Threat Intelligence Market Size & Share Analysis - Growth Trends and Forecast (2026 - 2031)
Industry: Cybersecurity
URL: https://www.mordorintelligence.com/industry-reports/threat-intelligence-market

Threat Intelligence Market Size and ShareMarket OverviewStudy Period | 2020 - 2031 |
Market Size (2026) | USD 10.38 Billion |
Market Size (2031) | USD 18.85 Billion |
Growth Rate (2026 - 2031) | 12.70 % |
Fastest Growing Market | Middle East and Africa |
Largest Market | North America |
Market Concentration | Medium |
Major Players*Disclaimer: Major Players sorted in no particular order

Image © Mordor Intelligence. Reuse requires attribution under CC BY 4.0.

 |
Image © Mordor Intelligence. Reuse requires attribution under CC BY 4.0.

Threat Intelligence Market Analysis by Mordor IntelligenceThreat intelligence market size in 2026 is estimated at USD 10.38 billion, growing from 2025 value of USD 9.21 billion with 2031 projections showing USD 18.85 billion, growing at 12.7% CAGR over 2026-2031. Expanding cloud adoption, rapid attacker use of AI, and tighter regulatory frameworks such as the EU-NIS2 directive are lifting spending on proactive intelligence platforms. Security leaders are prioritizing context-rich analytics that shorten response times and lower breach costs, while insurers and investors now examine live intelligence feeds before underwriting cyber risk. Consolidation among large vendors is accelerating platform breadth, yet specialist providers remain relevant where sector-specific intelligence is required. Heightened nation-state activity and ransomware cartel funding through cryptocurrencies are expected to keep the threat environment volatile, sustaining investment momentum across every major vertical.

Key Report Takeaways* By component, Solutions captured 55.40% of the threat intelligence market share in 2025, whereas Services are projected to expand at a 14.12% CAGR through 2031.
* By deployment, on-premise held 54.30% of the market size in 2025; cloud is slated to grow at a 16.25% CAGR during 2026-2031.
* By threat-intelligence type, Strategic intelligence contributed 33.60% revenue in 2025, while Operational intelligence is tracking a 16.35% CAGR to 2031.
* By organization size, large enterprises accounted for 67.20% of the threat intelligence market size in 2025; the SME segment is advancing at a 14.95% CAGR.
* By end-user sector, IT and Telecommunications led with 20.60% of the market share in 2025; BFSI is the fastest-growing vertical at a 14.70% CAGR.
* By geography, North America commanded 37.50% of global revenue in 2025; the Middle East exhibits the quickest regional CAGR at 15.35% to 2031.
Note: Market size and forecast figures in this report are generated using Mordor Intelligence’s proprietary estimation framework, updated with the latest available data and insights as of 2026.

Market Trends and InsightsDrivers Impact Analysis of Threat Intelligence Market* Driver | (~) % Impact on CAGR Forecast | Geographic Relevance | Impact Timeline |
AI-driven polymorphic malware targeting cloud-native workloads | +3.5% | North America with spillover to Europe and APAC | Medium term (2-4 years) |
EU-NIS2 compliance spend by critical infrastructure operators | +2.8% | European

 Union; global multinationals | Short term (≤2 years) |
Zero Trust roll-outs in APAC large enterprises | +2.2% | Japan, South Korea, Aus tralia | Medium term (2-4 years) |
RaaS cartels fuelling crypto-wallet monitoring demand | +1.9% | North America an d Europe | Short term (≤2 years) |
Outsourced threat-hunting by South American mid-tier BFSI | +1.5% | Brazil, Arge ntina, Chile | Medium term (2-4 years) |
Cyber-insurance premium discounts tied to live feeds in Middle East energy | +1. 0% | UAE, Saudi Arabia | Long term (≥4 years) |
Source: Mordor Intelligence |
AI-driven Polymorphic Malware Targeting Cloud-Native WorkloadsAI-generated polym orphic malware can rewrite its code on the fly, defeating traditional signature tools and forcing defenders to rely on behavioural analytics. IBM research shows such malware now negotiates ransoms without human contact and pivots tactics ba sed on cloud configuration, complicating incident response.[1]Matthew Kosinski, “How to Fight AI Malware,” ibm.com The U.S. Department of Justice recently disma ntled a ring that stole USD 263 million in cryptocurrency through AI-enabled exp loits, underscoring the financial risk.[2]U.S. Department of Justice, “Cryptocur rency Theft Conspiracy,” trmlabs.com North American enterprises are boosting bud get for machine-learning detection, making the threat intelligence market essent ial for cloud workload protection.

EU-NIS2 Compliance Spend by Critical Infrastructure OperatorsEffective October 2 024, the NIS2 directive subjects roughly 300,000 European entities to mandatory risk assessments, incident reporting, and supply-chain scrutiny.[3]Skadden Arps, “Implications of the EU NIS2 Directive,” skadden.com Penalties can reach EUR 10 million or 2% of global turnover, pushing boards to prioritise real-time intell igence. Multinationals outside the bloc must also comply when serving EU custome rs, widening opportunity for vendors that package ready-to-audit intelligence fe eds.

Zero Trust Roll-outs in APAC Large EnterprisesIn APAC, in 2024, 97% of enterpris es have begun Zero Trust projects, up from 16% in 2019 . Threat intelligence enr iches these frameworks by adding adversary context to every access decision. Des pite progress, only 2% of firms have reached mature Zero Trust status, so demand for turnkey intelligence-enabled solutions remains high.[4]Xiou Ann Lim, “25 on 2025: APAC Security Predictions,” csoonline.com

RaaS Cartels Fuelling Crypto-Wallet Monitoring DemandRansomware-as-a-Service gro ups collected USD 459.8 million in 2024 payments, laundering proceeds through ob fuscated crypto routes. Exchanges and banks now invest in blockchain-aware intel ligence that spots ransom wallets early to avoid sanctions violations, further e xpanding the threat intelligence market.

Restraints Impact Analysis of Threat Intelligence Market*Restraint | (~) % Impac t on CAGR Forecast | Geographic Relevance | Impact Timeline |
STIX/TAXII interoperability gaps in legacy SOCs | -1.2% | Global mature SOCs | M edium term (2-4 years) |
Escalating subscription costs for actionable intel data | -0.8% | SMEs worldwide | Short term (≤2 years) |
Data-sovereignty barriers in China CSL and India DPDP | -0.6% | China, India | L ong term (≥4 years) |
Analyst fatigue and alert overload | -0.5% | Regions with talent shortages | Sho rt term (≤2 years) |
Source: Mordor Intelligence |
STIX/TAXII Interoperability Gaps in Legacy SOCsAlthough STIX and TAXII became OA SIS standards in 2021, many legacy platforms still process proprietary formats, preventing seamless data sharing. An exploratory study identified integration co mplexity and inconsistent notation as primary hurdles. As a result, organisation s delay platform upgrades, restraining short-term spending.

Escalating Subscription Costs for Actionable Intel DataAdvanced feeds that bundl

e machine learning and analyst validation now command premium pricing. Security leaders worry that multi-feed strategies may outpace budget growth, particularly in small and medium enterprises. Vendors are experimenting with tiered access, yet cost-to-value concerns are likely to temper adoption among resource-constrained buyers.

*Our forecasts treat driver/restraint impacts as directional, not additive. The impact forecasts reflect baseline growth, mix effects, and variable interactions.

Threat Intelligence Market Segment AnalysisBy Component:Solutions Dominate While Services AccelerateSolutions generated 55.40% of global revenue in 2025, giving platforms an outsized hold on the threat intelligence market. Microsoft Defender Threat Intelligence alone processes 78 trillion signals per day, highlighting scale advantages. This dominance underlines why the market size attached to platforms is expected to keep rising through 2031. Leading vendors incorporate AI for behaviour analytics, easing analyst workload and improving detection fidelity.

Managed and professional services are outpacing product growth with a 14.12% CAGR, reflecting talent shortages and rising complexity. SANS surveys show many enterprises outsource hunting duties to close skill gaps. Partnerships that wrap training around deployments allow buyers to derive quicker value, propelling service uptake, especially across the threat intelligence industry’s mid-market segment.

Image © Mordor Intelligence. Reuse requires attribution under CC BY 4.0. By Deployment:Cloud Adoption Accelerates Security TransformationOn-premise deployments held 54.30% of spending in 2025 as heavily regulated sectors prefer local data residency. Even so, cloud-hosted platforms are the fastest riser at 16.25% CAGR, signalling confidence in provider hardening and FedRAMP expansions such as Microsoft Defender Threat Intelligence gaining High attestation. Segment observers see the threat intelligence market size for cloud deliveries eclipsing on-premise totals late in the forecast window.

Hybrid approaches blend legacy sensors with SaaS analytics, appealing to organisations modernising at their own pace. Financial regulators now publish blueprints for secure cloud adoption that specifically mention continuous intelligence integration, accelerating momentum.

By Threat-Intelligence Type:Strategic Insights Drive Decision-MakingStrategic intelligence held 33.60% share in 2025 as boards rely on geopolitical context and adversary motivation to steer risk budgets. Documents such as the ENISA Threat Landscape give executives a high-level view of campaigns shaping the market. Operational feeds are surging at 16.35% CAGR because security operations centres need near real-time mapping between Indicators of Compromise and active incidents, making the threat intelligence market size tied to SOC workflows grow sharply.

Tactical and technical feeds remain vital for signature creation and malware reverse engineering. Vendors blend these perspectives into unified workspaces, enabling faster pivot from a single artefact to strategic context, a feature showcased in Microsoft Security Copilot.

By Organization Size:Large Enterprises Lead, SMEs Gain MomentumLarge enterprises captured 67.20% of 2025 spending, driven by broad attack surfaces and compliance mandates. Microsoft tracks over 1,500 unique threat groups, illustrating the barrage facing Fortune-class networks. Yet SMEs are advancing at a 14.95% CAGR because cloud delivery and freemium tiers lower entry barriers, bringing them into the threat intelligence market.

Service providers embed curated intelligence into managed offerings, expanding t

he threat intelligence platforms market among smaller firms that lack dedicated analysts. Microsoft’s Defender Threat Intelligence Standard Edition widens profile access, an example of democratisation underway.

Image © Mordor Intelligence. Reuse requires attribution under CC BY 4.0. By End-user Industry:IT and Telecommunications Leads, BFSI AcceleratesIT and Telecommunications held 20.60% revenue in 2025, mirroring its exposure to supply-chain breaches and DDoS attacks. Continuous monitoring of 5G core and edge assets keeps spending high, sustaining the overall threat intelligence market. BFSI is progressing at a 14.70% CAGR as regulators compel threat intelligence integration into fraud analytics and risk scoring. India’s 2025 BFSI Digital Threat Report outlines ransomware and third-party breaches as top exposures, spurring fresh investment.

Healthcare, energy, government, and manufacturing are also scaling programmes. For Middle East utilities, insurance premium rebates now hinge on live feed adoption, tightening links between operational continuity and intelligence quality.

Geography AnalysisNorth America Threat Intelligence MarketNorth America commanded 37.50% of 2025 revenue owing to mature cloud uptake, joint public-private information sharing, and deep vendor presence. Legislators continue to refine disclosure laws, while federal bodies sponsor real-time data-exchange platforms that reinforce the threat intelligence market. AI-enabled malware against cloud workloads remains the top regional concern, keeping platform spending buoyant.

Europe Threat Intelligence MarketEurope’s outlook brightens under NIS2, which scales mandatory coverage from 20 000 to 300 000 entities, greatly enlarging the addressable threat intelligence market. Complementary legislation such as the Cyber Resilience Act furthers demand for continuous vulnerability context across supply chains. Vendors that package audit-ready reporting with multi-lingual threat data are well positioned.

GCC Threat Intelligence MarketThe Middle East shows the fastest CAGR at 15.35% through 2031. National agencies in the UAE and Saudi Arabia invest in sector-focused fusion centres while energy majors receive cyber-insurance discounts tied to live feeds. Rising geopolitical tension in the region elevates the strategic value of the threat intelligence market for both public and private sectors.

APAC Threat Intelligence MarketAsia-Pacific sees a double-digit attack uptick, notably in Indonesia where weekly incidents top 3,300. Rapid digitalisation, paired with diverse sovereignty rules, produces fragmented demand. Japan, South Korea, and Australia lead Zero Trust pilots that embed live intelligence into access decisions, while China and India’s data-localisation laws create preferences for in-country cloud nodes.

South America Threat Intelligence MarketSouth America’s adoption is spurred by mid-tier BFSI outsourcing threat-hunting to overcome skills shortages, adding to global revenue even if from a smaller base.

Image © Mordor Intelligence. Reuse requires attribution under CC BY 4.0.

Competitive Landscape

Market concentration tightened in 2024 amid 362 cybersecurity acquisitions that combined advanced detection, response, and intelligence assets into broader portfolios. Mastercard’s USD 2.65 billion purchase of Recorded Future and Google’s impending USD 32 billion deal for Wiz typify moves to embed threat intelligence within cross-domain security stacks.

AI capability is the prime differentiator. Microsoft Security Copilot analyses 7
8 trillion daily signals to enrich investigation workflows, while CrowdStrike’s
Charlotte AI automates response playbooks. Fortinet integrates FortiAI across it
s fabric, unifying network and endpoint context. Stand-alone vendors now special
ise in niche areas such as firmware telemetry or crypto-asset tracing to remain
competitive.

Open standards pressure vendors with proprietary schemas. Buyers value platforms
 that ingest STIX/TAXII without heavy customisation. Providers that deliver inte
roperability plus sector-specific enrichment are gaining favour as organisations
 expand coverage beyond traditional IT assets into OT and IoT.

Threat Intelligence Industry Leaders* Dell Inc.

* IBM Corporation

* Anomali, Inc.

* Fortinet, Inc.

* CrowdStrike, Inc.

* *Disclaimer: Major Players sorted in no particular order
Image © Mordor Intelligence. Reuse requires attribution under CC BY 4.0.Threat I
ntelligence Market Companies Covered in this Report* IBM Corporation
* Cisco Systems Inc.
* Dell Technologies Inc.
* CrowdStrike Holdings Inc.
* Check Point Software Technologies Ltd.
* Trend Micro Incorporated
* Palo Alto Networks Inc.
* Fortinet Inc.
* Rapid7 Inc.
* Secureworks Inc.
* FireEye - Trellix
* Recorded Future Inc.
* Anomali Inc.
* LookingGlass Cyber Solutions Inc.
* LogRhythm Inc.
* McAfee LLC
* Broadcom Inc. (Symantec)
* Juniper Networks Inc.
* F-Secure Corporation
* SentinelOne Inc.
* Microsoft Corp. (Defender Threat Intelligence)
Read Analysis of Threat Intelligence Companies

Recent Industry Developments in Threat Intelligence Market* May 2025: Check Poin
t agreed to acquire Veriti Cybersecurity to add automated exposure management to
 its Infinity suite.
* May 2025: Fortinet extended its Hybrid Mesh Firewall lineup with the AI-ready
FortiGate 700G series.
* April 2025: Palo Alto Networks revealed plans to buy Protect AI for up to USD
700 million to fortify AI governance.
* April 2025: CrowdStrike launched Charlotte AI Agentic Response and Workflows a
t RSAC 2025.
* April 2025: Rapid7 introduced Intelligence Hub within its Command Platform, de
livering curated insight.
* April 2025: Binarly released Transparency Platform v3.0 with exploitation-awar

e risk scores
* April 2025: CyberRisk Alliance bought Execweb to deepen CISO engagement capabilities.
* April 2025: Bitsight launched Pulse, consolidating open-source and dark-web intelligence into custom channels.

Table of Contents for Threat Intelligence Industry Report1. Introduction

* 5.4 By Organization Size* 5.4.1 Large Enterprises
* 5.4.2 Small and Medium-Sized Enterprises

* 5.5 By End-user Industry* 5.5.1 BFSI
* 5.5.2 IT and Telecommunications
* 5.5.3 Retail and E-commerce
* 5.5.4 Manufacturing
* 5.5.5 Healthcare and Life Sciences
* 5.5.6 Government and Defense
* 5.5.7 Energy and Utilities
* 5.5.8 Others

* 5.6 By Geography* 5.6.1 North America
* 5.6.1.1 United States
* 5.6.1.2 Canada
* 5.6.1.3 Mexico
* 5.6.2 South America
* 5.6.2.1 Brazil
* 5.6.2.2 Argentina
* 5.6.2.3 Chile
* 5.6.2.4 Peru
* 5.6.2.5 Rest of South America
* 5.6.3 Europe
* 5.6.3.1 Germany
* 5.6.3.2 United Kingdom
* 5.6.3.3 France
* 5.6.3.4 Italy
* 5.6.3.5 Spain
* 5.6.3.6 Rest of Europe
* 5.6.4 Asia-Pacific
* 5.6.4.1 China
* 5.6.4.2 Japan
* 5.6.4.3 South Korea
* 5.6.4.4 India
* 5.6.4.5 Australia
* 5.6.4.6 New Zealand
* 5.6.4.7 Rest of Asia-Pacific
* 5.6.5 Middle East
* 5.6.5.1 United Arab Emirates
* 5.6.5.2 Saudi Arabia
* 5.6.5.3 Turkey
* 5.6.5.4 Rest of Middle East
* 5.6.6 Africa
* 5.6.6.1 South Africa
* 5.6.6.2 Rest of Africa

6. Competitive Landscape

* 6.1 Strategic Developments
* 6.2 Vendor Positioning Analysis
* 6.3 Company Profiles (includes Global level Overview, Market level overview, Core Segments, Financials as available, Strategic Information, Products and Services, and Recent Developments)* 6.3.1 IBM Corporation
* 6.3.2 Cisco Systems Inc.
* 6.3.3 Dell Technologies Inc.
* 6.3.4 CrowdStrike Holdings Inc.
* 6.3.5 Check Point Software Technologies Ltd.
* 6.3.6 Trend Micro Incorporated
* 6.3.7 Palo Alto Networks Inc.
* 6.3.8 Fortinet Inc.
* 6.3.9 Rapid7 Inc.
* 6.3.10 Secureworks Inc.

Global Threat Intelligence Market Report ScopeThreat intelligence collects and evaluates information relevant to protecting an organization from internal and external threats and analyzes that information to detect deceptions for accurate and relevant intelligence.

The threat intelligence market is segmented by type (solutions and services), deployment (on-premise and cloud), end user (banking, financial services, and insurance (BFSI), IT and telecom, retail, manufacturing, healthcare), and geography (North America (United States, Canada), Europe (United Kingdom, Germany, France, Rest of Europe), Asia-Pacific (China, Japan, India, Australia, Rest of Asia-Pacific), Latin America (Mexico, Brazil, Rest of Latin America), Middle East and Africa (United Arab Emirates, South Africa, Rest of Middle East and Africa)). The market sizes and forecasts are provided in terms of value (USD) for all the above segments.

Segmentation OverviewBy ComponentSolutions | Threat Intelligence Platforms |
 | Security Information and Event Management (SIEM) Feeds |
 | Threat Hunting/Analytics Tools |
Services | Managed/Outsourced Services |
 | Professional and Consulting |
 | Training and Support |
By DeploymentOn-premise |
Cloud |
Hybrid |
By Threat-Intelligence TypeStrategic |
Tactical |
Operational |
Technical |
By Organization SizeLarge Enterprises |
Small and Medium-Sized Enterprises |
By End-user IndustryBFSI |
IT and Telecommunications |
Retail and E-commerce |
Manufacturing |
Healthcare and Life Sciences |
Government and Defense |
Energy and Utilities |
Others |
By GeographyNorth America | United States |
 | Canada |
 | Mexico |
South America | Brazil |
 | Argentina |
 | Chile |

			Peru
			Rest of South America
		Europe	Germany
			United Kingdom
			France
			Italy
			Spain
			Rest of Europe
		Asia-Pacific	China
			Japan
			South Korea
			India
			Australia
			New Zealand
			Rest of Asia-Pacific
		Middle East	United Arab Emirates
			Saudi Arabia
			Turkey
			Rest of Middle East
		Africa	South Africa
			Rest of Africa
By Component	Solutions	Threat Intelligence Platforms	
		Security Information and Event Management (SIEM) Feeds	
		Threat Hunting/Analytics Tools	
	Services	Managed/Outsourced Services	
		Professional and Consulting	
		Training and Support	
By Deployment	On-premise		
	Cloud		
	Hybrid		
By Threat-Intelligence Type	Strategic		
	Tactical		
	Operational		
	Technical		
By Organization Size	Large Enterprises		
	Small and Medium-Sized Enterprises		
By End-user Industry	BFSI		
	IT and Telecommunications		
	Retail and E-commerce		
	Manufacturing		
	Healthcare and Life Sciences		
	Government and Defense		
	Energy and Utilities		
	Others		
By Geography	North America	United States	
		Canada	
		Mexico	
	South America	Brazil	
		Argentina	
		Chile	
		Peru	
		Rest of South America	
	Europe	Germany	
		United Kingdom	
		France	
		Italy	
		Spain	
		Rest of Europe	

| |
Asia-Pacific	China
	Japan
	South Korea
	India
	Australia
	New Zealand
	Rest of Asia-Pacific
Middle East	United Arab Emirates
	Saudi Arabia
	Turkey
	Rest of Middle East
Africa	South Africa
	Rest of Africa

Key Questions Answered in the ReportWhat is the current value of the threat intelligence market? The threat intelligence market is worth USD 10.38 billion in 2026 and is projected to reach USD 18.85 billion by 2031.

Which region leads global demand for threat intelligence solutions? North America holds the largest regional share at 37.50% of 2025 revenue, supported by advanced cloud uptake and public–private information sharing alliances.

Why are services growing faster than products in this space? Skills shortages and rising attack complexity drive organisations to outsource threat-hunting and analysis, resulting in a 14.12% CAGR for the Services segment.

How does EU-NIS2 impact corporate spending? With fines of up to EUR 10 million or 2% of global turnover, the directive compels about 300,000 entities to invest in real-time intelligence for compliance and resilience.

What technologies differentiate leading vendors? Embedded AI that automates detection and response, open STIX/TAXII interoperability, and integrated cloud-to-edge visibility are primary differentiators among market leaders.

Which vertical shows the fastest growth rate? The BFSI sector is forecast to expand at a 14.70% CAGR through 2031 as financial institutions bolster defences against ransomware and digital payment fraud.

Related Reports Explore More Reports Find Latest Data onIndustry Outlook of Content IntelligenceCybersecurity Software IndustryInformation Security Market ReportOperational Intelligence IndustryRisk Analytics IndustrySecurity Analytics Market ShareIndustry Trends in Security And Vulnerability ManagementSecurity Assessment Market GrowthSecurity Software Market SizeReport on Threat Intelligence Security Services IndustryUnified Threat Management Industry