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

Market Report | 2024-02-17 | 102 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 Africa Cybersecurity Market size is estimated at USD 0.6 billion in 2024, and is expected to reach USD 1.14 billion by 2029, growing at a CAGR of 13.5% during the forecast period (2024-2029).

The growing digitalization primarily drives the African cybersecurity market; cyber attackers are inventing new ways to conduct cyberattacks; such factors are expected to boost the demand for cybersecurity solutions in the region.

Key Highlights
-Cybersecurity is primarily concerned with preventing unauthorized access to computers, networks, programs, and data. The importance of cybersecurity has recently grown as organizations, governments, and individuals collect, store, and send huge volumes of confidential information and data across networks.
-The rising focus of governments on improving regulations and compliance requirements is one of the primary factors that has aided the growth of the African cybersecurity industry. Aside from that, issues such as the requirement for unified cyber solutions, rising internet subscriptions, data disclosure mandates, greater workplace mobility, and increased spending patterns on security forums are driving the demand for cyber security solutions.
-The security of critical intellectual property and business information in digital form against theft and misuse is a crucial issue for all enterprises. One of the key concerns cited by African countries is a lack of cyber security infrastructure. Most of the region's prominent organizations, including oil and gas, utilities, and banks, have recently upgraded their cyber security capabilities. However, compared to other regions, the pace at which enterprises install security solutions is relatively modest.
-The market studied is dominated by the major players, such as Dell Technologies Inc., Fortinet, IBM, Cisco Systems, Symantec, Check Point, and many more, that have a strong client base in the market. These players constantly provide increased, and enhanced offerings in the form of individual components and suites delivered on-premises or through the cloud.

-INTERPOL is developing a cybercrime operations desk with UK funding to boost the capacity of 49 African countries to fight cybercrime. This project is expected to provide opportunities to take regular pulse checks on cybercrime in Africa and publish annual threat landscape assessments that underpin operational activities.
-In March 2022, the International credit bureau TransUnion confirmed that it had been a victim of the hack by a third-party criminal called the N4aughtysecTU, based in Brazil. The hackers have claimed to have accessed the personal information of 54 million consumers, amounting to roughly four terabytes of data. United Nations data currently peg that the South African population is 60.6 million people. Such incidents are more threatening to the region and increase the need for cybersecurity solutions across various end-user verticals.
-In January 2022, the country launched a cybersecurity forum called the Cybersecurity digital Alliance to demonstrate how the South African corporate sector is acting against the threat of cybercrime. Further, the forum aims to foster sophisticated security partnerships and cross-sector partnerships that will benefit South Africa, reduce the number of data breaches in the country, and establish cyber resilience.
-With the outbreak of COVID-19, there is a greater need for robust cybersecurity initiatives in the region. The same has resulted in people working from home and opting for contactless, e-payment options to pay for their goods and services. This has opened up opportunities for hackers to hack.

Africa Cybersecurity Market Trends

Growth digitization across the region

- Government digitization initiatives to cut costs and make services transparent and easier to reach citizens have strengthened the adoption of cybersecurity solutions. For instance, in Africa, the EAC has been a driving force in promoting cybersecurity legislation among its member states as a part of its e-government initiatives.
- Under ICT 2030 strategy, the Egyptian government is undertaking a series of investments, capacity building and training programs, digital government services reforms, and infrastructure upgrades. The strategy calls for launching new initiatives to maximize the contribution of the ICT sector to Egypt's economic growth by focusing on capacity building, electronics design and manufacturing, and technology parks. The strategy also includes a plan for the digital transformation of core government services in the following areas: education, healthcare, and government services.
- Moreover, The country has also participated in U.S.-Egypt Partnership for Young Leaders in Cybersecurity (USEP4YLC) is a leadership development program for students and young professionals from Egypt and the U.S. Such efforts to develop the digital dependency of the region will result in strengthened cyber security landscaper in Egypt over the forecast period.
- Africa is gaining momentum in the fourth industrial revolution in terms of technology, innovation, and digital investments. South Africa, Nigeria, Kenya, and other African countries are coordinating digital visions and policies in order to achieve digital transformation and become a digital industrial revolution technological hub.
- Despite the difficult conditions for many African Least Developed Countries (LDCs) to improve their use of technology, some remarkable progress is being achieved across the continent. 2021 was a record year for African digital companies, with approximately USD 2.15 billion USD invested in the sector. According to data from the research organization Disrupt Africa's African Tech Startups Funding Report, this represents a 206% increase above 2020 investment projections.

South Africa is Expected to Witness Significant Growth

- The adoption of technologies across organizations makes them vulnerable primarily to cyber-attacks and data breaches. The increasing instances of data breaches in the country are expected to boost cybersecurity solutions across the country.

- Organizations in the country are investing strategically and systematically in developing digital infrastructure, services, skills, and entrepreneurship. The Development Bank of Southern Africa (DBSA) has a clear objective of financing infrastructure development in the ICT sector. The Bank has developed policies and procedures to ensure that project development is implemented efficiently and sustainably.
- Moreover, in February 2021, TymeBank, a South African digital bank, announced that it had secured an R 1.6 billion (approximately USD 109 million) investment from investors in the U.K. and the Philippines. Other foreign investments also are aiding the region's fight against cybercrime.
- In September 2021, Debt-IN Consultants fell victim to a cyber attack that resulted in a data breach of 1.4 million South Africans. The violations mainly contained information about the customer's name, contact details, salary information, employment, and debt-related data such as payments and balances owned by Debt-IN.
- To overcome these situations, vendors in the market have invested in developing and expanding the adoption of cybersecurity in the country. In May 2021, INTERPOL announced plans to create a cybercrime operations desk team for 49 African countries, including South Africa.
- As part of the IT and telecommunication strategy, The Department's main goal is for all South Africans to have access to digital tools that will enable them to develop and take part in opportunities that will promote inclusivity, employment, and economic transformation in all of cities, towns, and provinces. By the middle of 2021, the Department had completed a plan for the digital economy and was working with various stakeholders to create an implementation strategy.

Africa Cybersecurity Industry Overview

The competitive landscape of the Africa cybersecurity market is highly competitive and remains fragmented, with several global and regional players operating in the market. The evolving needs of the end-user segments are driving the market vendors to offer innovative products. In addition, growing opportunities in the market are attracting new players and investments in the market.

- May 2021 - Kaspersky partnered with DataGroupITto provide the company with access to new markets in Nigeria and Ghana. DataGroupITis an African distributor capable of providing logistical support for the Kaspersky business and essential technical expertise on Kaspersky solutions. Kaspersky signed to give cybersecurity services to Africa House London, starting operations in Africa, and African organizations establishing operations in the UK as part of the agreement.

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 Value Chain Analysis
4.3 Porter's Five Forces Analysis
4.3.1 Threat of New Entrants
4.3.2 Bargaining Power of Buyers
4.3.3 Bargaining Power of Suppliers
4.3.4 Threat of Substitutes
4.3.5 Intensity of Competitive Rivalry
4.4 Impact of Covid-19 on the Market

5 MARKET DYNAMICS
5.1 Market Drivers
5.1.1 Growth digitization across the region
5.1.2 Rapidly Increasing Cybersecurity Incidents and Regulations Requiring Their Reporting
5.2 Market Restraints
5.2.1 Lack of Cybersecurity Professionals
5.2.2 High Reliance on Traditional Authentication Methods and Low Preparednes
5.3 Trends Analysis
5.3.1 Organizations leveraging AI to enhance their cyber security strategy
5.3.2 Exponential growth to be witnessed in cloud security owing to shift toward cloud-based delivery model.

6 MARKET SEGMENTATION
6.1 By Offering
6.1.1 Security Type
6.1.1.1 Cloud Security
6.1.1.2 Data Security
6.1.1.3 Identity Access Management
6.1.1.4 Network Security
6.1.1.5 Consumer Security
6.1.1.6 Infrastructure Protection
6.1.1.7 Other Types
6.1.2 Services
6.2 By Deployment
6.2.1 Cloud
6.2.2 On-premise
6.3 By End User
6.3.1 BFSI
6.3.2 Healthcare
6.3.3 Manufacturing
6.3.4 Government & Defense
6.3.5 IT and Telecommunication
6.3.6 Other End Users
6.4 By Geography
6.4.1 South Africa
6.4.2 Egypt
6.4.3 Morocco

7 COMPETITIVE LANDSCAPE
7.1 Company Profiles
7.1.1 Dell Technologies Inc.
7.1.2 Fortinet, Inc.
7.1.3 Cisco Systems Inc
7.1.4 IBM Corporation
7.1.5 Symantec Corporation
7.1.6 Check Point Software Technologies Ltd.
7.1.7 Trend Micro, Inc.
7.1.8 Kaspersky Labs
7.1.9 AVG TECHNOLOGIES (AVAST SOFTWARE)
7.1.10 DXC Technology

8 INVESTMENT ANALYSIS

9 FUTURE OF THE MARKET

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

Market Report | 2024-02-17 | 102 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	2026-03-04
		Signature	