

## **Italy Cybersecurity - 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 Italy Cybersecurity Market size is estimated at USD 3.63 billion in 2024, and is expected to reach USD 5.84 billion by 2029, growing at a CAGR of 9.96% during the forecast period (2024-2029).

The Italian government aims to bring a fast broadband connection to market failure areas where commercially-driven investment in internet infrastructure has not developed as expected, which is anticipated to propel the growth of internet users, subsequently boosting the target group for cybercriminals who hope to attack users in the region.

#### Key Highlights

- Remote working led to many attacks on PCs, as cyber criminals shifted their focus to the weakest point in the chain: the endpoint and the employee's PC. The risks associated with cyberattacks pushed larger companies to raise protection levels with tools such as firewalls or virtual private networks (VPN), providing employees with remote access to corporate VPNs and simultaneously augmenting perimeter protection in the country.
- TIM11 and Vodafone, one of the two largest mobile carriers, have already launched their 5G commercial services in some selected cities in Italy, with the remaining three, Wind-Tre, Iliad, and Fastweb, also preparing to do so. Fastweb recently struck a deal with Wind Tre to share 5G frequencies and build a joint proprietary 5G network to reach 90% of the nation by 2026.
- The public digital identity system (Sistema Pubblico di Identita Digitale - SPID) allows citizens to access the public administration's online services with a single digital identity. The Agency for Digital Italy is committed to creating a public administration cloud following the continuing rationalization of national public data centers. Many eGovernment platforms and services have already been implemented.
- According to National Cybersecurity Agency (NCA), Italy will be devoting 1.2% of gross national investment a year to cybersecurity. Italy presented its National Cybersecurity Strategy for 2022/26 and stated to reinforce the government's

**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)

commitment to addressing cyber threats and increasing the resilience of the country to cyber attacks.

-Further, the implementation of EU legislation and actions stemming from the National Framework and the National Cybersecurity Plan is expected to facilitate the market's growth in the region. As part of its Digital Agenda, the Italian government plans to make considerable investments in digital identity protection to increase digital transactions' security levels and ground consumers' trust by protecting citizens' identities. The Cyber Security Unit is an interagency and inter-governmental operational body designed to operate for cybersecurity within Italy's national cyber architecture. It is responsible for preventing and preparing for a national cyber crisis, declaring such a crisis, and coordinating competent responses following the prime minister's decisions.

-According to some studies, in Italy, the total cost for businesses and citizens for cyber-attacks in 2021 will be equal to approximately USD 6,000 billion. Moreover, as specified by the Minister for technological innovation, V. Colao, almost 95% of public administration servers are subject to the risk of cyber-attacks. Furthermore, organizations often consider cybersecurity a cost they can do without rather than an investment. On the contrary, improvements to the IT systems security would imply a lower price compared to the value of the risk of a cyber-attack, with loss of data or the disruption of normal operations.

## Italy Cybersecurity Market Trends

On-Premise deployment segment is expected to register a significant growth in the market

- An on-premise security solution provides businesses with enhanced control over data. These solutions also offer significantly better threat protection as compared to cloud deployments. The availability of necessary expertise among staff and sufficient provision of resources are necessities for deploying on-premise solutions. On-premise web and email security solutions are expected to continue to play a significant role in an enterprise's security infrastructure, owing to the benefits of managing and protecting on-premise assets and on-premise security.

- These types of deployments, being structured in annual or multi-layer plans, eliminate the need for monthly expenses. Furthermore, they can be highly customized to an individual organization's processes and regulatory requirements. Cloud solutions, which are being increasingly adopted, still face the challenge of security concerns, and hence, on-premise solutions will play a significant role in the market.

- However, with increasing technological innovations, the cloud platform would become more secure, allowing enterprises to respond faster to security threats, focusing on mitigating business risks and saving the on-premise infrastructure investment.

- On-premise deployment of cybersecurity services can only be undertaken by firms that have huge funds, as this is an expensive approach. The expenses are primarily due to the need for infrastructure and human resources that will have to be developed exclusively for the firm's needs. The banking and Financial Services sector has been the prime adopters of on-premise solutions primarily to safeguard consumer data.

- The cloud-based solutions are becoming one of the most viable options for various applications since they, to an extent, satisfy the needs of cloud users at a relatively low cost. Although the deployment of cloud-based solutions has increased rapidly over the past few years, the area still lacks behind on-premise systems in some aspects to fully protect the data and applications for users.

BFSI Segment to hold significant share in the market

- The BFSI industry is one of the critical infrastructure segments that face multiple data breaches and cyber-attacks, owing to the massive customer base that the sector serves and the financial information that is at stake. Being a highly lucrative operation model that has phenomenal returns along with the added upside of relatively low risk and detectability, cybercriminals are optimizing a plethora of diabolical cyberattacks to immobilize the financial sector. These attacks' threat landscape ranges from

**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)

Trojans, malware, ATM malware, ransomware, mobile banking malware, data-breaches, institutional invasion, data thefts, fiscal breaches, etc.

- Various public and private banking institutes are focusing on implementing the latest technology to prevent cyber attacks with a strategy to secure their IT processes and systems, secure customer critical data, and comply with government regulations. Besides, with greater customer expectations, rising technological capabilities, and regulatory requirements, banking institutions are pushed to adopt a proactive security approach.

- With the growing technological penetration, coupled with the digital channels, such as internet banking, mobile banking, etc., online banking has become the preferred choice of customers for banking services. There is a significant need for banks to leverage advanced authentication and access control processes.

- In 2022, financial firms worldwide were impacted by innovative new ransomware tactics that maximized ROI for the threat actors. While financial firms represent a small percentage of victims directly targeted by ransomware attacks, they can and have been impacted by attacks on third parties, who are prime targets. Such threats are poised to increase the usage of cybersecurity solutions in the BFSI sector in the country.

## Italy Cybersecurity Industry Overview

Italy Cybersecurity Market is fragmented and has some major players who have adopted various growth strategies, such as mergers and acquisitions, new product launches, expansions, joint ventures, partnerships, and others, to strengthen their position in this market. The major players in the market are IBM Corporation, Cisco Systems Inc, Trend Micro Incorporated, Broadcom Limited, Dell Technologies., among others.

- June 2022: Microsoft Italy launched a cybersecurity training programme, preparing an online certification scheme to train new IT security professionals in skills to prevent cybercrime. The training programme Alliance for Work will develop digital skills for students, professionals and organisations.

- March 2022: Investcorp acquired Italy's cybersecurity company, HWG, which helps companies proactively prevent, manage and reduce the impact arising from modern cybersecurity threats in an increasingly connected and digital world.

## 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

**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)

- 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 Increasing Demand for Digitalization and Scalable IT Infrastructure
  - 5.1.2 Need to tackle risks from various trends such as third-party vendor risks, the evolution of MSSPs, and adoption of cloud-first strategy
- 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 Trends Analysis
  - 5.3.1 Organizations in Italy increasingly 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

## 7 COMPETITIVE LANDSCAPE

- 7.1 Company Profiles
  - 7.1.1 IBM Corporation
  - 7.1.2 Cisco Systems Inc
  - 7.1.3 Trend Micro Incorporated

**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)

- 7.1.4 Broadcom Limited
- 7.1.5 Dell Technologies Inc.
- 7.1.6 Fortinet Inc.
- 7.1.7 Palo Alto Networks
- 7.1.8 McAfee, LLC
- 7.1.9 Intel Security (Intel 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](mailto:support@scotts-international.com)

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

## Italy Cybersecurity - 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	2025-05-07
		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)