

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

Market Report | 2025-06-01 | 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:

North America Cyber Security Market Analysis

The North America Cyber Security Market size is estimated at USD 95.75 billion in 2025, and is expected to reach USD 159.90 billion by 2030, at a CAGR of 10.80% during the forecast period (2025-2030). Stringent federal and state regulations, the spread of sophisticated threats, and accelerated digital-transformation programs across critical industries are the primary growth engines. Mandatory breach-disclosure laws in all 50 U.S. states and new Securities and Exchange Commission reporting rules compel firms to invest in preventive controls instead of purely reactive incident response models. Spending is further fueled by the federal transition to post-quantum cryptography, which requires agencies and contractors to overhaul encryption systems by 2030-2035. The United States retains the lion's share of regional demand, yet Canada registers the fastest expansion as Bill C-26 tightens critical-system requirements and stimulates vendor activity. Across offerings, solutions still represent 65.5% of revenue, although managed and professional services are growing faster as enterprises outsource security operations to close skills gaps.

North America Cyber Security Market Trends and Insights

Mandatory Breach Disclosure Laws and Surging Attack Volumes

Regulatory scrutiny intensified when the SEC levied USD 7 million in penalties on four listed technology companies for deficient SolarWinds-related disclosures, underscoring that incomplete cyber-risk reporting now carries tangible financial consequences. Coupled with 583 enforcement actions and USD 8.2 billion in remedies during fiscal 2024, the climate pushes boards to treat

Scotts International. EU Vat number: PL 6772247784

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

www.scott-international.com

cybersecurity as a core compliance function rather than a discretionary IT spend. At the same time, Mexico logged 42.4 million malware attempts in 2024-116,000 per day-reflecting the wider regional surge in threat volume that now hits manufacturing hardest. Because every U.S. state enforces a notification statute and federal rules require disclosure within four business days of a material incident, enterprises have shifted budgets toward continuous monitoring, automated detection, and breach-containment platforms that shorten response cycles and cap liability.

Cloud Migration and Zero-Trust Adoption Momentum

Zero-trust models replaced perimeter-centric strategies once federal Executive Orders and NIST SP 800-207 established identity-focused architectures as the public-sector default. Today, 60% of North American enterprises have an active zero-trust program, and 94% have deployed at least one element; the transition is inseparable from sustained cloud-adoption waves that re-shape network edges and authentication flows. Organizations implementing zero-trust within hybrid or multi-cloud environments report 152% ROI through diminished incident handling and policy-maintenance burdens, a finding that resonates with finance and healthcare entities balancing regulatory mandates with cost discipline. The confluence of cloud migration and zero-trust tooling propels demand for secure access service edge (SASE) and identity-and-access-management platforms, reinforcing a structural service opportunity for MSSPs that specialize in multi-cloud governance.

Acute Shortage of Skilled Cyber-Security Professionals

North America entered 2025 with 542,687 open cybersecurity positions, a 4% increase even after employer headcount cuts of 2.7% in 2024. Budget freezes struck 37% of firms, but 90% still reported material skill gaps, particularly in AI-enabled analytics and zero-trust configuration. Mexico alone needs 35,000 specialists by 2025, yet 65% of local organizations cite talent scarcity as their top barrier, triggering an 80% uptick in advanced-technology spending to compensate. Skills shortages expose enterprises to prolonged dwell times, and breaches blamed on understaffed teams averaged USD 4 million in direct losses, adding pressure to adopt managed detection and response services that wrap technology and expertise in subscription packages.

Other drivers and restraints analyzed in the detailed report include:

Explosion of IoT/IIoT Endpoints Across Industry / U.S. Federal Post-Quantum Cryptography Transition Deadlines / Legacy OT Systems Expanding Unmanaged Attack Surface /

For complete list of drivers and restraints, kindly check the Table Of Contents.

Segment Analysis

Solutions retained a 65.5% share of the North America cybersecurity market in 2024, yet services are on pace for 13.8% CAGR through 2030 as organizations outsource 24/7 monitoring to counter evolving threats. The services uptrend directly mitigates the skills shortage while giving firms rapid access to AI-driven analytics platforms. Professional services for quantum-safe cryptography assessments and zero-trust road-mapping have also risen. Managed detection and response illustrates this shift: eSentire now protects data for 2.5 million patients, underscoring demand in regulated fields.

The North America cybersecurity market size for managed services is expanding fastest among healthcare and mid-market manufacturing firms. Service-based consumption models help firms consolidate sprawling toolsets and secure board approval by treating cybersecurity as an operating expense. Vendors, in turn, bundle AI, threat intelligence, and human expertise, capturing sticky multiyear contracts and boosting recurring revenue visibility.

On-premise deployments still made up 56.2% of the North America cybersecurity market size in 2024, but cloud security spending

Scotts International. EU Vat number: PL 6772247784

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

www.scotts-international.com

is advancing at 17.2% CAGR as hybrid work exposes perimeter-centric gaps. Federal zero-trust mandates, coupled with executive orders on cloud-first strategies, accelerate cloud-native adoption in defense and civil agencies. For private-sector adopters, the pivot lowers capital expenditure, integrates policy orchestration, and enables continuous compliance.

Large enterprises operate hybrid models for data-sovereignty reasons, while SMEs leapfrog straight to fully managed cloud-security service edges. Oracle's framework for zero-trust cloud controls demonstrates how identity governance, micro-segmentation, and encryption converge to tighten attack surfaces. Vendors that automate policy creation and misconfiguration remediation find traction as multicloud complexity scales.

North America Cyber Security Market is Segmented by Offering (Solutions and Services), Deployment Mode (Cloud and On-Premise), Organization Size (Small and Medium Enterprises and Large Enterprises), End-User (BFSI, Healthcare, IT and Telecom, and More), and Country. The Market Forecasts are Provided in Terms of Value (USD).

List of Companies Covered in this Report:

Palo Alto Networks, Inc. / Fortinet, Inc. / CrowdStrike Holdings, Inc. / Cisco Systems, Inc. / Check Point Software Technologies Ltd. / Zscaler, Inc. / Okta, Inc. / Cloudflare, Inc. / SentinelOne, Inc. / Tenable Holdings, Inc. / Rapid7, Inc. / Qualys, Inc. / Proofpoint, Inc. / Trend Micro Incorporated / Sophos Group plc / CyberArk Software Ltd. / Imperva, Inc. / F5, Inc. / Forcepoint LLC / Darktrace plc / Bitdefender LLC / Varonis Systems, Inc. / Arctic Wolf Networks, Inc. / Elastic N.V. / Mandiant (Google Cloud) /

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 LANDSCAPE

4.1 Market Overview

4.2 Market Drivers

4.2.1 Mandatory breach/disclosure laws and surging attack volumes

4.2.2 Cloud migration and zero-trust adoption momentum

4.2.3 Explosion of IoT/IIoT endpoints across industry

4.2.4 U.S. federal post-quantum cryptography transition deadlines

4.2.5 Cyber-insurance underwriting tying premiums to controls

4.2.6 AI-powered SecOps platforms cutting mean-time-to-respond

4.3 Market Restraints

4.3.1 Acute shortage of skilled cyber-security professionals

4.3.2 High cost and complexity of multi-vendor tool stacks

4.3.3 Legacy OT systems expanding unmanaged attack surface

Scotts International. EU Vat number: PL 6772247784

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

www.scotts-international.com

- 4.3.4 Energy footprint of always-on analytics limiting adoption
- 4.4 Industry Value Chain Analysis
- 4.5 Regulatory Landscape
- 4.6 Technological Outlook
- 4.7 Industry Attractiveness - Porter's Five Forces Analysis
 - 4.7.1 Threat of New Entrants
 - 4.7.2 Bargaining Power of Suppliers
 - 4.7.3 Bargaining Power of Buyers
 - 4.7.4 Threat of Substitutes
 - 4.7.5 Intensity of Competitive Rivalry
- 4.8 Impact of Macroeconomic Factors on the Market

5 MARKET SIZE AND GROWTH FORECASTS (VALUES)

- 5.1 By Offering
 - 5.1.1 Solutions
 - 5.1.1.1 Application Security
 - 5.1.1.2 Cloud Security
 - 5.1.1.3 Data Security
 - 5.1.1.4 Identity and Access Management
 - 5.1.1.5 Infrastructure Protection
 - 5.1.1.6 Integrated Risk Management
 - 5.1.1.7 Network Security Equipment
 - 5.1.1.8 Endpoint Security
 - 5.1.1.9 Other Solutions
 - 5.1.2 Services
 - 5.1.2.1 Professional Services
 - 5.1.2.2 Managed Services
- 5.2 By Deployment Mode
 - 5.2.1 Cloud
 - 5.2.2 On-Premise
- 5.3 By Organization Size
 - 5.3.1 Small and Medium Enterprises (SMEs)
 - 5.3.2 Large Enterprises
- 5.4 By End-user
 - 5.4.1 BFSI
 - 5.4.2 Healthcare
 - 5.4.3 IT and Telecom
 - 5.4.4 Industrial and Defense
 - 5.4.5 Retail
 - 5.4.6 Energy and Utilities
 - 5.4.7 Manufacturing
 - 5.4.8 Other End-users
- 5.5 By Country
 - 5.5.1 United States
 - 5.5.2 Canada
 - 5.5.3 Mexico

Scotts International. EU Vat number: PL 6772247784

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

www.scotts-international.com

6 COMPETITIVE LANDSCAPE

6.1 Market Concentration

6.2 Strategic Moves

6.3 Market Share Analysis

6.4 Company Profiles (includes Global level Overview, Market level overview, Core Segments, Financials as available, Strategic Information, Market Rank/Share for key companies, Products and Services, and Recent Developments)

6.4.1 Palo Alto Networks, Inc.

6.4.2 Fortinet, Inc.

6.4.3 CrowdStrike Holdings, Inc.

6.4.4 Cisco Systems, Inc.

6.4.5 Check Point Software Technologies Ltd.

6.4.6 Zscaler, Inc.

6.4.7 Okta, Inc.

6.4.8 Cloudflare, Inc.

6.4.9 SentinelOne, Inc.

6.4.10 Tenable Holdings, Inc.

6.4.11 Rapid7, Inc.

6.4.12 Qualys, Inc.

6.4.13 Proofpoint, Inc.

6.4.14 Trend Micro Incorporated

6.4.15 Sophos Group plc

6.4.16 CyberArk Software Ltd.

6.4.17 Imperva, Inc.

6.4.18 F5, Inc.

6.4.19 Forcepoint LLC

6.4.20 Darktrace plc

6.4.21 Bitdefender LLC

6.4.22 Varonis Systems, Inc.

6.4.23 Arctic Wolf Networks, Inc.

6.4.24 Elastic N.V.

6.4.25 Mandiant (Google Cloud)

7 INVESTMENT ANALYSIS

8 MARKET OPPORTUNITIES AND FUTURE TRENDS

8.1 White-Space and Unmet-Need Assessment

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 (2025 - 2030)**

Market Report | 2025-06-01 | 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="2026-02-27"/>
		Signature	

Scotts International. EU Vat number: PL 6772247784

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

www.scotts-international.com

