Incident Response Services - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-06-01 | 120 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License $4750.00
- Team License (1-7 Users) $5250.00
- Site License $6500.00
- Corporate License $8750.00

Report description:

Incident Response Services Market Analysis

The incident response services market reached USD 41.95 billion in 2025 and is forecast to expand to USD 99.14 billion by 2030 at an 18.77% CAGR, underscoring the sector's rapid shift from reactive support toward always-on resilience programs. Rising attack sophistication, stricter data-protection mandates, and cloud-first architectures are redefining service expectations in ways that favor automation, artificial intelligence, and cross-border response expertise. Vendor consolidation is underway as platform providers acquire managed detection and response (MDR) specialists to integrate threat hunting and containment under one operating model. Cloud workload migration continues to expand the incident response services market, yet on-premises tooling still dominates highly regulated environments that must meet local data-sovereignty rules. Meanwhile, cyber-insurance underwriters are tightening policy language and rewarding buyers that can show signed response retainers, incentivizing organizations of every size to reassess coverage gaps.

Global Incident Response Services Market Trends and Insights

Surge in Frequency and Sophistication of Cyber-Attacks in BFSI and Critical Infrastructure

Financial institutions and utility operators now contend with attack dwell times measured in minutes rather than days, forcing a pivot to containment-first playbooks that emphasize rapid isolation of endpoints and network segments. The Unit 42 Global Incident Response Report recorded that 86% of 2024 breaches disrupted business operations, while adversaries exfiltrated data

inside the first hour of compromise. Legacy system convergence with open banking APIs compounds risk in BFSI, whereas operational technology (OT) environments in energy and transport require response teams to preserve uptime even while eradicating malware. Government guidance, such as the Texas Department of Banking's 2025 notice that basic cyber hygiene blocks 98% of threats, reinforces the view that specialized responders are essential for the remaining high-grade incidents.

Stricter Data-Protection Regulations Driving Compliance-Mandated Investments

The European Union's NIS2 directive obliges essential entities to report significant incidents within 24 hours and faces violators with fines up to EUR 10 million (USD 11.3 million). Similar momentum exists in North America, where PCI-DSS 4.0 and evolving state privacy laws demand verifiable incident response programs that extend beyond technical logs to downstream reporting and stakeholder communication. Compliance overlap across regions has spurred multinational firms to seek global response partners that can align evidence collection, legal holds, and public disclosure standards in one coordinated workflow.

Global Shortage of Skilled Incident Responders Constraining Growth

The worldwide cybersecurity workforce gap climbed significantly in 2025, with incident responders among the scarcest skill sets. Staffing deficits raise time-to-contain metrics and inflate breach liabilities; IBM estimates an average USD 1.76 million premium for firms lacking dedicated incident response resources. Outsourcing partners benefit, yet capacity bottlenecks persist during multi-client surge events, spurring investments in AI-driven triage to extend human expertise

Other drivers and restraints analyzed in the detailed report include:

Cloud-First Adoption Expanding Attack Surface / Rise of Ransom-Cloud and BEC 3.0 Exploiting OAuth Tokens / High Cost of Premium IR Retainers Limiting SME Adoption /

For complete list of drivers and restraints, kindly check the Table Of Contents.

Segment Analysis

Containment and Mitigation captured 33.2% of the incident response services market in 2024, reflecting the urgency to isolate compromised assets before attackers pivot or exfiltrate data. Rapid isolation of endpoints and privileged credentials has become standard practice as median attacker dwell time shrinks. Over the forecast horizon, Managed Detection and Response will expand at a 21% CAGR, elevating continuous threat-hunting and proactive remediation from optional add-ons to core contract deliverables.

MDR momentum is powered by AI-assisted analytics that surface anomalies human analysts might miss. Vendors infuse large-language-model copilots that accelerate root-cause discovery and automated playbook execution, slashing response hours. Remediation and Recovery maintain relevance, particularly when regulatory reporting or litigation requires certified evidence handling. Digital Forensics and Analytics is evolving through machine-learning-based pattern recognition, enabling incident responders to reconstruct attacker timelines faster while satisfying evidentiary standards for court proceedings.

On-Premises installations still held 57.2% share of the incident response services market size in 2024 due to sovereignty mandates and board-level preferences for local custody of sensitive logs. Financial institutions and public agencies continue to limit external data transfers, especially in jurisdictions that prohibit customer information from leaving national borders. Yet cloud-based response tooling will outpace overall growth at a 20.2% CAGR as security teams embrace plug-and-play scalability.

Hybrid deployment models now fuse local log retention with cloud analytics engines, giving organizations the forensic visibility

they require without sacrificing elastic compute capacity. Zero-trust philosophies reinforce the shift by de-emphasizing network location as a security boundary and normalizing remote examination of forensic artifacts. Providers differentiate by offering "bring-your-own-key" encryption and in-region data storage to satisfy compliance audits.

Incident Response Services Market is Segmented by Service Type (Containment and Mitigation, Remediation and Recovery, and More), by Deployment Mode (On-Premises, Cloud-Based, and More), by Enterprise Size (Small and Medium Enterprises and Large Enterprises), by End-User Industry (BFSI, Government and Defense, and More), by Geography. The Market Forecasts are Provided in Terms of Value (USD).

Geography Analysis

North America retained the regional lead with 38.3% incident response services market share in 2024, propelled by mature breach-notification laws and robust security ecosystems. United States financial regulators, such as the New York Department of Financial Services, require formalized incident response plans, reinforcing demand across large banks and fintechs. Canada's critical-infrastructure directives and Mexico's expanding fintech rules extend regional volume.

Asia-Pacific is on track for a 20.6% CAGR to 2030. Regulatory harmonization in Japan, Singapore, and Australia now mandates 24-hour breach disclosure and certified response processes, encouraging organizations to secure retainers before incidents occur. The region recorded 34% of global attacks in 2024, intensifying demand for bilingual, cross-jurisdictional responders who can navigate local rules and diverse cloud stacks.

Europe's compliance-driven adoption accelerates under NIS2, which broadens the scope of "essential entities" and elevates fines for insufficient preparedness. Organizations must harmonize GDPR data-breach reporting with NIS2 security-incident disclosure, fueling bundled privacy-plus-security response engagements. Eastern European members look to consultancies for playbook localization, while larger economies deepen contracts to cover supply-chain and OT threats.

Latin America, the Middle East, and Africa remain nascent but rising. Digital-commerce expansion and new data-protection statutes open opportunities, though budgetary and talent constraints temper immediate growth. International providers partner with local MSSPs to bridge language, culture, and compliance gaps, a model expected to scale as regional investment in cyber resilience continues.

List of Companies Covered in this Report:

CrowdStrike Holdings Inc. / Check Point Software Technologies Ltd. / BlackBerry Cybersecurity (Cylance) / Mandiant Inc. (Google Cloud) / Kaspersky Lab / Rapid7 Inc. / IBM Corporation / NCC Group plc / Optiv Security Inc. / Secureworks Inc. / Trustwave Holdings Inc. / KPMG International Ltd. / Deloitte Touche Tohmatsu Ltd. / Ernst and Young Global Ltd. / PricewaterhouseCoopers (PwC) / Accenture plc / Palo Alto Networks (Unit 42) / Cisco Systems Inc. (Talos IR) / Booz Allen Hamilton Inc. / BAE Systems Digital Intelligence /

Additional Benefits:

 The market estimate (ME) sheet in Excel format /
3 months of analyst support /

Table of Contents:

Incident Response Services - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-06-01 | 120 pages | Mordor Intelligence

To place an Order with Scotts International:

- - Print this form
- - Complete the relevant blank fields and sign
- - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	$4750.00
	Team License (1-7 Users)	$5250.00
	Site License	$6500.00
	Corporate License	$8750.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2026-03-04
		Signature