The Swedish Market

Cybersecurity

Open Trade
Gate Sweden
National Board of Trade

The purpose of the market study

The purpose of this market study is to provide a comprehensive guide for companies from low- and middle-income countries that are interested in entering the Swedish cybersecurity market. The study focuses specifically on cybersecurity services and aims to offer valuable insights and support actionable strategies for service providers seeking to establish a presence in Sweden. It outlines key market trends, details regulatory and technical requirements, and provides guidance for identifying and securing business partners.

Table of contents

List of acronyms

Acronym	Full term	Explanation
CRA	Cyber Resilience Act	Proposed EU regulation requiring cybersecurity features in digital products and software throughout their lifecycle.
CSEC	Certification Body for IT Security in Sweden	Supervises evaluations of IT products based on common criteria.
DORA	Digital Operational Resilience Act	Upcoming EU regulation for ICT risk management in financial sectors.
GDPR	General Data Protection Regulation	EU regulation governing the protection of personal data and privacy, with direct implications for cybersecurity practices and compliance.
IAM	Identity and Access Management	Systems and processes for controlling user identities and access privileges.
ICS	Industrial Control System	Systems used to manage industrial operations such as manufacturing or energy.
IMY	Integritetsskyddsmyndigheten (Swedish Authority for Privacy Protection)	Sweden’s national supervisory authority for the processing of personal data.
MDR	Managed Detection and Response	Outsourced service providing threat detection and response.
MSSP	Managed Security Service Provider	Company that provides outsourced monitoring and management of security systems.
NIS 2	EU Directive on Security of Network and Information Systems (revised)	Updated cybersecurity regulation for critical infrastructure and essential services.
OT	Operational Technology	Hardware and software used to detect or cause changes in physical processes.
RED	Radio Equipment Directive	EU regulation ensuring the safety and cybersecurity of connected radio equipment.
SOC	Security Operations Centre	Centralised unit for continuous monitoring and response to cybersecurity threats.
VAD	Value-Added Distributor	A distributor that provides additional services beyond logistics, such as pre-sales support or configuration.
XDR	Extended Detection and Response	Advanced threat detection integrating multiple security layers (endpoint, network, server, etc.).

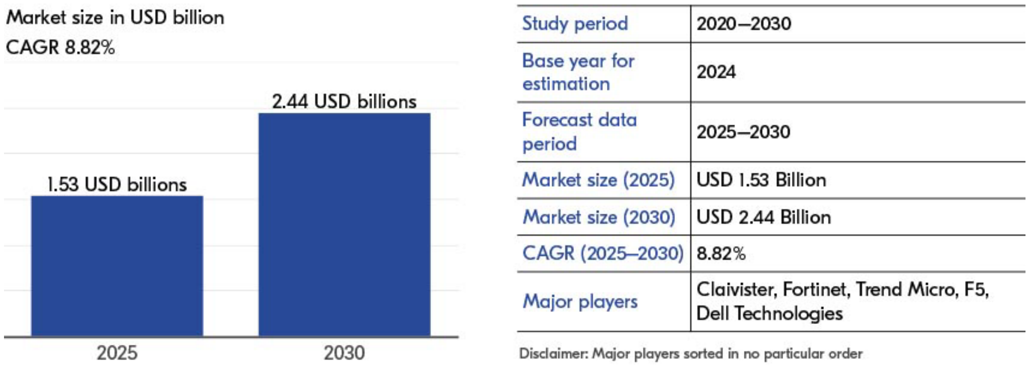
The Swedish cybersecurity market

Sweden has a highly digitalised economy, with reliable internet access reaching more than 98 per cent of households (Statista, 2024a). Although the country has a modest population of roughly 10.6 million, digital literacy is high, and cybersecurity is treated as both a board-level priority and a matter of national security (InnovationQuarter, 2024). For service providers from low- and middle-income countries considering entry into the Swedish market, it is essential to understand the market's size and growth, Sweden's openness to international service providers, and how Swedish organisations make purchasing decisions.

Background and key facts

Sweden's cybersecurity market is expected to reach USD 1.53 billion in 2025 and grow at a compound annual rate of approximately 8.8 per cent through 2030, reaching close to USD 2.44 billion (Mordor Intelligence, 2024). While this estimate includes both software and hardware-based solutions, the market is increasingly driven by demand for cloud services, software subscriptions, and managed security, which are the focus of this report.

Figure 1. Forecast growth of the Swedish cybersecurity market, 2025–2030 (USD billions)



Study period	2020–2030
Base year for estimation	2024
Forecast data period	2025–2030
Market size (2025)	USD 1.53 Billion
Market size (2030)	USD 2.44 Billion
CAGR (2025–2030)	8.82%
Major players	Claivister, Fortinet, Trend Micro, F5, Dell Technologies

Disclaimer: Major players sorted in no particular order

Source: Mordor Intelligence, 2024.

Growth is strongly influenced by European legislation, most notably the General Data Protection Regulation (GDPR) and the upcoming NIS-2 Directive, as well as national initiatives such as the National Cybersecurity Centre[1] (NCSC), which coordinates critical actors across infrastructure, defence, and telecommunications (International Trade Administration, 2024).

International suppliers and market openness

While Sweden is home to several specialised cybersecurity firms, it also maintains a high level of openness to international service providers. According to the

[1] https://www.ncsc.se/sv/ (in Swedish)

International Trade Administration (2024), foreign cybersecurity solutions, including software, platforms, and related services, contributed significantly to the Swedish market between 2020 and 2023, with combined imports valued at around USD 550–556 million per year. This figure includes both hardware and non-hardware components and reflects the structural role those external providers play in the Swedish cybersecurity ecosystem.

Many Swedish companies complement their local presence by collaborating across borders to access specialised talent and scale service delivery. Holm Security maintains a large part of its technical team in Poland in order to ensure cost-effective access to skilled resources. Axians delivers most of its services from Sweden but leverages in-house expertise from countries such as the Czech Republic and Germany to fill internal competence gaps when needed. These collaborations typically remain within the same corporate group, allowing companies to meet compliance and quality standards while meeting client expectations.

> “*It’s crucial to build strong European collaborations in cybersecurity. While it can be challenging to work with providers in Asia due to compliance requirements, it’s often much easier to bring in professionals from countries like Ukraine.”*
>
> Ola Skoog, Sales Manager, Axians

International partnerships also extend to global cybersecurity vendors. Allurity, for example, works with providers such as Microsoft, Okta, and Proofpoint to align on innovation roadmaps, support local compliance requirements, and co-develop go-to-market strategies.

> “*What matters most in an international partnership is technological innovation, a clear roadmap, support for local compliance, and a willingness to co-develop and go to market together.”*
>
> Maria Lörne, CMO at Allurity

Areas with strong market potential

Several cybersecurity segments in Sweden are experiencing strong growth and represent promising areas for service providers. The insights below are based on recent analyses by Mordor Intelligence (2024), Verified Market Research (2024), and Metastat (2025).

- **Cloud security services:** With over 85 per cent of Swedish enterprises using cloud services in 2023 and rapid migration away from on-premise infrastructure, demand for secure cloud architecture, monitoring, and compliance is high.
- **Managed Security Services (MSS):** SMEs and mid-sized companies that lack in-house capabilities are increasingly seeking out outsourced security operations such as threat monitoring and incident response.

- **Endpoint and email security services:** Remote work, increased IoT usage, and the rise of digital mailboxes have driven demand for managed protection against phishing, malware, and ransomware.
- **Compliance and data protection services:** Stricter legal requirements under the GDPR and the upcoming NIS-2 Directive have led to a 30 per cent increase in companies seeking compliance-focused cybersecurity consulting.
- **Sector-specific cybersecurity for BFSI and the public sector:** The financial services sector continues to lead cybersecurity spending, while the public sector is the fastest-growing user segment due to growing threats to national infrastructure.
- **Cybersecurity solutions for SMEs:** SMEs represent 99 per cent of Swedish businesses and are especially vulnerable to cyberattacks. Government-backed initiatives such as Secure Tech Hub and NCC-SE grants are supporting increased adoption of scalable and affordable cybersecurity services.

Spending patterns and purchasing behaviour

Cybersecurity spending in Sweden is distributed across multiple sectors. Finance and banking generate nearly 30 per cent of demand, government and defence around 20 per cent, and IT and telecommunications about 16 per cent (InnovationQuarter, 2024). A majority of organisations report rising budgets, but decision-makers remain cost-conscious. Swedish organisations favour usage-based licensing, transparent pricing, and clear total-cost-of-ownership models.

Because more than half the market value is tied to consulting projects, Swedish clients expect premium service levels. Rates for 24/7 security operations support typically exceed the EU average, and suppliers are expected to issue incident reports in Swedish and to participate in the national threat-sharing framework. Vendors that combine competitive subscriptions with support offerings in line with typical expectations for language requirements and responsiveness tend to shorten sales cycles and secure long-term contracts.

Strategic guidance for service providers

- **Stand out with specialised expertise.** Swedish clients are more likely to engage with providers that focus on specific areas, such as cloud security, IAM, or OT protection, rather than general offerings.
- **Ensure compliance early.** Meeting international standards such as ISO 27001 and preparing for NIS-2 alignment are essential for public-sector and critical-infrastructure projects.
- **Build trusted partnerships.** Most contracts flow through Swedish managed service providers or cybersecurity consultancies. Working with these partners enhances credibility and service delivery.
- **Communicate costs clearly.** Transparent per-user or per-site pricing, consistent with Swedish cost expectations, helps build trust and facilitates smoother procurement.

Market structure and access

Sweden’s cybersecurity demand is shaped by strict compliance requirements, high digital maturity, and a preference for local language support. Foreign service providers typically enter the market through specialised partners rather than direct sales. A clear understanding of these partners, and of the purchasing preferences of Swedish organisations, can significantly accelerate market entry and adoption.

Competitive landscape

Industry analysts describe Sweden’s cybersecurity market as moderately concentrated. The five largest suppliers – Clavister, Trend Micro, F5, Fortinet, and Dell Technologies – together account for just under half of all cybersecurity turnover in Sweden (Mordor Intelligence, 2024). Below this top tier, major global firms such as Microsoft, Cisco, and Palo Alto Networks hold strong positions in software-defined segments, while domestic scale-ups and specialised service providers – including Sectra, Recorded Future, Yubico, Detectify, and Truesec – add innovation and expertise in niche areas (InnovationQuarter, 2024).

Below are a few examples of companies active in Sweden's cybersecurity market, representing both international suppliers and domestic firms:

- **Clavister:** A Swedish cybersecurity provider headquartered in Örnsköldsvik, specialising in network security, particularly within critical infrastructure sectors such as defence, telecommunications, and public administration.
- **Trend Micro:** An international cybersecurity firm headquartered in Japan, offering cloud security, endpoint protection, and network security services. The company has a notable presence in Sweden's public sector.
- **F5:** A US-based company providing application-layer security and cloud-based cybersecurity services. In Sweden, the company mainly serves enterprise and public-sector clients.
- **Fortinet:** An American cybersecurity provider focusing on firewall technologies, secure networking solutions, and intrusion detection systems, with broad market penetration through local partners in Sweden.
- **Dell Technologies:** An American multinational with a significant market share in Sweden, delivering integrated cybersecurity solutions ranging from endpoint protection to comprehensive infrastructure security.
- **Axians:** A subsidiary of the French group VINCI Energies, Axians offers managed cybersecurity services in Sweden, including Security Operations Centre (SOC) operations and compliance management.
- **Holm Security:** A Stockholm-based cybersecurity company founded in 2015, offering vulnerability assessment, phishing simulation, and related risk management services, primarily to Swedish clients.

- **Allurity:** A cybersecurity group headquartered in Sweden, comprising eleven specialist firms across Europe, including Onevinn, the Arctic Group, and ID North. Allurity provides a full spectrum of services from threat prevention to incident response, with a mission to enable a safe digital society through local expertise and cross-border collaboration.
- **Sectra:** A Swedish firm focusing on secure communications and data protection, particularly for clients within the healthcare and defence sectors.
- **Truesec:** A Swedish cybersecurity consultancy providing managed detection and response (MDR), penetration testing, and incident response services, with notable activities within Sweden's cybersecurity consulting market.

Distribution and service partnerships

While international service providers play an important role in the Swedish cybersecurity ecosystem, local partners often act as a bridge to market entry. These partners handle localisation, client relationships, and ongoing service delivery.

The following types of actors are especially influential:

Type of partner	Examples in Sweden	What they do
Pan-Nordic value-added distributors (VADs)	Arrow ECS Sweden; Exclusive Networks Sweden	Provide pre-sales support, service packaging, and financing. Most new service providers begin with at least one of these partners.
Broad-line IT distributors	Ingram Micro Nordic; TD Synnex Sweden	Offer national logistics and credit, although with less focus on cybersecurity-specific services.
Systems integrators & large resellers	Atea Sverige, Advania, Telia Cygate, Nordlo, Iver	Deliver turnkey cybersecurity solutions and manage large-scale public-sector and enterprise contracts.
Specialist MSSPs & consultancies	Truesec, Sentor (Accenture), Outpost24, Combitech	Operate security operations centres (SOCs), offer managed detection and response (MDR), and account for a large share of Sweden's annual cybersecurity services spending.

For new service providers, building relationships with a strong VAD, along with one or two systems integrators or MSSPs, is often the most effective path to local market presence and credibility.

Routes to market preferred by Swedish organisations

Swedish organisations tend to favour structured, well-supported routes when procuring cybersecurity solutions. This reflects both regulatory expectations and a preference for local service, integration, and language support.

The most common sales and delivery models can be described as follows:

- Two-tier distribution remains common. Even cloud-native services are often channelled through a VAD and a systems integrator or reseller to meet localisation, billing, and support requirements.
- Managed services are growing rapidly. Due to talent shortages and 24/7 availability requirements, many organisations outsource security operations to MSSPs. These services are often white-labelled and delivered via VAD-backed SOC platforms.
- Direct SaaS with local support. Major providers such as Microsoft and CrowdStrike operate via Swedish subsidiaries, but typically partner with local firms for implementation and incident response.
- Framework agreements govern public-sector procurement. Sweden lacks a single national e-procurement platform; ministries and municipalities use several commercial portals, and contracts above EU thresholds are published on TED. Securing a framework agreement, often in partnership with a Swedish integrator, is key to unlocking long-term public-sector demand.
- Cloud marketplaces are growing among SMEs. Many small organisations procure seat-based security services via Microsoft Azure Marketplace, AWS Europe (Stockholm), or distributor-operated portals. While margins are thin, these platforms offer reach into a broad base of smaller clients.

Localisation remains essential, especially for public-sector and larger enterprise contracts.

> “*If you don’t have Swedish-language support, or if your reporting isn’t in Swedish, you’ll be filtered out early in most procurements.”*
>
> Stefan Thelberg, CEO of Holm Security

To succeed in Sweden, service providers should focus on building local partnerships, preparing Swedish-language onboarding materials, and aligning with established procurement practices, especially those linked to frameworks and compliance.

Trends and market drivers

Sweden’s cybersecurity market continues to evolve in response to regulatory change, the digital transformation, and increasing threats. Current trends influencing demand include tighter EU regulations, cloud migration, a shift toward zero-trust architectures, growing reliance on managed services, OT security in industrial sectors, persistent ransomware threats, support for SMEs, and increased defence-related investment. Understanding these trends can help international service providers better align their offerings with Swedish expectations.

Regulation tightens

The EU’s revised Network and Information Systems Directive (NIS 2) brings stricter requirements for risk management, supply chain oversight, and incident reporting across critical sectors. These changes are already influencing purchasing priorities in Sweden and are helping to drive strong demand for compliant cybersecurity services.

Service providers targeting the Swedish market should be prepared to demonstrate alignment with NIS 2 control areas, as compliance expectations are becoming an important factor in procurement decisions. The broader regulatory landscape, including both NIS2 and the upcoming DORA regulation, is expected to raise the bar for cyber resilience across sectors.

> “*Sweden is unique due to a high level of digitalisation, which means the potential risks for society may be greater compared to other countries in Europe. Domestic legislation is strong, but adding the NIS2 and DORA regulations is a welcome boost that will hopefully motivate companies that haven’t yet made cyber resilience a priority to take action.”*
>
> Roman Kovalchuk, Head of Cyber Consulting Nordics at Marsh

Cloud adoption and zero-trust architectures

Swedish spending on cloud-delivered cybersecurity services is expected to grow by around 10 per cent annually through 2029, outpacing on-premise solutions (Statista, 2024b). The near-universal use of BankID, which has been adopted by 97 per cent of adults, is driving demand for federated identity and conditional-access controls, which are central to zero-trust architectures (InnovationQuarter, 2024). Microsoft’s SEK 33.7 billion investment in new Azure regions, announced in June 2024, is further accelerating cloud adoption for sensitive workloads (Microsoft, 2024). Services that integrate with hyperscale platforms such as Azure, AWS (Stockholm), or Google Cloud, and that offer reference architectures aligned with zero-trust models, will be highly relevant to Swedish organisations.

This broader shift is reflected in the increasing demand for identity and access management (IAM), multifactor authentication, cloud-native security tools, and automated lifecycle management. Industry observers also note growing interest in protecting sensitive data across distributed environments, including the classification and encryption of information stored in Microsoft 365, AWS, and other platforms.

Demand for managed detection and response (MDR/XDR) has also accelerated, as organisations seek proactive solutions that go beyond alerting to include hands-on incident response.

> “*We’ve seen a significant rise in demand for identity and access management, cloud security, and zero-trust solutions, particularly as compliance expectations grow. Customers are maturing in their approach and now expect integrated, scalable architectures that support both protection and digital transformation.”*
>
> Maria Lörne, CMO, Allurity

Managed detection and response addresses talent shortages

Sweden continues to face a national shortfall of cybersecurity professionals. Consultancy and project-based services already account for an estimated SEK 6 billion of annual spending, and MSSPs report steady double-digit growth (InnovationQuarter, 2024). SonicWall’s July 2024 launch of a 24/7 Nordic SOC is one example of growing demand for regional MDR capabilities (SonicWall, 2024). Services that support rapid integration into SOC environments, use flexible billing models, and include Swedish-language documentation or training are well positioned.

Industrial and OT security gains momentum

As Sweden advances its Industry 4.0 ambitions, manufacturers, utilities, and logistics firms are connecting operational-technology (OT) systems to the cloud. The U.S. Commercial Service identifies industrial-control-system (ICS) security as one of the market’s fastest-growing segments. Since many domestic cybersecurity actors remain focused on traditional IT environments, service providers that offer protocol-aware detection, low-latency analytics, and IEC 62443-compliant solutions are especially well positioned.

Ransomware drives demand for resilience tools

Between 2019 and 2024, reported ransomware attacks in Sweden increased by 144 per cent, with attackers now also targeting supply-chain partners and end customers (Statista, 2024c). A major breach in early 2024 compromised more than one million personal records. Swedish organisations are responding by investing in immutable backup, incident-response retainers, and insurance-ready toolkits. Offerings that reduce dwell time, support automated containment, and enhance forensic visibility are gaining board-level interest.

SME adoption accelerates

Small and medium-sized enterprises (SMEs) make up 99 per cent of Swedish businesses. Public grants are channelled through the National Coordination Centre for Cybersecurity Research and Innovation and the EU-backed Secure Tech Hub, which subsidises basic cybersecurity controls and training (InnovationQuarter, 2024). Subscription-based services that combine endpoint protection, email security, and automated backup, especially when bundled with user-friendly onboarding, are increasingly distributed via web portals managed by local partners.

Defence, NATO, and public services remain priority verticals

Geopolitical tensions and Sweden's accession to NATO in 2024 have marked a significant turning point in the country's national security policy, accelerating investment in cyber defence and reinforcing its alignment with NATO's cybersecurity frameworks. This strategic shift is driving demand for services that meet NATO standards for interoperability, resilience, and secure communications.

In early 2024, the Swedish government allocated just over SEK 100 million to Cybercampus Sweden – a national initiative aimed at strengthening cybersecurity research, education, and workforce development. Coordinated by KTH Royal Institute of Technology, the programme brings together academia, industry, and government agencies to address national capability gaps and enhance resilience through joint research and innovation (KTH, 2024).

Sweden is also participating in NATO's Defence Innovation Accelerator for the North Atlantic (DIANA), and joined the NATO Innovation Fund in 2024. These platforms aim to foster technological innovation across allied nations, particularly in areas such as cyber resilience, secure communication systems, and emerging digital threats (NATO Innovation Fund, 2024).

As a result, Swedish defence and public-sector organisations are tightening procurement requirements, placing greater emphasis on:

- secure-by-design software and sovereign cloud compliance;
- interoperability with NATO systems and frameworks; and
- participation in joint cyber exercises and cross-border incident response.

This presents growing opportunities for service providers that can contribute to:

- military-grade threat intelligence and secure DevSecOps pipelines;
- managed detection and response (MDR) services that meet NATO resilience standards; and
- solutions for incident response coordination and secure system integration across public-sector and defence networks.

Implications for service providers from low- and middle-income countries

Trend	Practical opportunity
NIS 2 compliance	Offer gap-assessments, toolkits, and templates aligned with EU control areas
MDR and talent shortages	Partner with MSSPs; provide Nordic-relevant threat intelligence and SOC add-ons
Cloud-first security	Deliver SaaS tools integrated with Azure/AWS/GCP and zero-trust models
OT security	Provide ICS/OT services with protocol-level awareness and IEC 62443 compliance
SME enablement	Develop packaged services with user-friendly onboarding for reseller distribution
Ransomware resilience	Offer fast-deployment response kits, backup, and forensic-ready services
NATO and defence	Pursue joint bids or tech partnerships in NATO-aligned innovation programmes

What requirements do suppliers need to meet?

To successfully enter and operate in the Swedish cybersecurity market, foreign service providers must meet a range of legal, regulatory, technical, and business requirements. These include compliance with EU and Swedish legislation, alignment with recognised cybersecurity and quality standards, and adherence to broader governance and sustainability expectations. This chapter outlines what service providers need to know and how to prepare.

Legal requirements for service providers

Export controls for dual-use items

Some cybersecurity products may be classified as "dual-use" technologies under Regulation (EU) 2021/821, meaning they can be used for both civilian and military purposes. Products such as intrusion detection systems, deep packet inspection software, and certain encryption technologies fall under this regulation. Non-EU service providers must ensure that any relevant products are approved by the Swedish Inspectorate of Strategic Products (ISP), which enforces EU export controls in Sweden (International Trade Administration, 2024).

Data protection and the GDPR

All service providers operating in Sweden must comply with the General Data Protection Regulation (GDPR). This includes ensuring cybersecurity solutions support key principles such as privacy-by-design, data minimisation, and breach notification within 72 hours. Solutions must also facilitate lawful data transfers and robust data access controls (European Commission, 2024).

Lawful interception and privacy

While Swedish organisations may monitor their own IT infrastructure to detect threats, tools must comply with Swedish privacy legislation. Providers should ensure their monitoring solutions support legal boundaries, particularly concerning employee privacy and user data.

Cybersecurity regulations

Several EU-wide regulations are directly relevant to cybersecurity providers:

- **The NIS 2 Directive** sets baseline cybersecurity requirements across critical sectors, including incident handling, supply chain risk management, and secure development practices.
- **The Cybersecurity Act (Regulation EU 2019/881)** establishes a common EU cybersecurity framework and outlines a certification scheme that may affect procurement in Sweden.

Additionally, national sector-specific laws may apply depending on the area of operation, such as finance, energy, or healthcare.

Industry standards and certifications

Swedish organisations value recognised international standards and certifications. Aligning with these frameworks demonstrates both technical reliability and compliance readiness.

Information security management (ISO/IEC 27001)

Widely adopted in Sweden, especially among public sector bodies and large companies, this standard provides a robust framework for information security management systems (ISMS) and is considered a strong trust signal.

Industrial cybersecurity (IEC 62443)

This series of standards focuses on cybersecurity for industrial automation and control systems. It is particularly relevant for service providers targeting critical infrastructure, manufacturing, and energy sectors.

Common criteria (ISO/IEC 15408)

Sweden’s Certification Body for IT Security (CSEC) supervises evaluations of security products based on the Common Criteria framework. Certification to these criteria is often required for solutions used by public agencies or critical infrastructure operators.

Other quality standards

In addition to security-focused certifications, Swedish organisations also value broader quality and service standards:

- **ISO 9001** (Quality Management Systems)
- **ISO/IEC 20000-1** (IT Service Management)
- **ISO 22301** (Business Continuity Management)

These standards are especially relevant when competing in public tenders or working with enterprise clients.

Professional certifications

Swedish clients often expect service teams to hold industry-recognised certifications such as:

- **CISSP** (Certified Information Systems Security Professional)
- **CISM** (Certified Information Security Manager)
- **CEH** (Certified Ethical Hacker)

These credentials help establish credibility and technical competence, especially when entering a new market. In addition to individual qualifications, organisational certifications aligned with international standards are becoming increasingly relevant.

Swedish organisations, especially those in the public sector and high-risk industries, often consider these certifications essential for vendor evaluation, due diligence, and risk mitigation.

> “*International certifications like ISO 27001 and SOC 2 are playing an increasingly important role in procurement. They serve as a quality seal, simplify due diligence, and give customers peace of mind, especially in sensitive or large-scale deployments.”*
>
> Maria Lörne, CMO at Allurity

Governance and ethical business conduct

Swedish companies expect high standards of ethics and transparency from their suppliers. Foreign service providers must demonstrate:

- legal compliance and tax transparency;
- clear business ownership structures (e.g. ultimate beneficial owners);
- ethical financial practices and anti-corruption measures;
- respect for human rights and fair labour practices; and
- financial soundness and long-term viability.

These expectations are increasingly embedded in Swedish public procurement processes and risk assessments, especially in sensitive sectors such as government, defence, and healthcare.

Sustainability expectations and ESG alignment

Sustainability is an increasingly important factor in public and private procurement in Sweden, including in the cybersecurity sector. While cybersecurity services are not inherently high-emission, Swedish organisations, especially in government and regulated industries, expect their service providers to align with broader Environmental, Social and Governance (ESG) principles. This creates opportunities for cybersecurity providers who can offer:

- secure platforms for ESG data collection and reporting;
- protection of sustainability and compliance systems from cyber threats; and
- cyber risk management linked to ESG-related supply chains.

Service providers that align with the UN Sustainable Development Goals, the European Green Deal, or Sweden’s national climate goals will have a competitive advantage in procurement processes.

New EU cybersecurity regulations

In addition to NIS 2, other newly adopted or upcoming EU rules may also affect foreign service providers:

The Cyber Resilience Act (CRA)

The CRA was officially published in November 2024 and entered into force shortly thereafter. It introduces binding cybersecurity requirements for digital products and software, with a phased implementation:

- From late 2026, providers must begin reporting serious cybersecurity incidents.
- From late 2027, full compliance is required for CE-marking and market access.

Service providers will need to ensure:

- built-in security by default and design;
- ongoing patching and update mechanisms; and
- incident response capabilities.

These requirements apply to both standalone software and software embedded in digital products. Providers are encouraged to begin aligning their development and support processes well in advance of the deadlines.

The Radio Equipment Directive (RED)

Cybersecurity provisions under the updated RED were adopted via Delegated Regulation (EU) 2022/30 and will become mandatory on 1 August 2025. The directive applies to wireless and IoT devices with radio functionality and affects any embedded software or service component.

Providers offering software within such connected devices must ensure:

- protection against network threats;
- safeguards for personal data and privacy; and
- defence against fraud or unauthorised access.

Together, the CRA and RED establish a new baseline for cybersecurity in digital and connected products within the EU, and compliance will be essential for market access from 2025 onwards.

Find a business partner

Sweden offers a well-connected and mature cybersecurity ecosystem. Foreign service providers can accelerate market entry by leveraging trade fairs, business associations, and databases to build partnerships, gain visibility, and adapt to local Swedish client preferences.

Trade fairs and conferences

Personal interaction remains a key factor in building trust and credibility. Sweden hosts several relevant events:

- **Cyber Security & Cloud Expo (Stockholm):** Typically held in **May**, this event focuses on cloud security and cybersecurity innovation, offering excellent networking opportunities.
- **Stockholm Tech Show (Stockholm):** Usually takes place in **May**, covering AI, cybersecurity, cloud, DevOps, and more.
- **CyberSec Nordic (Helsinki):** Typically held in **late autumn**. This Nordic-wide cybersecurity conference is highly relevant for companies targeting the region.
- **SecTech (Stockholm):** Held every other year in **October**, this event features physical and digital security solutions and attracts security managers from across industries.
- **Homeland Security Expo Sweden:** Typically held in **March**, focusing on public-sector defence and cybersecurity.

By attending these or other regional events, service providers can demonstrate their capabilities, gather competitive intelligence, and build the personal relationships that often precede formal contracts.

Sources of information and networking platforms

Joining established business associations and/or networking platforms can ease market entry. At the same time, many of the platforms listed below offer reliable market information.

- **SOFF – Swedish Security and Defence Industry Association:** The leading trade association for companies active in civil and military security, including cybersecurity. Offers policy insights, matchmaking, and visibility among key stakeholders in Sweden’s defence and security sectors.
- **Sweden Secure Tech Hub:** A national initiative promoting innovation and collaboration in cybersecurity. Provides access to scale-up support, matchmaking opportunities, and connections to regional actors across Sweden.
- **Cybernode (National node for cybersecurity):** A strategic collaboration between academia, industry, and government that coordinates Swedish cybersecurity innovation efforts. Useful for understanding the Swedish ecosystem and identifying potential partners.

- **RISE – Center for Cybersecurity:** A research and innovation centre providing testbeds and collaboration opportunities in cybersecurity. Not a business association, but relevant for providers interested in co-development, validation, or certification efforts.
- **Business Sweden:** Jointly owned by the Swedish state and business sector, it offers matchmaking, introductions, and support for market entry, including public-private partnerships.

In addition, local chambers of commerce and regional industry networks can offer targeted opportunities for networking and market engagement.

Online tools and company databases

Digital tools can be valuable for identifying partners, customers, and competitors:

- **LinkedIn:** Use filters to identify cybersecurity-related companies and professionals.
- **Allabolag.se (Swedish):** Offers detailed company information, including financials and ownership structure.
- **Upphandling.se:** Public procurement site listing tenders from municipalities and government agencies. Winning public contracts can also serve as valuable references, increasing credibility and helping providers enter the private market.
- **Crunchbase / Vainu / OpenCorporates:** International databases useful for strategic research and prospecting.

What Swedish clients expect

Swedish organisations tend to prioritise reliability, responsiveness, and compliance. They expect service providers to deliver technically strong solutions while also demonstrating a clear understanding of the local market context and client needs.

> “*We look for partners who are proactive, accessible, and who understand our needs and the market context. Swedish is not required – English works perfectly – but there must be a clear and responsive point of contact. On the technical side, strong competence and certifications are key.”*
>
> Ola Skoog, Sales Manager, Axians

This emphasis on strong relationships and clear communication reflects broader expectations across the market. Swedish clients value documentation and customer support in Swedish, especially in public institutions or critical infrastructure. Solutions that align with the GDPR, the NIS Directive, and international standards such as ISO/IEC 27001 are seen as more trustworthy and lower-risk.

> “*Sweden is a mature but open market. We often discover new partners through global vendor ecosystems, conferences, or recommendations. For companies entering the market, compliance, transparency, and clear differentiation are key, and trust must be built over time.”*
>
> Maria Lörne, CMO at Allurity.

Swedish clients also appreciate fast incident response and robust after-sales service, particularly in high-stakes environments. A local presence or Swedish-speaking representatives can further strengthen credibility. Above all, long-term partnerships are built on trust, clear communication, and a demonstrated commitment to meeting local expectations.

Local presence vs. remote delivery

While Swedish clients appreciate face-to-face contact and cultural familiarity, they are also accustomed to working with remote teams. A hybrid model is often preferred: Swedish-speaking representatives who handle client communication, supported by offshore or nearshore teams that provide round-the-clock coverage or specialised skills.

> “*One of the biggest challenges in cybersecurity is scaling. Having people available when, for example, several clients are attacked at the same time is almost impossible to plan for. But if we had small teams in different countries that we could call in when needed, that would be incredibly valuable. Knowing that a team in, for example, Ukraine is ready to step in if something happens provides a level of reassurance that is hard to overstate.”*
>
> Ola Skoog, Sales Manager, Axians

This type of flexible support model is particularly relevant for managed services and incident response, where availability and responsiveness are critical. Service providers from low- and middle-income countries may be well positioned to fill this gap, especially if they can offer certified staff, integrate with Swedish workflows, and commit to being available on short notice.

To succeed in this role, providers must demonstrate not only technical competence but also strong communication skills, responsiveness, and an understanding of the Swedish client’s expectations. A single, reliable point of contact and the ability to collaborate openly and proactively are often more important than speaking Swedish.

Summary:
What you need to do to secure business

To successfully enter the Swedish cybersecurity market, companies from low- and middle-income countries should follow a clear, strategic approach based on both general market entry practices and specific expectations in the cybersecurity sector.

General aspects

- **Market research:** Understand the size and structure of Sweden's cybersecurity market, including the role of public and private actors. Use sources such as Business Sweden, Allabolag.se, and Upphandling.se to gather market intelligence.
- **Product/market fit:** Identify your niche, such as public-sector cybersecurity services, penetration testing, or managed SOC, and tailor your offer accordingly.
- **Business communication:** Communicate clearly and transparently in English or Swedish. Swedish clients expect high clarity and reliability.
- **Business registration (when applicable):** If planning to operate locally, register your business with relevant authorities through platforms such as Verksamt.se.
- **Good online presence:** Ensure your website and LinkedIn profiles are up to date and clearly describe your cybersecurity services and certifications.

Additional aspects for service providers

- **Compliance and certifications:** Be prepared to show compliance with EU standards such as GDPR and the NIS Directive. Certifications such as ISO/IEC 27001 are viewed as strong trust signals.
- **Documentation and language support**: Provide documentation and customer support in Swedish when possible, especially for public sector or larger enterprise clients.
- **Responsiveness and support:** Swedish clients value short response times and strong after-sales service, especially in case of security incidents.
- **Networking and visibility:** Attend relevant trade shows such as Cyber Security & Cloud Expo, Stockholm Tech Show, or SecTech to meet potential partners and clients. Use platforms such as LinkedIn and Allabolag.se to find business opportunities and build relationships.
- **Local presence or partnerships:** While not always required, having a local representative or Swedish-speaking staff can improve credibility and ease of collaboration.

By actively addressing these areas, cybersecurity service providers from low- and middle-income countries can enter the Swedish market more effectively, build trust with Swedish clients, and lay the foundation for long-term partnerships.