

## **Cybersecurity Market - Growth, Trends, Covid-19 Impact, and Forecasts (2023 - 2028)**

Market Report | 2023-01-23 | 110 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 global cybersecurity market was valued at USD 150.37 billion in 2021, and it is expected to reach a value of USD 317.02 billion by 2027, registering a CAGR of 13.37% during the forecast period 2022-2027. Cybersecurity protects the network, information, and personal data from cyberattacks. The trends of BYOD, AI, IoT, and machine learning in cybersecurity are rapidly growing. For instance, machine learning offers advantages in outlier detection, which benefits cybersecurity.

#### Key Highlights

The cybersecurity industry ecosystem comprises several regional clusters of cybersecurity firms contributing to global market dynamics. In the current market scenario, the cybersecurity industry operates in three distinct mega-clusters: the San Francisco Bay Area (SFBA), Metropolitan Washington, DC, and Israel.

The three cybersecurity mega-clusters share two essential characteristics. The first is that the startup and high-tech innovation culture is a significant growth driver for all three ecosystems. SFBA and Israel have thriving startup ecosystems with a substantial associated flow of risk capital. They are heavily focused on products, while Washington exhibits a higher proportion of service-based firms (in Washington, only 11% of cybersecurity firms are focused solely on products). The second characteristic is the link between human capital and national security.

Ransomware attacks have ravaged many state and local public sector agencies. In some cases, entire local governments were forced to declare an emergency due to massive leaks of sensitive data and loss of services. For instance, in June 2021, JBS Foods, the world's leading meatpacking enterprise, declared that it had paid a USD 11 million ransom to REvil ransomware threat actors following a cyberattack that forced the company to shut down production at several sites worldwide, including its production facilities in United States, Australia, and Canada.

One of the major causes of growing cyberattacks is the lack of skilled cybersecurity personnel in each industry. The number of experienced cybersecurity professionals, especially in Europe, Asia-Pacific, Latin America, and Middle-East are low compared to

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)

the need for security professionals to handle cyber threats for financial institutes, government organizations, and private sector/industrial businesses.

Due to the ongoing COVID-19 pandemic, countries worldwide have implemented preventive measures. With schools being closed and communities being asked to stay at home, multiple organizations have found a way to enable their employees to work from their homes. This has, thus, resulting in a rise in the adoption of video communication platforms.

## Cybersecurity Market Trends

### Growing M2M/IoT Connections Require Strengthened Cybersecurity in Enterprises

Significant reduction in device costs coupled with emerging business models has been instrumental in increasing the market penetration rates of IoT and, consequently, the number of connected devices, such as connected cars, machines, meters, wearables, and consumer electronics.

Attacks on consumer IoT are prevalent, but the possibility of disruption in manufacturing and similar industries enhances cybersecurity's penetration in the current market dynamics. Further, the emergence of 5G is expected to expedite the use of connected devices in industries already pushing toward Industrial Revolution 4.0.

Industrial Revolution 4.0 aids cellular connectivity throughout the industry through the rise of IoT. Machine-to-machine connections have also been instrumental in driving market traction.

Further, security researchers working in Palo Alto Networks discovered another Mirai malware variant that targeted new IoT vulnerabilities. Researchers from Unit 42, the cybersecurity division of the company, discovered several attacks in February 2021 that leveraged vulnerabilities. In this case, the compromised devices downloaded Mirai malware binaries, which added them to a larger IoT botnet capable of carrying out network attacks on devastating scales. Such vulnerabilities are expected to drive cybersecurity solutions.?

With the increase in the number of devices connected to the internet, the cyber world is expected to witness a rise in the occurrence and emergence of new threats and attacks. The attacks of WannaCry and Petya, which affected over 150 countries across the world, further revealed the vulnerability of IoT devices as end-points, thus, fueling the need for better security for consumer devices that are highly susceptible to cyberattacks.?

### Asia-Pacific Expected to be the Fastest-growing Market

The Asia Pacific is expected to witness the highest market growth for cybersecurity solutions over the forecast period. The presence of several market incumbents and recent security threats in the region are expected to accelerate these solutions further.

Increasing cyberattacks in the country have propelled China to strengthen its defensive capabilities. However, the government is also a major source of origin for cyberattacks in other parts of the world. For instance, Microsoft blamed a Chinese cyber-espionage group for attacks on its mail server software in March 2021. Microsoft's Threat Intelligence Center attributed the attacks with high confidence to Hafnium, a group assessed to be state-sponsored and operating out of China.

Further, in November 2021, Japan and Vietnam signed a cybersecurity agreement as the two Asian nations rapidly stepped up their military ties amid concerns over China's growing assertiveness. In April 2021, Japan stepped up cyber defense cooperation with the United States, Australia, and other partners and participated in a NATO cyberspace exercise. Japan has also held cybersecurity talks with Vietnam, Singapore, and Indonesia. The Japanese Defense Ministry considers cyberattacks to be part of rising security threats from China as it becomes more assertive in the region, a concern shared by the United States and other allies in the region.

**Scotts International. EU Vat number: PL 6772247784**

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

www.scotts-international.com

Moreover, in April 2022, the Indian government issued new directives requiring organizations to report cybersecurity incidents to CERT-IN within six hours, even if those incidents are port or vulnerability scans of computer systems. The requirement was promoted by India's Computer Emergency Response Team (CERT-In), which stated that it had identified specific gaps causing difficulties in security incident analysis and response, and to address them, more aggressive measures needed to be imposed.

## Cybersecurity Market Competitor Analysis

The global cybersecurity market is highly fragmented and competitive, comprising several international and regional players. Innovation can bring about a sustainable, competitive advantage to these firms. New fields, such as Big Data and IoT, are reshaping security trends, and the firm concentration ratio is expected to record higher growth during the forecast period. Key players in the market are AVG Technologies, Cisco Systems Inc., and IBM Corporation.

March 2022 - Mandiant Inc. announced the launch of mWISE, the Mandiant Worldwide Information Security Exchange. mWISE is a dynamic, vendor-neutral cyber security event series that brings together practitioners, executives, and visionaries worldwide to discuss best practices, uncover new and emerging trends, and translate knowledge into collective action to decrease cyber threats.

February 2022 - Check Point Software Technologies Ltd acquired Spectral, a key innovator in developer-first security tools. This acquisition is expected to help the company extend its cloud solutions, Cloud Guard, using developer-first security platforms and provide the broadest range of cloud application security use cases.

### 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 INDUSTRY ECOSYSTEM ANALYSIS

#### 5 MARKET DYNAMICS

##### 5.1 Current Market Scenario and Evolution of Cybersecurity-related Practices

##### 5.2 Market Drivers

###### 5.2.1 Rapidly Increasing Cybersecurity Incidents and Regulations Regarding their Reporting

###### 5.2.2 Growing M2M/IoT Connections' Demand for Strengthened Cybersecurity in Enterprises

##### 5.3 Market Challenges

###### 5.3.1 Lack of Cybersecurity Professionals

###### 5.3.2 High Reliance on Traditional Authentication Methods and Low Preparedness

**Scotts International. EU Vat number: PL 6772247784**

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

www.scotts-international.com

- 5.4 Market Opportunities
- 5.5 Industry Attractiveness - Porter's Five Forces Analysis
  - 5.5.1 Bargaining Power of Suppliers
  - 5.5.2 Bargaining Power of Consumers
  - 5.5.3 Threat of New Entrants
  - 5.5.4 Intensity of Competitive Rivalry
  - 5.5.5 Threat of Substitutes

## 6 ANALYSIS OF MAJOR SECURITY BREACHES AT A GLOBAL AND REGIONAL LEVEL

## 7 IMPACT OF COVID-19 ON THE CYBERSECURITY MARKET

## 8 MARKET SEGMENTATION

- 8.1 By Product Type
  - 8.1.1 Solutions
    - 8.1.1.1 Application Security
    - 8.1.1.2 Cloud Security
    - 8.1.1.3 Consumer Security Software
    - 8.1.1.4 Data Security
    - 8.1.1.5 Identity and Access Management
    - 8.1.1.6 Infrastructure Protection
    - 8.1.1.7 Integrated Risk Management
    - 8.1.1.8 Network Security Equipment
    - 8.1.1.9 Other Solutions
  - 8.1.2 Services
    - 8.1.2.1 Professional
    - 8.1.2.2 Managed
- 8.2 By Deployment
  - 8.2.1 On-premise
  - 8.2.2 Cloud
- 8.3 By End-user Industry
  - 8.3.1 BFSI
  - 8.3.2 Healthcare
  - 8.3.3 Aerospace and Defense
  - 8.3.4 IT and Telecommunication
  - 8.3.5 Government
  - 8.3.6 Retail
  - 8.3.7 Manufacturing
  - 8.3.8 Other End-user Industries
- 8.4 By Geography
  - 8.4.1 North America
  - 8.4.2 Europe
  - 8.4.3 Asia-Pacific
  - 8.4.4 Rest of the World
    - 8.4.4.1 Latin America
    - 8.4.4.2 Middle-East

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)

## 9 VENDOR MARKET SHARE ANALYSIS

### 10 COMPETITIVE LANDSCAPE

#### 10.1 Company Profiles

##### 10.1.1 AVG Technologies

##### 10.1.2 Check Point Software Technologies Ltd

##### 10.1.3 Cisco Systems Inc.

##### 10.1.4 CyberArk Software Ltd

##### 10.1.5 Dell Technologies Inc.

##### 10.1.6 Mandiant Inc.

##### 10.1.7 Fortinet Inc.

##### 10.1.8 IBM Corporation

##### 10.1.9 Imperva Inc.

##### 10.1.10 Intel Security

##### 10.1.11 Palo Alto Networks Inc.

##### 10.1.12 Proofpoint Inc.

##### 10.1.13 Rapid7 Inc.

##### 10.1.14 Nortonlifelock Inc.

##### 10.1.15 Trend Micro Inc.

### 11 INVESTMENT ANALYSIS

### 12 FUTURE OF THE MARKET

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)

**Cybersecurity Market - Growth, Trends, Covid-19 Impact, and Forecasts (2023 - 2028)**

Market Report | 2023-01-23 | 110 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="2026-03-01"/>
		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](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)