Cybersecurity Agentic AI Market Size & Share Analysis - Growth Trends And Forecast (2026 - 2031)
Industry: Artificial Intelligence & ML
URL: https://www.mordorintelligence.com/industry-reports/cybersecurity-agentic-artificial-intelligence-market

Cybersecurity Agentic AI Market Size and ShareMarket OverviewStudy Period | 2020 - 2031 |
Market Size (2026) | USD 2.43 Billion |
Market Size (2031) | USD 9.63 Billion |
Growth Rate (2026 - 2031) | 31.71 % |
Fastest Growing Market | Asia Pacific |
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.

Cybersecurity Agentic AI Market Analysis by Mordor IntelligenceThe cybersecurity agentic AI market size is projected to be USD 1.83 billion in 2025, USD 2.43 billion in 2026, and reach USD 9.63 billion by 2031, growing at a CAGR of 31.71% from 2026 to 2031. This shift in enterprise security architecture marks a move from fixed rule-based automation to systems capable of reasoning, planning, and taking defensive actions with minimal human input. Unlike earlier AI adoption cycles, enterprises now assign investigative tasks to autonomous systems rather than relying solely on AI as an analyst support tool. According to the World Economic Forum, 94% of respondents identified AI as the key driver of cybersecurity change for the year ahead, with 77% of organizations already deploying AI for phishing detection, intrusion response, and SOC automation. Large platform vendors are shaping the cybersecurity agentic AI market by embedding agentic functions into endpoint, cloud, identity, and SOC offerings, enhancing cross-sell opportunities and increasing switching costs for buyers. The strongest market opportunities lie with organizations requiring continuous monitoring across hybrid environments and regulated workflows, though concerns over model transparency, governance, and compute efficiency may slow adoption.

Key Report Takeaways* By component, software platforms led with a 39.71% share of the cybersecurity agentic AI market in 2025, while hardware accelerators are projected to expand at a 32.31% CAGR through 2031.
* By security level, network security accounted for 28.23% of the cybersecurity agentic AI market in 2025, while OT and IoT security are forecast to grow at a 33.31% CAGR through 2031.
* By deployment mode, cloud-native accounted for a 61.54% share of the cybersecurity agentic AI market in 2025, while hybrid deployment is expected to record a 32.31% CAGR through 2031.
* By organization size, large enterprises accounted for 67.89% of the revenue of the cybersecurity agentic AI market in 2025, while SMEs are projected to grow at a 32.11% CAGR through 2031.
* By industry vertical, BFSI captured 24.52% of the revenue of the cybersecurity agentic AI market in 2025, while energy and utilities are expected to grow at a 33.11% CAGR through 2031.
* By geography, North America retained a 34.86% share of the cybersecurity agentic AI market in 2025, while Asia-Pacific is projected to expand at a 32.71% CAGR through 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 January 2026.

Market Trends and InsightsDrivers Impact Analysis of Cybersecurity Agentic AI Market*Driver | (~) % Impact on CAGR Forecast | Geographic Relevance | Impact Timeline |
Real-Time Threat Mitigation Through Autonomous Response Loops | +6.8% | Global, with highest intensity in North America and Europe | Short term (≤ 2 years) |
Expansion of Machine-Generated Attack Surfaces in Multi-Cloud Environments | +5.9% | Global, particularly Asia-Pacific and North America | Short term (≤ 2 years) |
Regulatory Mandates for AI-Driven Continuous Controls Monitoring | +4.7% | Europe, North America, Asia-Pacific | Medium term (2-4 years) |
Cyber Workforce Shortage Accelerating AI Security Adoption | +6.2% | Global, with acute pressure in North America and Western Europe | Medium term (2-4 years) |

Integration of LLM Agents in DevSecOps Pipelines | +3.3% | North America, Western Europe, Asia-Pacific technology hubs | Medium term (2-4 years) |
Venture Funding for Specialized AI Security Startups | +3.6% | North America, Israel, the United Kingdom, Singapore | Short term (≤ 2 years) |
Source: Mordor Intelligence |
Real-Time Threat Mitigation Via Autonomous Response LoopsThe cybersecurity agentic AI market is growing as threat activity outpaces manual triage models. CrowdStrike reported in March 2026 that adversaries reduced breakout time to 29 minutes, leaving little room for analyst-led containment.[1]CrowdStrike, “CrowdStrike Delivers Agentic MDR to Stop Breaches at Machine Speed,” CrowdStrike, crowdstrike.com Autonomous response loops are crucial because they integrate investigation, prioritization, and containment into a single process, avoiding delays caused by team handoffs. IBM’s Autonomous Threat Operations Machine, launched in April 2025, demonstrates this shift by using multi-agent workflows and domain-specific models for triage and remediation with minimal human input. These loops create a feedback effect, generating data to enhance future detection and response.

Explosion of Machine-Generated Attack Surfaces in Multi-Cloud EnvironmentsThe cybersecurity agentic AI market is expanding as AI-enabled workloads increase the attack surface for security teams. Cisco noted in February 2026 that enterprises seek AI-aware policy enforcement as agentic workloads spread across clouds, driving demand for autonomous security controls. Palo Alto Networks' 2025 research found that 99% of organizations using AI in production experienced at least one attack on their AI systems, with 41% reporting increased API attacks. Orca Security found 55% of organizations used two or more cloud providers in 2025, up from 12% in 2024, highlighting a fragmented identity and policy environment. This strengthens demand for security systems that interpret context and coordinate actions across clouds, APIs, and trust zones.

Chronic Cyber Workforce Shortage Accelerating AI Security AdoptionThe cybersecurity-agentic AI market is advancing amid a persistent shortage of security talent. ISC2 reported in December 2025 that 59% of cybersecurity professionals identified critical skill gaps in their organizations, a 15-point rise from 2024. This shortage shifts enterprise priorities, positioning AI as a coverage layer to maintain response capacity. The impact is most evident in SOC environments, where alert volumes and identity complexity outpace hiring. Consequently, demand is growing for systems that handle routine investigations, standardize decisions, and enable analysts to focus on high-risk cases.

Regulatory Mandates for AI-Driven Continuous Controls MonitoringThe cybersecurity agentic AI market is bolstered by regulations requiring continuous oversight rather than periodic reviews. NIST’s AI Agent Standards Initiative, launched in February 2026, highlights the shift toward agent-level governance. Research in AI and Ethics (January 2026) emphasized that transparency, traceability, interpretability, and explainability are critical under European policies, though practical implementation remains unresolved. Automated audit trails and policy-aware ac

tion logging are now key purchasing criteria, especially in regulated sectors. Vendors that align autonomy with monitoring, documentation, and governance have a stronger foothold in enterprise environments.

Restraints Impact Analysis of Cybersecurity Agentic AI Market*Restraint | (~) % Impact on CAGR Forecast | Geographic Relevance | Impact Timeline |
Adversarial AI and Model Poisoning Risks | -3.2% | Global, especially regulated sectors such as BFSI, healthcare, and government | Medium term (2-4 years) |
Limited Explainability of Agentic AI Decisions | -2.5% | Europe and North America, especially financial and healthcare settings | Medium term (2-4 years) |
High Computational Costs of Security-Specific Foundation Models | -2.1% | Global, with stronger impact in SMEs and cost-sensitive regions | Medium term (2-4 years) |
Fragmented Data Provenance Standards Across Jurisdictions | -1.7% | Cross-border deployments between Europe, North America, and Asia-Pacific | Long term (≥ 4 years) |
Source: Mordor Intelligence |
Adversarial AI and Model Poisoning RisksThe cybersecurity agentic AI market faces challenges as the same autonomy that enhances defense can amplify damage if models or data pipelines are compromised. OWASP identifies data and model poisoning as critical risks, including backdoor insertion, output manipulation, and denial-of-service attacks.[2]OWASP Gen AI Security Project, “LLM04:2025 Data and Model Poisoning,” OWASP, genai.owasp.org Research at ICLR 2025 revealed that even a 0.1% poisoning rate during pre-training can persist into deployed models. Google’s Threat Intelligence Group documented AI misuse by threat actors in 2025, showing its practical application in cyberattacks. These risks may slow adoption in regulated sectors, as buyers impose stricter permissions, narrower deployment scopes, or demand extensive validation before allowing autonomous actions in production systems.

Limited Explainability of Agentic AI DecisionsLimited explainability constrains the cybersecurity agentic AI market, as autonomous systems can act without producing a clear decision trail for legal, compliance, and response teams. The 2026 AI and Ethics study highlighted that transparency, traceability, interpretability, and explainability are distinct obligations, with regulatory practices still lacking clarity. The Federation of American Scientists noted in 2025 that interpretability research lags behind capability development, potentially slowing deployment confidence. CISA's 2025 guidance warned against using large language models for safety-critical decisions due to concerns about explainability. As a result, adoption in regulated, safety-sensitive environments may remain slow despite technological advancements.

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

Cybersecurity Agentic AI Market Segment AnalysisBy Component:Software Platform Leadership Reflects Platform ConsolidationSoftware platforms held a 39.71% share in 2025, reflecting enterprise preference for integrated agentic orchestration across endpoint, cloud, identity, and network telemetry. This segment benefits from shared policy, memory, and unified response logic, simplifying autonomous actions at scale. Fragmented agent deployments are seen as a risk due to inconsistent decisions and duplicate actions. Services remained the second-largest component as many organizations require external support for deployment, workflow redesign, policy mapping, and model governance.

Service demand is increasingly recurring as buyers shift from one-time implementation to ongoing tuning and oversight. GitLab’s 2025 public beta of the Duo Agent Platform highlighted how orchestration extends into development and security workflows, driving advisory and integration needs. Hardware accelerators are proj

ected to grow at a 32.31% CAGR through 2031, driven by the need for local inference in latency-sensitive environments. This shift positions hardware as a key enabler of real-time autonomous defense in edge and high-speed settings, reducing reliance on slower cloud round-trip times.

 By Security Level:Network Security Leads While OT and IoT Expands FastestNetwork security commanded a 28.23% share of the cybersecurity agentic AI market in 2025 because network telemetry still provides the broadest real-time view of east-west movement, lateral escalation, and policy violations. For many enterprises, the network layer remains the backbone that allows agentic systems to correlate behavior across assets and environments. Endpoint security also retained a strong position because it is often the easiest place to introduce autonomous investigation and guided remediation into an existing security stack. This has made endpoint platforms a common entry point for agentic adoption in the cybersecurity agentic AI market.

SentinelOne reported in March 2026 that its Purple AI autonomous investigation capability was included in over 50% of licenses sold in Q4 FY26, highlighting how endpoint vendors leverage their installed base to distribute agentic features. Cloud and SaaS security and IAM are also growing as organizations handle an increasing number of non-human identities and API-driven access paths. OT and IoT security, the fastest-growing segment at a 33.31% CAGR through 2031, is driven by the rapid convergence of digital and physical infrastructure. The cybersecurity agentic AI market is shifting toward platforms that interpret both network intent and operational context, rather than just detecting anomalies.

By Deployment Mode:Cloud-Native Leads While Hybrid Fits Regulated WorkloadsCloud-native deployment accounted for 61.54% in 2025, reflecting early adoption in environments built around APIs, event streams, and elastic compute. This model suits the cybersecurity agentic AI market as autonomous systems require fast access to telemetry, policy engines, and remediation workflows across distributed infrastructure. Cloud delivery also enables faster model updates, which are critical in a constantly evolving threat landscape. On-premises deployment remains relevant in government, defense, and critical infrastructure sectors due to strict data handling policies.

Hybrid deployment is expected to grow at a 32.31% CAGR through 2031, driven by enterprises retaining sensitive or regulated data on-site while using cloud-based orchestration for coordination. This architecture balances control, sovereignty, and speed. In May 2026, Microsoft reported its MDASH multi-model agentic defense system scored 88.45% on the CyberGym benchmark across 1,507 real-world vulnerability tasks, emphasizing the value of distributed model architectures. Hybrid is likely to become the preferred structure for large, regulated enterprises that need both autonomy and strict data control.

By Organization Size:Large Enterprises Lead While SMEs Expand FasterLarge enterprises accounted for 67.89% of revenue in 2025, driven by their extensive telemetry, larger budgets, and ability to implement AI governance frameworks. Their dominance in the cybersecurity agentic AI market stems from platform vendors bundling agentic functions into enterprise agreements, making adoption an upgrade rather than a separate purchase. These organizations invest in workflow redesign, policy enforcement, and model oversight due to the scale of risk, maintaining the market's reliance on large enterprises.

SMEs are expected to grow at a 32.11% CAGR through 2031, aided by managed detection and response channels that simplify adoption. Smaller firms require faster investigation and better coverage but lack the resources for a full internal SOC. ISC2’s 2025 workforce study highlights a skills gap driving demand for external security capacity and automated response. However, SME adoption depends on governance, as poorly supervised remediation can cause disruptions. Growth will favor service-led models combining autonomy with oversight and policy control.

Image © Mordor Intelligence. Reuse requires attribution under CC BY 4.0. By Industry Vertical:BFSI Leads While Energy and Utilities Gains PaceBFSI accounted for 24.52% of the market in 2025 due to its high-value threat profile, compliance requirements, and early adoption of AI for monitoring and anomaly detection. These institutions rely on continuous surveillance, control mapping, and rapid threat containment. The European Banking Authority reported in September 2025 that 92% of EU banks used AI, with 55% employing agentic or general-purpose AI models in consumer-facing processes, highlighting strong familiarity with AI governance. Healthcare, life sciences, government, and defense also drive demand due to insider risk, supply chain exposure, and sensitive data protection needs.

Manufacturing is gaining importance as ransomware attacks and digital integration increase. Dragos reported in April 2026 a 64% year-over-year rise in ransomware attacks on industrial organizations, boosting demand for adaptive defensive models. Energy and utilities, growing at a 33.11% CAGR through 2031, are increasingly focused on protecting critical infrastructure, where disruptions have widespread consequences. Cisco's 2026 utilities study revealed that 87% of utility firms viewed AI as key to stronger cybersecurity, with 47% planning to adopt AI for grid operations within five years. Retail and e-commerce remain less mature in the cybersecurity agentic AI market due to tighter budgets and a focus on fraud over advanced intrusions.

Geography AnalysisNorth America Cybersecurity Agentic AI MarketNorth America accounted for 34.86% of the cybersecurity agentic AI market in 2025, driven by its strong vendor base and early enterprise adoption. Policies promoting continuous monitoring and cyber resilience in regulated sectors further support growth. ISC2 reported in December 2025 that critical cybersecurity skill gaps in the region are boosting demand for platforms that reduce manual effort.[3]ISC2, "2025 ISC2 Cybersecurity Workforce Study," ISC2, isc2.org Market growth is also tied to enterprise contract expansions, with customers adopting agentic functions through broader platform relationships rather than stand-alone purchases.

APAC Cybersecurity Agentic AI MarketAsia-Pacific is projected to grow at a 32.71% CAGR through 2031, making it the fastest-growing regional market. This growth is fueled by rapid digital expansion, multi-cloud adoption, and concerns over AI-enabled attacks. Organizations in the region are scaling cyber defenses faster than they can expand skilled security teams. Critical infrastructure modernization and distributed environment monitoring also drive demand, though data localization rules and regulatory maturity may create uneven opportunities.

EMEA and South America Cybersecurity Agentic AI MarketEurope ranked third in 2025, with demand focused on financial services, manufacturing, and critical infrastructure, where governance and documentation are as important as detection. Research published in AI and Ethics in 2026 highlighted Europe's emphasis on transparency and explainability, supporting demand for auditable autonomous systems. The Middle East and Africa are growing from a smaller base through digital transformation programs, while South America is gradually expanding amid rising ransomware threats and financial sector digitization. Both regions are in an early development stages but show increasing demand for scalable monitoring and response models.

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

Competitive Landscape

The cybersecurity agentic AI market is moderately fragmented, with a few large vendors like CrowdStrike, Palo Alto Networks, Microsoft, SentinelOne, and IBM dom

inating due to their control over telemetry estates, enterprise relationships, and platform bundling. These leaders embed agentic functions into existing security environments, leveraging proprietary data flows and integrated control surfaces. The market rewards vendors combining autonomy with visibility across endpoint, cloud, identity, and network layers.

CrowdStrike expanded its ecosystem in 2026 by launching the Charlotte AI AgentWorks Ecosystem with partners such as AWS, Anthropic, NVIDIA, and OpenAI, positioning Falcon as a governance layer for both custom and third-party agents. IBM integrated agentic functions across workflows with Autonomous Security, while Palo Alto Networks enhanced capabilities by acquiring Protect AI in July 2025, adding model scanning, AI red teaming, and runtime protection to Prisma AIRS.[4]Palo Alto Networks, “Palo Alto Networks Completes Acquisition of Protect AI,” Palo Alto Networks, paloaltonetworks.com These strategies highlight the importance of ecosystem control, acquisitions, and embedding agentic functions into enterprise workflows.

Competitive opportunities are strongest below the top enterprise tier, where smaller organizations seek simpler pricing, easier deployment, and managed support. This has allowed specialist vendors like Noma Security to emerge, focusing on AI agent governance and AI-native monitoring. Noma raised USD 100 million in Series B funding in July 2025 to scale its platform. However, the market still favors large platforms, as most buyers prefer extending existing security stacks rather than adopting new standalone solutions.

Cybersecurity Agentic AI Industry Leaders* CrowdStrike Holdings Inc.

* Palo Alto Networks, Inc.

* Microsoft Corporation

* SentinelOne Inc.

* Darktrace Plc

* *Disclaimer: Major Players sorted in no particular order
Cybersecurity Agentic AI Market Companies Covered in this Report* CrowdStrike Holdings Inc.
* Palo Alto Networks Inc.
* Darktrace plc
* SentinelOne Inc.
* IBM Corporation
* Microsoft Corporation
* Cisco Systems Inc.
* Fortinet Inc.
* Check Point Software Technologies Ltd.
* Trend Micro Incorporated
* Rapid7 Inc.
* Arctic Wolf Networks Inc.
* Sophos Ltd.
* Elastic N.V.
* Google LLC
* Amazon Web Services Inc.
* Accenture plc
* Noma Security
* Vectra AI
* Okta Inc.

Recent Industry Developments in Cybersecurity Agentic AI Market* May 2026: Senti

nelOne unveiled Wayfinder Frontier AI Services in partnership with Anthropic, of fering AI-accelerated discovery of undisclosed vulnerabilities, exploitability-g rounded prioritization, and disruption of exploitation chains across endpoint, c loud, identity, and AI attack surfaces.
* April 2026: IBM announced new enterprise cybersecurity measures, including IBM Autonomous Security, a multi-agent-powered service designed to integrate across an organization's full security stack, identity, risk, and governance functions to automate vulnerability remediation and contain threats at machine speed.
* March 2026: CrowdStrike launched the Charlotte AI AgentWorks Ecosystem, a no-c ode platform for building custom security agents using frontier AI models from A nthropic, NVIDIA, and OpenAI, in collaboration with Accenture, AWS, Deloitte, Sa lesforce, and Telefónica Tech.
* February 2026: Cisco expanded its AI Defense portfolio with the AI BOM, the MC P Catalog for agent governance, real-time agentic guardrails integrated with NVI DIA NeMo, and the introduction of IOS XE 26 with full-stack post-quantum cryptog raphy for enterprise routing.

Table of Contents for Cybersecurity Agentic AI Industry Report1. INTRODUCTION

* 6.4.6 Microsoft Corporation
* 6.4.7 Cisco Systems Inc.
* 6.4.8 Fortinet Inc.
* 6.4.9 Check Point Software Technologies Ltd.
* 6.4.10 Trend Micro Incorporated
* 6.4.11 Rapid7 Inc.
* 6.4.12 Arctic Wolf Networks Inc.
* 6.4.13 Sophos Ltd.
* 6.4.14 Elastic N.V.
* 6.4.15 Google LLC
* 6.4.16 Amazon Web Services Inc.
* 6.4.17 Accenture plc
* 6.4.18 Noma Security
* 6.4.19 Vectra AI
* 6.4.20 Okta Inc.

7. MARKET OPPORTUNITIES AND FUTURE OUTLOOK

* 7.1 White-Space and Unmet-Need Assessment

Global Cybersecurity Agentic AI Market Report ScopeThe Cybersecurity Agentic AI Market refers to the global industry focused on the development, deployment, and adoption of autonomous or semi-autonomous artificial intelligence systems designed to detect, prevent, analyze, and respond to cybersecurity threats with minimal human intervention. These AI-driven cybersecurity solutions leverage technologies such as machine learning, large language models, generative AI, autonomous agents, behavioral analytics, and real-time threat intelligence to enhance security operations, automate incident response, improve threat detection accuracy, and reduce response times across enterprise environments.

The Cybersecurity Agentic AI Market is Segmented by Component (Software Platforms, Services, and Hardware Accelerators), Security Level (Network Security, Endpoint Security, Application Security, Cloud/SaaS Security, Indentity and Access Management, and OT/IoT Security), Deployment (Cloud-Native, On-Premises, and Hybrid), Organization Size (Large Enterprises, and Small and Medium Enterprises), Industry Vertical (BFSI, Healthcare and Life Sciences, Government and Defense, IT and Telecom, Manufacturing, Retail and E-Commerce, and Energy and Utilities), and Geography (North America, Europe, Asia-Pacific, South America, and Middle East and Africa). The Market Forecasts are Provided in Terms of Value (USD).

By ComponentSoftware Platforms |
Services (MDR, Advisory, Integration) |
Hardware Accelerators (AI-Optimized Silicon, Sensors) |
By Security LevelNetwork Security |
Endpoint Security |
Application Security |
Cloud and SaaS Security |
Identity and Access Management |
OT / IoT Security |
By Deployment ModeCloud-Native |
On-Premises |
Hybrid |
By Organization SizeLarge Enterprises |
Small and Mid-Sized Enterprises |
By Industry VerticalBFSI |
Healthcare and Life Sciences |
Government and Defense |
IT and Telecom |
Manufacturing |
Retail and E-Commerce |

Energy and Utilities |
By GeographyNorth America | United States |
 | Canada |
 | Mexico |
South America | Brazil |
 | Argentina |
 | Rest of South America |
Europe | United Kingdom |
 | Germany |
 | France |
 | Italy |
 | Rest of Europe |
Asia-Pacific | China |
 | Japan |
 | India |
 | South Korea |
 | Rest of Asia-Pacific |
 | |
Middle East and Africa | Middle East | United Arab Emirates |
 | | Saudi Arabia |
 | | Rest of Middle East |
 | |
Africa	South Africa
	Egypt
	Rest of Africa
By Component	Software Platforms
Services (MDR, Advisory, Integration)
Hardware Accelerators (AI-Optimized Silicon, Sensors)
By Security Level	Network Security
Endpoint Security
Application Security
Cloud and SaaS Security
Identity and Access Management
OT / IoT Security
By Deployment Mode	Cloud-Native
On-Premises
Hybrid
By Organization Size	Large Enterprises
Small and Mid-Sized Enterprises
By Industry Vertical	BFSI
Healthcare and Life Sciences
Government and Defense
IT and Telecom
Manufacturing
Retail and E-Commerce
Energy and Utilities
By Geography	North America	United States
	Canada
	Mexico
South America	Brazil
	Argentina
	Rest of South America
Europe	United Kingdom
	Germany
	France
	Italy
	Rest of Europe
Asia-Pacific	China

	Japan
	India
	South Korea
	Rest of Asia-Pacific
Middle East and Africa	Middle East	United Arab Emirates
		Saudi Arabia
		Rest of Middle East
	Africa	South Africa
		Egypt
		Rest of Africa

Key Questions Answered in the ReportWhat is the 2031 value forecast for cybersecurity agentic AI? The cybersecurity agentic AI market is projected to reach USD 9.63 billion by 2031, up from USD 2.43 billion in 2026, reflecting a 31.71% CAGR over 2026 to 2031.

Which region leads current demand for cybersecurity agentic AI solutions? North America leads current demand with a 34.86% share in 2025, supported by a deep vendor base, strong enterprise adoption, and higher regulatory pressure.

Which region is growing fastest through 2031? Asia-Pacific is the fastest-growing region, with a projected 32.71% CAGR from 2026 to 2031 as digital expansion and cloud adoption increase security complexity.

Which deployment model dominates today? Cloud-native deployment leads with a 61.54% share in 2025 because agentic systems depend heavily on APIs, event streams, and scalable compute.

Which use area is expanding fastest by security level? OT and IoT security is the fastest-growing security layer, with a 33.31% CAGR through 2031, driven by the convergence of digital and physical infrastructure.

Why are large enterprises leading adoption while SMEs are growing faster? Large enterprises lead revenue with a 67.89% share because they have larger budgets and stronger governance capacity, while SMEs are growing faster at a 32.11% CAGR through service-led and MDR-based delivery models.

Related Reports Explore More Reports Find Latest Data onAI Cybersecurity Solutions Market AnalysisAgentic AI Market ShareIndustry Outlook of Agentic AI Development PlatformIndustry Outlook of Agentic AI FrameworksHealthcare Agentic AI Industry OverviewAgentic AI In Legal And Regulatory Tech Market SizeAgentic AI Safety And Alignment Solutions Industry OverviewAgentic AI In Manufacturing And Industrial Automation MarketAgentic AI Monitoring, Analytics, And Observability Tools IndustryAgentic AI In Financial Services MarketBreach And Attack Simulation Market Share