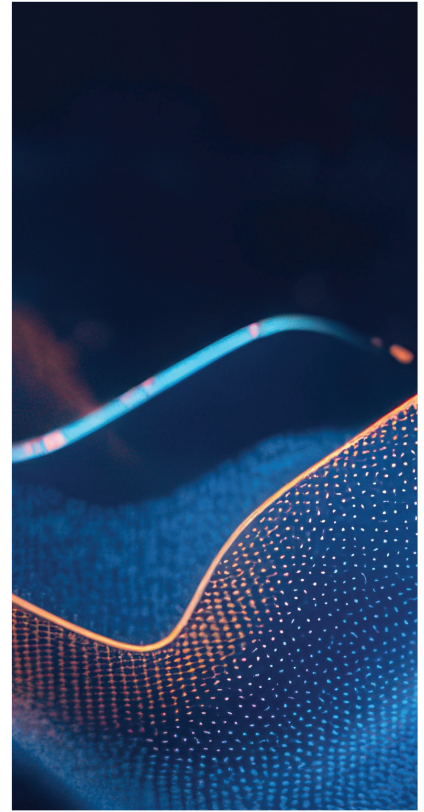
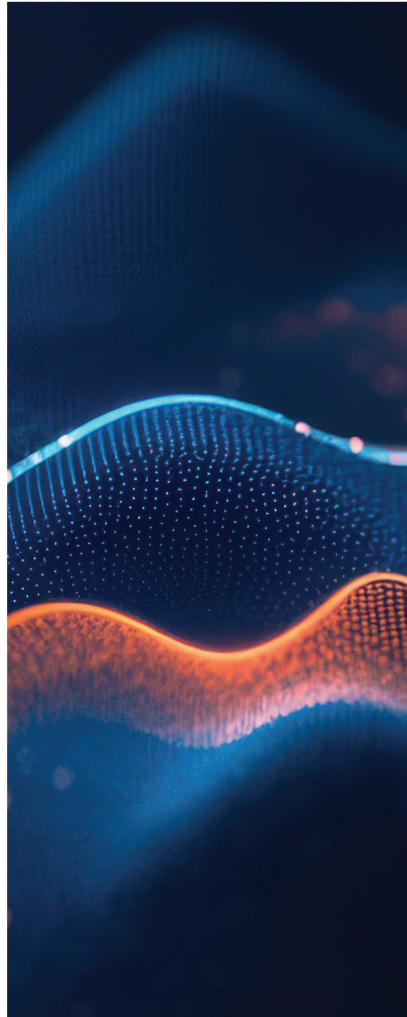


FROST & SULLIVAN
BEST PRACTICES



2026

GLOBAL MANAGED
SECURITY SERVICES

COMPANY OF THE YEAR

LevelB/ue

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. LevelBlue excels in many of the criteria in the global Managed Security Services space.

RECOGNITION CRITERIA	
<i>Visionary Innovation & Performance</i>	<i>Customer Impact</i>
Addressing Unmet Needs	Price/Performance Value
Visionary Scenarios Through Megatrends	Customer Purchase Experience
Leadership Focus	Customer Ownership Experience
Best Practices Implementation	Customer Service Experience
Financial Performance	Brand Equity

The Transformation of the Managed Security Services market

Cybersecurity has become harder to manage as organizations defend increasingly distributed environments spanning cloud, SaaS, endpoints, identities, networks, and, in many cases, OT and IoT. At the same time, ransomware, AI-enabled attacks, supply chain compromises, and nation-state activity continue to raise the stakes, while regulatory expectations and scrutiny keep increasing.

These pressures are colliding with persistent cybersecurity skills shortages and the limits of fragmented, siloed security models. Many organizations can no longer rely on their security teams to handle the massive scale of alerts and false positives, resulting in slow investigations and inconsistent incident response. They need to simplify security operations, improve visibility across hybrid environments, embed automation and AI into the Security Operations Center (SOC), and shift from reactive defense toward more continuous, exposure-led risk reduction.

Managed security services (MSS) have become essential because they help organizations turn security from a staffing problem into an operating model. MSS providers combine 24/7 monitoring, detection and response, threat intelligence, exposure management, automation, and increasingly platform-based delivery to improve resilience without requiring customers to build full-spectrum internal teams. This value proposition is driving sustained market expansion. Frost & Sullivan projects continued double-digit growth in MSS spending for the foreseeable future, supported by platform-centric strategies, AI-augmented SOCs, cloud and network security convergence, and the growing need for measurable security outcomes.

To be an absolute leader in the global MSS market, a firm must combine scale with consistency: a unified, platform-based delivery model, AI-augmented operations, deep integration across cloud, identity, network, and endpoint security, and the ability to deliver measurable customer outcomes. Leadership also requires regional adaptability, trust, and operational transparency, since customers expect global reach without losing local relevance. The firms that lead globally are those that turn complexity into simpler, outcome-driven, and continuously evolving security operations at scale worldwide.

LevelBlue: A Legacy of Managed Security Services Success

LevelBlue has emerged as one of the most significant pure-play MSSPs in the global cybersecurity market. The company brings together an extensive cybersecurity heritage rooted in AT&T Cybersecurity and augmented by a series of portfolio-expanding strategic acquisitions. This has enabled the creation of a unified organization with deep expertise across managed security, advisory, threat intelligence, incident response, digital forensics, offensive security, and cloud-first security operations.

LevelBlue's current position is the result of a multi-decade evolution. AT&T introduced managed security services in the 1990s, later expanded its cybersecurity consulting capabilities through VeriSign Consulting, and strengthened its threat detection and response offering through the acquisition of AlienVault. AlienVault's USM platform, Alien Labs threat intelligence, and Open Threat Exchange (OTX) became central building blocks in the company's managed security strategy.

The launch of LevelBlue in 2024 as a joint venture between AT&T and WillJam Ventures marked a decisive step in the company's transformation. LevelBlue accelerated its innovation in managed security services, cybersecurity consulting, and threat intelligence, and forged these capabilities into a unified, comprehensive approach. In 2025, LevelBlue further developed this strategy through the acquisitions of Stroz Friedberg, Elysium Digital, Cybereason, Trustwave, and AlertLogic, which expanded the company's consulting, digital forensics, incident response, advisory, offensive security, and MDR capabilities. The acquisition of Trustwave was particularly important for LevelBlue; it integrated Trustwave Fusion platform functionality, cloud-native MDR, SpiderLabs threat intelligence, offensive security services, strategic advisory, penetration testing, incident response, database security, and email security.

The acquisition of Cybereason, completed at the end of 2025, added an advanced XDR platform, high-quality threat intelligence, and digital forensics and incident response expertise, complementing Trustwave's MDR capabilities at the endpoint layer. It also strengthened LevelBlue's regional footprint in Asia, and particularly in Japan, where Cybereason is among the leading cybersecurity providers, giving the firm local delivery capability in a market that global MSSPs have historically struggled to serve. The transaction brought SoftBank Corp., SoftBank Vision Fund 2, and Liberty Strategic Capital into LevelBlue as investors, and former US Treasury Secretary Steven T. Mnuchin joined the company's board of directors.

In January 2026, LevelBlue announced a long-term strategic partnership with Fortra, acquiring the managed services business of its Alert Logic unit, including MDR, XDR, and WAF services. The transaction added Alert Logic's MDR customer base and telemetry to LevelBlue's operations, while Fortra became one

of LevelBlue's leading technology partners, making its software and platforms available to LevelBlue's global client base across data security, brand protection, email security, and offensive security.

These acquisitions have bolstered LevelBlue's growth trajectory and reinforced its position as one of the largest and fastest-growing players in the MSS market. The Trustwave acquisition boosted LevelBlue's revenue base, increased its reach across industries and regions, and created additional cross-sell and upsell opportunities across managed operations, consulting, readiness, and response. The Cybereason acquisition extended LevelBlue's footprint into APAC. The AlertLogic transaction added further scale to the MDR business specifically, broadening threat telemetry and extending coverage across public cloud, hybrid, and on-premises environments. The company's global scale underpins its success: it brings 30 years of cybersecurity consulting experience, 24/7 global security operations across seven SOC's staffed by over 2,500 cybersecurity professionals, more than 300 dedicated digital forensics and incident response specialists who have investigated over 9,000 incidents worldwide, trillions of monitored security events per year, and billions of threat intelligence indicators. Through these capabilities and differentiators, LevelBlue will continue to lead the next phase of MSS market development.

Portfolio Depth that Drives Transformation and Delivers Effective Security Outcomes

LevelBlue's managed security services portfolio is one of the broadest in the market. It is structured around three major managed service domains:

- **Managed Cloud Security** – includes SASE, SSE, firewall-as-a-service, cloud secure web gateway, zero trust network access, CASB, SD-WAN, WAAP, and DDoS protection.
- **Managed Network Infrastructure Security** – includes next-generation firewall, email security, data security, CDN, log management, and secure connectivity.
- **Managed Detection and Response** – includes global threat intelligence, cyber threat hunting, forensics and incident response, EDR/XDR/SIEM coverage, mobile threat defense, and SOC-as-a-Service.

LevelBlue complements this managed security service offering with cyber advisory, exposure management, strategy and transformation consulting, GRC, IP risk and litigation support, penetration testing, red teaming, managed vulnerability services, incident readiness, incident response, tabletop exercises, and security retainers.

With this highly comprehensive approach, LevelBlue guides customers through the entire planning, setup, deployment, and execution of their cybersecurity strategies, leveraging its broad portfolio to create a positive feedback loop that delivers continuous improvement to cyber resilience. This allows LevelBlue to deliver on all the most important unmet needs in the MSS market:

- effective security outcomes, including detection, response, and remediation of the most sophisticated threats through an advanced security portfolio;
- alleviating the need to hire and retain SOC analysts and cybersecurity experts, who are increasingly hard to find;

- reduced operational complexity and increased clarity and transparency through guidance, knowledge, and expertise provided by an external team; and
- and support when it comes to re-thinking security priorities and developing security strategies that can stand against the rapid evolution of the threat landscape.

Moreover, LevelBlue's portfolio breadth allows the firm to help customers of vastly different cybersecurity maturity levels transform security operations in multiple ways depending on their environment and business constraints. For example, less mature organizations can leverage MDR or SOC services to gain 24/7 coverage and support, while mature customers can harness managed SIEM, a co-managed SOC approach, MXDR, advisory, and exposure management to extend existing security investments. In contrast, organizations seeking to modernize their network and cloud architectures can adopt LevelBlue's vendor-agnostic SASE/SSE model, while others seeking application and API protection can rely on the firm's WAAP capabilities with support from specialists.

Beyond the Basics: Unique Features and Differentiators to Multiply Value

LevelBlue's portfolio of highly advanced managed and professional security services is impressive and a significant differentiator. However, the firm truly stands out in the mature, highly advanced managed security space—where massive service integrators, pure-play providers, and other MSSPs fiercely compete for market share—because it is an expert at guiding organizational transformations and delivering value beyond the sum of its parts.

LevelBlue's public-sector capabilities address one of the most important issues organizations are facing in today's rapidly evolving threat landscape: compliance. Following the acquisition of Trustwave, the company is the only pure-play cybersecurity provider authorized for both FedRAMP and GovRAMP. It boasts government-specific capabilities such as a Fusion platform designed for government-related clients and SOC and MDR capabilities replicated and operated in AWS GovCloud. It also provides operations at GCC High for Azure Government Cloud, and purpose-built services for clients with FedRAMP, GovRAMP, CUI, CMMC, DFARS, ITAR, and US-only monitoring and data restrictions. This allows LevelBlue to guide the cybersecurity transformation of all kinds of organizations in high-assurance environments, where security outcomes, compliance, sovereignty, and trust are essential to continue operations.

Furthermore, the Trustwave acquisition provided LevelBlue with world-class SpiderLabs threat intelligence, cloud-native MDR, Trustwave Fusion, and myriad other tools and services that enable the firm to support the full security lifecycle. But there's also an unsung gem in the acquired portfolio: Security Colony. Security Colony is a large library of security resources developed for real clients, offering access to security IP, compliance guidelines, a NIST CSF security maturity assessment tool, vendor risk scoring, cyber awareness training strategies, and consulting guidance across industries and maturity levels. By incorporating Security Colony into the broader LevelBlue model, the provider can help customers improve maturity and decision-making even when they cannot invest in every consulting engagement.

A further differentiator that few global MSSPs can match is the scale of LevelBlue's incident response practice and its standing within the cyber insurance ecosystem. Drawing on the digital forensics and incident response heritage of Stroz Friedberg, Elysium Digital, Trustwave Spiderlabs, and Cybereason, the firm has investigated over 9,000 incidents worldwide. This has been enabled by more than 300 dedicated

DFIR specialists operating a follow-the-sun model, with most engagements beginning in under one hour. Additionally, LevelBlue is approved on more than 50 cyber insurance panels connecting its managed services more directly with broader cyber risk and insurance needs. Customers can access incident response resources quickly, while the forensic work also supports insurance claims, regulatory requirements, litigation, and recovery efforts. Insurability and business risk are areas that many MSSPs address only partially, making these capabilities an important differentiator for LevelBlue, particularly for security and risk leaders.

Creating Synergy Through a Unifying Platform and AI Capabilities

Beyond the variety and quality of managed and professional services in LevelBlue's arsenal, the firm's platform strategy creates synergy and multiplies value for its customers. The LevelBlue Indigo™ Security Platform is designed to support both clients and operators through a unified experience. It brings together self-service tools, chatbots, reports, dashboards, operational toolsets, threat intelligence, and streamlined remote access, while supporting a hybrid third-party vendor ecosystem. This is crucial for organizations with different technology stacks, maturity levels, and security journeys. LevelBlue empowers its customers to work with multiple tools and technologies according to their preferences: USM Anywhere can integrate more than 600 LevelBlue Apps from multiple security and technology vendors via Syslog, API, and S3 connections, expanding visibility and enabling an integrated, efficient response.

The company is working to unify inherited technologies and capabilities from LevelBlue USM Anywhere, Trustwave Fusion, Cybereason XDR, automated policy management tools, Open Threat Exchange, and Security Colony into a harmonized operating environment. LevelBlue's goal is to create a unified platform experience that improves analyst workflows, telemetry enrichment, automation, customer visibility, and service delivery. As customers increasingly expect consolidation across all aspects of security, including telemetry, analytics, orchestration, and reporting, this approach aligns with one of the most important megatrends in the MSS space.

On top of this platform, LevelBlue is making significant investments in AI and automation to enhance its operating model. The firm continuously invests in improving its portfolio's AI-driven managed detection and response features. This includes developing agentic AI capabilities that assist analysts with triage, routing, enrichment, and response. The integration of Trustwave Fusion has contributed additional AI-oriented capabilities that can accelerate the broader LevelBlue service architecture, while USM's SOAR engine provides deterministic playbook orchestration. LevelBlue also applies automation to areas such as SASE, SSE, and firewall policy management through its automated policy management platform, which centralizes service management, monitoring, change management, issue resolution, compliance, reporting, patching, and threat-informed rule adjustments.

Overall, LevelBlue's platform and AI strategy support faster detection and response, more consistent service delivery, improved transparency, and better alignment between security operations and business risk. For analysts, it reduces repetitive work and improves the consistency of triage, investigation, and response across a large multi-tenant environment. For LevelBlue, it provides a scalable foundation for growth in a fiercely competitive market. Importantly, LevelBlue's approach does not position AI as a replacement for human expertise. Instead, AI and automation augment security professionals, enabling them to focus on the most complex investigations, contextual judgment, and customer-specific decisions.

In the current context of AI-powered operations and AI SOC's, where organizations are focused on obtaining explainability, accountability, and outcomes, this balance between automation and human-led security operations is essential.

Standardizing Delivery While Preserving Flexibility: The LevelBlue Framework

Securing customers' environments is more than just offering an extensive portfolio of managed and professional security services, even when they are complemented by adjacent tools, integrated into synergistic platforms, and augmented by agentic AI. To truly protect business-critical data and become a business-enabler, a managed security services partner needs to weave all these elements seamlessly into the customer environment, working as one to achieve full protection. This knowledge underpins LevelBlue's entire ITIL-aligned MSS framework.

It is divided into three different phases: Day 0, Day 1, and Day 2. Day 0 focuses on service design, trusted advisory, solution review, customer security outcome assessment, technical guidance, demos or proofs of concept, and solution proposals. Day 1 focuses on service transition and enablement, including design validation, security policy and data collection, platform configuration and access, infrastructure deployment, testing, turn-up, and co-management setup when applicable. Day 2 focuses on ITIL-based service operations, including asset management, availability management, capacity planning, change management, configuration management, event management, incident management, knowledge management, problem management, release management, request management, service-level reporting, and vendor management.

In essence, Day 0 sets the stage for a successful deployment, aligning strategy and goals. Day 1 enables a structured process and detects potential issues before resolving them; while Day 2 allows for a smooth ongoing service. Overall, the framework provides an easy way to repeat the process for LevelBlue while reducing friction and still allowing the firm to tailor all aspects according to each customer's environment, needs, and security maturity level.

Conclusion

LevelBlue has established itself as a global leader in the MSS market, combining its legacy with a strong acquisition and partnership strategy, most recently the AlertLogic managed services acquisition and Fortra alliance, to build a portfolio that delivers 24/7 prevention, detection, and response to organizations across all industry verticals and security maturity levels. Underpinned by a robust government and compliance focus, an incident response practice built on over 9,000 investigations and approved on more than 50 cyber insurance panels, and major value-multiplying complementary services such as Security Colony, LevelBlue understands how to guide enterprises on their security transformation journeys. As the firm continues to develop its unifying platform, invest in AI and automation capabilities, and enhance its comprehensive Day 0/1/2 deployment framework, it will continue to spearhead innovation and growth in the cybersecurity industry. LevelBlue earns Frost & Sullivan's 2026 Global Company of the Year Recognition for its strong overall performance in the managed security services market.

What You Need to Know about the Company of the Year Recognition

Frost & Sullivan's Company of the Year 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 Company of the Year Recognition, Frost & Sullivan analysts independently evaluated the criteria listed below.

Visionary Innovation & Performance

Addressing Unmet Needs: Customers' unmet or under-served needs are unearthed and addressed to create growth opportunities across the entire value chain

Visionary Scenarios Through Megatrends: Long-range scenarios are incorporated into the innovation strategy by leveraging megatrends and cutting-edge technologies, thereby accelerating the transformational growth journey

Leadership Focus: The company focuses on building a leadership position in core markets to create stiff barriers to entry for new competitors and enhance its future growth potential

Best Practices Implementation: Best-in-class implementation is characterized by processes, tools, or activities that generate consistent, repeatable, and scalable success

Financial Performance: Strong overall business performance is achieved by striking the optimal balance between investing in revenue growth and maximizing operating margin

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)**

