Pillar

# 2025 COMPETITIVE STRATEGY LEADER

*Transforming Innovation Into High-Growth Performance and Competitiveness*

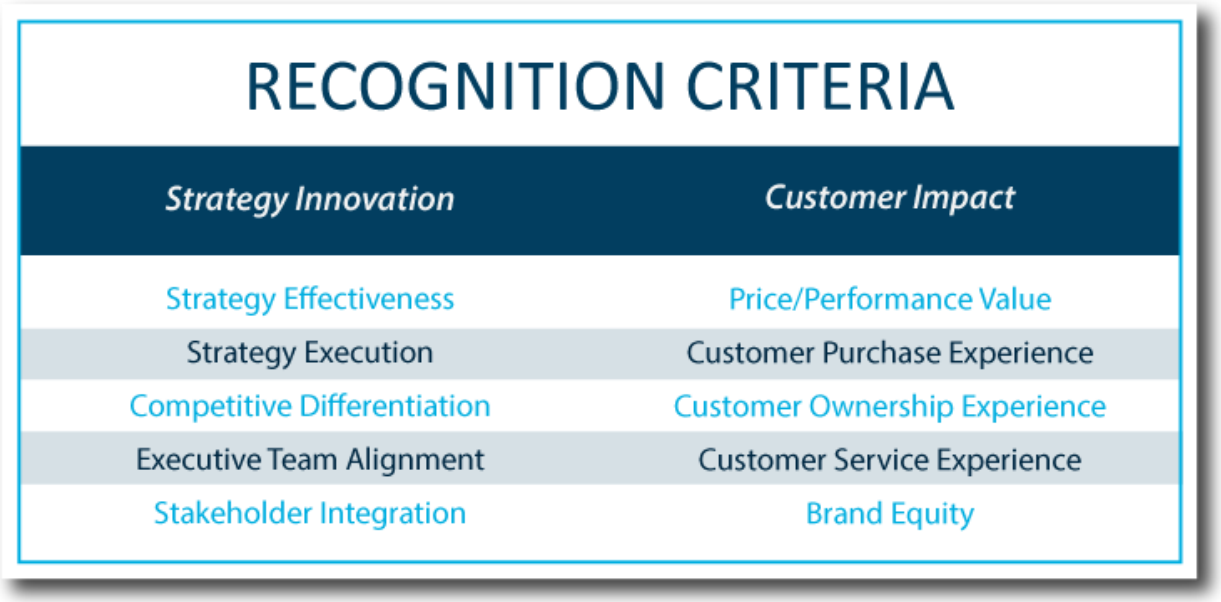
*RECOGNIZED FOR BEST PRACTICES IN THE GLOBAL GENERATIVE AI SECURITY INDUSTRY*

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. Pillar Security excels in many of the criteria in the generative AI security space.




## The Transformation of the Generative AI Security Industry

As enterprises embrace the promise of generative AI (GenAI), they are also confronted with a profound transformation in their cybersecurity posture. AI systems are no longer confined to isolated innovation projects; they are rapidly becoming integral to development pipelines, internal workflows, customer-facing applications, and increasingly autonomous agents. With this shift, the nature of digital risk has undergone a dramatic change, introducing new threat vectors that extend beyond traditional software environments. For organizations aiming to adopt AI at scale, visibility, control, and trust have become non-negotiable.

Frost & Sullivan analysts observe how Pillar Security has emerged as a defining force in this evolving landscape. Its unified GenAI security platform is engineered specifically to secure the entire AI lifecycle, from initial planning to runtime operations. Frost & Sullivan believes that what sets Pillar apart is its first-principles approach: rather than retrofitting existing tools, it addresses the unique risks and behaviors introduced by GenAI systems. By identifying, assessing, and mitigating threats such as prompt injection, model poisoning, and agentic overreach, the platform empowers security teams and AI leaders with both strategic clarity and operational control.

In a market defined by complexity and constant change, Pillar stands out not only for the depth and breadth of its technology, but for its ability to harmonize security, compliance, and innovation. It enables

organizations to move fast without losing visibility, to scale confidently without compromising safety, and to build with AI, securely and responsibly, from the start.

### Built for the Future: Pillar's Strategy for Securing the Full AI Lifecycle

Pillar Security's approach to the generative AI security landscape reflects a deep and nuanced understanding of both current market vulnerabilities and the long-term evolution of AI threats. While many vendors have hastily adapted existing tools to meet the growing demand for AI protection, Pillar has taken a radically different route. It has built its platform from the ground up, guided by a DevSecOps-for-AI philosophy that places security at the core of every phase in the AI lifecycle. This philosophy not only bridges the gap between AI developers, data scientists, and security teams, but also reshapes how enterprises approach governance, trust, and operational control in AI systems.

This strategic clarity is matched by consistent and tangible execution. Pillar's platform provides comprehensive protection across six distinct phases of the AI lifecycle: planning, development, testing, deployment, operation, and monitoring. Rather than viewing security as a static checkpoint, Pillar integrates it as a continuous process, ensuring that risk is managed proactively from ideation through production use.

Despite offering an expansive suite of capabilities, including AI discovery, security posture management (SPM), adversarial red teaming, adaptive runtime guardrails, agentic sandboxes, and telemetry, Pillar maintains architectural flexibility. Each module can be adopted independently or as part of an integrated ecosystem, enabling organizations to tailor their deployments to specific priorities, resources, and levels of AI maturity.

> *"Pillar also leads in AI asset discovery, a critical need as organizations grapple with the rise of shadow AI. Through deep integration with source control, ML Ops, and data infrastructure, Pillar offers unparalleled visibility into models, prompts, and datasets, often surfacing assets that teams didn't know existed."*
>
> ***- Claudio Stahnke, Industry Analyst***

Pillar's commitment to enterprise readiness is evident in its real-world traction. Even at the seed stage, it has secured deployments with Fortune 500 organizations operating in highly regulated industries. Its support for cloud, hybrid, and on-premise architectures, coupled with onboarding processes that can be completed in under an hour, demonstrates a rare balance of depth and deployability.

Crucially, Pillar backs its technology with thought leadership. The company is deeply invested in research and industry collaboration, regularly publishing insights into prompt injection attacks, AI agent behavior, and the limits of current security models. This work feeds directly into its platform capabilities while contributing to the broader industry dialogue. The company's leadership in developing an open-source AI security framework, with input from industry giants such as Google and Salesforce, underscores its role as a trusted ecosystem builder, not just a vendor.

Together, these strategic and operational choices have positioned Pillar not only as a product innovator, but as a trusted guide for enterprises navigating the complex terrain of generative AI risk.

## Securing the Future: Pillar's Competitive Advantage in the GenAI Era

In an increasingly competitive field where vendors often specialize in narrow segments or adapt legacy tools to AI environments, Frost & Sullivan appreciates how Pillar Security sets itself apart through architectural discipline, technological depth, and a laser focus on the unique threat landscape of generative AI. Its platform is not a superficial wrapper or a collection of repurposed security modules; it is a purpose-built, AI-native framework that reflects a profound understanding of what securing modern AI systems truly requires.

A prime example of this differentiation is Pillar's adversarial red teaming capability. While many vendors rely on basic fuzz testing or single-prompt attacks, Pillar simulates complex, multi-step threats using both white-box and black-box methodologies. This enables organizations to evaluate how their AI systems might behave under coordinated attacks or adversarial pressure, conditions far closer to real-world threat scenarios.

The platform's deployment-phase guardrails take this realism a step further. Designed to be model-agnostic and continuously adaptive, these guardrails don't merely block known prompt injections; they evolve, learning from red teaming results and live usage patterns. This ensures that policies remain effective even as the nature of generative AI usage changes or new vulnerabilities emerge.

Pillar also leads in AI asset discovery, a critical need as organizations grapple with the rise of shadow AI. Through deep integration with source control, ML Ops, and data infrastructure, Pillar offers unparalleled visibility into models, prompts, and datasets, often surfacing assets that teams didn't know existed. One mid-sized enterprise recently uncovered 40 previously undetected models scattered across more than 170 repositories, thanks to Pillar's automated scanning.

Moreover, while most solutions remain focused on static AI use cases, Pillar is already addressing the future: agentic AI. With the emergence of autonomous agents capable of invoking tools, browsing, and executing workflows, the risks and opportunities grow exponentially. Pillar's sandbox feature provides a secure, containerized environment for running these agents, complete with access controls and forensic-grade logging, ensuring these powerful capabilities do not become security liabilities.

Finally, Pillar has gone to great lengths to ensure its solution is enterprise-ready. Its architecture supports hybrid, cloud, and on-premise deployment, and is backed by SOC 2 Type II certification, robust role-based access controls, and seamless integration with SIEM and compliance systems. This makes it particularly appealing to enterprises in regulated sectors and geographies, especially across Europe and the Asia-Pacific region, where deployment flexibility and auditability are non-negotiable.

These capabilities position Pillar not just as another tool in the AI security toolkit, but as a foundational security layer for enterprises committed to scaling generative AI with confidence. As organizations seek solutions that offer both depth and adaptability, Pillar is fast emerging as the go-to partner for securing the future of AI.

## Confidence Engineered: How Pillar Earns Trust Across the Enterprise

Pillar Security's impact on its customers goes well beyond product functionality; it delivers clarity, control, and a sense of confidence in an area where ambiguity and risk often dominate. At a time when enterprises

struggle to understand how to deploy AI securely, Pillar offers more than just a platform; it provides transformation. It helps security leaders and AI teams reimagine how trust, visibility, and control are engineered into AI workflows.

One of Pillar's defining strengths lies in its price-to-performance value. Despite being in the early stages of growth, the company delivers outsized returns through a modular platform architecture that can be implemented rapidly. Customers are not forced into an all-or-nothing deployment; instead, they can target critical lifecycle phases, such as guardrails for runtime protection or red teaming for pre-deployment validation, allowing security investments to scale in tandem with AI maturity.

This flexibility is reinforced by a customer experience model built on deep engagement. From the very first engagement through deployment and post-sales support, Pillar takes a consultative approach. It works side-by-side with client security and data teams to co-design implementation strategies that reflect each organization's technical architecture, regulatory constraints, and innovation goals. The result is not a one-size-fits-all rollout, but a tailored deployment that aligns security with business priorities.

> *"One of Pillar's defining strengths lies in its price-to-performance value. Despite being in the early stages of growth, the company delivers outsized returns through a modular platform architecture that can be implemented rapidly. Customers are not forced into an all-or-nothing deployment; instead, they can target critical lifecycle phases, such as guardrails for runtime protection or red teaming for pre-deployment validation, allowing security investments to scale in tandem with AI maturity."*
>
> ***- Claudio Stahnke, Industry Analyst***

As organizations incorporate Pillar into their broader AI governance strategies, the platform transforms from a utility into a cornerstone. Clients don't merely "use" Pillar; they embed it into how they define trust across AI systems. For many, especially those in regulated or high-risk sectors, Pillar is the first solution that delivers both peace of mind and strategic value in securing AI. The pride with which these early adopters describe their experience speaks volumes to the company's long-term retention prospects.

Pillar's growing brand equity amplifies this customer impact. Despite its youth, the company has established itself as a respected voice in the emerging AI security sector. Its leadership is visible in high-quality research reports, active participation in community events, and the development of an open-source framework that invites broad industry collaboration. Rather than pursuing proprietary lock-in strategies, Pillar fosters shared progress, earning trust not only as a vendor, but as a thought leader shaping the future of responsible AI adoption.

Critically, Pillar understands that AI security cannot be addressed in isolation. Its platform is designed to empower cross-functional collaboration between security professionals, developers, data scientists, and compliance teams. By giving all stakeholders access to the same insights and risk posture data, Pillar acts as a unifying force that strengthens internal alignment and streamlines decision-making.

Collectively, these attributes not only improve the technical security of AI deployments; they also raise the organizational maturity of Pillar's clients. In an environment where digital trust is not just a differentiator but a requirement, Pillar helps enterprises lead with confidence and remain resilient in the face of change.

## Conclusion

In a market that is evolving faster than most organizations can adapt, Pillar Security offers clarity, control, and a credible path forward. Its strategic innovation, grounded in first-principles thinking and DevSecOps for AI, has resulted in a robust, full-lifecycle platform that is years ahead of many incumbents. Frost & Sullivan concludes that Pillar Security's competitive differentiation lies in its depth of capabilities, red teaming excellence, enterprise-readiness, and its unwavering focus on real AI use cases, especially autonomous agents.

Yet beyond product features, what truly sets Pillar apart is its impact on customers and the broader industry. Through visionary leadership, technical excellence, and a community-first approach, Pillar is shaping not only how AI is secured, but also how it is responsibly deployed and governed.

With its strong overall performance, Pillar Security earns the 2025 Frost & Sullivan Global Competitive Strategy Leadership Recognition in the generative AI security industry.

# What You Need to Know about the Competitive Strategy Leadership Recognition

Frost & Sullivan's Competitive Strategy 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 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 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)