FROST & SULLIVAN

BEST PRACTICES

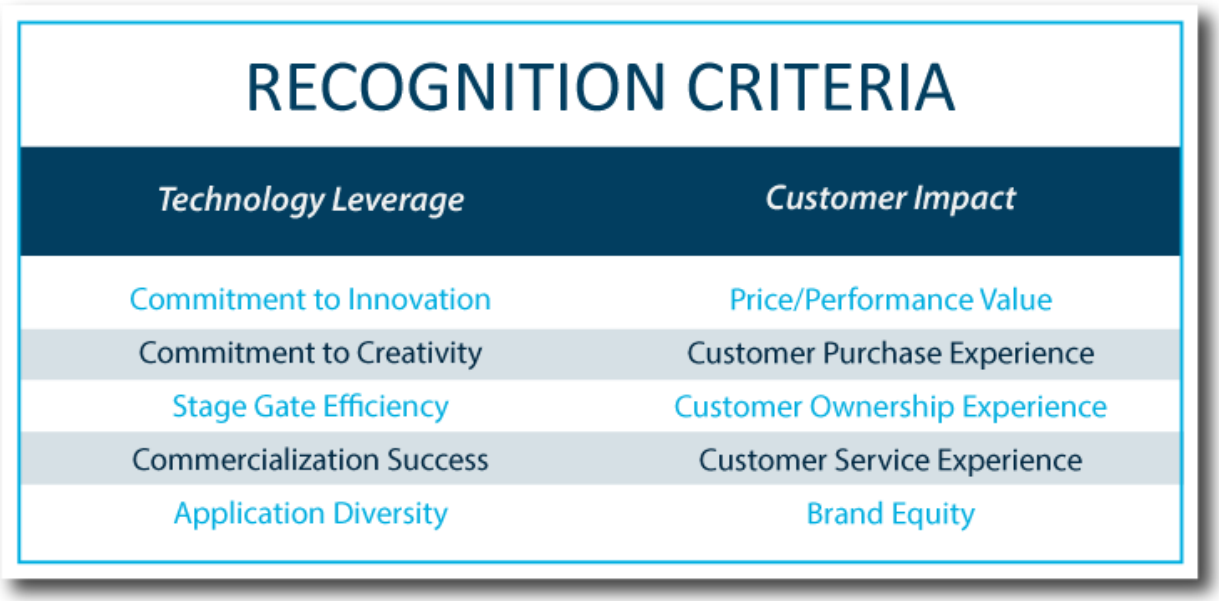
2026 AMERICAS AI-DRIVEN CYBERSECURITY

ENABLING TECHNOLOGY LEADERSHIP

securonix

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. Securonix excels in many of the criteria in the AI-driven cybersecurity space.



RECOGNITION CRITERIA

Technology Leverage	*Customer Impact*
Commitment to Innovation	Price/Performance Value
Commitment to Creativity	Customer Purchase Experience
Stage Gate Efficiency	Customer Ownership Experience
Commercialization Success	Customer Service Experience
Application Diversity	Brand Equity

The Transformation of the AI-driven Cybersecurity Industry

The cybersecurity operations industry is moving from a model built around tools, rules, and manual review toward one built around AI-guided operational judgment. Traditional SOC systems were designed to detect, sort, and escalate threats based on real-time or post-incident activity. In contrast, emerging SOC solutions are being designed to interpret, prioritize, and act on potential threats or risk factors proactively. That shift is being forced by the simple reality that the volume, speed, and variety of security data requiring monitoring and mitigation now exceeds the limits of human-first operations, especially in environments spanning cloud, identity, endpoint, API, and behavioral telemetry. AI is no longer simply augmenting existing workflows; it is increasingly being embedded into security operations processes to help organizations manage growing telemetry volumes, accelerate investigations, and maintain operational effectiveness at enterprise scale.

Within the cybersecurity operational workflow, what is changing most is not just detection capability, but the nature of security reasoning. Static rules and predefined correlations are too brittle for attacks that now move through identities, trusted accounts, long dwell times, and subtle behavior changes rather than obvious signatures. Modern security operations increasingly depend on systems that can connect weak signals across time, understand context across entities, and surface risk before a clear incident has fully formed. That is why the industry is shifting from event management to entity understanding, and from isolated alerts to continuous risk interpretation. The value of AI in this environment lies in its ability to

correlate large volumes of security data, provide contextual analysis, and help analysts identify meaningful risk signals more efficiently.

The role of the security analyst is changing in parallel. A large share of SOC efforts have historically gone into repetitive, manual work such as data enrichment, report drafting, cross-console checking, and low-value alert triage. AI is beginning to absorb that load, which is reshaping productivity economics inside the SOC. The most meaningful impact is not full autonomy, but the compression of time spent on routine tasks so analysts can spend more time on analytical judgments, event investigation, and threat response. In this sense, the industry is not replacing the SOC analyst but redefining their role from repetitive manual tasks to higher-value investigation, threat analysis, and response activities.

> *"Securonix reframed AI from a standalone detection capability into an operational force multiplier capable of increasing the effectiveness and scalability of existing security teams without proportionally increasing operational overhead."*
>
> ***Pranav Sahai***
> ***Industry Analyst, Security***

The next phase of this transformation will be determined by trust, governance, and economics. Enterprises will not adopt AI-enabled cybersecurity systems at scale unless they can prove that decisions are explainable, data is isolated, automation is controlled, and value is measurable. That is why the strongest platforms will be those that combine AI with data discipline, operational transparency, and secure deployment architecture. At this critical industry phase, successful AI-enabled SecOps vendors will be those that combine AI innovation with operational transparency, governance controls, measurable outcomes, and enterprise-scale deployment models.

Turning AI Innovation into Scalable SOC Outcomes

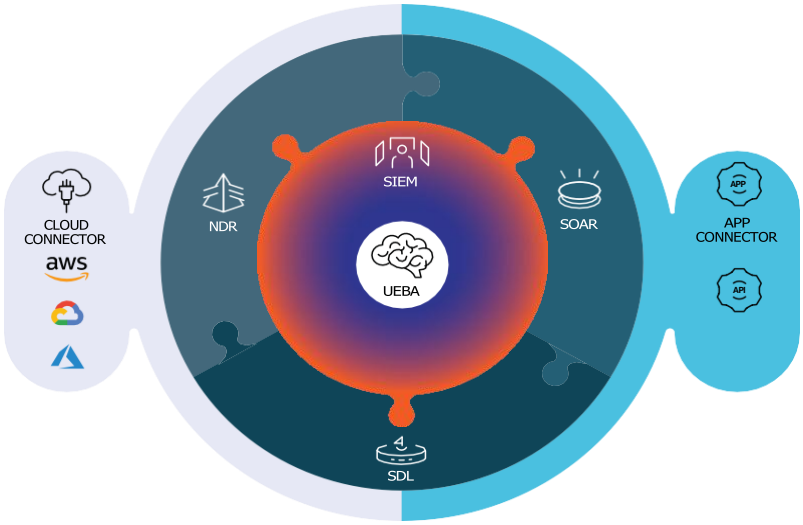
Securonix's innovation strategy is centered on redesigning the operational structure of the modern SOC environment. While much of the cybersecurity industry has positioned AI as a conversational assistant or overlay capability, Securonix embeds AI-assisted capabilities directly into operational workflows such as investigations, alert enrichment, threat prioritization, insider threat analysis, and analyst decision support. This distinction is strategically important as it shifts AI from a user interface enhancement into a core operational capability that enhances how security teams investigate, prioritize, and respond to threats. The company's development of AI SOC Analysts, agentic workflows, and behavioral intent analytics reflects a broader industry vision in which AI augments human expertise rather than attempting to replace it outright. Securonix recognizes that the future SOC will not be fully autonomous but governed through coordinated human-machine collaboration where repetitive investigative and enrichment tasks are automated or AI-assisted while analysts retain oversight, judgment, and strategic authority.

The defining strength of Securonix's innovation model is its focus on measurable analyst productivity and operational efficiency. Instead of pursuing AI as a purely detection-centric capability, the company concentrated on reducing the operational inefficiencies that materially burden SOC teams, including alert enrichment, investigative preparation, multi-tool correlation, and executive-level threat summarization.

This approach transforms AI from an experimental feature into a measurable operational lever capable of compressing response timelines, accelerating investigations, and improving analyst throughput. More importantly, it reflects a disciplined understanding of enterprise cybersecurity needs for autonomous platforms that can improve security outcomes without proportionally increasing staffing complexity, operational fatigue, or budget exposure. By grounding AI development in real operational constraints, Securonix differentiates itself from competitors that continue to position AI primarily as an assistant layer rather than as an operational workflow framework that helps automate and accelerate common SOC activities.

> *"By simultaneously solving for operational intelligence, economic scalability, and governed deployment, Securonix positioned itself as an enabler of the next operational model for enterprise cybersecurity"*
>
> ***Pranav Sahai***
> ***Industry Analyst, Security***

Securonix establishes a differentiated position by addressing the data economics challenge for SecOps teams, one of the industry's most significant operational challenges. As telemetry volumes now span cloud, identity, endpoint, and hybrid infrastructures, organizations increasingly struggle to balance visibility requirements against escalating SIEM and storage costs. Securonix addressed this challenge through its Data Pipeline Manager (DPM), which filters, routes, and prioritizes telemetry based on security value, compliance requirements, and operational relevance.



Securonix: Security for the cloud in the cloud

Rather than treating all security data equally, the company introduced a tiered operational model that preserves long-term visibility and searchability while optimizing storage economics. This is strategically significant because it reframes AI not only as a detection mechanism, but also as an operational and financial optimization layer for cybersecurity infrastructures. In effect, Securonix has expanded access to advanced analytics while helping customers manage telemetry costs more effectively.

The company's ability to operationalize innovation at enterprise scale is reinforced by a highly customer-centric stage-gate model. Securonix integrates customer advisory participation, design partnerships, technical account engagement, and direct operational feedback into roadmap development and feature

prioritization. This allows the company to identify operational friction points early and accelerate the conversion of emerging concepts into deployable capabilities. The integration of ThreatQuotient further strengthened this model by combining behavioral analytics with continuously updated threat intelligence and community-driven detection insights, creating a more adaptive and intelligence-driven security ecosystem. Importantly, Securonix has paired this innovation velocity with a strong governance foundation. The company invested heavily in sovereign AI controls, customer-level data isolation, cryptographic separation mechanisms, and governance frameworks designed to prevent unauthorized cross-tenant data access in multi-tenant cloud environments. By solving simultaneously for innovation, operational trust, and enterprise governance, Securonix positioned itself not simply as an AI-enabled cybersecurity vendor, but as an enabler of governed, enterprise-scale AI-driven cybersecurity operations. In doing so, the company is helping establish best practices for governed AI deployment within enterprise security operations.

Building Customer Confidence from Purchase to Ongoing Support

Securonix's customer purchase experience deliberately removes friction from the enterprise buying process. Rather than asking customers to assemble a broader security operations stack around the platform, the company offers direct access to security operations and product specialists, a high technical-account-manager-to-customer ratio, and a transparent engagement model that surfaces customer's program roadmap direction, feature priorities, and implementation realities early in the relationship. That matters because enterprise security buyers are not simply purchasing software but gaining confidence and in-depth understanding of the Securonix platform and its role within their SecOps program. Securonix appears to have embedded that confidence into the purchase journey through design partnerships, customer-community input, and executive-level participation via the customer advisory board.

What makes that purchase experience commercially strong is that it is tied to the customer's economics. Rather than forcing customers into a one-size-fits-all cost model, Securonix's Data Pipeline Manager gives customers a practical buying advantage by allowing high-value telemetry to flow into real-time analytics while routing lower-value data into cheaper tiers, expanding capacity and lowering the barrier to broader coverage. The result is a clearer value proposition for the buyer around greater visibility, more efficient telemetry management, and improved cost predictability.

On service experience, Securonix combines high-touch support with continuous product co-creation. The customer community is not treated as a marketing forum, but functions as a structured mechanism for roadmap input, feature suggestions, issue escalation, and operational collaboration. The customer advisory board adds a more strategic layer, allowing customers across industries to shape long-term direction and challenge Securonix to stay relevant to their evolving operational needs. That model is especially valuable in cybersecurity, where service quality is judged not only by response speed, but by the vendor's ability to translate emerging threats into action. Securonix's threat research team can proactively push detections and sensors to customers, which turns service into a proactive operational support model that helps customers improve detection coverage and security outcomes.

This service model creates a strong retention and expansion engine. Customers are not simply receiving support, but gaining a vendor partner that continuously reduces their operational burden, shortens time-to-value, and justifies security spend with concrete outcomes such as reduced triage time, more

automated investigations, and faster executive-ready reporting. AI-assisted summarization, alert enrichment, and cross-source correlation all materially improve analyst throughput, strengthening renewal logic because the value is visible in day-to-day operations rather than abstract promise.

Just as importantly, Securonix has addressed one of the biggest adoption barriers in AI-driven security: trust. The company invests in strict data governance, cryptographic isolation across subtenants, and governance controls aligned to emerging AI management and governance practices to ensure customer data does not cross-contaminate, even in shared cloud environments. That lowers perceived risk in procurement and makes enterprise buyers more willing to move from experimentation to production deployment.

Redefining the Economics of Cybersecurity Operations

Securonix understands that its customers are not only buying software, but a solution that enables them to maintain broad security visibility and effective threat response while controlling operational costs. Securonix helps customers improve the economics of security operations without forcing them to compromise on the depth or duration of threat visibility. That makes the platform attractive not only as a security tool, but as a budget-conscious operating model.

The fundamental value proposition is improved security outcomes and operational efficiency from existing security investments. Securonix reduces the hidden costs that often erode ROI in security programs, such as excessive telemetry spending, repetitive manual work, duplicated operational effort, and inefficiencies due to platform limitations.

What strengthens Securonix commercially is that the platform's economics are embedded into the product experience rather than layered on as an afterthought. This reduces the need for customers to build separate workaround stacks or absorb excessive integration overhead just to realize value. The result is a stronger value proposition and return on security investment: customers get a platform that is designed to scale with operational reality, not against it.

Conclusion

With Securonix's solution design that embeds AI-assisted capabilities into core SOC workflows, the company enables SecOps teams to achieve faster investigations, improved analyst productivity and operational scalability, and more efficient threat prioritization without compromising human oversight. Securonix also demonstrates strong strategic differentiation through its focus on productivity economics, helping organizations improve security outcomes while controlling telemetry growth, operational complexity, and staffing pressures. Its innovations in AI-driven operational intelligence, data economics, and enterprise-scale governance reflect a pragmatic and commercially relevant approach to next-generation cybersecurity operations. Equally important, Securonix has paired technological innovation with a customer-centric operating model built around transparency, collaboration, and measurable operational value. Through this combination of innovation maturity, operational relevance, and scalable enterprise execution, Securonix is helping shape the future of AI-driven, enterprise-scale security operations.

For its strong overall performance, Securonix is presented with Frost & Sullivan's 2026 Americas Enabling Technology Leadership Recognition for the AI-driven Cybersecurity industry.

What You Need to Know about the Enabling Technology Leadership Recognition

Frost & Sullivan's Enabling Technology Leadership Recognition identifies the company that applies its technology in new ways to improve existing products and services and elevate the customer experience.

Best Practices Recognition Analysis

For the Enabling Technology 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

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)