Deception Technology - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 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:

The Deception Technology Market size is estimated at USD 2.27 billion in 2024, and is expected to reach USD 4.51 billion by 2029, growing at a CAGR of 14.75% during the forecast period (2024-2029).

Key Highlights
-Deception technology is an advanced security solution to detect and prevent targeted attacks. Deceptions are achieved through purposeful obstructions, incorrect responses, misdirection, and forgery.
-Owing to the higher level of cyber threats, there is an increasing need for organizations to detect and mitigate advanced risks that have already breached the network. It is boosting deception technology adoption.
-The current security tools have effectively flagged anomalies but need to be more significant in defining their impact and risk potential. These tools generate many alerts, most of which must be investigated by security teams despite many of them being a waste of time. The resources are spent wastefully assessing these false threats, while the real and present threats must be addressed. By altering the asymmetry of an attack, deception technology helps security teams focus on real threats to the network. Scenes like these have aided the deception technology to gain momentum over the forecast period.
-Many deception solutions have AI and machine learning (ML) built into their core. These features ensure that deception techniques are kept dynamic and help reduce the operational overheads and the impact on security teams by freeing them from continually creating new deception campaigns.
-There was a sharp rise in cyberattacks harming individuals, businesses, and organizations during the COVID-19 outbreak. Consequently, several impacted enterprises are investing in upgrading outdated systems, thereby contributing to the deception technology market. For instance, the US Department of Homeland Security warned about emerging pandemic-related cybercriminals and advanced persistent threat groups. Interpol released a warning about criminals deliberately targeting medical facilities.

Deception Technology Market Trends

Network Security is expected to grow at a higher pace

- A zero-day attack is a targeted attack in which the attacker discovers software vulnerabilities and exploits them with other hackers until the organization becomes aware of the vulnerability. The zero-day exploit leaves no opportunity for detection initially.
- In 2021, Mandiant Threat Intelligence found 80 zero-day exploits in the wild, which was more than twice as many as the year before. The main actors exploiting zero-day vulnerabilities continue to be state-sponsored organizations with Chinese groups as leaders. The proportion of financially motivated actors deploying zero-day exploits has also increased significantly, with nearly one in every three identified actors exploiting zero-day exploits in the year before being financially motivated.
- Further, threat actors most commonly exploited zero-day vulnerabilities in Microsoft, Apple, and Google products, which reflects the popularity of these manufacturers. The significant growth in zero-day exploitation in the previous year, as well as the diversification of actors exploiting them, broadens the risk portfolio for businesses in practically every industry area and geography, particularly those that rely on these widely used systems.
- According to the research, a variety of factors contribute to an increase in the number of zero-day exploits. For example, the continued adoption of cloud hosting, mobile, and Internet-of-Things (IoT) technologies increases the volume and complexity of Internet-connected systems and devices. In other words, more software leads to more software flaws. The rise of the exploit broker industry is also likely contributing to this trend, with more resources being moved into zero-day research and development by private organizations, researchers, and threat groups alike.
- Due to the increase in zero-day attacks and APTs, organizations worldwide are deploying deception technologies to detect attacks as early as possible and minimize their effect on sensitive data. Therefore, the growing costs of data breaches, as indicated in the graph, are expected to drive the deception technology market during the forecast period.

North America is Expected to Hold Major Market Share

- The North American region is expected to hold a significant share in the global deception technology market owing to the increasing adoption of deception technology solutions in highly regulated industries such as financial services, health care, and government. Several US states, most notably California with its California Consumer Privacy Act (CCPA), have enacted privacy laws, significantly driving the demand for deception technology solutions among end-user industries.
- California passed a law, separate from the California Consumer Privacy Act, addressing default passwords on IoT devices and IoT vulnerabilities. Owing to this, the National Cybersecurity and Communications Integration Center (NCCIC) introduced the Technical Alert (TA), which provides information and guidance to assist MSP customer network and system administrators with the detection of malicious activity on their networks and systems and the mitigation of associated risks.
- This TA provides an overview of the TTP that APT actors use in MSP network environments, suggestions for mitigation, and details on reporting incidents. The high availability of adequate infrastructure, the presence of numerous global financial institutions, the high frequency of cyber-attacks, and the increased adoption of technologies are expected to drive the growth of the deception technology market in the North American region.
- The major trends responsible for the growth of deception technology in the North American region include the growing number of smartphone devices and an increase in the adoption of social apps, which generate sample data that contains valuable information. This has significantly increased the risk of cyber threats.
- In addition, the presence of prominent market vendors and increasing data volume in various organizations are driving the

demand for deception technology solutions in the region. Furthermore, the early adoption of advanced technologies, such as 5G, AI, cloud, and IoT, in various end-user sectors is driving the demand for deception technology solutions at a rapid pace.

Deception Technology Industry Overview

The deception technology market is highly fragmented, with the presence of major players like Illusive Networks, Commvault Systems Inc., Smokescreen Technologies Pvt. Ltd., Attivo Networks Inc. (Sentinelone Inc.), and Rapid7 LLC. Players in the market are adopting strategies such as partnerships, innovations, mergers, and acquisitions to enhance their product offerings and gain a sustainable competitive advantage.

In February 2023, Rapid7 and the University of South Florida (USF) announced a partnership to create a cyber threat intelligence laboratory that will support interdisciplinary research efforts by faculty experts and students from four colleges and myriad disciplines.

In September 2022, Commvault announced the general availability of Metallic ThreatWise, an early warning system that proactively surfaces unknown and zero-day threats to minimize compromised data and business impact.

Additional Benefits:

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

Table of Contents:

Deception Technology - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 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	2026-03-04
		Signature