Threat Intelligence - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 220 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 Threat Intelligence Market size is estimated at USD 8.15 billion in 2024, and is expected to reach USD 14.96 billion by 2029, growing at a CAGR of 12.90% during the forecast period (2024-2029).

In the past few years, there has been a paradigm shift between attack sources, targets, destination attack profiles, and different types of technologies. While the attack types and targets can be revealing, attack sources remain problematic because of the difficulties in assigning attribution for a specific attack.

Key Highlights
-The growing number of cyberattacks and data breaches has shifted organizations' focus to various cybersecurity solutions. More organizations are focusing on cyber intelligence because of the escalating cyber arms race between attackers and defenders. As a result, threat intelligence has enabled defenders to make faster, more informed security decisions and shift their behavior in the fight against breaches from reactive to proactive.
-Most organizations are focusing their intelligence efforts on more basic use cases (that depend on existing case studies and attacks), such as integrating intelligence feeds with current IPS, firewalls, and SIEMs, without taking full advantage of the intelligence insights they can offer.
-The threat intelligence market is primarily driven by increasing uniqueness in the attacking techniques leaving the data vulnerable. The rising volumes of data generated by different enterprises are the key factor driving the market.
-By integrating cloud and threat intelligence, organizations can block cyber threats and leverage the global threat community to identify unknown threats and ultimately stop them before they emerge, thus, targeting the attack surface. Therefore, the adoption of threat intelligence solutions has increased significantly.
-Cybercrime has increased over the last few years, and there are no signs of a slowdown. With the ongoing pandemic,

telecommuting has grown, increasing the rate of cyberattacks. Enterprises have adopted a remote working model, which raises concerns about corporate security, and these factors further drive the threat intelligence market.
-The COVID-19 pandemic has positively impacted the market's growth, and government bodies across the world are coming up with new strategy implementation to help support the cyber concerns organizations raise. The increasing number of cyber vulnerabilities is driving the growth of the threat intelligence market.

Threat Intelligence Market Trends

BFSI Segment is Expected to Occupy a Significant Share

- The BFSI industry is one of the critical infrastructure segments that face multiple data breaches and cyber-attacks, owing to the massive customer base that the sector serves and the financial information that is at stake. Being a highly lucrative operation model with phenomenal returns and the added upside of relatively low risk and detectability, cybercriminals are optimizing many diabolical cyberattacks to immobilize the financial sector. These attacks' threat landscape ranges from Trojans, malware, ATM malware, ransomware, and mobile banking malware to data breaches, institutional invasion, data thefts, fiscal breaches, etc.
- For instance, according to Orange Cyberdefense, malware was the most common type of cyber attack in financial and insurance organizations between October 2021 and September 2022. Around 40% of organizations worldwide were targeted by the attack vector. Network and application anomalies came in second, with 23% of organizations experiencing such cyber attacks, followed by system anomalies (20%).
- With a strategy of protecting IT processes and systems, protecting critical customer data, and complying with government regulations, public and private banking institutions are focused on implementing the latest technologies to prevent cyberattacks. In addition, rising customer expectations, technological advances, and regulatory requirements require banking institutions to take a proactive approach to security. With the increasing penetration of technology and digital channels, such as internet banking and mobile banking, online banking has become a favorite choice for customers of banking services. Banks must use advanced authentication and access control processes, including threat intelligence strategies.
- For instance, in February 2022, the Department of Justice (DoJ) and Bankers Association of the Philippines (BAP) signed a memorandum of understanding (MoU) to raise cybersecurity awareness and combat cybercrime in the Philippines. The BAP aims to strengthen the banking industry's cyber-resilience and develop a collaborative partnership with the Justice Department to achieve a coordinated, collective, and strategic cyber response through information sharing and collaboration in the wake of rising cybercrime incidents in the country.
- In January 2022, the federal banking regulators of the United States issued a cybersecurity rule requiring prompt notification of a breach. The proposed rule is poised to warn the agencies early of considerable computer security incidents. It would need information as soon as possible and by 36 hours after a banking enterprise determines that an incident has occurred. Such regulations could control cyber attacks in the banking sector of the United States.

North America to Hold the Largest Market Share

- The BFSI sector in the United States has more than 1 exabyte of stored data. These data are generated from various sources, such as credit/debit card histories, customer bank visits, banking volumes, call logs, account transactions, and web interactions.
- Due to the high availability of adequate infrastructure, numerous global financial institutions increased the adoption of IoT devices, and internet users are expected to drive the growth of threat intelligence solutions in the North American region.
- Government entities and private players across regions invest in R&D to introduce advanced threat intelligence solutions. The US Department of Homeland Security (DHS) Cybersecurity and the Infrastructure Security Agency (CISA) mentioned that they

experienced a massive rise in phishing and malware distribution using COVID-19-themed lures, registration of new domain names containing wording related to coronavirus or COVID-19, and attacks against newly and rapidly deployed remote access and teleworking infrastructure.
- Additionally, organizations are focusing on testing security strategies and practices. For instance, according to a survey conducted by Accenture in February 2022, its cyber threat intelligence and incident response team has investigated several suspected cyber-spy and financially motivated targeting cases. During these investigations, threat intelligence and incident response analysts gained first-hand insight into the tactics, techniques, and procedures (TTP) employed by some of the most sophisticated cyber attackers. The survey revealed that intrusions made by ransomware and extortion were up to 35%, and 30% were malware threats in 2021.
- Investments in threat intelligence solutions are essential for strengthening the security posture of a country. Implementing threat intelligence solutions will help organizations provide smooth and secure operations across North America.

Threat Intelligence Industry Overview

The threat intelligence market is dominated by a few major players, with more secure software solutions being launched. Dell Inc., IBM Corporation, Anomali Inc., Fortinet Inc., and CrowdStrike Inc. are key players in the market that offer dedicated solutions for threat intelligence.

- February 2022 - IBM announced the acquisition of Neudesic, a US cloud services consultancy. This acquisition will further help the company significantly expand its hybrid multi-cloud services portfolio and enhance its hybrid cloud and AI strategy solutions.
- March 2022 - Fortinet announced a partnership with five new service providers - Etihad Atheeb Telecom Company 'GO,' Microland, Radius Telecoms Inc., Spectrotel, and TIME dotcom. This partnership may deliver a simplified network architecture with enhanced security, all powered by a single operating system to achieve operational effectiveness everywhere, from the data center to multi-cloud environments to SaaS locations.

Additional Benefits:

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

Table of Contents:

SCOTTS INTERNATIONAL

Threat Intelligence - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 220 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	2026-03-01
		Signature