Netherlands Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 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 Netherlands Cybersecurity Market size is estimated at USD 2.35 billion in 2025, and is expected to reach USD 3.55 billion by 2030, at a CAGR of 8.61% during the forecast period (2025-2030).

The need for cybersecurity solutions increased in order to deal with the threat of an increase in the frequency and sophistication of cyber attacks. In the coming years, this trend is expected to probably be sustained as more businesses and individuals are made aware of the importance of safeguarding their digital assets.

Key Highlights
- New opportunities and challenges in cybersecurity are expected to emerge with the growing use of emerging technologies like artificial intelligence, cloud computing, and the Internet of Things (IoT), which will require more innovative and advanced solutions to mitigate these risks. For instance, in 2023, Chinese operatives exploited a Dutch military network with malware. Fortunately, the compromised network was isolated from the leading defense ministry network, mitigating potential harm. This is the first time the Netherlands has publicly accused China of cyber espionage, encouraging the Netherlands to build comprehensive cybersecurity solutions to prevent such attacks.
- In 2023, the Royal Dutch Football Association (KNVB) became the victim of a ransomware attack by the Russian cybercriminal group Lockbit. The hackers demanded a ransom, threatening to expose sensitive documents. KNVB eventually paid the ransom, approximately EUR 1 million. Lockbit threatened to disclose crucial data of 300 GB, comprising passports and salary details of Oranje players. While KNVB confirmed the ransom payment, they also expressed concerns that the data might still be leaked. Such attacks encourage companies to invest in robust security solutions.
- In February 2024, the CIF-NL from the Netherlands Enterprise Agency offered funding to Dutch companies and research organizations working on projects that advance cybersecurity solutions. This consists of small and medium-sized enterprises, big

enterprises, and research institutions. The Digital Trust Center (DTC) encourages collaborations between businesses in non-essential industries through a funding program.
- These potential partnerships could be environmentally friendly within the supply chain, local area, specific field, or business sector. Business projects in the Netherlands can get up to EUR 200,000 (USD 213,870) in funding to enhance their cyber resilience on a scalable basis.
- Moreover, the lack of professional cybersecurity staff in all sectors is a major factor behind the growing number of cyberattacks. In addition, there is a lack of skilled professionals in cybersecurity across Europe who are needed to deal with cyber risks in financial services organizations and government bodies, as well as the private sector.
- Post-COVID-19, there was a surge in cyberattacks, which included phishing attacks, ransomware, and other cybercrimes. Moreover, there was a rapid shift toward hybrid work setups and increased use of data on online platforms. Many organizations adapted quickly to cybersecurity measures for secure remote connections, leading to potential security gaps. These risks insisted that businesses and the government focus more on enhancing network security measures in the Netherlands, leading to the growth of the market.

Netherlands Cybersecurity Market Trends

Cloud Segment to Witness Significant Growth

- The demand for cloud solutions is driven by a growing awareness among businesses about the cost and resource savings achieved when they move their data to the cloud rather than building or maintaining new data stores. Given the various advantages, cloud platforms and ecosystems are expected to produce a rapid explosion of digital innovation over the next few years.
- Companies considering moving from on-premise software to a cloud-based solution are primarily checking the potential solutions for their capabilities concerning crucial security features, including standards compliance, intrusion prevention, and detection. As per the EuroStats data, there is growth in SMEs operating in the Netherlands, which is 59,154 SMEs in 2023, which are eventually opting for a cloud solution for their business requirements.
- IT provision has shifted from on-premise to outside the boundaries of the business, and security has been crucial at every stage of the cloud adoption cycle. SMEs prefer cloud deployment because it frees them up to concentrate on their core skills rather than investing their limited cybersecurity funds in security infrastructure. Moreover, the use of public cloud services also provides an organizational trust boundary and gives security a critical role to play in cloud infrastructure.
- While phishing, brand impersonation, and business email compromise (BEC) remain prevalent tactics for threat actors, there has been a notable rise in the adoption of more obscure methods to breach global organizations. This surge is reported by the Central Statistics Online (CSO), which revealed that the Netherlands and Sweden experienced a 92% increase in these attacks in 2023.
- Moreover, companies across the Netherlands are regularly assessing and adjusting the technical controls and methods to identify and mitigate emerging cybersecurity risks. They mainly use a layered approach with overlapping controls to defend against cybersecurity attacks and threats on networks, end-user devices, servers, applications, data, and cloud solutions.
- For instance, in October 2023, IBM announced the launch of its new managed detection and response service offerings with new AI technologies. The new Threat Detection and Response Services (TDR) provide 24-hour monitoring, investigation, and automated remediation of security alerts from all relevant technologies across the client's hybrid cloud environments.

IT and Telecommunication to Witness Growth

- Information technology (IT) and telecommunications are vital in businesses, government agencies, and organizations. The need for robust cybersecurity measures has become crucial with the increasing reliance on interconnected networks, cloud computing, and digital communication. IT and telecom end-users form a substantial portion of the global cybersecurity market as they seek to protect their sensitive data, networks, and communications from evolving cyber threats.

- Since the telecom industry touches almost all aspects of life alongside critical infrastructure, it is prone to cyberattacks. Significantly, the industry builds and operates complex networks and stores massive amounts of sensitive data associated with individuals and corporations. These are among the several reasons that make this field more lucrative to malicious actors or hackers across the region. As per the Ericsson data, the 5G deployment by area in the Netherlands is expected to reach 21% by 2030.
- In 2023, the Dutch Data Protection Authority (AP) received 25,694 reports of data leaks, marking a 21% surge from the previous year, which signifies an average of 70 daily breaches. The government's privacy watchdog highlighted a concerning trend regarding Dutch entities, both businesses and organizations, undervaluing the critical threat of cyberattacks. Notably, more than 1,300 of the reported data breaches were attributed to cyberattacks. They recorded a common target for cybercriminals, which is IT suppliers, who often oversee substantial volumes of personal data for various organizations.
- IT and telecom enterprises typically store personal information in the form of computer data and act as a target for insiders or cyber-criminals looking to steal money, steal identity, blackmail customers, or launch further attacks. DDoS attack is one of the most standard types of direct cyberattacks that could make a computer or network resource unavailable to its required users, indefinitely or temporarily disrupting services a host in connection with the internet. By attacking internet service providers, such attacks are capable of having network capacity, increasing bandwidth costs, disrupting services, and thereby compromising access to the internet.
- For instance, as of May 2024, the Netherlands Enterprise Agency has successfully taken down five different botnets that were utilized globally for cybercrime, disrupting ransomware criminal networks. A botnet consists of a group of computers that have been infected with harmful software. This covertly unlocks the victims' online entrance. Criminals purchase this access to various computer systems owned by other individuals in order to conduct ransomware attacks as they hold valuable information of their targets 'hostage' and demand payment before releasing it.
- The telecom sector is booming with opportunities for operators to transform their revenue models by introducing new and innovative digital services related to IoT, 5G, e-commerce, data, content, OTT communications, and mobile payments or managed services. The increase in IT infrastructure components, such as desktops, servers, information systems, data centers, and virtual machines, further adds to the demand.

Netherlands Cybersecurity Industry Overview

The market is fragmented, with thousands of firms trying to develop cybersecurity technologies. With a supportive legislative and regulatory framework, the Netherlands has established its position as Europe's leading cybersecurity center. As cybersecurity businesses search for new ways to deploy cutting-edge AI, automation, analytics, and collaboration technology that business executives cannot afford to ignore, the market has produced a vibrant ecosystem of collaboration and invention.

- November 2023: FRISS announced the launch of the FRISS Accelerator for Claims Analytics for ClaimCenter Cloud. The accelerator leverages the latest capabilities of the Guidewire Cloud Integration Framework and uses a wide variety of powerful AI techniques, internal and 3rd-party data, network analytics, and risk and fraud indicators to analyze claims consistently. It promptly flags suspicious claims and allows for trustworthy claims to go on a fast track, all directly within ClaimCenter.
- October 2023: FRISS collaborated with Microsoft to enhance its AI fraud model explanations using Microsoft Azure OpenAI Service, where Azure OpenAI Service enables FRISS to present potential fraud cases into more engaging and understandable stories, using the art of storytelling as the essence of the explanation. With this approach, understanding and conveying potential fraud incidents to insurance professionals and fraud investigators becomes remarkably seamless.

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

5 MARKET DYNAMICS
5.1 Market Drivers
5.1.1 Increasing Cyberattacks in Different Industries
5.1.2 Growing Need of Identity Access Management
5.2 Market Restraints
5.2.1 Lack of Infrastructure
5.3 Analysis of Major Use-cases and Case-studies
5.4 Key Regulations Monitoring the Market

6 MARKET SEGMENTATION
6.1 By Offering
6.1.1 Solutions
6.1.1.1 Application Security
6.1.1.2 Cloud Security
6.1.1.3 Data Security
6.1.1.4 Identity and Access Management
6.1.1.5 Infrastructure Protection
6.1.1.6 Integrated Risk Management
6.1.1.7 Network Security Equipment
6.1.1.8 End point Security
6.1.1.9 Other Solutions

6.1.2 Services
6.1.2.1 Professional Services
6.1.2.2 Managed Services
6.2 By Deployment Mode
6.2.1 Cloud
6.2.2 On-premise
6.3 By Organization Size
6.3.1 SMEs
6.3.2 Large Enterprises
6.4 By End User
6.4.1 BFSI
6.4.2 Healthcare
6.4.3 IT and Telecom
6.4.4 Industrial & Defense
6.4.5 Retail
6.4.6 Energy and Utilities
6.4.7 Manufacturing
6.4.8 Others

7 COMPETITIVE LANDSCAPE
7.1 Company Profiles
7.1.1 EclecticIQ
7.1.2 FRISS
7.1.3 eharmony Inc.
7.1.4 ReaQta
7.1.5 LogSentinel
7.1.6 Keezel
7.1.7 RedSocks
7.1.8 BitSensor
7.1.9 Praesidion Smart Security Solutions
7.1.10 People Media
7.1.11 Onegini
7.1.12 SecurityMatters
7.1.13 Madaster

8 INVESTMENT ANALYSIS

9 FUTURE OF THE MARKET

SCOTTS
INTERNATIONAL

Netherlands Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 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*

Phone*

First Name*

Last Name*

Job title*

Company Name*

EU Vat / Tax ID / NIP number*

Address*

City*

Zip Code*

Country*

Date 2026-02-06

Signature

Scotts International. EU Vat number: PL 6772247784
tel. 0048 603 394 346 e-mail: support@scotts-international.com
www.scotts-international.com