US Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 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:

The US Cybersecurity Market size is estimated at USD 85.79 billion in 2024, and is expected to reach USD 126.57 billion by 2029, growing at a CAGR of 8.09% during the forecast period (2024-2029).

The difficulty of protecting against a persistent information security breach is one that businesses in all industries in the United States are currently confronting. To fight against incoming threats and safeguard sensitive data, security experts are expected to keep ahead of dangers and use technologies, policies, and processes. Additionally, enterprises need to be able to swiftly and securely modify their core business applications across on-premise, SDN, and cloud environments as they speed up their digital transformation activities. This means that to manage these operations, IT and security teams need to have a complete awareness of fine-grained control over their whole network architecture.

Key Highlights
-The market's expansion might be ascribed to the sophistication of cyberattacks, which is rising. Over the past ten years, the number and severity of cybercrimes and scams have escalated, causing enormous losses for enterprises. As cybercrimes have dramatically escalated, businesses have focused their expenditure on information security solutions to bolster their internal security infrastructures. The use of targeted assaults, which penetrate targets' network infrastructure while remaining anonymous, has increased recently. Endpoints, networks, on-premises devices, cloud-based apps, data, and numerous other IT infrastructures are frequently targeted by attackers who have a specific target.
-For instance, in March 2021, Hackers targeted four security flaws in Microsoft Exchange Server email software; they used the bugs on the Exchange servers to access email accounts of at least 30,000 organizations across the United States, which included small businesses, towns, cities, and local governments. The attack allowed the hackers to remotely control the affected systems, allowing them access to potential data theft and further compromise.

-Following a public call asking government agencies in the region to join forces with the private sector and academia to ensure that medical facilities are protected from cyber threats. Various collaborations have been taking place in the industry. For instance, in March 2022, Senators of the United States Parliament introduced Healthcare Cybersecurity Act. The Act aims to promote collaboration between Cybersecurity and Infrastructure Security Agency (CISA) and HHS to enhance cybersecurity efforts across the healthcare and public health sector.
-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 provide the agencies with an early warning of considerable computer security incidents. It would need notification as soon as possible and no later than 36 hours after a banking enterprise determines that an incident has occurred. Such regulations could control the cyber attacks in the banking sector of the United States.
-According to the US Department of Homeland Security (DHS) Cybersecurity, there has been a sharp increase in phishing and malware distribution using COVID-19-themed lures, the registration of new domain names containing words related to coronavirus or COVID-19, and attacks against recently and swiftly deployed remote access and teleworking infrastructure. As businesses prepare to implement months-long business continuity plans (BCP), including information security monitoring and response while working under quarantine circumstances, focusing on increasing cybersecurity, the pandemic has further expedited the need for cybersecurity.

US Cybersecurity Market Trends

Need For Identity Access Management is One of the Factor Driving the Market

- With the rapid digitalization across the country, digital identity has become crucial to enforcing access controls. As a result, identity and access management (IAM) has become a significant priority for modern enterprises.
- The United States has one of the highest digital penetration rates globally, with many users and organizations depending upon IoT devices and computing solutions. Organizations all over the US increasingly depend on computer networks, smart devices, and electronic data to conduct their daily operations, which has led to growing pools of personal and financial information transferred and stored online. Hence, the need for identity and access management solutions increased over time.
- IAM, viewed as an operational back-office issue, is now gaining board-level visibility following several high-level breaches that have occurred due to the failure of organizations to manage and control user access effectively. The prominence of IAM has been further elevated by an evolving regulatory landscape and trends, such as Bring your Device (BYOD) and cloud adoption. The risks related to accessing information and data have also increased significantly.
- According to the Federal Trade Commission, the prevalence of identity thefts in the banking and payment industries in the United States would encourage more people to use biometric solutions. Financial institutions like TD Bank that operate in the United States are reportedly focusing on digital identity verification solutions to strengthen the customer onboarding processes, with a significant contribution to verifying the CIP and KYC procedures, according to Pymnts' release of the Digital Identity Tracker Report in March 2022. The software solutions are expected to gain more traction as financial institutions nationwide examine implementing various identity verification tools.
- The impact of an identity management cybersecurity breach by organized crime, state-sponsored militaries, and others is packed with implications that can impact staff productivity and morale, apart from substantial financial and potential life losses and further damage to the IT network and company reputation. These risks demand a new level of identity and access management solutions.

BFSI Segment Is Boosting The Cybersecurity Market Growth

- 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 a plethora of diabolical cyberattacks to immobilize the financial sector. These attacks' threat landscape ranges from Trojans, malware, ATM malware, ransomware, mobile banking malware, data breaches, institutional invasion, data thefts, fiscal breaches, etc.
- With a strategy to secure their IT processes and systems, secure customer critical data, and comply with government regulations, public and private banking institutes focus on implementing the latest technology to prevent cyber attacks. Besides, with greater customer expectations, rising technological capabilities, and regulatory requirements, banking institutions are pushed to adopt a proactive security approach. With the growing technological penetration and digital channels, such as Internet banking, mobile banking, etc., online banking has become customers' preferred choice for banking services. There is a significant need for banks to leverage advanced authentication and access control processes.
- The country also marked the increase of ransomware and phishing attacks targeted at organizations that involved less manual effort and were highly automated in 2022. In 2022, financial firms worldwide were impacted by innovative new ransomware tactics that maximized ROI for the threat actors. While financial firms represent a small percentage of victims directly targeted by ransomware attacks, they can and have been impacted by attacks on third parties, who are prime targets. Such threats are poised to increase the usage of cybersecurity solutions in the BFSI sector.
- Moreover, in light of Russia - Ukraine conflict and a virtually endless cycle of threat campaigns and vulnerability disclosures towards the country, the US State Department, on April 2022, launched a new agency, the Bureau of Cyberspace and Digital Policy (CDP), responsible for developing online defense and privacy-protection policies and direction as the Biden administration seeks to integrate cybersecurity into America's foreign relations.

US Cybersecurity Industry Overview

The united states cybersecurity market is moderately consolidated, with the presence of a large number of SME vendors and dominant major companies in the market. The companies are continuously investing in making strategic partnerships and product developments to gain more market share. Some of the recent developments in the market are:

- May 2022 - Google plans to acquire Mandiant, a United States-based cybersecurity firm. Post-acquisition the company will most likely join Google's cloud computing division. The move to acquire Mandiant stems from Google's plan to strengthen its cybersecurity footprint and create a robust portfolio compared to its competitors in the market.
- May 2022: Cisco Systems Inc. announced that, it has released the Cisco Cloud Controls Framework (CCF) to the public. Cisco CCF is a comprehensive set of national and international security compliance and certification requirements, aggregated in one framework.

Additional Benefits:

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

Table of Contents:

US Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

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