FROST & SULLIVAN

BEST PRACTICES

2026 ASIA-PACIFIC ENDPOINT SECURITY

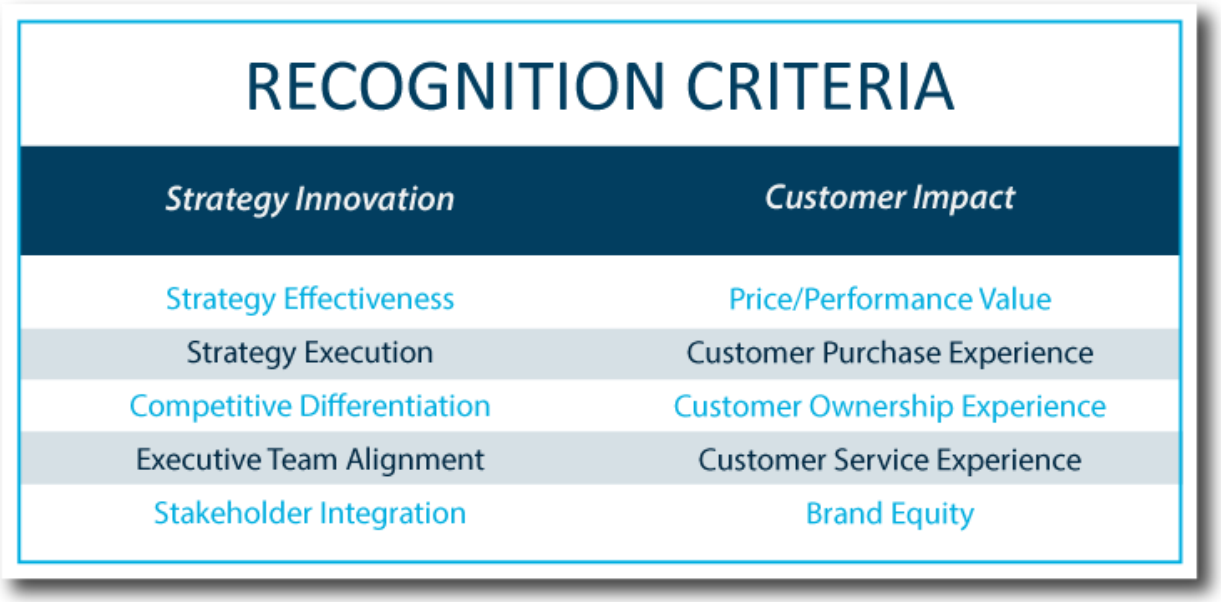
COMPETITIVE STRATEGY LEADERSHIP

AhnLab

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. AhnLab excels in many of the criteria in the Asia-Pacific endpoint security space.



The Transformation of the Asia-Pacific Endpoint Security Industry

The Asia-Pacific endpoint security market is undergoing a significant transformation as organizations accelerate digitalization, cloud adoption, artificial intelligence (AI) deployment, and hybrid work initiatives. Endpoint security is no longer limited to protecting user devices against malware; it now serves as a critical control point for safeguarding distributed workforces, cloud-connected assets, and increasingly autonomous AI-enabled environments. At the same time, threat actors are leveraging AI to identify vulnerabilities, automate attack execution, and accelerate attack lifecycles, placing greater pressure on organizations to detect and respond to threats more quickly and effectively.

These developments are reshaping customer expectations. Enterprises increasingly seek integrated security platforms that deliver comprehensive visibility, intelligence-driven detection, and streamlined operations rather than relying on standalone security tools. Simultaneously, cybersecurity talent shortages continue to challenge organizations across the region, driving demand for greater automation, managed security services, and AI-assisted security operations. As threat intelligence, extended detection and response (XDR), endpoint detection and response (EDR), managed detection and response (MDR), and AI become increasingly interconnected, customers are prioritizing security providers capable of orchestrating these capabilities into a unified operating model.

From Endpoint Protection to Security Operations: Addressing Modern Enterprise Security Requirements

Founded in 1995, AhnLab has evolved from a pioneering endpoint security provider into one of Asia-Pacific's most comprehensive cybersecurity companies. Through its integrated strategy encompassing endpoint protection, EDR, XDR, threat intelligence, MDR, and AI-driven security operations, the company has established a differentiated position within the region's increasingly complex cybersecurity landscape. The company focuses on platform integration, intelligence-driven security operations, and AI-native innovation to establish itself as a leading entity in this space.

As cyber threats become more sophisticated, organizations face growing challenges in managing fragmented security environments. Many enterprises have deployed multiple layers of security technologies over time, yet struggle to maintain visibility across attack chains, correlate threats effectively, and respond quickly to emerging incidents. The increasing prevalence of ransomware, supply chain attacks, fileless threats, and AI-enhanced attack techniques has further amplified these operational challenges.

AhnLab's strategy recognizes that the future of endpoint security lies not in individual products but in integrated security operations. Rather than positioning endpoint protection as a standalone capability, the company has developed a comprehensive ecosystem that unifies endpoint protection, EDR, vulnerability management, patch management, privacy management, device control, threat intelligence, and managed detection services within a cohesive platform framework.

The company's integrated approach creates meaningful differentiation. Through single-agent, single-console architecture, customers gain centralized visibility into their endpoint environment while benefiting from native interoperability among security controls. Information generated by endpoint protection, EDR, threat intelligence, vulnerability management, and response services is shared across the ecosystem, enabling automated correlation and coordinated response actions. This approach reduces operational complexity, minimizes security silos, and improves overall security effectiveness.

> *"By focusing on operational simplification, integrated visibility, and ecosystem-wide coordination, AhnLab addresses one of the most pressing challenges facing security teams today: achieving meaningful security outcomes in increasingly complex environments."*
>
> ***- Vivien Pua***
> ***Industry Principal***

AhnLab has further strengthened this strategy through extensive platform integration. Endpoint security solutions are increasingly connected with XDR, threat intelligence, zero-trust access technologies, and operational technology security management solutions, providing customers with broader visibility across modern enterprise environments. These capabilities help organizations move beyond isolated security alerts and toward contextualized threat understanding that supports faster, more informed decision-making.

A particularly important differentiator is the company's ability to combine technology and services within a unified security ecosystem. Through integrated MDR services, expert threat analysis, and intelligence-driven response processes, customers gain access to operational expertise in addition to technology

capabilities. This integrated model allows organizations to strengthen detection, analysis, and response without increasing security complexity or operational overhead.

By focusing on operational simplification, integrated visibility, and ecosystem-wide coordination, AhnLab addresses one of the most pressing challenges facing security teams today: achieving meaningful security outcomes in increasingly complex environments. This strategy forms the foundation of the company's competitive differentiation and long-term market relevance.

Building an AI-Native Security Future Through Intelligence-Led Automation

AI is emerging as one of the most disruptive forces in cybersecurity. Threat actors increasingly utilize AI to accelerate reconnaissance, automate vulnerability discovery, and launch more sophisticated attacks. At the same time, organizations expect security vendors to use AI not merely as an enhancement but as a foundational capability that improves detection, analysis, response, and operational efficiency.

AhnLab has responded to this market shift by embracing an AI-native strategy that extends across its endpoint security portfolio. The company has developed a long-term vision centered on integrating AI into security operations workflows, threat intelligence analysis, and incident response processes. Rather than introducing isolated AI features, AhnLab is embedding AI into the broader security lifecycle to create a more intelligent and automated operating environment.

A central element of this strategy is AhnLab AI PLUS, the company's Agentic AI-based security platform. Designed to enhance detection, analysis, and operational efficiency, AI PLUS serves as a foundation for integrating AI capabilities across AhnLab's product and service portfolio. Complementing this initiative is Annie, AhnLab's conversational AI security assistant, which helps security teams investigate events, understand attack context, identify response recommendations, and streamline security workflows through natural language interactions.

The company has also introduced AI Insight capabilities within its EDR platform. This functionality enables AI-driven interpretation of security events, helping analysts understand attacker intent, risk context, and recommended response strategies through automated narrative reporting. By reducing investigative complexity and accelerating analysis, AI Insight improves both analyst productivity and response effectiveness.

Beyond automation, AhnLab is increasingly connecting AI capabilities with its threat intelligence ecosystem. Through deeper integration among threat intelligence platform (TIP), EDR, XDR, and AI-driven analytics, the company enables organizations to transform threat intelligence into actionable security outcomes. Security teams can move from reactive investigations toward more proactive risk identification and prioritization, improving overall security resilience.

Importantly, AhnLab's vision extends beyond using AI for defense. As organizations increasingly deploy AI systems and AI agents within business operations, the company recognizes the need to secure these emerging environments as well. This forward-looking perspective positions AhnLab to address future cybersecurity requirements arising from broader AI adoption across enterprise ecosystems.

Rather than treating AI as a supplementary feature, AhnLab has aligned its innovation strategy and product roadmap around AI-driven security operations. This commitment reflects strong executive

alignment around a vision that emphasizes automation, intelligence, and operational efficiency as critical enablers of future cybersecurity success.

Orchestrating Intelligence Across the Security Ecosystem

AhnLab has built its execution strategy around a simple but powerful principle: intelligence should drive every stage of cybersecurity operations. By integrating threat research, intelligence generation, security analytics, and response capabilities within a coordinated ecosystem, the company has established a repeatable framework for delivering proactive and context-driven security outcomes.

At the center of this model is ASEC, the company's security intelligence organization responsible for threat collection, analysis, and research. Insights generated by ASEC are continuously fed into the AhnLab TIP, where threat indicators, threat actor intelligence, dark web monitoring data, and contextual threat information are consolidated and operationalized. This intelligence is subsequently integrated with XDR and EDR platforms, creating an intelligence-driven operating model that spans detection, investigation, and response.

This intelligence-led approach enables AhnLab to move beyond traditional security monitoring toward a more proactive and contextualized model of cybersecurity operations. Security teams gain access to real-time threat intelligence, automated correlation capabilities, and integrated response workflows that help reduce the time required to identify and mitigate emerging threats. The addition of AI-assisted analysis further strengthens these capabilities by automating event interpretation and generating meaningful response recommendations.

AhnLab's execution discipline is also evident in its continuous product enhancement strategy. Customer feedback directly influences roadmap priorities, leading to ongoing improvements in usability, multilingual support, platform integration, identity management compatibility, and endpoint management functionality. Recent enhancements include broader language support, expanded Microsoft Entra ID integration, increased third-party interoperability, and enhancements across EDR, privacy management, device control, and patch management capabilities.

The company's stakeholder integration strategy extends beyond technology. By connecting threat researchers, product developers, security analysts, managed service teams, channel partners, and customers within a coordinated operating model, AhnLab creates a continuous feedback loop that accelerates innovation and improves customer outcomes. This collaborative ecosystem enables the company to align strategic objectives with customer requirements while maintaining consistency across product development and service delivery.

More importantly, AhnLab does not treat threat intelligence, endpoint security, XDR, and managed services as separate business units. Instead, the company orchestrates these capabilities as a unified security ecosystem in which intelligence generated from one area continuously strengthens the others. This approach allows threat discoveries to be rapidly incorporated into products and services, enabling faster innovation cycles, more responsive customer protection, and a stronger connection between research, operations, and business execution.

The resulting framework transforms strategy into repeatable outcomes. AhnLab's ability to connect intelligence, innovation, execution, and stakeholder collaboration creates a sustainable competitive advantage that strengthens both customer value and long-term market relevance, reinforcing its position as a strategic leader in the Asia-Pacific endpoint security market.

Delivering Measurable Customer Outcomes Through Platform Consolidation

AhnLab's customer impact is driven by a strategy focused on simplifying security operations while enhancing protection effectiveness. This balance between operational efficiency and security performance creates meaningful value across the customer journey.

> *"AhnLab's ability to connect intelligence, innovation, execution, and stakeholder collaboration creates a sustainable competitive advantage that strengthens both customer value and long-term market relevance, reinforcing its position as a strategic leader in the Asia-Pacific endpoint security market."*
>
> ***- Vivien Pua***
> ***Industry Principal***

The company's platform-based approach delivers compelling price-performance value by reducing the need for multiple standalone security tools and management interfaces. Through a unified architecture built on a single agent and single management console, organizations can consolidate security operations, reduce management overhead, and improve visibility without increasing complexity. This approach enables customers to achieve stronger security outcomes while optimizing operational resources.

Customer purchase experience is strengthened through the breadth of AhnLab's integrated offerings. Organizations can access endpoint protection, EDR, threat intelligence, MDR services, privacy protection, vulnerability management, device control, and patch management through a unified ecosystem rather than assembling capabilities from multiple vendors. This reduces procurement complexity and accelerates deployment and adoption.

Customer ownership experience is enhanced through continuous platform evolution. Native integrations among AhnLab solutions, interoperability with third-party technologies, and ongoing feature enhancements ensure that customers can expand capabilities without disrupting existing operations. The company's commitment to localization, multilingual support, and regional adaptation further strengthens the ownership experience for organizations operating across diverse Asia-Pacific markets.

Service experience represents another important area of differentiation. AhnLab complements its technology offerings with MDR services delivered directly by the vendor's security experts. This approach provides customers with access to threat analysis, expert guidance, and incident response support while maintaining consistency between the technology platform and service delivery model. Unlike outsourced approaches that separate technology and operations, AhnLab's integrated structure enables deeper visibility and stronger alignment between detection and response.

The effectiveness of this model is reflected in customer feedback and deployment outcomes. Organizations report improved visibility into attack chains, faster ransomware investigation, stronger contextual understanding of threats, and reduced recovery times. One financial-services customer highlighted the value of AhnLab EDR in enabling real-time behavioral analysis and providing visibility

across the entire attack lifecycle, significantly improving its ability to investigate and respond to security incidents.

These customer outcomes reinforce AhnLab's brand equity. With more than three decades of cybersecurity expertise, strong regional recognition, sustained participation in MITRE ATT&CK evaluations, and a growing portfolio that spans products and services, AhnLab has built a reputation for expertise, innovation, and trust. This credibility continues to strengthen customer confidence and support the company's long-term strategic positioning within the Asia-Pacific endpoint security market.

Conclusion

AhnLab's success in the Asia-Pacific endpoint security market stems from a strategy that extends far beyond traditional endpoint protection. The company's integrated cybersecurity ecosystem combines endpoint security, threat intelligence, AI-powered analytics, XDR, MDR, and security operations into a cohesive platform strategy designed to address both current and emerging cybersecurity challenges. Its ability to align strategic innovation, operational execution, ecosystem collaboration, and customer outcomes has enabled AhnLab to establish a differentiated position within an increasingly competitive market. Through AI-native security initiatives, intelligence-driven operations, and a strong commitment to platform integration, the company continues to demonstrate leadership in shaping the future of endpoint security.

As organizations continue to navigate an increasingly dynamic threat landscape, AhnLab's integrated ecosystem, intelligence-driven capabilities, and AI-native vision position the company to remain a trusted partner in helping customers improve visibility, operational efficiency, and cyber resilience. With its strong overall performance, AhnLab earns Frost & Sullivan's 2026 Asia-Pacific Competitive Strategy Leadership Recognition in the endpoint security industry.

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)