

## **Benelux Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029**

Market Report | 2024-02-17 | 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 Benelux Cybersecurity Market size is estimated at USD 4.04 billion in 2024, and is expected to reach USD 5.90 billion by 2029, growing at a CAGR of 7.90% during the forecast period (2024-2029).

#### Key Highlights

- In the current market environment, cybersecurity clusters can arise naturally or through local governments' deliberate, frequent top-down activities. Regulations and policies of local governments have a considerable impact on the growth of these clusters.
- Increasing cyberattacks in the Benelux Union have propelled it to strengthen its defensive capabilities. The surge in demand for digitalization and scalable IT infrastructure, the increasing need to tackle risks from third-party vendor risks, and the adoption of a cloud-first strategy have been driving the growth of cybersecurity solutions and services in the region. Additionally, as the number of Internet of Things (IoT) devices has expanded, so has the vulnerability and exposure to various cyber-attacks.
- The cloud deployment segment is estimated to register significant growth in the market. As IT provision has shifted from being on-premise to being outside of a company's borders, security has been extremely crucial at every stage of the cloud adoption cycle. SMEs prefer cloud deployment since it frees them up to concentrate on their core skills rather than investing their limited cybersecurity funds in security infrastructure.
- In 2022, there were around 2 million small and medium-sized businesses (SMEs) in Belgium, the Netherlands, and Luxembourg (Benelux). The Netherlands possesses about 1.28 million SME businesses operating in non-financial business sectors this year, according to DIW forecasts. This was a lot more SMEs than there were in Belgium and Luxembourg. Hence, the rise in the number of SMEs also acts as a key driver in this market.
- The lack of cybersecurity professionals in several businesses is a crucial challenge in terms of facing cyberattacks. Also, the high reliance on traditional authentication methods and low preparedness could be significant factors that could hamper the market's overall growth.

**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 COVID-19 outbreak has brought severe attention to the need for increased online safety. In order to maintain their interpersonal and professional connections, people have boosted their online presence. On the other hand, hackers have profited from the circumstance and have targeted the healthcare system, e-commerce, and e-payment businesses. On a workforce level, businesses are having difficulty deciding how to strike the optimum balance between employee flexibility and corporate culture. The various advantages of a cloud-first design are being compared on a technological level to the difficulties in controlling complexity and expense in a multi-cloud environment.

## Benelux Cybersecurity Market Trends

IT and Telecommunication segment is poised to grow at a faster pace.

- EEAS (European External Action Service), the EU's external action service, unveiled several new cybersecurity strategies. Most of them aim to make Europe more resilient to cyberattacks while guaranteeing that all individuals and businesses can fully benefit from reliable services and advanced digital technologies. On March 22, 2021, the European Council approved the cybersecurity strategy conclusions, highlighting the significance of cybersecurity in building a resilient, eco-friendly, and digital Europe.
- Critical industries like transportation, energy, healthcare, and finance have increasingly relied on digital technologies to conduct daily operations. While the COVID-19 situation exposed the economy and society to cyber threats, it also opened up vast potential and offered solutions to many of Europe's current problems. The increased expenditure on prevention is due to the massive increase in the risk of cyber assaults on businesses. Compared to 2020, companies in Belgium, France, Germany, Ireland, the Netherlands, Spain, and the United Kingdom boosted their investments in cybersecurity last year.
- According to Hootsuite, there were approximately 16.5 million internet users in the Netherlands as of January 2022, compared to 613,000 people in Luxembourg. This amount seems to be relatively minimal at first. However, in terms of the entire population, Luxembourg had the highest rate of internet use in the Benelux area. By 2022, Belgium had approximately 11 million internet users, accounting for 94% of the country's entire population, compared to 99% of internet users in Luxembourg.
- Furthermore, according to We Are Social, a global agency, as of February 2022, Luxembourg had the highest internet penetration rate in the Benelux region, with 99% of the population online. Belgium had the lowest internet penetration rate, at about 94%.
- In addition, according to Hootsuite, the Netherlands had the highest penetration rate of active social media users on desktops and mobile devices as of 2022, with a figure of 90.7%. Luxembourg had the lowest penetration rate, with just over 72% of the population being active social media users. Hence, with the rise in active social media and internet users in Benelux, the overall demand for cybersecurity will increase considerably in the region, thereby driving market growth exponentially. Such developments would trigger the demand for cybersecurity solutions and services in the IT and Telecom Sector.

## The Netherlands is Expected to Witness Significant Growth

- The Netherlands, one of the most wired nations in the world, is considered the digital gateway to Europe. Moreover, due to its robust research, startup, and practitioner ecosystems, the Netherlands is recognized as a leader in Europe in the field of cyber security. Additionally, the country has seen a sharp rise in the number of managed service providers based on public cloud alliances in recent years, resulting in rapid growth for the cloud and cybersecurity sectors. Moreover, the government actively encourages the domestic cybersecurity industry because data security is a top priority. The regional end-user sectors' increasing usage of cloud and digital services is broadening the B2B cloud computing service industry's reach, which has positive implications for the cybersecurity market.
- The Amsterdam Internet Exchange (AMS-IX) is one of the biggest internet exchanges in the world, where various major tech

**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)

firms have decided to domicile their European operations. Also, over the past 10 years, the Hague region in the Netherlands has established itself as a cybersecurity hotspot. The Dutch government has established the Global Forum for Cyber Expertise in The Hague, where the NATO Communications and Information (NCI) Agency and Europol's European Cyber Crime Center (EC3) are already located. Additionally, it is the location of The Hague Security Delta, the most significant security cluster in Europe, where firms involved in (cyber) security, governmental organizations, and academic institutions collaborate. Hence, with a substantial startup ecosystem, the Netherlands is emerging as a European leader in FinTech, AgTech, and technology-based transportation solutions.

- Four significant problems with cybersecurity in the Netherlands were outlined in the NCSC's 2022 "Cyber Security Assessment Netherlands" report: Unauthorized access to information through espionage, process inaccessibility due to sabotage and the use of ransomware or preparations for this, breaches of cyberspace, such as through the abuse of international IT supply chains, and large-scale outages. Thus, with the rise in these significant issues related to cybersecurity in the Netherlands, the demand for cybersecurity in the region will rise exponentially, thereby driving the market growth.

- According to a 2019 survey by the insurance company Hiscox, Dutch businesses invest an average of USD 1.9 million yearly in cybersecurity. In 2022, this number is anticipated to rise. The Dutch government's spending on cybersecurity in the coming years is also expected to rise. As per IMF, government revenue and spending in the Netherlands were around EUR 328.6 billion and USD 363.99 billion, respectively, in 2020, which is predicted to rise to approximately USD 468.36 billion by 2027. Hence, with the rise in government spending on cybersecurity, the market is expected to experience significant growth opportunities throughout the forecast period.

- According to the annual DHL Global Connectedness Index, the nation has consistently ranked first. Over 6% of the Dutch GDP is estimated to be accounted for by the internet economy, which is expected to expand over the next few years. In addition, according to We Are Social, a global agency, there were 16.5 million internet users in the Netherlands as of January 2022, or 96% of the country's entire population, and there were 15.6 million active social media users in the nation. Thus, with the rise in internet and social media users, the overall demand for cybersecurity will also increase considerably.

## Benelux Cybersecurity Industry Overview

The Benelux Cybersecurity Market is moderately competitive due to several vital market players' presence. Some major players are IBM Corporation, Cisco Systems Inc., Dell Technologies Inc. Intel Security, and Fortinet Inc. The market players are heavily indulging in product launches, strategic partnerships, and acquisitions as lucrative ways to enhance their market share.

In June 2022, to bring advanced technologies and services to European organizations, NightDragon, an investment and advisory firm specializing in the cybersecurity, safety, security, and privacy sectors declared a new strategic partnership with Orange Cyberdefense, a world leader in cybersecurity services. The partnership will provide NightDragon's portfolio firms access to the European market and give Orange consumers access to emerging technologies and services that will help them stay one step ahead of online threats.

In April 2022, Cisco and the Telenor Group declared their expanded partnership to address opportunities like the digital divide, enterprise cyber security, and digital transformation through the fourth iteration of their JPA. The companies intend to expand Telenor's capabilities beyond connectivity for business clients and create more customer-centric, scalable, and flexible "as-a-service" solutions.

## Additional Benefits:

- The market estimate (ME) sheet in Excel format
- 3 months of analyst support

## Table of Contents:

**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)

## 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 Increasing Demand for Digitalization and Scalable IT Infrastructure

#### 5.1.2 Rapidly Increasing Cyber Security 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 Preparedness

### 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 Security 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

**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)

- 6.3.3 Manufacturing
- 6.3.4 Government and Defense
- 6.3.5 IT and Telecommunication
- 6.3.6 Other End Users
- 6.4 By Geography
  - 6.4.1 Belgium
  - 6.4.2 Netherlands
  - 6.4.3 Luxembourg

## 7 COMPETITIVE LANDSCAPE

- 7.1 Company Profiles
  - 7.1.1 IBM Corporation
  - 7.1.2 Cisco Systems Inc.
  - 7.1.3 Dell Technologies Inc.
  - 7.1.4 Fortinet Inc.
  - 7.1.5 Intel Security (Intel Corporation)
  - 7.1.6 F5 Networks Inc.
  - 7.1.7 AVG Technologies
  - 7.1.8 FireEye Inc.
  - 7.1.9 Fujitsu

## 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)

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

Market Report | 2024-02-17 | 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*	<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="2025-05-06"/>
		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)