North America Security Testing - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 100 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 North America Security Testing Market size is estimated at USD 4.05 billion in 2025, and is expected to reach USD 10.76 billion by 2030, at a CAGR of 21.58% during the forecast period (2025-2030).

North America is a highly regulated region globally with numerous regulations and compliances, such as the Federal Energy Regulatory Commission (FERC), HIPAA, PCI DSS, and SOX, across verticals. North American companies are quite advanced at deploying security, penetration testing, and vulnerability management solutions and have best practices for everyday business processes, thereby driving the adoption of penetration testing solutions.

Key Highlights
- The North American region is a technology hub. Therefore, the federal government has made very stringent rules regarding security testing services. Moreover, it is compulsory for industries, such as BFSI, to adhere to compliance testing.
- The increasing need for safety from security threats is driving the growth of the security testing market. The combination of digital transformation initiatives, cloud computing, IoT, and regulatory requirements has created a demand for comprehensive security testing services to help organizations identify and address vulnerabilities in their systems, applications, and digital infrastructure.
- Government regulations play a significant role in driving the security testing market. Governments in North America have recognized the importance of cybersecurity and have introduced regulations and standards to ensure the protection of sensitive data, critical infrastructure, and citizen privacy.
- Organizations unaware of the benefits of security testing may be less likely to adopt such practices. They might need to pay more attention to the importance of proactive security measures and rely solely on reactive measures like incident response and recovery. This limited adoption of security testing can hinder the growth of the market.

- With the widespread COVID-19, the adoption of remote work, securing remote access to corporate networks and resources became a top priority. Organizations invested in security testing to assess the security of their remote access infrastructure, including virtual private networks (VPNs), remote desktop protocols, and other remote connectivity solutions. Security testing helped identify vulnerabilities in these systems and ensured that remote access was adequately protected.

North America Security Testing Market Trends

Healthcare End User Industry Segment is Expected to Hold Significant Market Share

- Security testing is crucial in healthcare end-user systems by protecting sensitive patient data, maintaining regulatory compliance, and preventing potential security breaches. Security testing in healthcare end-user systems is essential for protecting patient data, maintaining regulatory compliance, preventing unauthorized access, securing medical devices, and mitigating operational risks. By prioritizing security testing, healthcare organizations can ensure their systems' confidentiality, integrity, and availability and provide patients with safer and more secure healthcare services.
- Healthcare systems handle many sensitive patient information, including medical records, personal details, and financial data. Security testing helps identify vulnerabilities and weaknesses in the software and infrastructure that could expose this data to unauthorized access or breaches. By proactively testing and addressing these security gaps, healthcare organizations can safeguard patient data and maintain confidentiality.
- The healthcare industry is subject to various regulatory requirements, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States. Security testing ensures that healthcare systems comply with these regulations by assessing their security controls, encryption measures, access controls, and other relevant security practices. Meeting these compliance standards helps healthcare organizations avoid penalties and legal issues.
- According to Identity Theft Resource Center, In 2023, there were more than 809 incidents of data compromises in the healthcare sector in the United States. Security testing helps identify vulnerabilities and weaknesses in healthcare systems that attackers could exploit to gain unauthorized access. This includes testing for vulnerabilities such as weak authentication mechanisms, inadequate access controls, or unencrypted communication channels. Healthcare organizations can prevent unauthorized access to patient records, medical devices, or critical systems by addressing these vulnerabilities.
- The healthcare industry relies on various medical devices, including IoT devices and connected systems. Security testing ensures these devices resist potential attacks and vulnerabilities that could compromise patient safety or expose sensitive information. By testing the security of medical devices, organizations can identify weaknesses and work with manufacturers to apply necessary patches or updates.
- Security testing helps identify potential risks and vulnerabilities that could impact the operational continuity of healthcare systems. Organizations can proactively address weaknesses by identifying them and reducing the risk of system downtime, data loss, or disruption of critical healthcare services.

United States is Expected to Hold Significant Market Share

- The security testing market in the United States is rapidly growing due to the increasing awareness of cybersecurity threats and the need for robust security measures across industries.
- The United States has stringent regulations and industry-specific compliance requirements, such as HIPAA for healthcare and PCI DSS for payment card data security. These regulations drive the demand for security testing services as organizations strive to ensure compliance and protect customer data.
- In September 2022, The National Institute of Standards and Technology (NIST) issued Draft Security Recommendations for IoT

Devices in the United States. Because IoT regularly posed a cybersecurity risk through hacks and data breaches, the NIST's Core Baseline highlighted recommended security features for manufacturers to incorporate into their IoT devices and guidelines for consumers to look for on a device's box or online description while shopping.
- According to the US Office of Management and Budget, In 2022, the overall cyber security spending in the United States was projected to increase in 2023, with the total proposed agency cyber security funding for the year approximately USD 10.46 billion.
- With the proliferation of digital transformation initiatives, cloud adoption, and an increasing number of connected devices, the demand for security testing services has grown significantly. Organizations in the United States realize the importance of proactive security measures and are willing to invest in comprehensive security testing solutions.

North America Security Testing Industry Overview

The North American Security Testing Market is highly fragmented with the presence of major players like Hewlett Packard Enterprise Development LP, IBM Corporation, VERACODE, McAfee LLC, and Cisco Systems Inc. Players in the market are adopting strategies such as partnerships and acquisitions to enhance their product offerings and gain sustainable competitive advantage.

In April 2023, Noname Security, one of the significant API security providers, partnered with IBM to protect clients against misconfigurations, vulnerabilities, and design defects. Customers can use Noname Security's API security solution and IBM DataPower's existing enterprise security capabilities to provide an extra layer of protection for IBM API Connect with the new Noname Advanced API Security for IBM. Enterprise users would benefit from enhanced API security, such as discovery, posture management, runtime protection, and security testing, with the Noname API Security Platform.

In September 2022, Cybeats Technologies Inc. ("Cybeats" or the "Company"), one of the leading providers of software supply chain risk and security technologies, announced a strategic partnership with Veracode, one of the global leaders in application security testing solutions.

Additional Benefits:

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

Table of Contents:

North America Security Testing - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 100 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	2026-02-26
		Signature