SCOTTS INTERNATIONAL

# Cognitive Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-07-01 | 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:**

Cognitive Security Market Analysis

The cognitive security market stands at USD 17.09 billion in 2025 and is forecast to reach USD 46.71 billion by 2030, translating into a robust 22.27% CAGR. Persistent AI-enabled threats, expanding attack surfaces created by cloud adoption, and mounting regulatory scrutiny combine to fuel this growth. Enterprises invested heavily after discovering that conventional tools miss AI-specific vulnerabilities such as model poisoning, adversarial prompts, and synthetic data leakage, prompting an accelerated pivot toward advanced analytics and autonomous defense. Parallel advances in large-language-model deployments inside corporate workflows further sharpen demand, because every generative-AI rollout creates new entry points that must be continuously monitored and hardened. Vendors respond by embedding self-learning algorithms into incident-response playbooks, reducing mean time to detect and contain breaches from hours to minutes while simultaneously shrinking false-positive noise that overwhelms human analysts. These dynamics position the cognitive security market as one of the fastest-expanding segments within broader cybersecurity spending.

Global Cognitive Security Market Trends and Insights

Exponential Rise of Unstructured Enterprise Data

Massive growth in emails, collaboration files, sensor readings, and multimedia escalates both the visibility challenge and the attack surface. Cognitive engines ingest terabytes of raw logs to pinpoint deviations in user behavior, cutting false-positive alerts by 95% while surfacing stealthy lateral movements that bypass rule-based systems. However, attackers benefit from the same information richness, scraping content to craft context-aware spear-phishing campaigns. Security teams therefore integrate self-learning analytics directly into data-lakes to correlate identity, device, and network telemetry in near real time, turning previously dormant archives into actionable intelligence that enhances breach-detection accuracy. The net result is an elevated baseline for analytic depth that positions the cognitive security market for sustained expansion across all verticals.

Surge in IoT Dark Data

Industrial and consumer IoT deployments add billions of unmanaged endpoints, creating a torrent of operational telemetry that standard SIEM platforms cannot parse. Cognitive engines model baseline behavior for each device class and flag deviations such as anomalous firmware changes or unexpected east-west traffic. In energy grids and smart-factory floors, this functionality directly mitigates downtime risks while protecting life-safety systems. The security gap widens as OT networks converge with IT backbones, prompting manufacturing and utilities firms to invest in edge-resident AI analytics that operate under stringent latency constraints. Consequently, demand for scalable, device-agnostic platforms inside the cognitive security market continues to accelerate through 2030.

Scarcity of AI/ML Cyber-Analytics Talent

Demand for practitioners able to code reinforcement-learning defenses, tune prompt-shield models, and interpret threat telemetry vastly exceeds global supply. Organizations counter by outsourcing to managed-service specialists and by investing in low-code orchestration layers that let fewer engineers protect larger asset bases. Although automation handles level one triage, level two and level three escalations still require hybrid skill sets spanning mathematics, secure coding, and regulatory interpretation. The resulting wage inflation inflates project TCO, nudging some smaller firms toward consumption-based cloud subscription models instead of bespoke builds.

Other drivers and restraints analyzed in the detailed report include:

Cloud-Native AI Toolchains Democratizing Cognitive Security / Escalating Threats on Open-Source and Cloud Stacks / Multi-Jurisdictional Data Governance Complexity /

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

Segment Analysis

On-premises solutions retained 60.40% cognitive security market share in 2024 because defense agencies, financial institutions, and critical-infrastructure operators continue to mandate local data residency and air-gapped environments. However, cloud deployments are expanding at a 27.10% CAGR as hyperscalers integrate purpose-built telemetry collectors and model-integrity validation into their platforms, lowering entry cost. The cognitive security market size for cloud-based offerings is projected to rise steeply as subscription pricing and continuous threat-feed updates shorten procurement cycles and transfer capital expenditure into operating budgets.

Hybrid architectures now dominate new implementations, pairing edge inference nodes with central cloud analytics that feed global threat-intel graphs. Vendors pre-package reference blueprints that encrypt training data at rest while enabling secure compute enclaves for federated learning between on-prem and public-cloud zones. Security-operations centers benefit from unified dashboards that normalize detections across environments, closing visibility gaps that attackers exploit when workflows straddle multiple hosting models. These capabilities collectively position cloud variants as the principal expansion engine within the cognitive security market through 2030.

Consulting and integration engagements captured 60.40% revenue share in 2024 because enterprises require customized data pipelines, model-validation frameworks, and regulatory mappings before cognitive controls deliver value. The cognitive security market size attributed to managed services is forecast to grow at a 28.40% CAGR as organizations outsource round-the-clock monitoring, model retraining, and adversarial-simulation exercises.

Specialist providers now bundle threat-hunting squads with MLOps engineers to maintain dynamic baselines tuned to each client's evolving risk profile. Government contracts such as the USD 2 billion NSIN task order awarded to GovCIO illustrate how public agencies leverage external expertise to accelerate acquisition timelines while meeting classified accreditation requirements. Commercial buyers mirror this pattern, shifting budget from headcount to outcome-based subscriptions that guarantee detection-accuracy service-level agreements. The managed-services boom is therefore a structural, not temporary, phenomenon underpinning the growth trajectory of the cognitive security market.

Cognitive Security Market Segmented by Deployment, Service (Professional Services, Managed Services), Application (Cognitive Threat Intelligence, Predictive Maintenance, and More), End-User Industry (BFSI, Healthcare and Life Sciences and More), Component (Solutions and Services) and by Geography. The Market Forecasts are Provided in Terms of Value (USD).

Geography Analysis

North America remains the largest regional cluster, holding 35.70% cognitive security market share in 2024. State and federal agencies allocate multibillion-dollar budgets to safeguard critical infrastructure, exemplified by the USD 2 billion Department of Defense NSIN task order and the USD 185 million F-35 cybersecurity support contract. Enterprises face an equally complex environment as AI-specific risk-management rules emerge alongside existing data-privacy statutes, raising compliance overhead yet simultaneously expanding addressable spend for platform vendors. Venture funding remains abundant, sustaining a pipeline of startups that commercialize niche capabilities such as prompt-injection testing and autonomous red-teaming. Nevertheless, growth rates moderate relative to emerging regions because many Fortune 1000 firms have already executed first-generation AI-security programs and now focus on incremental optimization rather than green-field rollouts.

Asia-Pacific records the fastest trajectory at a 25.66% CAGR. Government programs in China, Singapore, and South Korea promote AI adoption while investing in national cybersecurity centers that procure local and international technology. Rapid digital-payment expansion and smart-city rollouts generate enormous telemetry volumes, providing fertile data for machine-learning-driven defenses but also luring cybercriminal syndicates that weaponize automated reconnaissance. Enterprises therefore prioritize AI-native security from the outset rather than layering it later, shortening sales cycles for full-stack platforms. Linguistic diversity and regulatory heterogeneity pose integration hurdles, yet hyperscalers' growing regional footprints alleviate infrastructure constraints, reinforcing demand for scalable cognitive controls.

Europe advances steadily as the EU AI Act transforms ambiguity into prescriptive obligations around transparency, robustness, and data governance. While compliance costs elevate project complexity, the legislative clarity encourages board-level approval for long-term investments in explainable-AI security. Vendors localize dashboards and audit trails to meet region-specific reporting schemas, and many offer sovereign-cloud options hosted in accredited data centers to respect cross-border transfer restrictions. Uptake is especially strong in Germany's manufacturing heartland and France's aerospace and defense sector, where cyber-physical risks intersect with intellectual-property protection imperatives. Together these factors ensure Europe remains a strategic revenue pillar for the cognitive security market, even if growth percentages trail Asia-Pacific's breakneck pace.

List of Companies Covered in this Report:

IBM Corporation / Microsoft Corp. (Azure) / Amazon Web Services Inc. / SAP SE / Cisco Systems Inc. / Trend Micro Inc. /

Broadcom Inc. (Symantec) /  Darktrace plc /  McAfee LLC /  LogRhythm Inc. /  Fortinet Inc. /  SAS Institute Inc. /  Splunk Inc. /  Google LLC /  Oracle Corp. /  Micro Focus Intl. /  Dell Technologies (EMC) /  Palantir Technologies /  CrowdStrike Holdings /  SAS Institute Inc. /

Additional Benefits:

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

**Table of Contents:**

6 COMPETITIVE LANDSCAPE
6.1 Market Concentration
6.2 Strategic Moves
6.3 Market Share Analysis
6.4 Company Profiles (includes Global level Overview, Market level overview, Core Segments, Financials as available, Strategic Information, Market Rank/Share for key companies, Products and Services, and Recent Developments)
6.4.1 IBM Corporation
6.4.2 Microsoft Corp. (Azure)
6.4.3 Amazon Web Services Inc.
6.4.4 SAP SE
6.4.5 Cisco Systems Inc.
6.4.6 Trend Micro Inc.
6.4.7 Broadcom Inc. (Symantec)
6.4.8 Darktrace plc
6.4.9 McAfee LLC
6.4.10 LogRhythm Inc.
6.4.11 Fortinet Inc.
6.4.12 SAS Institute Inc.
6.4.13 Splunk Inc.
6.4.14 Google LLC
6.4.15 Oracle Corp.
6.4.16 Micro Focus Intl.
6.4.17 Dell Technologies (EMC)
6.4.18 Palantir Technologies
6.4.19 CrowdStrike Holdings
6.4.20 SAS Institute Inc.

7 MARKET OPPORTUNITIES AND FUTURE OUTLOOK
7.1 White-space and Unmet-need Assessment

SCOTTS INTERNATIONAL

# Cognitive Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-07-01 | 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 | 2026-03-02 |
| | | Signature | |

**Scotts International. EU Vat number: PL 6772247784**
tel. 0048 603 394 346 e-mail: support@scotts-international.com
www.scotts-international.com