Deception Technology - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-06-01 | 155 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:

Deception Technology Market Analysis

The deception technology market posted USD 2.41 billion in 2025 and is set to advance at a 13.3% CAGR to USD 4.50 billion by 2030. Rising zero-day exploits, AI-driven deepfake fraud, and cloud-native workload expansion compel security teams to adopt early-warning controls that spot attackers inside the network before damage occurs. Vendors now weave decoys into zero-trust micro-segmentation, giving defenders tripwires that work even when identities or endpoints are compromised. Demand also accelerates because cyber-insurance carriers require proactive lateral-movement detection as a condition for favorable premiums. Although North America keeps spending leadership, the deception technology market gains rapid momentum in Asia-Pacific as multicloud adoption surges and local regulators tighten breach-notification rules.

Global Deception Technology Market Trends and Insights

Surge in Zero-Day Exploits and Targeted APTs

State-sponsored collectives automate reconnaissance with AI, finding novel vulnerabilities faster than signature-based defenses adapt. The Institute for Security and Technology notes that automated reconnaissance compresses attacker dwell time, forcing defenders to rethink reactive playbooks. Deception platforms insert believable but fake assets that weaponize curiosity; once probed, alerts trigger in seconds while production systems stay untouched. Because detection is based on attacker behavior rather than threat-intelligence feeds, the deception technology market provides resilience against bespoke malware that evades

hash-matching controls. Vendors now pre-package decoys for industrial control systems and SaaS APIs, reflecting attacker pivot toward operational technology.

Escalating Cloud-Native Workloads Broaden Attack Surface

Containerized and serverless applications can spin up and down within minutes, leaving security operations centers blind to east-west traffic. Zscaler deploys generative-AI decoys that mimic large-language-model endpoints, luring attackers into instrumented sandboxes. Because decoys scale automatically inside Kubernetes namespaces, defenders gain continuous coverage even as underlying microservices change. The deception technology market capitalizes on cloud providers' metadata APIs to place traps inside virtual private clouds without installing agents. As organizations adopt multi-cloud strategies, cross-provider decoy orchestration becomes a buying criterion, especially in regulated industries that cannot centralize logs in a single region.

Entrenched Reliance on Legacy Honeypots

Many firms still run static honeypots deployed years ago. Attackers now fingerprint such assets through protocol quirks or uptime patterns, bypassing them with ease. This sunk-cost bias delays upgrades to adaptive decoys able to morph operating-system banners or rotate credentials automatically. Legacy honeypots also demand manual log parsing, consuming resources that should focus on real attack paths. Because these tools produce few actionable alerts, boards question ROI, thereby constraining new investment and dampening growth of the deception technology market.

Other drivers and restraints analyzed in the detailed report include:

CISO Preference for Low-Friction, Agent-Less Detection Tools / Rise of AI-Generated Deepfake Identity Attacks / Scarcity of Deception-Skilled SecOps Staff /

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

Segment Analysis

On-premises deployment commanded 67.9% of deception technology market share in 2024, illustrating enterprises' need to keep high-interaction decoys close to crown-jewel systems for compliance and forensic control. That control, however, brings hardware refresh cycles and change-management overhead that limit agility. Cloud deployment contributes a modest slice today but is slated to rise at a 15.2% CAGR through 2030, the fastest pace within the deception technology market. Cloud-based consoles spin up decoys across regions within minutes, making them attractive for global branch rollouts.

Hybrid models emerge as a pragmatic bridge, letting teams place sensitive database decoys on-premises while offloading analysis and scaling tasks to public clouds. As multicloud adoption rises, buyers demand single-pane views across AWS, Azure, and Google Cloud, pushing providers to invest in identity federation and immutable infrastructure blueprints. These capabilities enhance the deception technology market size for cloud modules and convince regulation-bound sectors that shared-responsibility models can still satisfy audit controls.

Large enterprises retained 70.2% revenue share in 2024 and continue shaping feature roadmaps by insisting on API depth, MITRE ATT&CK alignment, and advanced analytics. Yet SMEs now register a 14.9% growth trajectory, outpacing big-company spending within the deception technology market. Subscription-based managed deception services, billed per asset, cut entry barriers and deliver curated alerts that fit smaller teams' bandwidth.

Savings compound because cloud consoles eliminate hardware purchase, allowing SMEs to reallocate capital toward employee awareness programs. For vendors, the segment's scale effect is compelling; thousands of mid-sized customers can equal the license revenue of a handful of Fortune 500 accounts. Consequently, roadmap priorities now include low-code playbooks and automated decoy placement, features designed to compress onboarding from weeks to hours and thereby expand deception technology market size among smaller firms.

The Deception Technology Market Report is Segmented by Deployment (On-Premises and Cloud), Organization Size (Large Enterprises and Small and Medium Enterprises (SMEs)), Service (Managed Services and Professional Services), Deception Stack (Data Security, Application Security, and More), End-User (Government, Defense, BFSI, IT and Telecommunication, and More), and Geography.

Geography Analysis

North America generated 41.8% of revenue in 2024, buoyed by stringent mandates such as CISA's directive on incident reporting and a concentration of Fortune 100 headquarters that can fund specialized controls. Federal contracts increasingly specify deception capabilities, further cementing the region's leadership within the deception technology market.

Europe advances steadily as the NIS2 Directive broadens the scope of entities required to maintain proactive threat-detection programs Local vendors stress data-sovereignty features, ensuring logs stay inside EU borders. Emerging EU cloud providers now embed deception natively, offering compliance-ready bundles that appeal to mid-market industrial manufacturers.

Asia-Pacific remains the fastest-growing territory at 13.8% CAGR. Governments in Japan, India, and Singapore launch grant programs that co-fund zero-trust pilots incorporating deception. Telecom rollouts of 5G standalone cores enlarge attack surfaces, pushing operators to install signaling-protocol decoys that detect rogue base-station registration attempts. These initiatives collectively enlarge deception technology market size in the region. Meanwhile, Latin America and Middle East and Africa start integrating deception into critical-infrastructure revamps, although budget constraints and talent gaps temper near-term uptake.

List of Companies Covered in this Report:

Illusive Networks / Attivo Networks (SentinelOne) / Rapid7 / Acalvio Technologies / CounterCraft / CyberTrap / TrapX Security / Smokescreen Technologies / Ridgeback Network Defense / LogRhythm / WatchGuard Technologies / Broadcom (Symantec) / Morphisec / Fortinet (FortiDeceptor) / Zscaler / Microsoft (Security Honeytokens) / Akamai / Palo Alto Networks / Fidelis Cybersecurity / Commvault (TrapX integration) /

Additional Benefits:

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

Table of Contents:

5.5.5 Healthcare
5.5.6 Other End-Users
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 Europe
5.6.2.1 Germany
5.6.2.2 United Kingdom
5.6.2.3 France
5.6.2.4 Italy
5.6.2.5 Spain
5.6.2.6 Russia
5.6.2.7 Rest of Europe
5.6.3 Asia-Pacific
5.6.3.1 China
5.6.3.2 Japan
5.6.3.3 India
5.6.3.4 South Korea
5.6.3.5 Australia and New Zealand
5.6.3.6 Rest of Asia-Pacific
5.6.4 South America
5.6.4.1 Brazil
5.6.4.2 Argentina
5.6.4.3 Rest of South America
5.6.5 Middle East and Africa
5.6.5.1 Middle East
5.6.5.1.1 Saudi Arabia
5.6.5.1.2 United Arab Emirates
5.6.5.1.3 Turkey
5.6.5.1.4 Rest of Middle East
5.6.5.2 Africa
5.6.5.2.1 South Africa
5.6.5.2.2 Nigeria
5.6.5.2.3 Rest of Africa

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 Illusive Networks
6.4.2 Attivo Networks (SentinelOne)
6.4.3 Rapid7
6.4.4 Acalvio Technologies

Deception Technology - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-06-01 | 155 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