Latin America Cybersecurity - 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 Latin America Cybersecurity Market size is estimated at USD 9.54 billion in 2025, and is expected to reach USD 13.35 billion by 2030, at a CAGR of 6.95% during the forecast period (2025-2030).

The region's expanding digital penetration, reinforced by internet usage and mobile development, drives demand for cybersecurity, but digital transformation is unattainable unless cybersecurity is prioritized. Rapid digitalization and extensive use of digital technology drive Latin American cybersecurity adoption.

Key Highlights
- Latin American emerging markets are the most exposed to hackers and breaches because they are still confronting cybersecurity. As things stand, Latin America requires a more strong cybersecurity basis in order to defend the future of its firms. In Latin America, cybercrime has manifested mostly through computer hacking strategies such as malware, phishing, and denial of service (DoS) attacks.
- Furthermore, the region's rising consumer bias towards mobile payments is driving up the need for application security as application-based payments become more widespread and investment in creating payment apps increases.
- The key drivers of the Latin American cybersecurity industry have been the use of new technologies such as the IoT, Big Data, and cognitive intelligence, as well as the acceptance of cloud-managed services. Cloud providers will exert more control over data centers, and companies will rely more on the public cloud during the epidemic to take advantage of its flexibility and scalability.
- The area needs more professionals with skill sets that benefit the cybersecurity sector. According to an Inter-American Bank and Organisation of American States assessment, the Latin American and Caribbean (LAC) area needs to be better equipped to deal with cyberattacks.
- COVID-19 has heightened the need for cybersecurity as businesses prepare to implement months-long business continuity plans

(BCP), including information security monitoring and response while working under quarantine circumstances to boost cybersecurity.

Latin America Cyber Security Market Trends

Growing M2M/IoT Connections Demanding Strengthened Cybersecurity in Enterprises

- The usage of cybersecurity solutions is likely to increase as internet access increases across Latin American countries. Furthermore, the expanding wireless network for mobile devices has increased data susceptibility, making cybersecurity a critical component of any Latin American organisation.
- IoT is increasingly being employed as part of a bigger corporate transformation plan in Latin America. Furthermore, in certain areas, like Brazil, the pressure to implement IoT solutions as part of digital transformation programmes is developing quickly.
- The IoT is a new wave of technological transformation that is upending Latin American industry. Companies and governments alike are investing in IoT solutions; the number of IoT connections in the area is estimated to reach 1,200 million by 2025, according to GSMA Intelligence.
- Across the area, industries are eager to invest in IoT and Industry 4.0 technologies. Agroindustrial Laredo, a sugar mill, for example, was an early adopter of M2M technologies. The firm collaborated with IoT supplier AZLogica to create an IoT solution for optimising harvesting logistics. The use of IoT resulted in a tenfold return on investment, a 16% reduction in fuel usage, and timely product delivery. As a result of such advancements, organisations in the area are aiming to implement IoT, driving up demand for security solutions.

Brazil to Witness the Growth

- The cybersecurity market. Brazil, Argentina, and Mexico have formed. To counteract cyber-attacks Cyber Emergency Response Teams and Computer Security Incident, Response Teams will be required, with demand expected to grow throughout the projected period.
- Brazilian businesses aggressively invest in cybersecurity solutions and services to secure corporate systems in danger during the epidemic and comply with new data protection rules. This tendency has also prompted fresh investments in the country's cybersecurity business.
- Brazil is the most significant revenue-generating country in the Latin American cybersecurity industry, thanks to the country's expanding digital revolution. Recent regulatory changes like the new General Data Protection Regulation (GDPR) and 5G will likely drive business investment.
- Furthermore, the government provides several commercial opportunities for foreign enterprises providing innovative cybersecurity solutions. Brazil's cybersecurity investment is mainly driven by the private sector, including banking and financial services, e-commerce, telecommunications, etc. The government sector accounts for approximately 20% of the Brazilian cybersecurity market.

Latin America Cyber Security Industry Overview

The Latin American cybersecurity market is riddled with major global vendors and smaller regional vendors that cater to various segments of the market, owing to which the competitive space of the market is expected to be high.

- May 2023 - Check Point Software Technologies Ltd has announced the expansion of its check point harmony endpoint protection solution by incorporating vulnerability and automated patch management capabilities. This enhancement addresses the mounting number of cyberattacks that exploit unpatched system vulnerabilities for unauthorized access. To deliver this advanced feature, Check Point has joined forces with Ivanti, integrating Ivanti Patch Management to assess and remediate software vulnerabilities from cloud to edge, into Check Point's Harmony Endpoint protection solution.
- May 2023 - Cyber ark software ltd and Identity Security has announced new products and features across the CyberArk Identity Security Platform, making It is one of the most powerful platforms available. Investments in cloud security and automation and artificial intelligence (AI) breakthroughs throughout the platform make it simpler than ever to apply intelligent privilege controls to all human and non-human identities from a single vendo.

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 Threat of Substitute Products
4.3.5 Intensity of Competitive Rivalry
4.4 Assessment of Impact of COVID-19 on the Market

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

6 MARKET SEGMENTATION
6.1 Security Type
6.1.1 Network Security

6.1.2 Cloud Security
6.1.3 Application Security
6.1.4 End-point Security
6.1.5 Wireless Network Security
6.1.6 Other Types of Security
6.2 Component
6.2.1 Hardware
6.2.2 Solution
6.2.2.1 Threat Intelligence and Response
6.2.2.2 Identity and Access Management
6.2.2.3 Data Loss Prevention
6.2.2.4 Security and Vulnerability Management
6.2.2.5 Intrusion Prevention System
6.2.2.6 Other Solutions
6.2.3 Services
6.2.3.1 Professional Services
6.2.3.2 Managed Services
6.3 Deployment
6.3.1 Cloud
6.3.2 On-premise
6.4 End-user Industry
6.4.1 Banking, Financial Services, and Insurance
6.4.2 Healthcare
6.4.3 Manufacturing
6.4.4 Retail
6.4.5 Government
6.4.6 IT and Telecommunication
6.4.7 Other End-user Industries
6.5 Country
6.5.1 Brazil
6.5.2 Argentina
6.5.3 Mexico
6.5.4 Rest of Latin America

7 COMPETITIVE LANDSCAPE
7.1 Company Profiles*
7.1.1 AVG Technologies
7.1.2 Check Point Software Technologies Ltd
7.1.3 Cisco Systems Inc.
7.1.4 Cyber Ark Software Ltd
7.1.5 Dell Technologies Inc.
7.1.6 FireEye Inc.
7.1.7 Fortinet Inc.
7.1.8 IBM Corporation
7.1.9 Imperva Inc.
7.1.10 Trend Micro Inc.
7.1.11 Intel Corporation

7.1.12 Symantec Corporation (Broadcom Inc.)

8 INVESTMENT ANALYSIS

9 MARKET OPPORTUNITIES AND FUTURE TRENDS

Latin America Cybersecurity - 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	2025-05-07
		Signature	