strategy&

Part of the PwC network

Nordic Cybersecurity positioned for Long-Term Growth

Point of view– Extract

Strategy&

October 2025

strategy&
Part of the PwC network

About Strategy&

Strategy& is a global team of over 4,000 dedicated top-tier management consultants. Senior executives at leading organizations turn to Strategy& when faced with the need for a strategic shift in response to particularly complex and time-critical challenges.

We specialize in strategy development and provide high-impact strategic advisory services to leadership teams navigating their most demanding and high-stakes issues. Our work spans across industries and includes close collaboration with private equity clients, where we support transactions, mergers and acquisitions (M&A), and post-deal value creation.

Our teams bring deep experience in unlocking growth and driving transformation in precisely these situations. With sharp industry insight, Strategy& delivers strategic solutions with the speed and precision required to help our clients gain competitive advantage—both as business leaders and as organizations.

As a global leader in strategy consulting, Strategy& is part of PwC Norway. We seamlessly leverage the full breadth of PwC's global and local multidisciplinary expertise to ensure our clients' strategic potential is both defined and realized.

4500+ strategy consultants worldwide

220+ consultants across the Nordics

75+ countries with active presence

Selected core capabilities

Corporate Strategy
Mergers & Acquisitions
Deal Value Realization

Cybersecurity is at the center of key megatrends that are shaping society

I. Emergence of AI and new technologies provide new vulnerabilities

- New technology shifts – especially Agentic AI, IoT, cloud and remote work – is driving an explosion of attack surfaces by exposing ever-more data, processes and hardware
- AI provides hostile actors with an ability to rapidly scale common attack vectors, such as spreading of disinformation. The swift evolution and proliferation of AI will produce unforeseen threats, compounding the challenges of cyber defense.
- At the same time, AI provides an opportunity for cybersecurity providers to increase efficiency and quality of detection creating a "high-stakes arms race" between the black and white hats

II. Geopolitical tensions drives overall spend and sourcing from allied nations

- Geopolitical tensions drives an increase in attacks form hostile state actors, with the Nordics seeing a ramp-up in hybrid threats, especially from Russia[1]
- This has led to an increased emphasis on Nordic or European-built security infrastructure, and sovereign solutions
- As well as governments expanding cyber wartime spending, exemplified by Finland's KYHA[2] exercises and Norway's preparedness plans
- According to PwC's global Trust Insight survey, 60% of organizations expect to increase investments in cyber in response to the ongoing volatility

III. NIS2 and other regulations pushes adoption and spend to be compliant

- To respond to the widespread digitalization, EU requires member states to enhance their capabilities through the NIS2[3] directive, in effect as of 2024
- NIS2 will be a key driver in growing cybersecurity services penetration across a broad range of industries[4], with mandatory requirements for a broad range of industries
- In addition to NIS2, EU Cyber Resilience Act (CRA), DORA and other legislations will continue to increase adoption and spend to avoid penalties

Notes: 1) Such as Alleged Russian hackers taking control of a hydro dam in Norway (Aug. '25), 2) KYHA stands for "Kyberturvallisuusharjoitus" which translates to cybersecurity Exercise, 3) Network and Information Systems Directive, 4) Mandatory for industries such as Healthcare, Financial services, Digital infra., and Water supply
Sources: Strategy& analysis

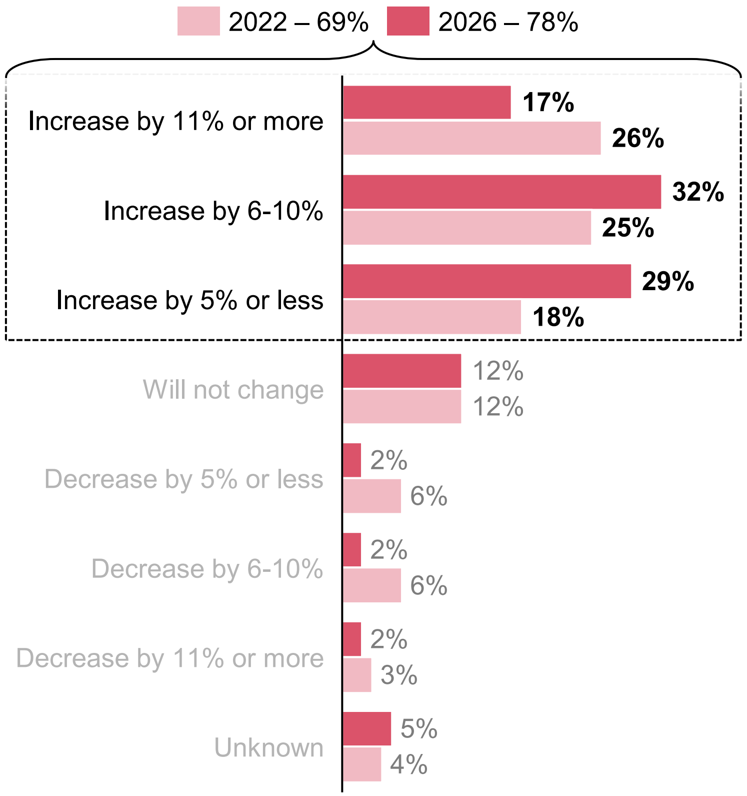
LINK TO FULL REPORT: PWC 2026 GLOBAL DIGITAL TRUST INSIGHTS

Trends supported by global security leaders that prioritise AI and cloud security, and anticipate relocation of critical infrastructure

PwC 2026 Global Digital Trust Survey – selected insights

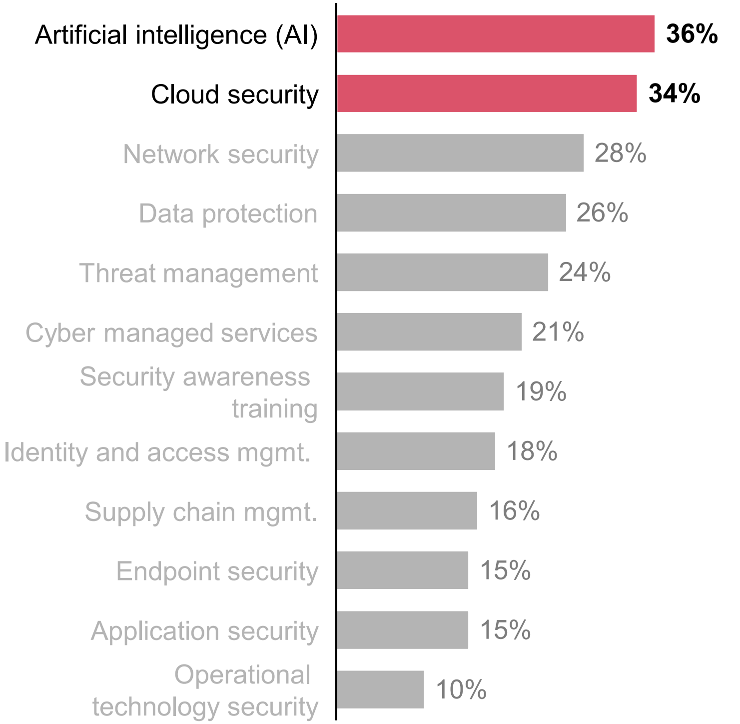
78% of security leaders anticipate increase in cyber budgets in 2026, up from 69% in 2022

Q: How will your organisation's cyber budget change?
n = 2027



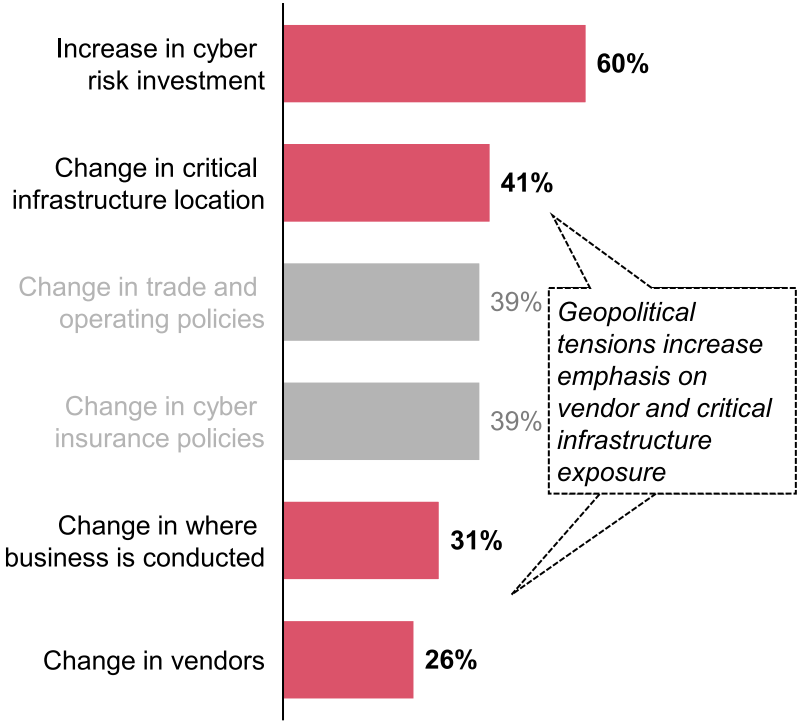
Security leaders are prioritising AI and cloud security when allocating cyber budgets

Q: Which of the following investments are you prioritizing when allocating your organization's cyber budget in the next 12 months?
n = 1740



Cyber strategy and sourcing changes in response to geopolitical landscape

Q: Over the next 12 months, which of the following areas of your organization's cyber strategy is changing in response to current geopolitical landscape
n = 3887



Source: PwC 2026 Global Digital Trust Insights

The cybersecurity market can be defined as Services, Software and Hardware, wherein most Nordic companies focus on Services

Cybersecurity market definition, % share of Nordic market revenue in 2024

Services

70%

Sub-segments (non-exhaustive)

Managed services (MSSP) and consultancy

- Managed cyber defense (incl. SOC[1])
- Incident response
- Post incident reviews
- Threat advisory and intelligence
- Consultancy
- Re-selling of software and hardware

Offerings

Deliver 24x7, cyber defense as a fully managed outcome - combining re-selling and implementation of best-of-breed tooling with expert analysts to **lower total cost of ownership and let customers team stay focused on core business**

Pure-play Consultancy

- Security strategy & assessment
- Governance, risk and compliance (GRC)
- Cloud security and architecture
- Penetration testing
- Implementation of security solutions
- Due diligence and transaction support
- Crisis exercise and programs

Align security strategy to business objectives - blending regulatory insight, threat intelligence, and implementation expertise to **accelerate compliance and de-risk digital transformation**

Software

25%

Software

- Infrastructure protection
- Identity access management (IAM, IGA, PAM[2])
- Application Security
- Cloud security
- Data Privacy & Security
- Integrated risk management

Develop and deliver software **to protect organizations from cyber threats while simplifying administration** across the hybrid environment

Hardware

5%

Network security equipment

- Firewall Equipment
- Intrusion detection (IDPS)
- Network Detection and Response
- Network Access Control
- Zero Trust Network Access

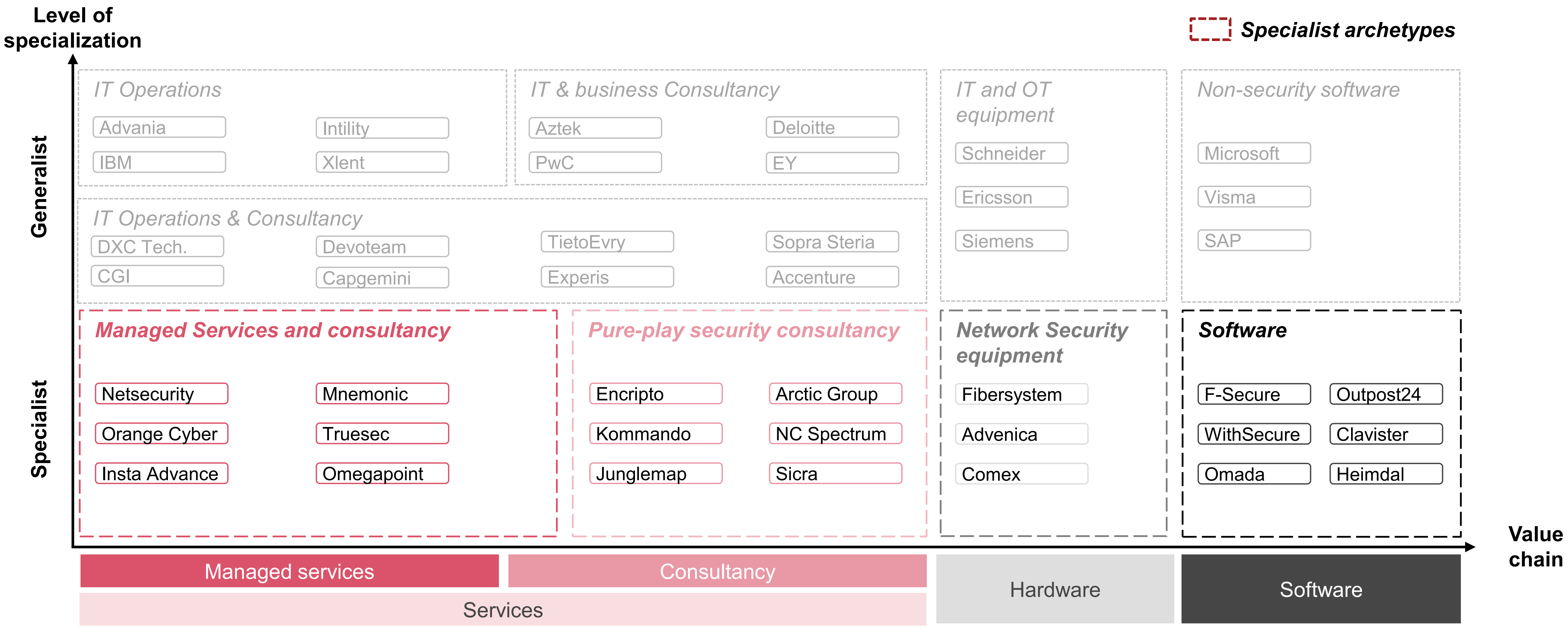
Develop and deliver hardware **safeguard against cyber threats**

Notes: 1) Security Operations Center, 2) Identity Governance & Administration, Privileged Access Management
Sources: Gartner, Strategy& analysis

Non-exhaustive

In the Nordic market, specialists compete against generalists delivering cybersecurity services and products

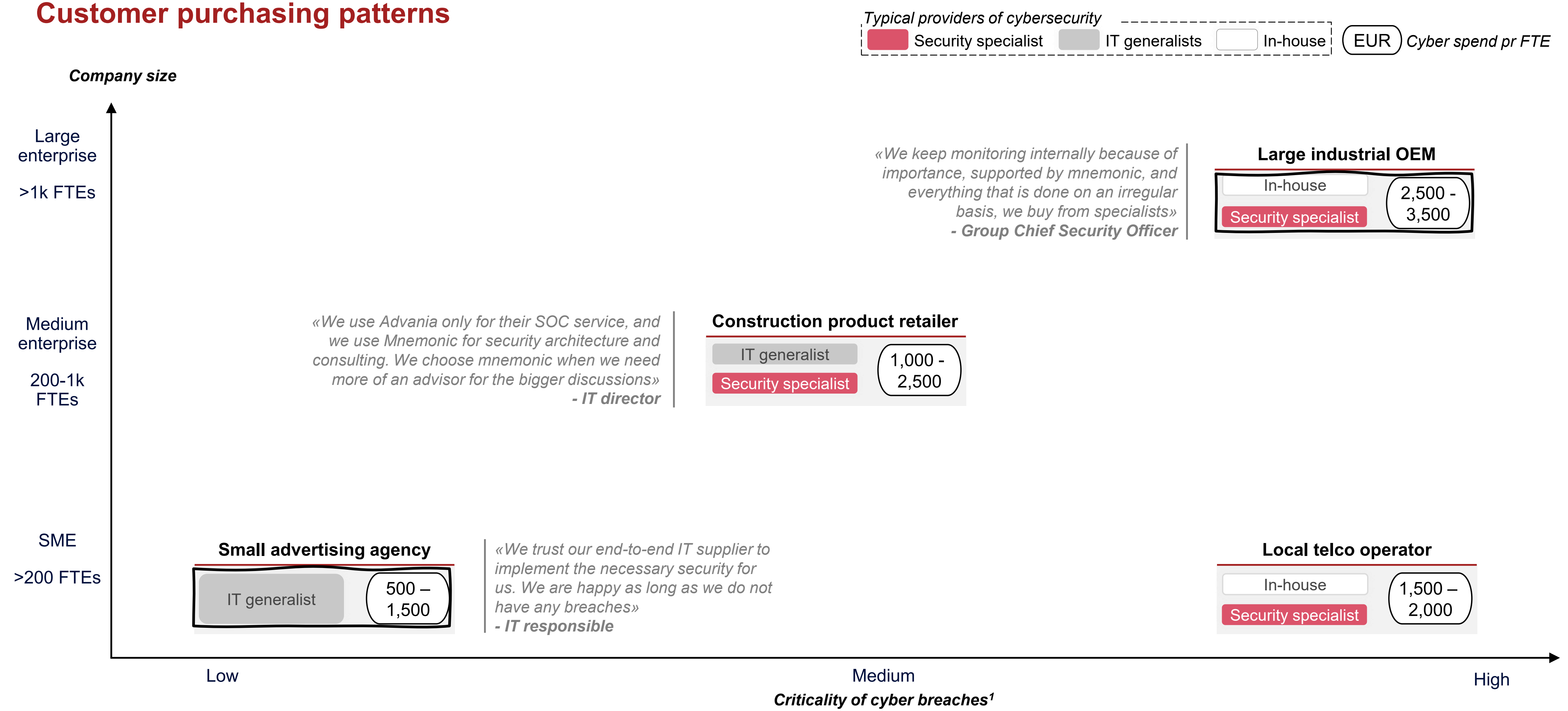
Nordic cybersecurity landscape



1) Managed Detection and Response, 2) Managed Security Service Provider
Source: Gartner, Strategy& analysis

Customer demand for cybersecurity protection vary by company size and criticality of breaches - spend to specialists increase with criticality

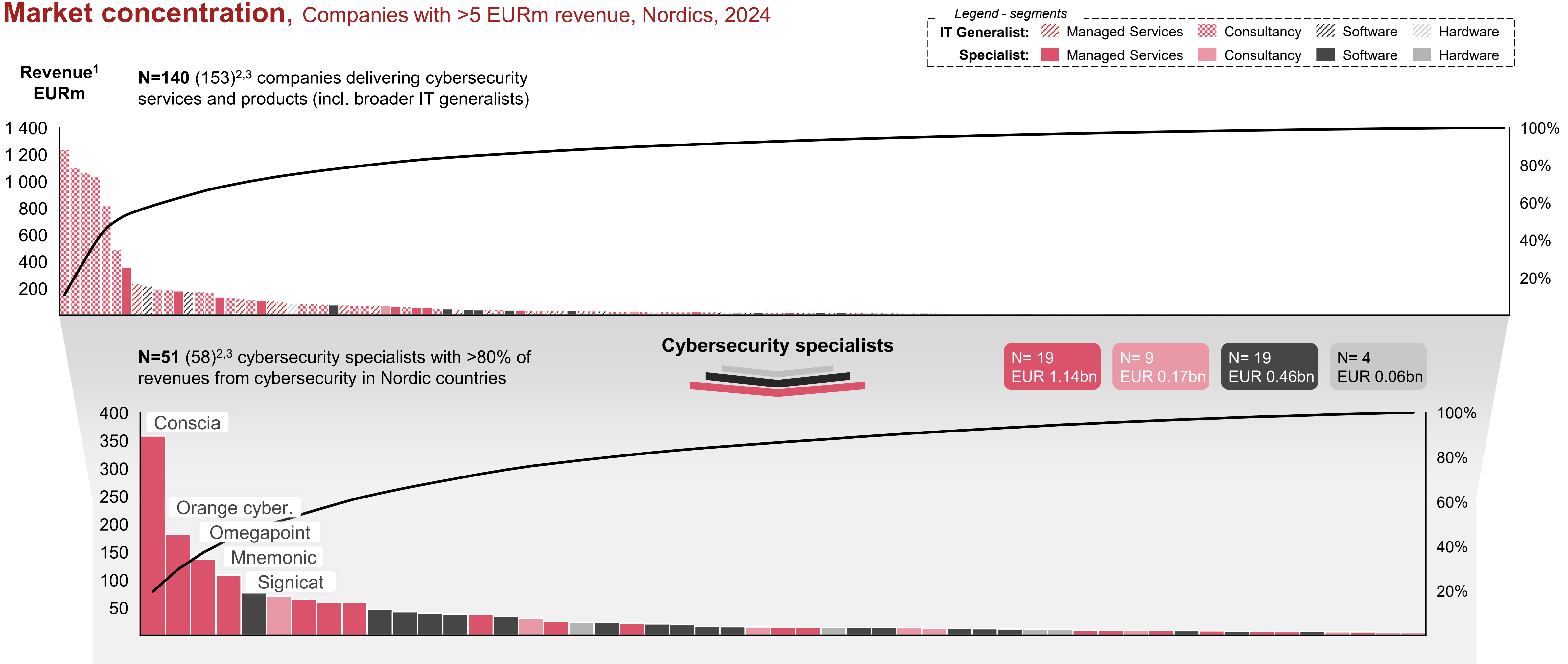
Customer purchasing patterns



Notes: 1) Companies in industries with large potential damages of breaches and/or with strict compliance requirements (government, utilities, healthcare, banking)
Source: Strategy& analysis, customer interviews

Including Generalists there are ~140 companies deliver cybersecurity, of which ~60 are specialized, with the largest being Managed Services

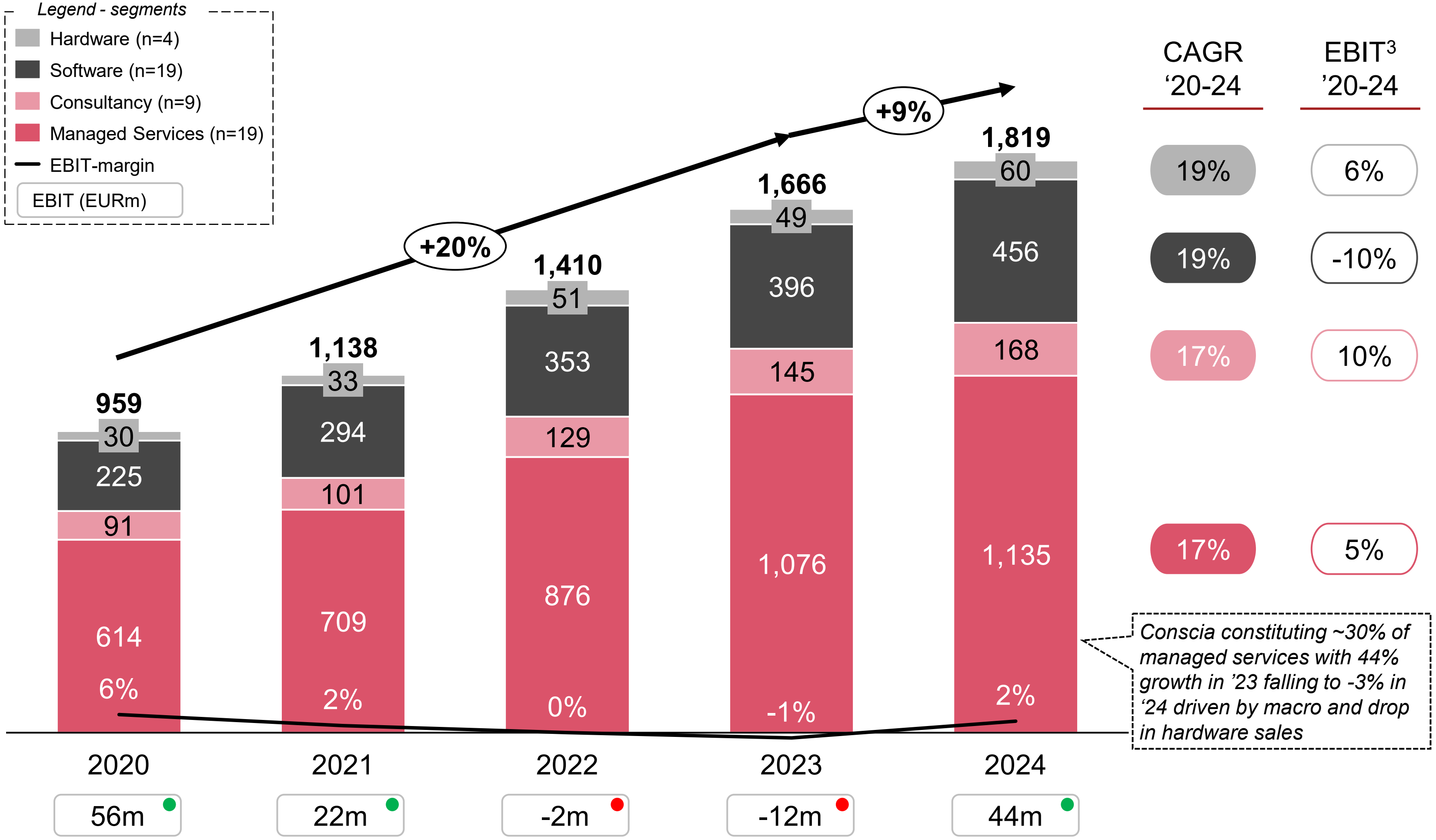
Market concentration, Companies with >5 EURm revenue, Nordics, 2024



Notes: 1) Exclude non-Nordic revenues – Yubico and Outpost24 not making the Nordic revenue criteria; 2) N=6 IT Generalists (Incl. Combitech) and N=7 specialists without 2024 financials available made the >EUR 5m threshold in 2023 (not included in visualization and revenue aggregation); 3) Number of company brands i.e. Accenture is counted as one, but financial figures are derived from aggregation of the Nordic entities (4 subsidiaries in NO, SE, DK, FI)
Sources: Valu8, Company reports, Desktop research, Strategy& analysis

The specialists has had strong ~20% growth and collective profitability decline '20-'23 - as growth slows to ~10% in '24, profitability improves

Financial development of identified cybersecurity specialists[1], companies with >5 EURm revenue 2024, Nordics, EURm



Revenue

- After robust 2020–2023 growth culminating in record 2023 results (e.g., Conscia), 2024 slowed to an above-industry 9% YoY, mainly on weaker Managed Services (+5%), with the pullback driven by several factors
  - Normalization of supply chain disruptions following COVID that boosted deliveries in 2022-2023 coupled with macroeconomic challenges such as high interest rate, especially impacting sales of "new products" through Managed services vendors
- Despite 2024 new-product sales declines, double-digit software/services growth persists, with a 10–15% long-term rebound expected, driven by AI, new tech, geopolitics, and regulation

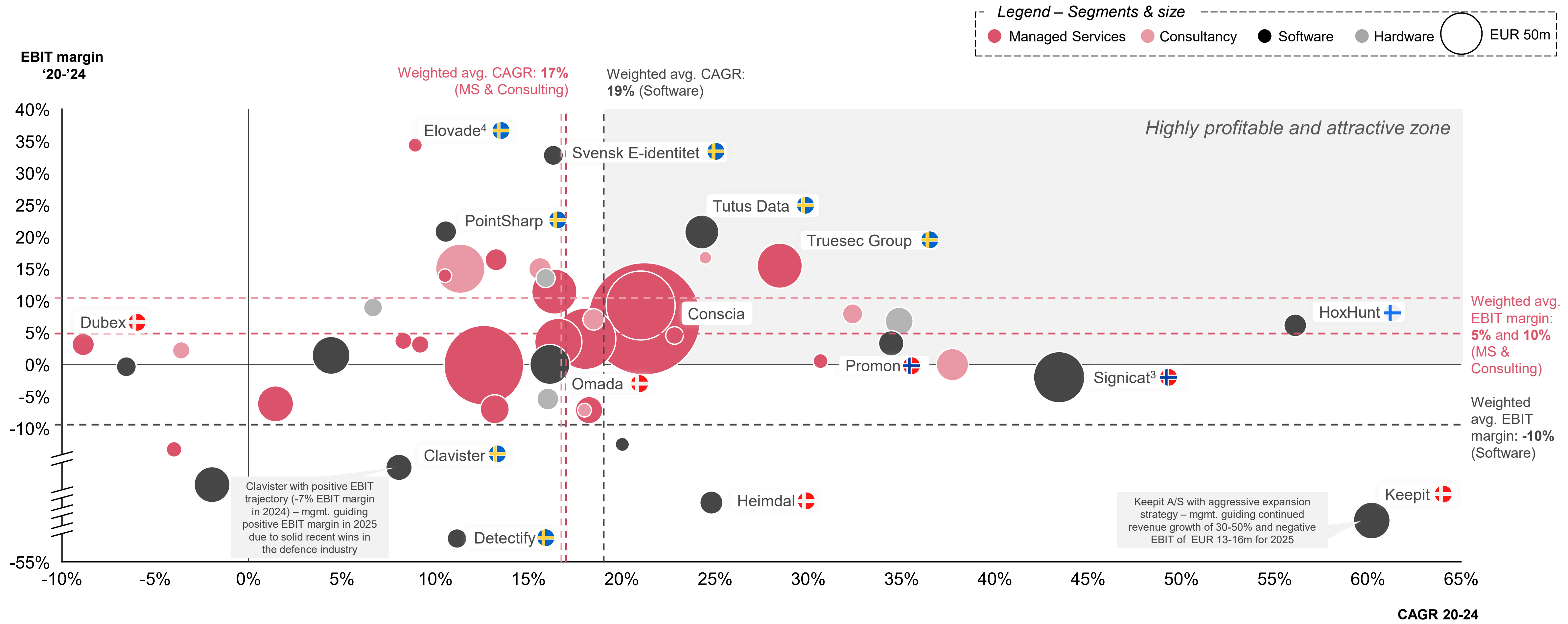
Profitability

- Collective profitability declines during the sharp 2020-2023 growth, and bounce back to positive territory during 2024 growth de-acceleration
  - Software led losses, with large players (e.g., Logpoint, KeepIt) investing heavily in product development and sales/marketing to position for future growth
  - Managed services struggled to scale; growth still required more human analysts despite AI, while teams built new detections for emerging tech and more sophisticated threats

Notes: 1) The figures exclude non-Nordic revenue and include non-cybersecurity related revenue, thereby revenue build up does not correspond to market size; 2) Number of company brands i.e. Accenture is counted as one, but financial figures are derived from aggregation of the Nordic entities (4 subsidiaries in NO, SE, DK, FI), 3) Weighted average EBIT margin
Sources: Valu8, Company reports, Desktop research, Strategy& analysis

Although the collective profitability is low, there are large variations with many highly profitable and attractive companies

Growth and profitability[1] of the Nordic cyber specialists[2], 2020-2024, EURm



Notes: 1) For companies without revenue for 2020 we have used CAGR & avg. weighted EBIT margin 21-24 (Promon AS, Defendable AS, Detectify AB, Heimdal Securty A/S, WithSecure, F-Secure Oyj & HoxHunt Oy); 2) Only companies with reported revenue (excluding those with estimated revenue based on DK gross margin); 3) Nordic revenues; 4) Previously Innosoft
Sources: Valu8, Annual reports, Company website, Strategy& analysis

The cybersecurity markets holds opportunities and challenges for both corporates and Private Equities to navigate going forward

The Nordic cybersecurity market remains very attractive with several opportunities and challenges fueled by both local factors and global megatrends

~60 specialized Nordic cybersecurity companies with strong historical 2020-2024 CAGR of 17%

Continue strong growth expected driven by megatrends shaping society; AI and emerging technologies, geopolitical tensions and regulatory push

Profitability remains a key challenge in a rapidly evolving industry with high growth and product innovation driving investments in R&D for future growth

Strategy& and PwC can help vendors, investors and management teams navigate the rapidly evolving cybersecurity market through e.g.

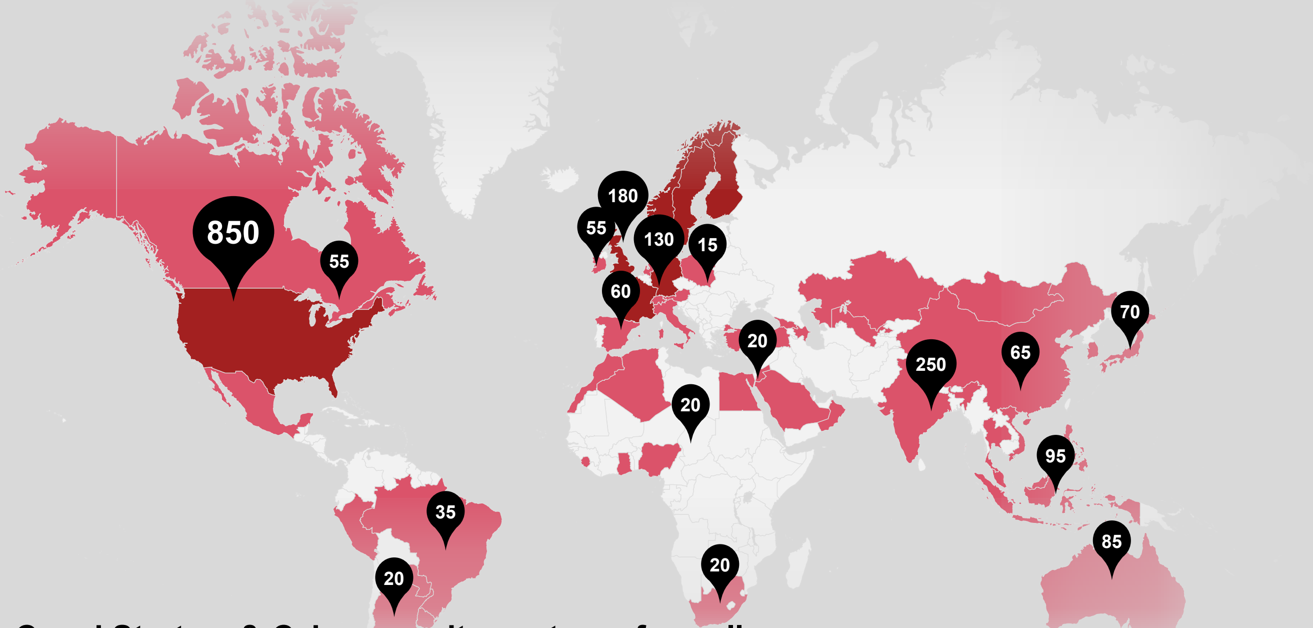
1. Due diligence and transaction support on specific targets
2. Strategy and go-to-market update
3. Product portfolio review and optimisation
4. Cost efficiency and scalability improvements
5. Vendor selection and navigating emerging technologies
6. Cybersecurity strategy, architecture and risk assessments

Our team combines strategy and deep cybersecurity domain expertise

+3,200
Number of PwC Cybersecurity consultants

+60
Technical security and forensics labs located in 40 countries

+600
No. of incident response cases managed by PwC per year



PwC and Strategy& Cybersecurity centers of excellence

In contrast to other strategic advisors, we are unique in our ability to leverage our globally recognized cybersecurity practice to provide deep and far-reaching market insights

Erling Fiskerud
Director, Strategy& Oslo
Email: erling.fiskerud@pwc.com
Tel: +47 98 82 92 86

Trygve Nøst Bergem
Senior Manager, Strategy& Oslo
Email: Trygve.bergem@pwc.com
Tel: +47 99 29 95 58

Anders Brun
Partner, Strategy& Oslo
Email: anders.brun@pwc.com
Tel: +47 98 20 40 10

Jan Henrik Straumsheim
Partner, PwC Cyber Oslo
Email: jan.straumsheim@pwc.com
Tel: +47 41 52 62 90

Erik Wall
Partner, Strategy& Stockholm
Email: erik.wall@pwc.com
Tel: +46 70 929 31 25

Jussi Lehtinen
Partner, Strategy& Helsinki
Email: jussi.lehtinen@pwc.com
Tel: +358 20 7878756

Contributors

Jørgen Frost Bø
Gaute Lien
Eldar Lillevik
Nelson Cheuque
Ole Kristian Larsgård
Even Bydal
Arvid Hanson
Hugo Durelius

strategy&
Part of the PwC network

Thank you

strategyand.pwc.com