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

Market Report | 2023-01-23 | 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 Nordic cybersecurity market is expected to register a CAGR of 6.8% over the next five years. The upswing of cyberattacks in various end-user industries primarily drives the Nordic cybersecurity market. Furthermore, as digitalization advances, cyberattackers are developing new methods of conducting cyberattacks; these factors are expected to increase demand for cybersecurity solutions in the country.

Key Highlights
Cybersecurity primarily prevents unauthorized computer, network, program, and data access. 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.
With the growing digitization across the end-user sectors in the country, cyberattacks have also increased over the past few years. With new destructive practices in cyberspace, further cyberattacks can be carried out relatively easily, at low cost, and with a relatively low risk for the attacker. This has made more end-user industries in this region want cybersecurity solutions to stop these kinds of cyberattacks.
Many companies are building new data centers in the region, which is boosting the market under consideration. For instance, in October last year, Acronis, the global provider of cyber protection, announced the availability of a new Acronis Cyber Cloud Data Center in Norway. The new data center, which is one of the company's 111 new data centers, gives service provider partners access to a full range of cyber protection solutions so they can build new services and give their clients faster access, constant data availability, and data sovereignty.
Moreover, in April this year, Truesec launched the IoT Cybersecurity Domain in Sweden and recruited IoT cybersecurity expert Patrik Axelsson as CEO from Telia's IoT group, Division X.
One of the major causes of growing cyberattacks is the lack of skilled cybersecurity personnel in each industry. Experienced

cybersecurity professionals are less in demand than security professionals, especially in Europe, Asia-Pacific, Latin America, and the Middle East. Security professionals are needed to handle cyber threats for financial institutions, government organizations, private sector businesses, and industrial businesses.
This region's cybersecurity market comprises several global and regional players vying for attention in a somewhat contested market space. Even though it's hard for new players to get into the market, a number of newcomers have been successful.
This market is characterized by moderate-to-high product differentiation, growing levels of product penetration, and high levels of competition. Generally, the solutions are offered as a package, making the consolidated offering look like a part of the product's service.
Most of the cyber threats intensified because of the opportunities during the COVID-19 outbreak. The fact that some small and medium-sized businesses adopted a "Bring Your Device" (BYOD) strategy (as opposed to a "Corporate Owned Personally Enabled" (COPE) strategy) and permitted employees to access corporate data using their devices (phones, tablets, or laptops) could be one of the causes of the rise in cyberattacks. The same level of cybersecurity was not provided when working from home as it was in an office setting. Users are more vulnerable to cyberattacks while accessing corporate files and data on a personal computer or laptop (even with the security of an MDM system). For instance, employees might not use antivirus or anti-malware software.
Small and medium-sized businesses were severely impacted by the COVID-19 outbreak but recovered within two years. However, many organizations continue to prefer that their employees work from home, resulting in a hybrid work culture that poses cyber threat issues.

Nordics Cybersecurity Market Trends

Initiatives Taken by Government on Cyber Security drives the Market Growth

The government represents the highest level of cybersecurity management within the region. They are responsible for providing political guidance and strategic security guidelines and making the required decisions regarding the resources and prerequisites to be allocated. All Nordic countries have a national Computer Security Incident Response Team (CSIRT) and have established international partnerships to share incident data.
The Nordic Region's primary countries implement antithetical strategies for designing and developing an ICT infrastructure. Sweden, Finland, and Iceland highlight human rights as fundamental rights and intend to establish a well-functioning ICT infrastructure to promote freedom of speech. To make sure that digital solutions and services for their citizens are reliable and safe, the governments of Norway and Denmark took opposite approaches.
The governments of Sweden, Norway, and Finland are working together to implement 5G networks ahead of Europe. Denmark has also just released its plan for rolling out 5G to help and speed up the digitization of businesses, especially for IoT automated production and smart transportation.
According to a new risk assessment study by the Norwegian National Security Authority (NSA), Russia's ongoing invasion of Ukraine can potentially increase cyber assaults against public and commercial organizations in Norway.
To overcome these attacks, the country is making significant strides to strengthen the country's cybersecurity space. For instance, in August this year, the Norwegian government approved an additional NOK 200 million (USD 21 million) in funding to strengthen national security against digital threats. The government provided NOK 392 million in special financing to strengthen the cyber defense capabilities of the Norwegian Defense Forces (NDF) and state national security organizations with national cyber defense tasks.
Denmark's government increased its cyber and information security efforts via the 2018-2023 Defense Agreement by investing DKK 1.4 billion (USD 200 million) in cyber and information security over the next few years to include better protection against cyberattacks by expanding the Centre for Cyber Security's sensor network for authorities and businesses.

Manufacturing is One of the Factor for Market Growth

As the manufacturing sector progresses toward a digital transformation, it has become vulnerable to cyberattacks with the advent of Industry 4.0. Thus, the industry needs companies to realign their security systems.
The benefits of advanced online systems make manufacturing organizations more vulnerable to cyber dangers.
Every sector in the manufacturing industry, including automotive, logistics, various engineering disciplines, power systems, the consumer goods industry, and chemicals, has adopted digital technologies to increase overall operational efficiency and reduce production costs. M2M communication and networking have been on the rise due to industries working toward data collection and using it for analytics to avoid downtime and keep the manufacturing industry operational round the clock.
This year, Sweden has a robust and profitable manufacturing and industrial engineering sector, which accounts for nearly 20% of the country's GDP (USD 125 billion), with advanced manufacturing accounting for roughly 40% of the total. The sector accounts for 75% of Swedish exports and employs over one million people.
According to a Checkpoint analysis, the average weekly attacks in the manufacturing sector will have increased 41% by the end of the previous year.This helped the manufacturers understand the types of cyber security threats and how to create efficient workflows for alert triage, incident response, and threat hunting.
As the war in Ukraine goes on and Finland tries to join the North Atlantic Treaty Organization, the Finnish government plans to use a voucher system in August to help companies pay for better cybersecurity.
The vouchers would provide small and medium-sized businesses and organizations up to 15,000 euros (about 15,000 USD). Larger companies may be eligible for vouchers worth up to 100,000 euros (around 100,000 USD). According to a Finnish Ministry of Transport and Communications official, higher-value vouchers may cover 70% of a cybersecurity initiative, with corporations responsible for the remaining 30%.

Nordics Cybersecurity Market Competitor Analysis

The competitive landscape of the Nordic cybersecurity market is 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 March 2022, Acronis announced another significant investment in the Nordics, opening a new Acronis Cloud Data Center in Stockholm, Sweden. The new sustainable cloud data center gives all service providers access to a full range of cyber protection solutions so they can build new services and give their clients faster access, constant data availability, and data sovereignty.

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 Demand for Digitalization and Scalable IT Infrastructure
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 Market Opportunities
5.3.1 Rise in Trends for IoT, BYOD, Artificial Intelligence, and Machine Learning in Cybersecurity

6 MARKET SEGMENTATION
6.1 By Product Type
6.1.1 Application Security
6.1.2 Cloud Security
6.1.3 Consumer Security Software
6.1.4 Data Security
6.1.5 Identity Access Management
6.1.6 Infrastructure Protection
6.1.7 Integrated Risk Management
6.1.8 Network Security Equipment
6.1.9 Other Solution Types
6.2 By Service
6.2.1 Professional
6.2.2 Managed
6.3 By Deployment
6.3.1 On-Premise
6.3.2 Cloud
6.4 By End-User Industry
6.4.1 BFSI
6.4.2 Healthcare
6.4.3 Aerospace and Defense
6.4.4 IT and Telecommunication
6.4.5 Government
6.4.6 Retail
6.4.7 Manufacturing

6.4.8 Other End-user Industries
6.5 By Geography
6.5.1 Denmark
6.5.2 Norway
6.5.3 Sweden
6.5.4 Finland

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 Clavister
7.1.6 F5 Networks, Inc.
7.1.7 AVG Technologies
7.1.8 Acronis International GmbH.
7.1.9 CyberArk Software Ltd.
7.1.10 Proofpoint Inc.
7.1.11 Trend Micro Inc.
7.1.12 Nortonlifelock Inc.

8 INVESTMENT ANALYSIS

9 FUTURE OF THE MARKET

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

Market Report | 2023-01-23 | 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	2026-03-01
		Signature