence, and automated enforcement, enabling security teams to keep pace with the fluid and unpredictable nature of modern applications in cloud and AI-native environments.

Match to Needs

> *"Unlike other ADR solutions that often rely on partial workload snapshots or post-incident forensics, Miggo's approach delivers deep function-level runtime context to prevent these emergent threats, providing security teams with a proactive edge over those tools that only react after alerts or are limited to surface signals. This also helps teams avoid blind spots and false-positive overload of traditional scanners that rely on static checks and known signatures."*
>
> ***- Anh Tien Vu***
> ***Industry Principal, Global Cybersecurity Practice***

Miggo, founded in Tel Aviv and New York in 2023, is an ADR pioneer, helping security teams address these challenges in the evolving threat landscape in the application industry. It is one of the few companies that delivers an innovative and full-stack ADR platform.

Miggo has built its platform to protect modern applications, including third-party, cloud-native, internal, as well as customer-facing apps in addition to AI-assisted applications, AI applications, and AI agents. Miggo's unique value is that it can secure all these distinct categories at runtime, providing comprehensive protection across the entire spectrum of adoption.

This breadth and depth of coverage stem from its innovative technologies that can offer broad protection to applications, from visibility and threat exposure to remediation guidance and preemptive mitigation through perimeter tools, and real-time detection and response through application blocking.

Unlike other ADR solutions that often rely on partial workload snapshots or post-incident forensics, Miggo's approach delivers deep function-level runtime context to prevent these emergent threats, providing security teams with a proactive edge over those tools that only react after alerts or are limited to surface signals. This also helps teams avoid blind spots and false-positive overload of traditional scanners that rely on static checks and known signatures.

Miggo's first differentiator lies in its DeepTracing™ technology that leverages extended Berkeley Packet Filter (eBPF) and OpenTelemetry to deliver function-level context with minimal overhead, enabling the transformation of every request into a detailed execution trace that allows for instant threat blocking. While competitors may require heavier instrumentation or miss granular runtime deviations, this approach allows security teams to deploy solutions easily with minimal overhead, enabling them to deploy the solution at scale, especially for cloud and AI-native applications.

Additionally, Miggo's observability, through its AppDNA, can correlate traces with configurations, profiles, and telemetry from container/OS workloads running applications to construct a dynamic graph that connects user actions to precise APIs, code lines, and syscalls, which offers real-time reachability and blast-radius insights that go beyond the static inventories or basic anomaly detection seen in rival traditional AppSec testing tools.

Moreover, Miggo maintains a proprietary vulnerability database augmented with predictive threat modeling that can identify and research both disclosed and undisclosed common vulnerabilities and exposures (CVEs). Its AI sensors uncover vulnerabilities that emerge only during execution, including prompt injection, logic abuse, and behavioral drift patterns invisible to legacy scanners. The insights from these activities can be fed into automated mitigations like WAF Copilot, which generates and deploys custom rules to edges or gateways, enabling AppSec teams to address key pain points, such as patching delays, manual rule creation, and false positives.

Miggo's WAF Copilot is an innovative way to complement its ADR solution, as it adds another layer of response, bridging the gaps between ADR's in-app detection and a traditional WAF's response at the network level. It leverages runtime application context, predictive vulnerability analysis, and an AI agent modeled after elite security researchers, allowing teams to respond to emerging threats, like AI-driven exploits or zero-day vulnerabilities, in minutes rather than days, without modifying their infrastructure. With WAF Copilot, Miggo can help organizations reduce the time to exposure by more than 90%, making it stand out against other AppSec tools that lack predictive enforcement or rely on manual interventions.

In addition, organizations can avoid installing heavyweight agents through Miggo's "bring-your-own sensor" model, ingesting existing traces and logs for full coverage in under an hour, eliminating friction that plagues agent-dependent alternatives. This helps improve an operating model that empowers developers with valued observability, researchers with predictive context, and SecOps with push-button responses aligned with continuous delivery.

Ahead of the Curve: Unique Designs to Position Itself as an Innovator

Miggo's ADR differentiates itself from many solutions on the market, including traditional AppSec testing tools, cloud-native application protection platforms (CNAPPs), and even other application runtime security solutions. While traditional AppSec tools, such as vulnerability management solutions, often rely on static scanning, generating excessive alerts, many of which might be false positives, due to the lack of runtime proof, Miggo only flags those loaded, reachable, and exploitable in runtime, and then virtually patches them at the edge for flexible remediation.

While runtime testing solutions like DAST and API security observe traffic at the perimeter, they often fail to trace it through backend logic and lack visibility into the internal service mesh. Miggo, on the other hand, can extend visibility into backend logic and syscalls and expose how benign sequences evolve into exploit chains, addressing visibility blind spots that external probes in competing solutions cannot penetrate.

While many organizations may see runtime application self-protection (RASP) as a promising protection solution at runtime to bridge the gaps of traditional WAF, they introduce heavy agents,

instrumentation, and manual mitigation, which cause challenges in deployment at scale. Miggo addresses this through its agentless approach while delivering custom WAF rules in minutes, significantly reducing mean-time-to-mitigate (MTTM) to near real-time, which is unmatched by other tools, which require custom scripting or delayed updates.

Miggo also stands apart among emerging ADR players with its broader coverage. While emerging ADR players deliver narrow capabilities, such as library profiling, container/runtime drift, or software bill of materials (SBOM) maintenance, which are useful but typically lack a comprehensive runtime graph, predictive AI pipeline, or sensor-agnostic ingestion, causing alert overload. Miggo's live AppDNA model, coupled with a research-driven prediction engine and its new WAF capability for response, forms a holistic approach to detect and respond to threats that few vendors can achieve.

In addition, while other ADR tools stop at detection, Miggo extends seamlessly to proactive action and prevention. Miggo ties detection to real-time app behavior and automates precise protections. Its observe-predict-enforce cycle, built on expertise in tracing, threat research, and AI, sets it apart from other platforms.

As organizations are increasingly focusing on holistic approaches, Miggo's solutions help them avoid the repetitive task of point product patchwork and alert fatigue to focus more on critical remediation, which makes it an excellent choice, with speed, precision, and operating-cost advantage.

Proven Outcomes for AppSec Teams

The platform's impact has been consistently observed across customers' deployment environments, with the solution delivering outcomes that clearly outperform fragmented AppSec alternatives. Miggo's solution enables AppSec teams to cut down policy-violation detection time by more than 30 times and identify hundreds of security issues that are missed by legacy scanners.

> *"With its strong runtime security, Miggo's solution can facilitate active investigations, enabling teams to identify root causes in a short time, often within the hour, by ingesting raw traces faster than standard AppSec workflows. Deployments across environments by its customers consistently show sharp reductions in mean-time-to-detect (MTTD), mean-time-to-respond (MTTR), and MTTM, translating to lower risk and faster releases than the alternatives."*
>
> ***- Anh Tien Vu***
> ***Industry Principal, Global Cybersecurity Practice***

When integrated with telemetry and cloud configuration data, security teams can map microservice baseline drift quickly without the custom scripts that other traditional tools require. This helps save significant time and automation effort. This is particularly important for organizations with limited AppSec staffing, as they can reduce thousands of open vulnerabilities into a handful of exploitable paths that show critical matters instead of theoretical and irrelevant vulnerabilities. The ability to match the depth of vulnerability management data and runtime insight for risk prioritization enables them to filter out the noise to focus more on the issues that matter the most.

In addition, with its strong runtime security, Miggo's solution can facilitate active investigations, enabling teams to identify root causes in a short time, often within the hour, by ingesting raw traces

faster than standard AppSec workflows. Deployments across environments by its customers consistently show sharp reductions in mean-time-to-detect (MTTD), mean-time-to-respond (MTTR), and MTTM, translating to lower risk and faster releases than the alternatives.

This has helped the company gain popularity among large organizations across key regulated industries, enabling it to propel a revenue path projected for explosive growth since its establishment. Additionally, Miggo's go-to-market (GTM) strategy aligns with its technical innovation as it focuses on partnership and outcome-oriented strategies. It accommodates diverse purchasing preferences through AWS Marketplace listings, managed security service providers (MSSPs), reseller channels, and scalable licensing, offering flexibility that is in sharp contrast with the rigid models of competitors. These factors are expected to help Miggo maintain a stellar growth pace moving forward.

Conclusion

As traditional AppSec solutions fall short, Miggo is changing the application runtime security space with its innovative ADR solution. By integrating deep runtime observability, predictive threat intelligence, and automated response in a unified, sensor-agnostic platform, Miggo provides AppSec teams with a precise and modern approach to application detection, investigation, and response, setting it apart from many competitors on the market. Its capacity to evolve detection into immediate, customized protection redefines runtime security benchmarks. With exceptional performance, strong customer value, and rapid innovation, Miggo receives the 2025 Frost & Sullivan Global New Product Innovation Recognition in the application security industry.

What You Need to Know about the New Product Innovation Recognition

Frost & Sullivan's New Product Innovation 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 New Product Innovation Recognition, Frost & Sullivan analysts independently evaluated the criteria listed below.

New Product Attributes

Match to Needs: Customer needs directly influence and inspire the product portfolio's design and positioning

Reliability: Product consistently meets or exceeds customer performance expectations

Quality: Product offers best-in-class quality with a full complement of features and functionality

Positioning: Product serves a unique, unmet need that competitors cannot easily replicate

Design: Product features an innovative design that enhances both visual appeal and ease of use

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 fuelled by the Innovation Generator™.

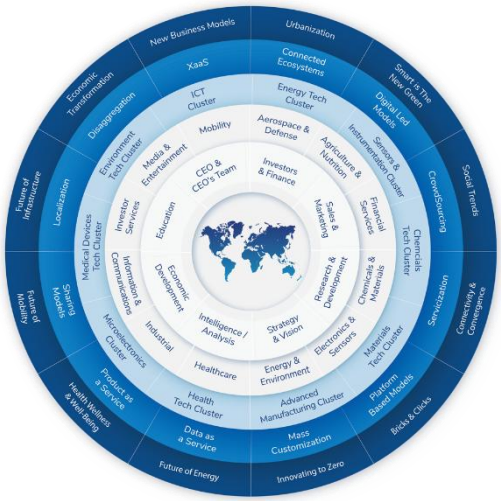
Learn more.

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: