MARKET RESEARCH, SECURITY CHALLENGES & ESET SOLUTIONS

Michal Jankech, Principal Product Manager, ESET HQ

ENJOY SAFER TECHNOLOGY™

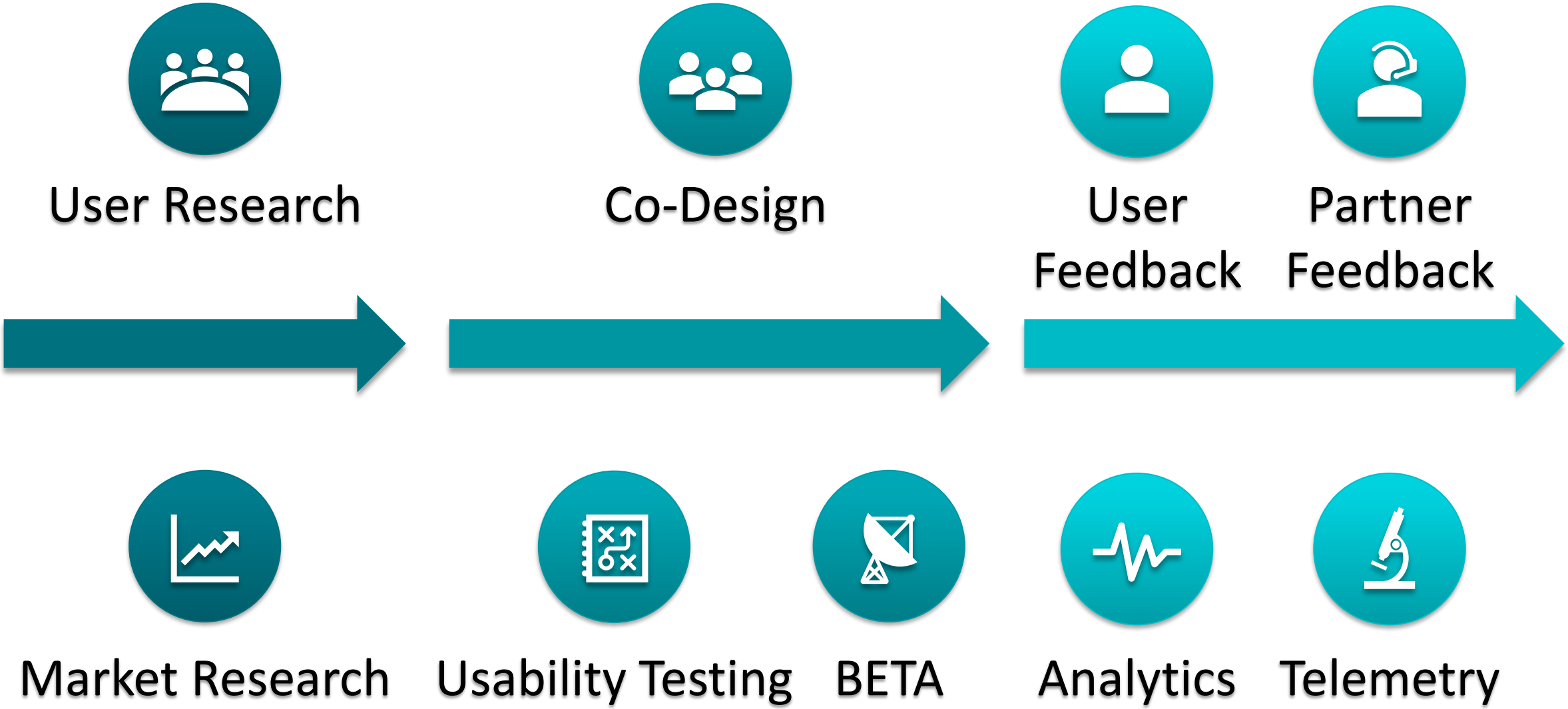
Michal Jankech

Principal Product Manager

SECURITY DAYS

User Research

ENJOY SAFER TECHNOLOGY™

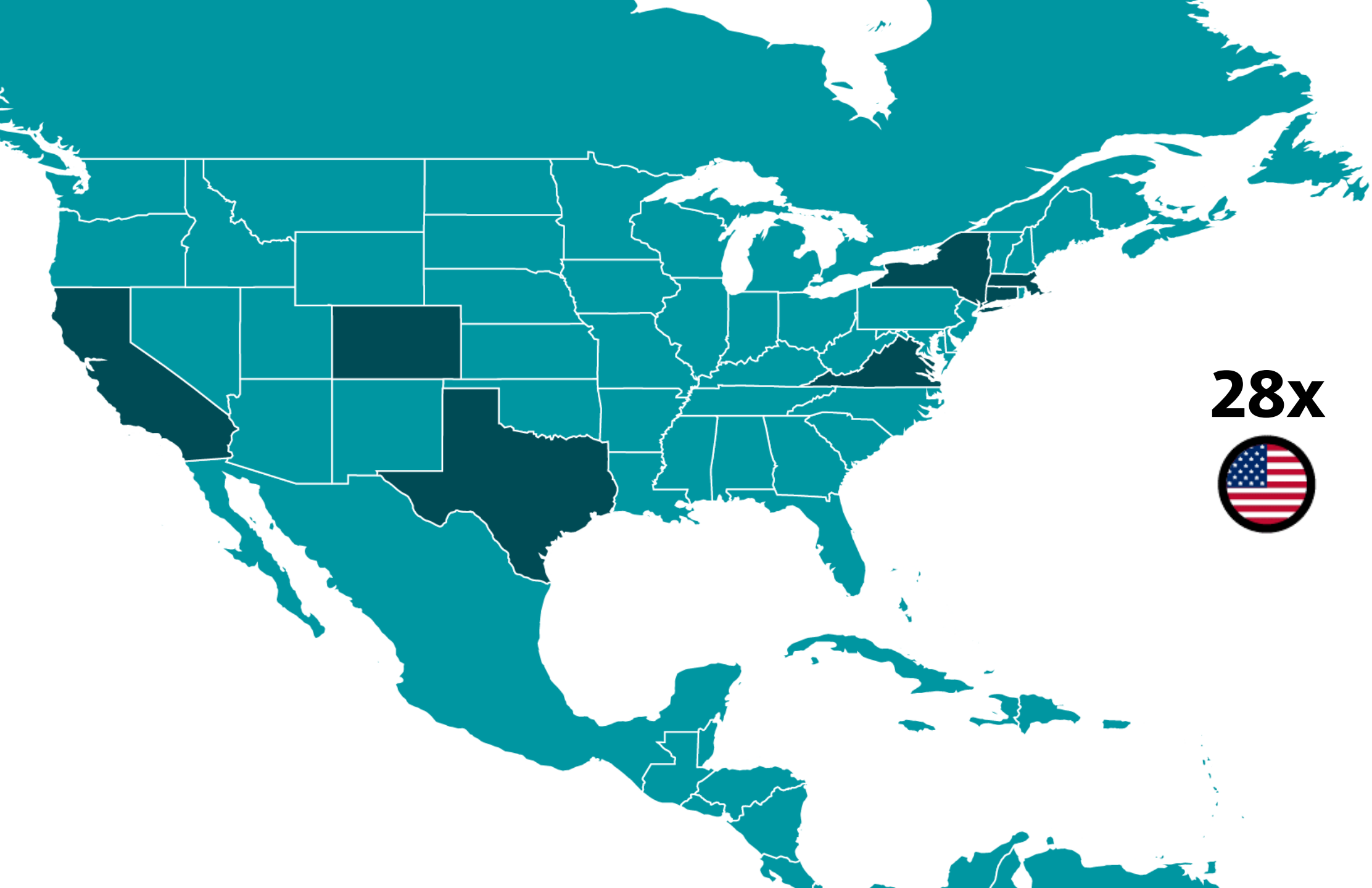

User Research
Co-Design
User Feedback
Partner Feedback
Market Research
Usability Testing
BETA
Analytics
Telemetry

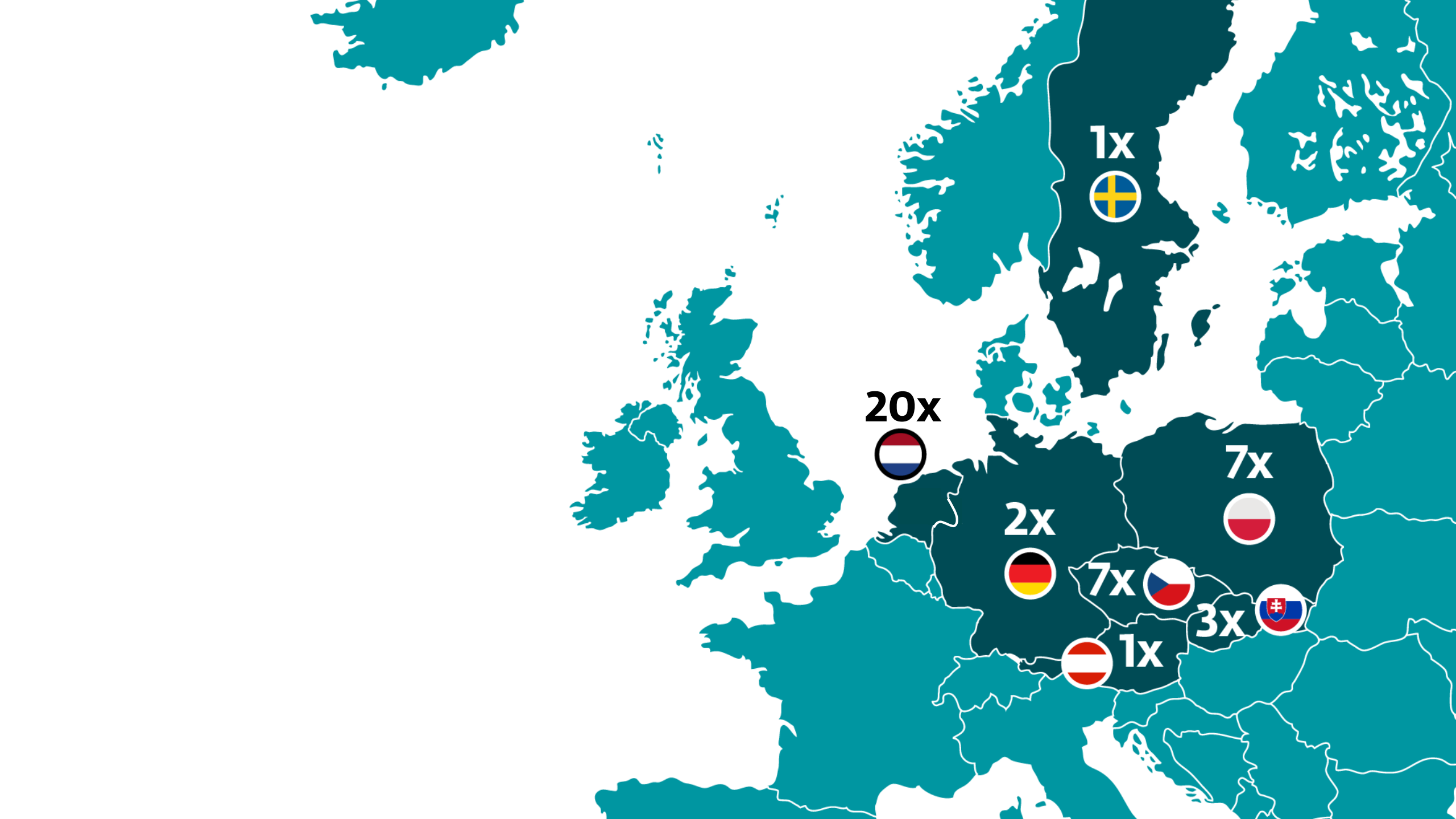
SECURITY DAYS

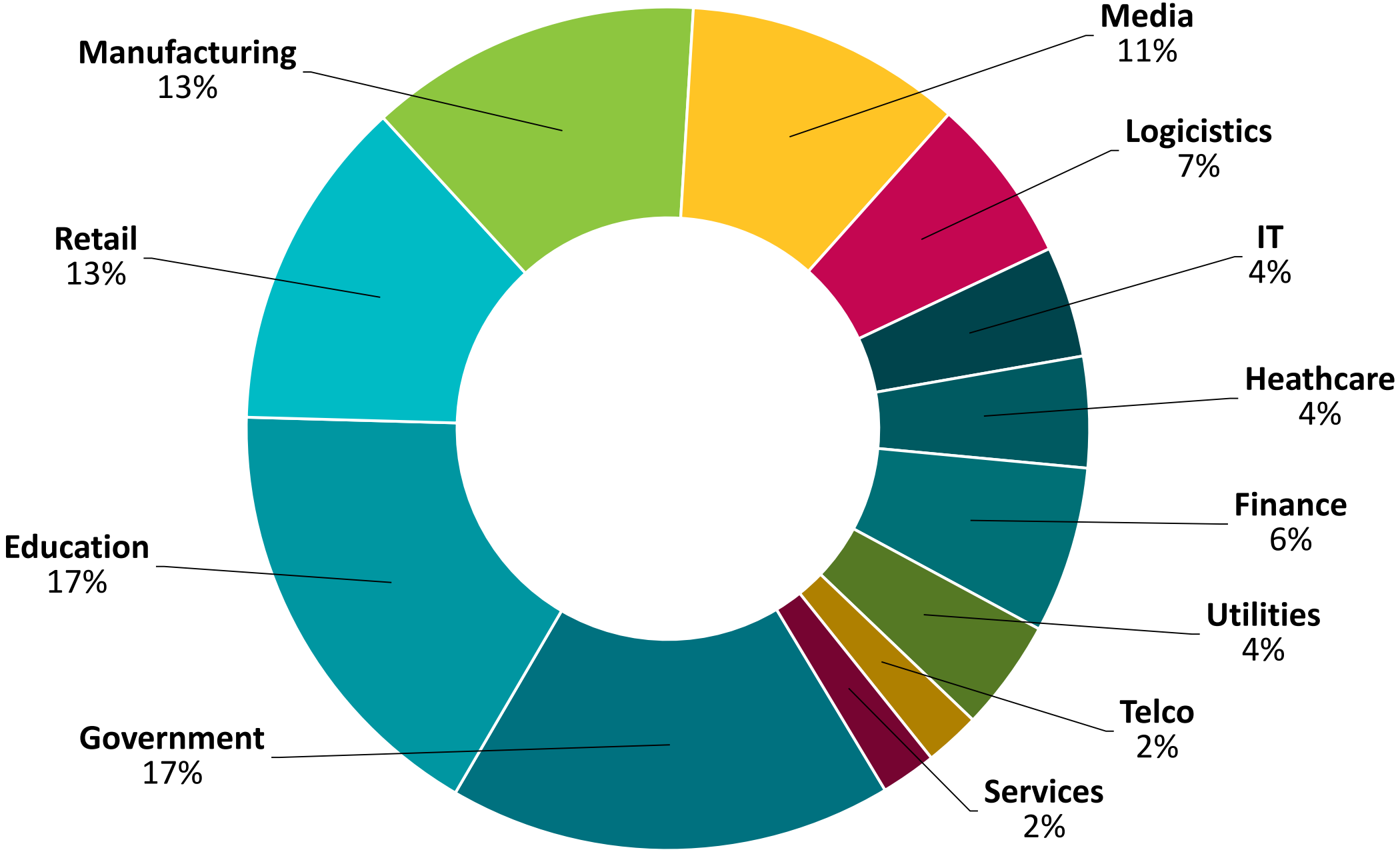
Enterprise Research

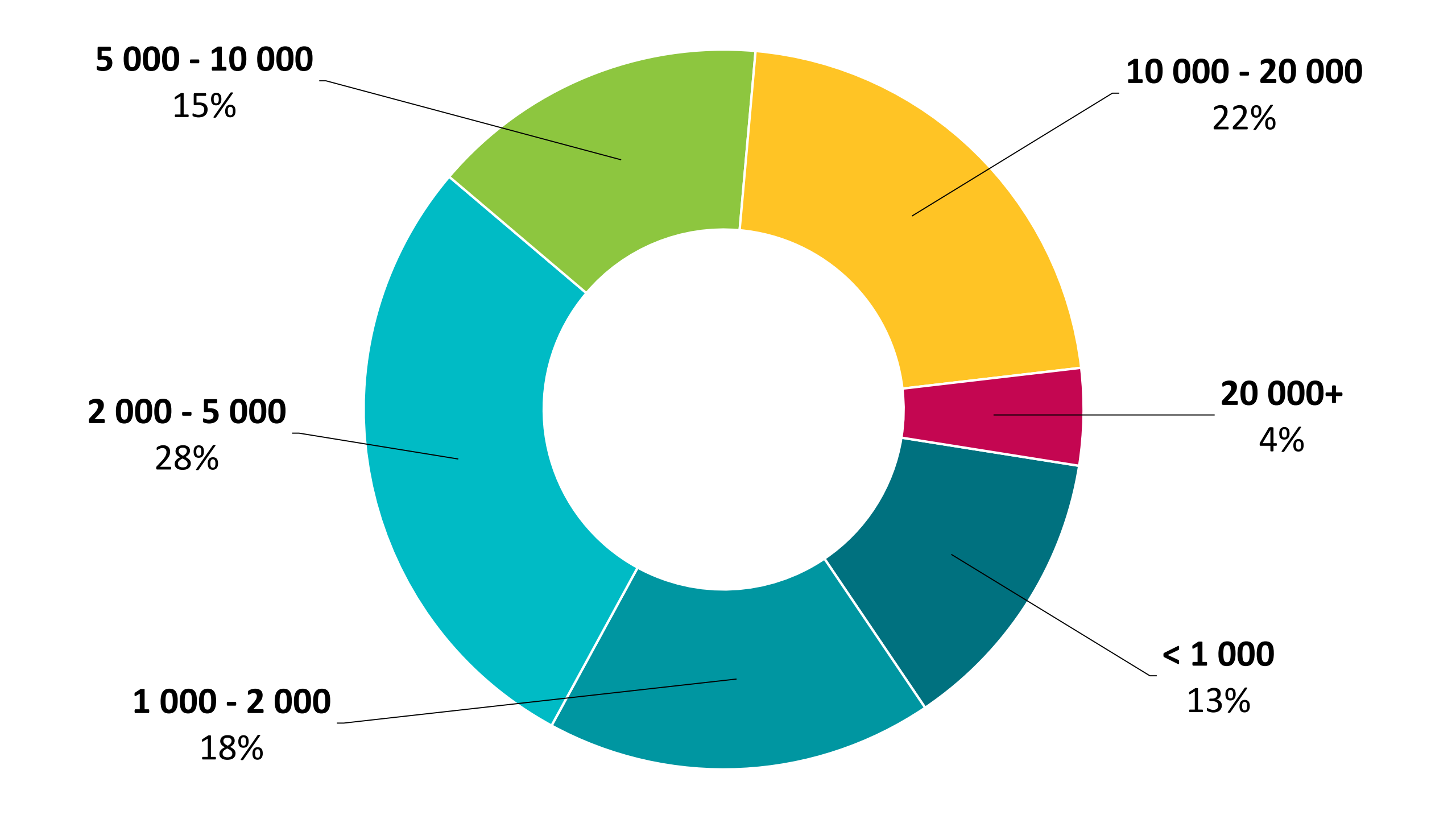
2017-2019

ENJOY SAFER TECHNOLOGY™


28x


1x
20x
7x
2x
7x
3x
1x


Media
11%
Logicistics
7%
IT
4%
Heathcare
4%
Finance
6%
Utilities
4%
Telco
2%
Services
2%
Government
17%
Education
17%
Retail
13%
Manufacturing
13%


5 000 - 10 000
15%
10 000 - 20 000
22%
20 000+
4%
< 1 000
13%
1 000 - 2 000
18%
2 000 - 5 000
28%

Administrators

User Personas

Other Employees

Served Personas

Companies

Organizational Personas

Administrators

Sophisticated Administrator
Basic Administrator

Sophisticated Administrator

- Lead by **CISO**
- **Motivated, capable**, eager to improve
- **Formal teams** and roles

- Wants to **automate & integrate**
- Likes and utilizes **ESET capabilities**

Basic Administrator

- Small, **informally organized** teams
- Often **leads IT-Security**
- **Limited** time, motivation and abilities

- Wants **help** and **fire & forget** behavior
- Struggles with **complexity**

Other Employees

CISO
Typical Employee
Empowered Employee

Chief Information Security Officer

- **Key factor** on many decisions
- Often **established IT Security**
- **Sets the direction** for adv. teams

- **Passive user** of ESMC
- Interested in **reports & auditing**

Typical Employee

- **Limited rights** on the computer
- **Minimal knowledge** about IT Security
- **Majority** of employees

- Security should be **invisible**

Empowered Employee

- **Permissive** company culture
- **Technical** users such as developers
- **Semi-managed systems**

- Has and sometimes uses **admin access**
- Benefits from **some control**

Companies

Top-down Corporation
Decentralized Organization

Top-down Corporation

- **Typical hierarchical** structure
- Clear responsibilities

- **Centralized** decision-making
- Administrators have **control**

Decentralized Organization

- Different regions with **autonomy**
- **Consensus**-focused culture
- **Sometimes hierarchical** structure

- **Top-level decisions** serve as guidance
- Applies to both **use and purchase**

SECURITY DAYS

Top challenges

ENJOY SAFER TECHNOLOGY™

What our customers percieve as „the challenge“ ?

Ransomware

Targeted attacks & hacking

Diversified landscape

Lack of network visibility &
pressure on operational effectiveness

Employee misbehavior

Lack of workforce

Ransomware

Cloud Sandbox (Dynamic Threat Defense)

Stops ransomware upon entry

Signature-less detection (Ransomware Shield)

Behavior-based prevention focusing on changes in system and content

EDR (Enterprise Inspector)

Post attack detection of ransomware behavior

(what was changed, when, and how – and by what / whom)

Targeted Attacks & Hacking

Multi-layered prevention

(UEFI Scanner, Exploit Blocker, AMS)

Reduce the attack surface

2FA for all admins

Map the holes and install patches

Detection management (EEI & EDTD & ESMC)

Finding the needle in a haystack approach

Diversified Landscape

At least one mac is always in there (management / designer)

Linux is gaining momentum in government & ICS (SCADA)

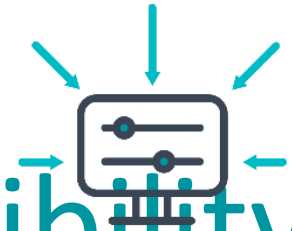
Centralized management with software / hardware asset management

ESMC – providing software / hardware inventory for all platforms with advanced filtering

Lack of network visibility & pressure on operational effectiveness

Reporting & Notifications

Hardware/software inventory + solutions focusing on reducing IT(sec) workloads



Data consolidation (All data in one system – ESMC + details in purpose built systems (EDTD / EEI))

Employee misbehavior

Web control, time-based blocking

Device control, time-based blocking

Reports (about potentially harmful activity)

EDR with customization & UEBA (Enterprise inspector rules, focusing on employee behavior (what they really do))

Outsource Lack of workforce Collaborate Consult

Deployment Services

Help to deploy and setup properly

Threat Hunting

Help to identify malicious activity when needed

Threat Intelligence

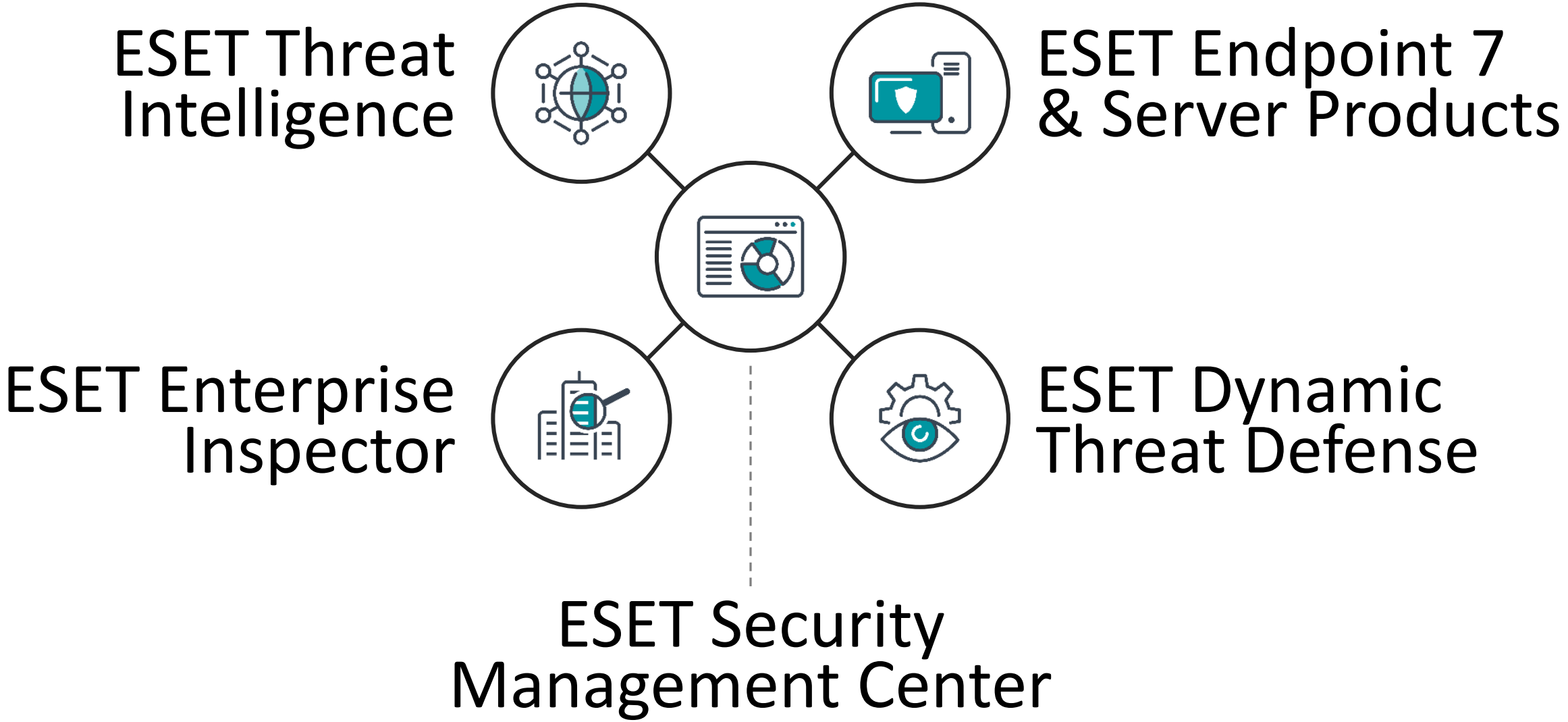
Help to provide security context

SECURITY DAYS

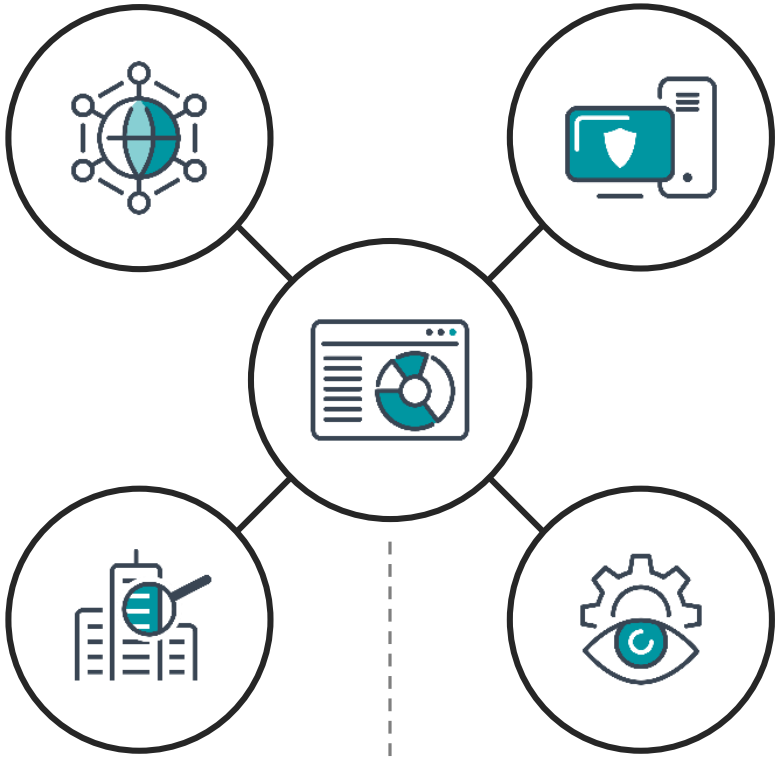
How ESET helps?

ENJOY SAFER TECHNOLOGY™

By products ...


ESET Threat Intelligence
ESET Endpoint 7 & Server Products
ESET Enterprise Inspector
ESET Dynamic Threat Defense
ESET Security Management Center

... That Fits Gartner CARTA framework



PREDICT
ESET Threat Intelligence

PREVENT
ESET Endpoint 7 & Server Products

RESPOND
ESET Enterprise Inspector

DETECT
ESET Dynamic Threat Defense

CONTINUOUS MONITORING & ASSESMENT
ESET Security Management Center

Key takeaways?

Next week:

- Upgrade your security product to the latest version
- Collect inventory across ALL your environment (software, hardware, appliances)

Next three months:

- Consider enabling 2FA for all users with admin rights (stolen password is still responsible for 80% of all breaches)
- Develop a “Threat Feed” to cross-reference CVEs against your inventory + build a dashboard using the three data feeds

Useful links

Vulnerability data feeds:

- MitreCVE Data Feed: https://cve.mitre.org/cve/data_feeds.html
- NIST National Vulnerability Database (NVD): https://nvd.nist.gov/vuln/data-feeds
- Microsoft KB info: https://www.microsoft.com/en-us/download/confirmation.aspx?id=36982

Check if your e-mail and password was not involved in a data breach

- https://haveibeenpwned.com/

SECURITY DAYS

Thank you!
Questions?

ENJOY SAFER TECHNOLOGY™

SECURITY DAYS

 /ESET

 @ESET

 +esetglobal

#ESETDay