SANGFOR

2025 CUSTOMER VALUE LEADER

Maximizing the Price/Performance ROI for Customers

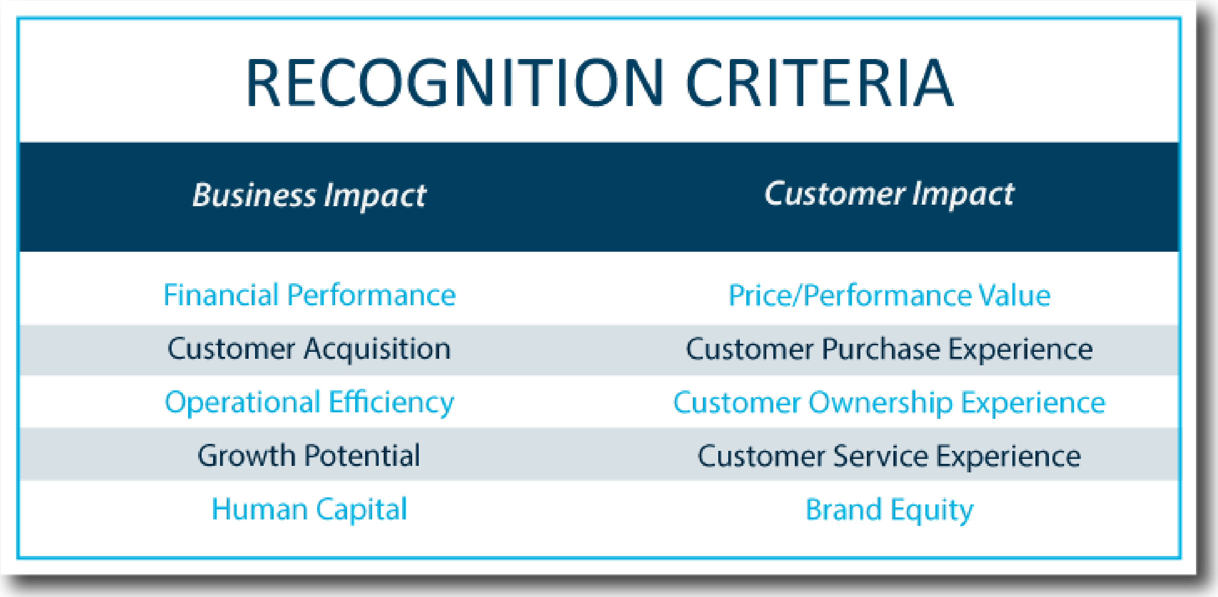
RECOGNIZED FOR BEST PRACTICES IN THE ASIA PACIFIC EXTENDED DETECTION AND RESPONSE INDUSTRY

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. Sangfor excels in many of the criteria in the XDR space.



RECOGNITION CRITERIA

Business Impact	*Customer Impact*
Financial Performance	Price/Performance Value
Customer Acquisition	Customer Purchase Experience
Operational Efficiency	Customer Ownership Experience
Growth Potential	Customer Service Experience
Human Capital	Brand Equity

The Transformation of the XDR Market

In the modern threat landscape, organizations suffer from mounting challenges that prevent them from securing their business-critical data. The technologies that enhance the efficiency of organizations' processes and security, such as artificial intelligence (AI), machine learning (ML), and generative AI (GenAI), also provides advantages for cybercriminals. Bad actors can use these tools to write more effective malicious code, analyze databases to discover information to deliver more targeted phishing campaigns, and generally automate many processes to target more organizations in a fraction of the time.

The use of such technology results in attacks that are more numerous, more sophisticated, and more costly for organizations. IBM's Cost of a Data Breach 2024 report confirms that security breaches are 10% more expensive than in 2023, with an average cost of $4.88 million. According to data from the Frost & Sullivan's Voice of the Enterprise Security Customer survey, significant consequences of successful cybersecurity attacks include loss of productivity (for 30% of organizations that suffered an incident), brand damage and erosion (23%), and higher customer churn (23%).

Additionally, the shortage of cybersecurity personnel continues to pummel organizations seeking to establish in-house SOCs. ISC2's 2024 Cybersecurity Workforce Study shows a workforce gap close to 4.8 million unfilled positions; this represents a 19.1% YoY increase, meaning that the issue continues to get worse for organizations looking to hire and retain cybersecurity professionals. The gap is even bigger in the APAC region, with a 26.4% YoY increase that has resulted in over 3.3 million unfilled cybersecurity roles.

Finally, digital transformation is significantly changing the environment of every organization, with remote work, widespread mobile device deployment, the ubiquity of IoT devices in workspaces, and the increased use of operational technology (OT) involved in the supply chain resulting in hybrid and multi-cloud environments becoming the norm. The digital footprint of organizations is increasingly difficult to monitor and protect; the attack surface continues to grow, creating more opportunities for threat actors to exploit.

Extended Detection and Response (XDR) is a vendor-agnostic solution that seeks to address these issues through its three core promises: cross-layered detection and response across the ecosystem, meaningful automation, and third-party integration of the entire security stack. XDR provides visibility and actionability across the entire ecosystem, ingesting telemetry from disparate sources (such as endpoint, network, cloud, email, mobile, identity, and others) and leveraging AI and ML to correlate the data and detect the most pervasive, insidious, and sophisticated threats.

XDR's features and capabilities enable organizations to address the most pressing issues across the threat landscape. However, customers across the globe, and specifically those in the Greater China region, seek to partner with security vendors that can offer extended value in the form of excellent ROI, world-class automation, and peace of mind for CISOs and security teams. The Chinese cybersecurity market has its own unique drivers and restraints, including a growing involvement from the government that must protect organizations against state-backed threat actors, and an even more severe shortage of cybersecurity personnel than organizations in the West are experiencing. In this context, XDR vendors serving organizations in the region should provide a customer-centric approach to XDR that leverages existing investments, increases operational efficiency, and guides customers through a path of increasing compliance.

Sangfor – Addressing the Need for Advanced, Customer-Centric Security

Sangfor is a Chinese cybersecurity company that aims to be exactly that kind of partner. Launched for the international market in March 2024 after a successful debut in the Greater China market in February 2022, Sangfor XDR offers comprehensive visibility, advanced AI capabilities, and exceptional integration with third-party tools. The firm's goal in the XDR space is to deliver enhanced customer value through operational flexibility and an intuitive customer experience. Its financial success, evidenced by its continuous, above-market-average growth since its launch, has allowed the firm to establish a small presence in the EMEA region to augment success in its core APAC market. Sangfor targets organizations of all sizes, focusing on the financial, education, government, and healthcare industries – sectors that understand the need for advanced cybersecurity solutions as business multipliers.

The firm reaches its customers in two distinct ways: through an in-house sales team that focuses on direct sales, targeting large organizations and offering a customized approach including assessments and consulting options on top of XDR; and a global channel partner network consisting of distributors and value-added resellers that can combine Sangfor XDR with additional services and support, extending its usefulness for organizations that can benefit from managed security or a more hands-on approach. With this strategy, Sangfor reaches a wide range of companies, ensuring the security outcomes they need from its XDR solution.

Integration and Automation to Establish the Foundation of Value-Multiplying XDR

Sangfor XDR provides comprehensive visibility across the ecosystem, including endpoints, network, cloud environments, and IoT devices. The solution allows customers to leverage existing security investments with a vendor-agnostic approach, fulfilling one of the core promises of XDR with over 300 third-party tool integrations. In this way, Sangfor XDR breaks the security siloes, eliminating blind spots and consolidating data from the environment to provide the complete picture of the attack, reducing the number of false alerts, and increasing the mean time to respond and detect.

Furthermore, Sangfor understands that the promise of automation is essential to make XDR the core of an organization’s SOC. Because of this, the firm has built AI-powered analysis engines within Sangfor XDR that continuously analyze and learn network and user behaviors to identify deviations that may indicate advanced threats such as zero-day attacks and advanced persistent threats (APTs). The solution also incorporates real-time threat intelligence to enrich alerts and provide contextual information for security analysts, and machine learning algorithms to provide proactive detection and response capabilities that are essential in today’s evolving threat landscape.

To solidify the promise of automation by upskilling cybersecurity professionals and multiplying their capabilities, Sangfor has included Security GPT in its XDR platform. Security GPT is a GenAI security assistant that streamlines investigation processes, enhancing decision-making by allowing security analysts to interact with the system using natural language queries. This allows less experienced security analysts to inquire about threat-hunting queries, best practices, and effective courses of action, multiplying their value at the same time it ramps up their development and learning. Conversely, more experienced professionals need to spend less time performing repetitive tasks, which generates a reduction in the time required for alert investigation, improving both the efficiency and accuracy of the SOC.

Finally, Sangfor understands the importance of XDR and will continue to invest in developing its capabilities for the foreseeable future. Key areas of innovation for the firm include:

- **Developing specialized modules like Detection GPT and Security Operations GPT for Security GPT**, further improving the threat investigation and hunting process and enhancing automated responses.
- **Launching its Phishing GPT module in the second half of 2025**, that will proactively detect and block adversarial emails on Microsoft Outlook, enhancing the prevention capabilities of the solution and reducing risk of ransomware incidents.
- **Introducing configurable user interfaces for third-party tools**, improving third-party connectivity and usability.
- **Expanding its general detection and response capabilities**, including detections, correlations, and advanced analysis to deliver more effective security outcomes.

With the three core aspects of XDR in mind, Sangfor future-proofs its XDR development to continue to thrive in a competitive market.

Catering to the Growing Demand for Support and Compliance

In combination with its customer-centric technology and innovation approach, Sangfor has also made significant efforts to enhance the user experience in its pricing model. Sangfor ensures cost transparency and predictability for its clients by offering clear, straightforward pricing without hidden costs. This is essential for organizations across all industries and of all sizes, but it provides particular benefit for organizations with low security maturity that are going through digital transformation; such firms often need to juggle more restrained security budgets but still need to protect their business-critical assets. To further enhance this value proposition, Sangfor XDR's all-in-one pricing model provides customers with full access to the XDR suite, eliminating the complexity typically associated with piecemeal pricing structures.

Sangfor includes on-premises and SaaS-based deployment options for its XDR solution, increasing flexibility and versatility and catering to the diverse needs of organizations across the Greater China region. Additionally, the platform's localized deployments ensure that data remains in its country of origin, addressing compliance requirements and preventing unauthorized data transfers. In its home market, this is an essential feature of the Sangfor XDR platform as, stemming from the current geopolitical tension and the East-West divide, the Chinese government is increasing regulations that favor data sovereignty and cybersecurity compliance. As a result, Sangfor is a strong partner for Chinese customers in the most heavily regulated environments that seek to work with a partner that understands the importance of regulations and compliance.

Additionally, the rapid adoption of cloud and hybrid environments in China has driven demand for scalable, AI-driven solutions such as Sangfor XDR. By continuously evolving its platform to meet the unique requirements of the Chinese market while also making efforts to expand internationally (such as its beachhead in the EMEA region), Sangfor demonstrates a well-rounded strategy that ensures growth across diverse regions.

Conclusion

Sangfor stands out in the XDR market, particularly in the Greater China and APAC regions, thanks to a customer-focused approach that permeates its innovation and technology development, roadmap, pricing structure, and deployment options. Sangfor understands the importance of the three core aspects of XDR: cross-layered detection and response, automation, and third-party integration. It ensures that these promises shape the future of its XDR platform, ensuring continued success for years to come. The firm maintains a clear focus on the Greater China region but has made strides to create a global presence and address the security needs of organizations of all maturity levels, sizes, and industries. With its strong overall performance, Sangfor earns Frost & Sullivan's 2025 APAC Customer Value Leadership Recognition in the XDR market.

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.

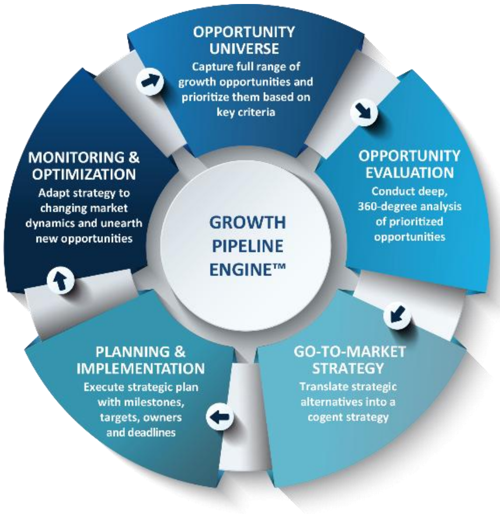
The Growth Pipeline Generator™

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*

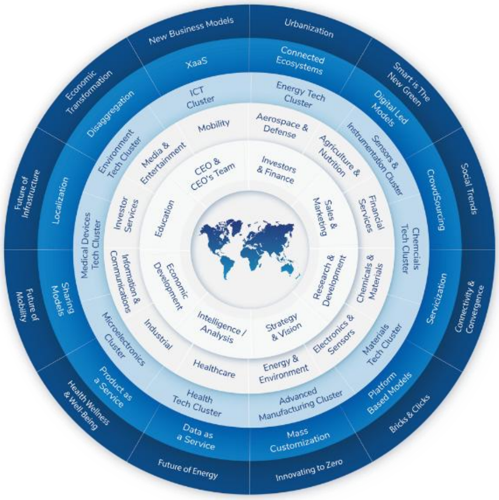

OPPORTUNITY UNIVERSE
Capture full range of growth opportunities and prioritize them based on key criteria
OPPORTUNITY EVALUATION
Conduct deep, 360-degree analysis of prioritized opportunities
GO-TO-MARKET STRATEGY
Translate strategic alternatives into a cogent strategy
PLANNING & IMPLEMENTATION
Execute strategic plan with milestones, targets, owners and deadlines
MONITORING & OPTIMIZATION
Adapt strategy to changing market dynamics and unearth new opportunities
GROWTH PIPELINE ENGINE™

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)


New Business Models
Urbanization
Smart is The New Green
Social Trends
Connectivity & Convergence
Bricks & Clicks
Innovating to Zero
Future of Energy
Health Wellness & Well-Being
Future of Mobility
Future of Infrastructure
Economic Transformation
XaaS
Connected Ecosystems
Digital Led Models
CrowdSourcing
Servicization
Platform Based Models
Mass Customization
Data as a Service
Product as a Service
Sharing Models
Localization
Disaggregation
ICT Cluster
Energy Tech Cluster
Sensors & Instrumentation Cluster
Chemcials Tech Cluster
Materials Tech Cluster
Advanced Manufacturing Cluster
Health Tech Cluster
Microelectronics Cluster
Medical Devices Tech Cluster
Environment Tech Cluster
Mobility
Aerospace & Defense
Agriculture & Nutrition
Financial Services
Chemicals & Materials
Electronics & Sensors
Energy & Environment
Healthcare
Industrial
Information & Communications
Investor Services
Media & Entertainment
CEO & CEO's Team
Investors & Finance
Sales & Marketing
Research & Development
Strategy & Vision
Intelligence / Analysis
Economic Development
Education