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

Market Report | 2025-04-28 | 149 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 Sweden Cybersecurity Market size is estimated at USD 1.53 billion in 2025, and is expected to reach USD 2.44 billion by 2030, at a CAGR of 8.82% during the forecast period (2025-2030).

The cybersecurity market in Sweden is experiencing growth, driven by the increasing prevalence of cyberattacks and widespread digital transformation across industries. The proliferation of connected devices, remote access, and online activities has led to a rise in reported cybercrimes. As the adoption of intelligent devices and IoT technologies grows, cyber threats are anticipated to become more sophisticated. Consequently, businesses are implementing advanced cybersecurity solutions to identify, mitigate, and manage cyber risks, thereby driving market expansion.

Key Highlights
- Sweden's cybersecurity market is at a pivotal stage, presenting both growth opportunities and significant challenges. The increasing sophistication of cyberattacks is heavily impacting critical sectors such as energy, manufacturing, finance, and public services. The Swedish National Coordination Centre for Cybersecurity Research and Innovation reports that while essential services in Sweden are rapidly adopting advanced digital technologies, cybersecurity measures are not advancing at the same pace. This disparity exposes the nation to heightened cyber risks and creates a demand for international expertise to strengthen its cybersecurity framework.
- Sweden is poised to experience swift digitalization across multiple sectors, such as banking, healthcare, retail, and government services. Central to this digital evolution is the widespread adoption of cloud technology. Organizations are increasingly transitioning from traditional on-premise data centers to adaptable cloud environments. This shift is primarily motivated by the operational efficiency, cost savings, and scalability that cloud infrastructure provides.
- For instance, according to a survey by the Swedish Internet Foundation (Internetstiftelsen), an IT management company, in

2024, 71% of surveyed adults in Sweden reported using digital mailboxes over the past year, marking a 16% increase from 2021. It's important to note that a digital mailbox is distinct from traditional email services. The increasing use of digital mailboxes has increased the number of touch points for cybercriminals to launch a cyber-attack through methods such as phishing attacks to access email accounts and gain access to sensitive information, thereby prompting enterprises to implement robust cyber security measures.
- Cyberattacks have increasingly targeted Sweden's critical infrastructure, notably its energy, healthcare, and transportation sectors. In response, both the government and private entities are ramping up investments in cybersecurity, underscoring the importance of operational continuity and national security.
- For example, in February 2024, the Swedish government unveiled plans to channel over SEK 100 million (approximately USD 9.42 million) into Cybercampus Sweden, a newly launched initiative at KTH Royal Institute of Technology. This investment aims to bolster both the skill set and research capabilities in the realm of cybersecurity.
- Sweden grapples with a shortage of trained cybersecurity experts as demand consistently outstrips supply across various industries. Organizations frequently find it challenging to recruit talent skilled in ethical hacking, incident response, and threat intelligence, causing delays in fortifying their cybersecurity measures.

Sweden Cybersecurity Market Trends

SMEs Expected to Witness Major Growth

- SMEs, accounting for 99% of Sweden's businesses, are integral to the nation's economy, driving employment, value creation, and turnover. Sweden's well-established financial ecosystem has positioned the country as a leading European hub for SME listings. According to the European Commission, there were estimated to be approximately 7.19 million SMEs operating across Sweden as of 2024. Key factors such as advanced digital maturity, a high ranking in ease of doing business, widespread cloud adoption, increased investments in digital technologies, and the integration of AI are accelerating the digital transformation of SMEs.
- However, this transition to cloud-based and digital environments has also increased their exposure to cyber threats. Cybercriminals frequently exploit smaller companies, especially those catering to larger clients, capitalizing on their weaker security measures to access more lucrative targets. Small and medium enterprises (SMEs) that serve regulated industries, critical infrastructure, and major global corporations are more vulnerable to cyber-attacks.
- SMEs frequently struggle to implement robust cybersecurity policies due to budget constraints. This challenge is exacerbated by a shortage of trained professionals. In response, the Swedish government has launched initiatives such as the development of cybersecurity systems and training programs aimed at promoting the swift adoption of cybersecurity measures among SMEs.
- For instance, The National Coordination Centre for Cybersecurity Research and Innovation (NCC-SE) offers grants to small and medium-sized enterprises (SMEs) to develop advanced cybersecurity projects. These grants aim to enhance Sweden's cybersecurity infrastructure and preparedness. Eligible projects may include workforce development, simulation exercises, and initiatives to foster youth engagement. The 2024 call for proposals is open to SMEs and other relevant stakeholders. Approved projects will be implemented between January 1, 2025, and March 31, 2025.
- Likewise, Sweden's Secure Tech Hub, a national cybersecurity innovation initiative, supports small and medium-sized tech enterprises in developing secure digital products. This initiative, a collaboration among six of Sweden's leading science parks and co-financed by the European Union, has introduced a "Basic Cybersecurity" course designed to address the cybersecurity challenges faced by SMEs.
- During the forecast period, SMEs are poised for growth, driven by rising demand for cybersecurity in the country owing to the government's proactive push to bolster cybersecurity in SMEs and heightened IT budgets allocated for cybersecurity solutions.

- Sweden's strategic geopolitical position and growing dependence on digital technologies have thrust its military and defense sector into the spotlight of cybersecurity initiatives. With the surge in hybrid warfare, cyber espionage, and mounting geopolitical tensions, there's an urgent need for fortified cybersecurity measures to protect vital infrastructure and defense networks.
- Surfshark reports that Sweden witnessed a significant surge in data breaches during Q1 2024, with over a million personal data points compromised. This uptick stands in stark contrast to the previous quarter. Notably, the peak for exposed data records was in Q2 2021, when over 1.6 million records were breached.
- Public institutions have increasingly become targets of cyberattacks, with ransomware and espionage leading the charge. This uptick in attacks underscores the urgent need for fortified cybersecurity measures, from secure data centers to encrypted communications and vigilant real-time threat monitoring. Since January 2024, multiple organizations in Sweden have been hit by cyberattacks, with hackers believed to have Russian affiliations. Additionally, Sweden's security service, Sapo, has pointed fingers at Iranian intelligence for breaching a text messaging service, sending out 15,000 messages to Swedish citizens.
- In Sweden, Critical National Infrastructure (CNI) includes vital systems like energy grids, transportation, communication networks, water supply, and healthcare services. As these infrastructures become more interconnected and digitized, they also become more vulnerable to exploitation by malicious actors. This evolving landscape has fueled Sweden's cybersecurity market, driven by an urgent demand for robust defenses against cyber threats to these essential systems.
- In October 2024, the Swedish Defence University (SEDU) and the National Cyber Security Centre hosted a cybersecurity competition. TietoEVRY, an IT consultancy firm that provides online security systems, confirmed the situation's severity, noting that repercussions could linger for weeks. The ransomware strike's fallout has hit retail hard, disrupting online purchases at Sweden's largest cinema chain and numerous department stores and shops.

Sweden Cybersecurity Industry Overview

The Swedish cybersecurity market comprises several multinational and local players in a competitive space. Although the market poses high barriers to entry for new players, several new entrants have gained traction.

Prominent global players such as Microsoft, Cisco, and Palo Alto Networks, alongside strong regional competitors like Clavister and Advenica, drive intense competition in the Sweden cybersecurity market across various cybersecurity domains.

This market is characterized by moderate/high product differentiation, growing levels of product penetration, and high levels of competition. Generally, the solutions are offered as a packaged solution, making the consolidated offering look like a part of the product's service.

Many users opt for annual contracts to cut their costs. Lately, companies have also been opting for services that provide faster security updates. This has increased demand for cloud-based services, as the updates can be received in real-time. The service-based industry prefers such deployment.

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 Attractiveness - Porter's Five Forces Analysis
4.2.1 Bargaining Power of Suppliers
4.2.2 Bargaining Power of Buyers
4.2.3 Threat of New Entrants
4.2.4 Threat of Substitutes
4.2.5 Intensity of Competitive Rivalry
4.3 Regulatory Landscape of the Sweden Cybersecurity Market

5 MARKET DYNAMICS
5.1 Market Drivers
5.1.1 Increasing Demand for Digitalization
5.1.2 Continuous Innovations in Cyberthreats
5.2 Market Restraints
5.2.1 Shortage of Skilled Professionals
5.2.2 Integration with Emerging Technologies
5.3 Key Metrics and Indicators
5.3.1 Number of breached data points in Sweden
5.3.2 Number of received complaints of data protection
5.3.3 Average time spent on processing complaints of data protection
5.3.4 Share of internet users who experienced online fraud
5.3.5 Most Critical Events of cyberattacks in the Country
5.4 Key Use Cases
5.4.1 AI-assisted cyber threat intelligence
5.4.2 Network Security Monitoring and Intrusion Detection
5.4.3 Data Loss Prevention
5.4.4 Endpoint protection and Response
5.5 Insights on Technology Landscape
5.6 Key Insights on the Events Involving the Major End-users and Working Groups Within Sweden

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 Clavister AB
7.1.2 Trend Micro, Inc.
7.1.3 F5, Inc.
7.1.4 Fortinet, Inc.
7.1.5 Dell Technologies Inc.
7.1.6 BM Corporation
7.1.7 Cisco Systems
7.1.8 Microsoft Corporation
7.1.9 Accenture
7.1.10 Kaspersky Lab
7.2 Vendor Market Share Analysis

8 FUTURE OF THE MARKET

SCOTTS INTERNATIONAL

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

Market Report | 2025-04-28 | 149 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	2025-05-02
		Signature	