

North America Cyber Security - 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 North America Cyber Security Market size is estimated at USD 92.31 billion in 2024, and is expected to reach USD 138.87 billion by 2029, growing at a CAGR of 8.51% during the forecast period (2024-2029).

The adoption of cybersecurity solutions is expected to increase with the increasing penetration of the Internet throughout North America. Also, the expanding wireless network catering to mobile devices has enhanced data vulnerability.

Key Highlights

- North America is one of the world's leading digital nations. Over the next few years, technology will bring about significant changes. Robotics, sensor technology, 3D printing, big data, and artificial intelligence are all examples of technological developments that have the potential to change society. As digitization increases, the nation's data security needs to be increased.
- The increasing frequency and sophistication of cyber-attacks are driving the adoption of cybersecurity solutions in North America. Moreover, the growing regulatory requirement leads many organizations to adopt and invest in cybersecurity solutions, as many industries in the United States are subject to regulations such as HIPPA, GDPR, and PCI DSS, which require the organization to implement.
- Ransomware and DDoS attacks are expected to increase further during the forecast period and, even more, targeted against large organizations in regions where the adoption rate is not as quick for cybersecurity solutions. Also, ransomware-as-a-service offerings and their construction kits have been estimated to fuel this increase, particularly as an easy tool for novice or low-skilled criminals.
- The rising usage of new service platforms, such as online and cloud computing, results in less transparent solutions, making it more difficult for users to assess risk and vulnerability and document their security.

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

-The COVID-19 pandemic emphasized the necessity for increased digital security. People increased their Internet access to maintain personal and professional work. On the other hand, hackers have taken advantage of the situation, focusing on e-commerce, e-payment businesses, and the healthcare system.

North America Cyber Security Market Trends

Aerospace, Defense, and Intelligence Industry to Drive the Market Growth

- The region invests heavily in cybersecurity solutions to avoid intellectual property theft and compromise systems that monitor and control the country's defense systems and capabilities. To keep pace with modern defense advancements, countries like the United States have developed new technologies, such as unmanned vehicles, hypersonic weapons, etc. These advancements depend highly on data and connectivity, making them susceptible to breaches and attacks. Thus, there is a growing necessity for the region to focus on developing countermeasures to safeguard critical information.
- The US Aerospace Industries Association focused on promoting policies strengthening the aerospace and defense industry. Defense companies, such as BAE Systems PLC, General Dynamics Corporation, and Finmeccanica SpA, are engaged in developing cybersecurity solutions in the defense industry, especially in developing network security solutions and software, preventing cyber-attacks on military software systems, indicating the demand for these solutions in the aerospace and defense sector.
- The Canadian Centre for Cyber Security (CCCS) was aware of over a thousand malicious impersonations of Government of Canada (GC) websites employing COVID-19-themed lures as of April 27, 2021, and provided information to initiate their elimination. The majority of these cybercriminals targeted the Canada Revenue Agency (CRA) and the Canadian Emergency Response Benefit (CERB).
- Moreover, the Canadian Government is taking initiatives in collaboration with the Canadian military and North American Aerospace Defence Command (Norad) to identify and mitigate cyber threats to critical civilian sites. The critical sites, like power grids, water treatment plants, or traffic systems, are especially focused on preventing attacks that could shut down civilian infrastructure.

United States to Hold Significant Market Share

- The country is strategically positioned to combat cybersecurity threats with key players like Symantec, Intel Security, IBM Security, and Dell EMC based in the country, along with the support of start-ups playing a major role in cyberspace. With a focus on innovations and multiple strategic partnerships, the studied market in the United States has become one of the prominent industries in the technological space.
- For the fiscal year 2023, the government of the United States proposed a USD 10.89 billion budget for cyber security, representing an increase from the previous fiscal year. These federal resources for cyber security are set to support a broad-based cyber security strategy for securing the government and enhancing the security of critical infrastructure and essential technologies.
- According to the world economic forum's Global Security Outlook 2022 report, Ransomware attacks saw a significant boost in the first six months of 2021, with global attack volume increasing by 151%. The United States Federal Bureau of Investigation (FBI) has warned that 100 different ransomware strains are circulating globally.
- Moreover, in light of the Russia - Ukraine conflict and a virtually endless cycle of threat campaigns and vulnerability disclosures towards the country, the US State Department, in 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. The bureau, supervised by a cyber ambassador confirmed in the Senate,

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

opened the door when physical war could flow into cyber warfare anytime.

- Increased investments in the industry mark the country for cybersecurity solutions and cyber threat detecting software. With the increased awareness amongst companies from small to large enterprises, US companies are deploying more rigid solutions to protect data and installing fraud and threat detection programs to find risks at an earlier stage to respond at an earlier stage driving the injection of funds into the industry. For instance, In June 2021, Horizon3.ai, a cybersecurity company based in California, raised an investment of USD 5 million in the Series A round of investment led by SignalFire.

North America Cyber Security Industry Overview

The North America cybersecurity market is fairly consolidated as it comprises several global and regional players. The key players are focusing on innovation in production technologies to improve efficiency. Moreover, players adopt strategic initiatives such as partnerships, mergers, and acquisitions.

In March 2022, Google Cloud announced it was acquiring cybersecurity firm Mandiant, a player in proactive SaaS-based security. The acquisition underscores the importance of security for all businesses, regardless of scale, as cybercrime is increasingly affecting all companies in the nation. The acquisition is all cash, valuing Mandiant at USD 23 per share in a deal worth USD 5.4 Billion. Mandiant will become a part of Google Cloud once the deal receives requisite stockholder and regulatory approvals.

In March 2022, HelpSystems declared that it had signed a merger agreement to acquire AlertLogic, a player in managed detection and response (MDR) services. The company's MDR solutions focus on reducing the intense pressure faced by organizations due to the increase in cyberattacks and the significant shortage of skilled professionals available to prevent and repair cyberattacks. Alert Logic will be the basis of HelpSystems' cybersecurity portfolio.

Additional Benefits:

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

Table of Contents:

1 INTRODUCTION

- 1.1 Study Assumptions and Market Definition
- 1.2 Scope of the Study

2 RESEARCH METHODOLOGY

3 EXECUTIVE SUMMARY

4 MARKET INSIGHTS

- 4.1 Market Overview
- 4.2 Industry Value Chain Analysis
- 4.3 Industry Attractiveness - Porter's Five Forces Analysis
 - 4.3.1 Bargaining Power of Suppliers
 - 4.3.2 Bargaining Power of Consumers
 - 4.3.3 Threat of New Entrants
 - 4.3.4 Competitive Rivalry within the Industry
 - 4.3.5 Threat of Substitute

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

4.4 Industry Guidelines and Policies

4.5 Assessment of Impact of COVID-19 on the Industry

5 MARKET DYNAMICS

5.1 Market Drivers

5.1.1 Rapidly Increasing Cybersecurity Incidents and Regulations Requiring Their Reporting

5.1.2 Growing M2M/IoT Connections Demanding Strengthened Cybersecurity in Enterprises

5.2 Market Restraints

5.2.1 Lack of Cybersecurity Professionals

5.2.2 High Reliance on Traditional Authentication Methods and Low Preparedness

5.3 Market Opportunities

5.3.1 Rise in the Trends of IoT, BYOD, Artificial Intelligence, and Machine Learning In Cybersecurity

6 MARKET SEGMENTATION

6.1 By Product Type

6.1.1 Solutions

6.1.1.1 Identity and Access Management

6.1.1.2 Threat Detection and Prevention (Unified Threat Management and Threat Mitigation)

6.1.1.3 Security and Vulnerability Management

6.1.1.4 Next Generation Firewall

6.1.1.5 IDS/IPS?

6.1.1.6 Security Information and Event Management

6.1.1.7 DDOS Mitigation

6.1.1.8 Other Solution Types

6.1.2 Services

6.2 By Deployment

6.2.1 On-cloud

6.2.2 On-premise

6.3 By End-user Industry

6.3.1 Aerospace, Defense, and Intelligence

6.3.2 Banking, Financial Services, and Insurance

6.3.3 Healthcare

6.3.4 Manufacturing

6.3.5 Retail

6.3.6 Public Utility

6.3.7 IT and Telecommunication

6.3.8 Other End-user Industries

6.4 By Country

6.4.1 United States

6.4.2 Canada

7 COMPETITIVE LANDSCAPE

7.1 Vendor market Share Analysis

7.2 Company Profiles

7.2.1 Cisco Systems Inc.

7.2.2 Cyber Ark Software Ltd

7.2.3 Dell Technologies Inc.

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

- 7.2.4 FireEye Inc.
- 7.2.5 IBM Corporation
- 7.2.6 Fortinet Inc.
- 7.2.7 Imperva Inc.
- 7.2.8 Intel Security (Intel Corporation)
- 7.2.9 Palo Alto Networks Inc.
- 7.2.10 Proofpoint Inc.
- 7.2.11 Rapid7 Inc.
- 7.2.12 Symantec Corporation

8 INVESTMENT ANALYSIS

9 FUTURE OF THE MARKET

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

**North America Cyber Security - 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*	<input type="text"/>	Phone*	<input type="text"/>
First Name*	<input type="text"/>	Last Name*	<input type="text"/>
Job title*	<input type="text"/>		
Company Name*	<input type="text"/>	EU Vat / Tax ID / NIP number*	<input type="text"/>
Address*	<input type="text"/>	City*	<input type="text"/>
Zip Code*	<input type="text"/>	Country*	<input type="text"/>
		Date	<input type="text" value="2026-03-02"/>
		Signature	

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com



Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com