



F-Secure.

CYBERSECURITY INNOVATION IN THE NORDICS

Janne Pirttilahti

Vice President, Cloud Protection @F-Secure

SCATTERED MARKET – SOME SEGMENTS GROW FAST, SOME LESS SO, SOME VERY PROFITABLE, SOME LOSS MAKING



Source: Momentum Partners.

Advanced ▾

crunchbase

Investors Funding Rounds Acquisitions People Events

1-50 NEXT ▸ of 33,103 results

Organization Name ▾	IPO Status ▾	Operating Status ▾	Number of Employees ▾
Lacework	Private	Active	501-1000
Gate.io	Private	Active	101-250
Socure	Private	Active	251-500
GitLab	Public	Active	1001-5000
CrowdStrike	Public	Active	1001-5000
SentinelOne	Public	Active	501-1000
Sift	Private	Active	101-250
Drata	Private	Active	51-100
BT	Public	Active	
Darktrace	Public	Active	
CLEAR	Public	Active	
Contrast Security	Private	Active	
Cybereason	Private	Active	
Expel	Private	Active	
Cloudflare	Public	Active	

HOW MANY “STARTUPS” IN SECURITY?

security, cloud security,
cyber security, network security
33 103 companies

NORDICS
721 companies (2.2% out of 33k)



NORDICS VIEW

Highly digitalized market
Strong Startup & Innovation ecosystem
Home markets hardly big enough
What works here – (typically) works everywhere

A Nordic Startup should consider to:

- Go global fast
- Hire remotely
- Be cost efficient
- Think slow, act fast

SECURITY CHARACTERISTICS IN THE NORDICS

**Security....
Same same?
But still the same?**



Image source: pixabay (CC license)

THEMES FOR THE COMING YEARS



- Computing is commodity – distributed AI maintaining security and privacy can make a difference
- Everyone is big on AI – trustworthiness is an important challenge
- Multi-cloud (and on-premise / cloud hybrid) at times with data sovereignty requirements
- Cyber security is HUGE market (and growing)



JOINT RESEARCH, CO-OPERATION AND PUBLIC FUNDING ENABLE GROWTH AND NEW INITIATIVES

- Horizon 2020 (Horizon Europe) is the most attractive funding instrument by the European Commission for F-Secure's R&I activities
- Competition is intense but the high Horizon funding rates and EU-wide collaboration opportunities justify the efforts.
- European Cyber Security Organization (ECSO) facilitates Horizon project partnerships within the European cybersecurity community

A LOOK AT A FEW RESEARCH PROJECTS

- **SSICLOPS** (2015 – 2018): designed and prototyped key content distribution and client query handling algorithms of F-Secure Security Cloud
- **SOCCRATES** (2019 – 2022): combining vulnerability information, asset and information inventory with attack detection capabilities
- **CC-DRIVER** (2020 – 2023): developing an ML-assisted platform for Threat Intelligence handling
- **SIFIS-HOME** (2020 - 2023): working on improving the resilience of Smart Home systems and privacy-aware network traffic analytics

HORIZON PROJECTS AS ENABLERS

F-Secure research activities in certain domains were essentially enabled by Horizon 2020 funding and collaboration:

- **SHERPA** (2018 - 2021) research on security of ML-powered systems – how those can be attacked and abused and how to defend them
(we publish actively on the topic at <https://blog.f-secure.com/artificial-intelligence-cyber-security/>)
- The work started in SHERPA is now continuing in **SPATIAL** (2021 – 2024)
(<https://www.f-secure.com/en/press/p/f-secure-aims-for-more-secure-ai-as-a-part-of-spatial->)
- **SAPPAN** (2019 – 2022) was an initial point of our Project Blackfin
(<https://www.f-secure.com/content/dam/f-secure/en/business/common/collaterals/f-secure-whitepaper-blackfin.pdf>; <https://sappan-project.eu/>)

CASE EXAMPLE: SAPPAN PROJECT

Sharing and Automation for Privacy-Preserving Attack Neutralization

(received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement no. 833418)

- Consortium: Fraunhofer FIT (DE), Masaryk University (CZ), F-Secure (FI), RWTH Aachen University (DE), Hewlett Packard Enterprise (IE), CESNET (CZ), University of Stuttgart (DE), Dreamlab Technologies (CH)
- Main objectives:
 - Distributing of attack detection and response capabilities among endpoints, organizational security backends and security service provider backends
 - Sharing of cybersecurity data and detection and response models (ML) in confidentiality- and privacy-preserving ways

P R O J E C T **BLACKFIN**



INNOVATIONS FROM THE F-SECURE'S AI RESEARCH STREAM (initiated by the **SAPPAN** project)

ADAPTIVE DETECTIONS

Intelligent, on-client anomaly detection
(UEBA)

•

What is 'anomalous' depends on the context: models constructed locally, aggregated on the level of an organization, and aggregated globally provide increased attack detection power

INTELLIGENT RESPONSE

Augmented Threat Hunting: Human with
AI

•

Supporting security personnel in handling cyber incidents. Defining 'incident similarity' aptly, we significantly reduce the handling time or even fully automate the response operations

CONTEXTUAL SWARM INTELLIGENCE

Agents interact and collaborate for the ultimate situational awareness

THANK YOU

3 cool things

- Cyber Security
- Nordics (sometimes literally)
- Collaboration and research

Image by Remi Lanvin (source: [A proper winter in Helsinki](#) | [Rémi Lanvin](#) | Flickr)
used under CC BY-SA 2.0



F-Secure®