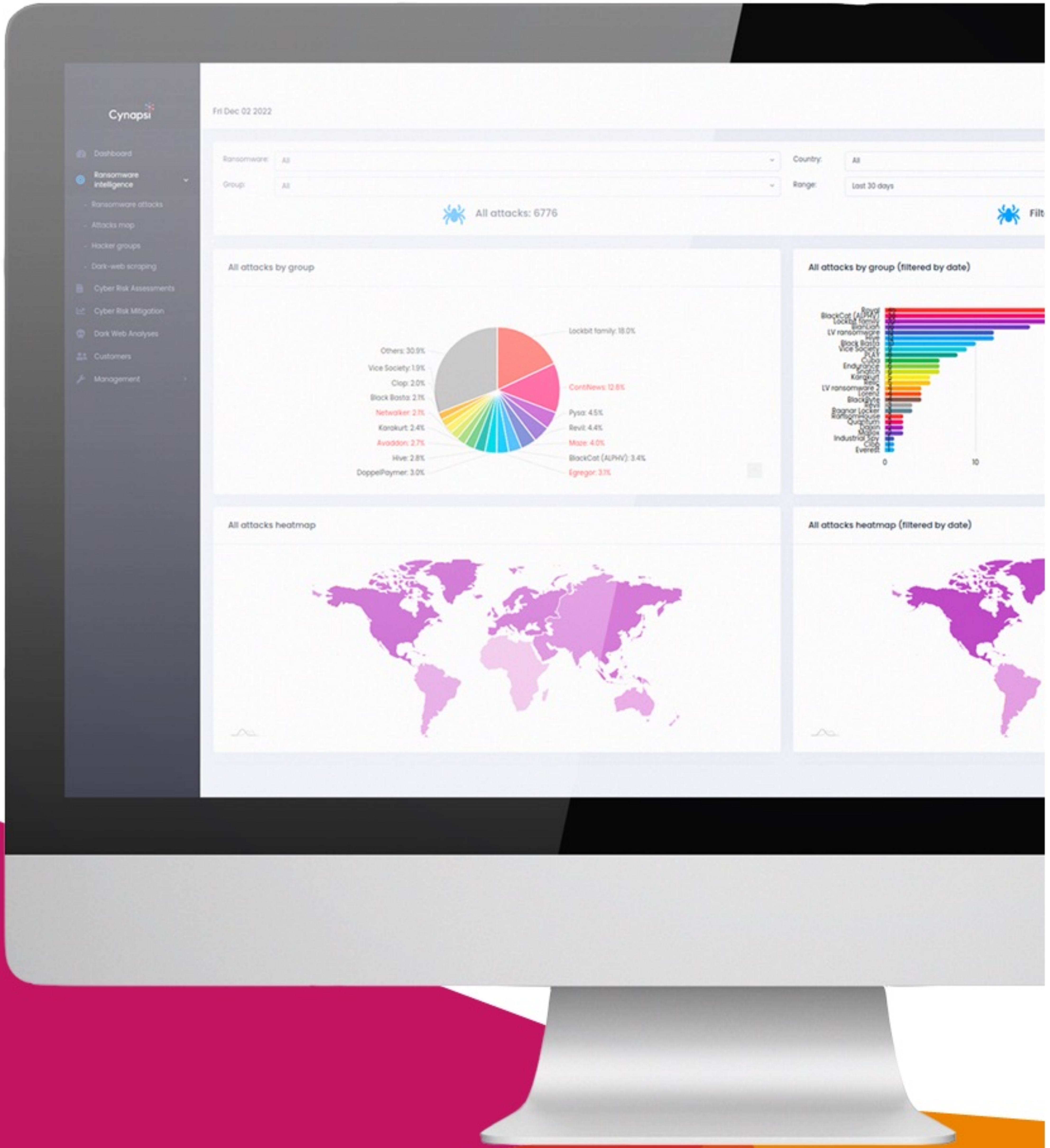
Coinnect
CYBER INSURTECH

RANSOMWARE INTELLIGENCE GLOBAL REPORT 2023

EMERGING TRENDS, WORLDWIDE AND REGIONAL VIEWS



Fri Dec 02 2022

Ransomware: All

Group: All

Country: All

Range: Last 30 days

All attacks: 6776

Ransomware Attacks

A VIEW OF THE **CURRENT SCENARIO**

Ransomware attacks have become a growing concern for organizations of all sizes, with small and medium-sized businesses (**SMBs**) being particularly vulnerable. These attacks involve malicious actors encrypting a company's data and demanding a ransom payment in exchange for the decryption key.

The frequency and severity of these attacks have been on the rise in recent years, and the trend shows no sign of slowing down. The impact of a ransomware attack can be devastating for a business, leading to lost revenue, reputational damage, and in some cases, permanent data loss.

This report aims to provide a comprehensive **overview of ransomware attacks in 2021 and 2022**, highlighting the type of companies, the sectors and geographies most affected by these attacks. Presented data are aggregated views of "double extortion" ransomware attacks **extracted from the Dark Web with Coinnect proprietary platform**.

The impact of ransomware on the **Cyber Insurance Industry** has been significant in recent years. As the frequency and severity of ransomware attacks have increased, so too have the number of claims made by organizations affected by these attacks.
In fact, ransomware is now considered to be **the leading cause of cyber insurance claims**.

One of the main reasons for this is that ransomware attacks are becoming more sophisticated, with attackers using increasingly advanced techniques to evade detection and encrypt a company’s data.

This makes it more difficult for organizations to **prevent and recover from attacks**, and increases the likelihood of a successful ransom demand.

Another reason is that many **SMBs are particularly vulnerable to ransomware attacks**, as they often lack the resources and expertise to effectively protect themselves.
This makes them an attractive target for attackers, who know that these companies are more likely to pay the ransom to regain access to their data.

The increasing frequency and severity of ransomware attacks are also affecting the cyber insurance industry in other ways.
One of the most notable is that it’s **driving up the cost of cyber insurance**.

As the number of claims related to ransomware attacks increases, insurance companies are having to charge higher premiums to cover the cost of these claims.

Summary

Global view

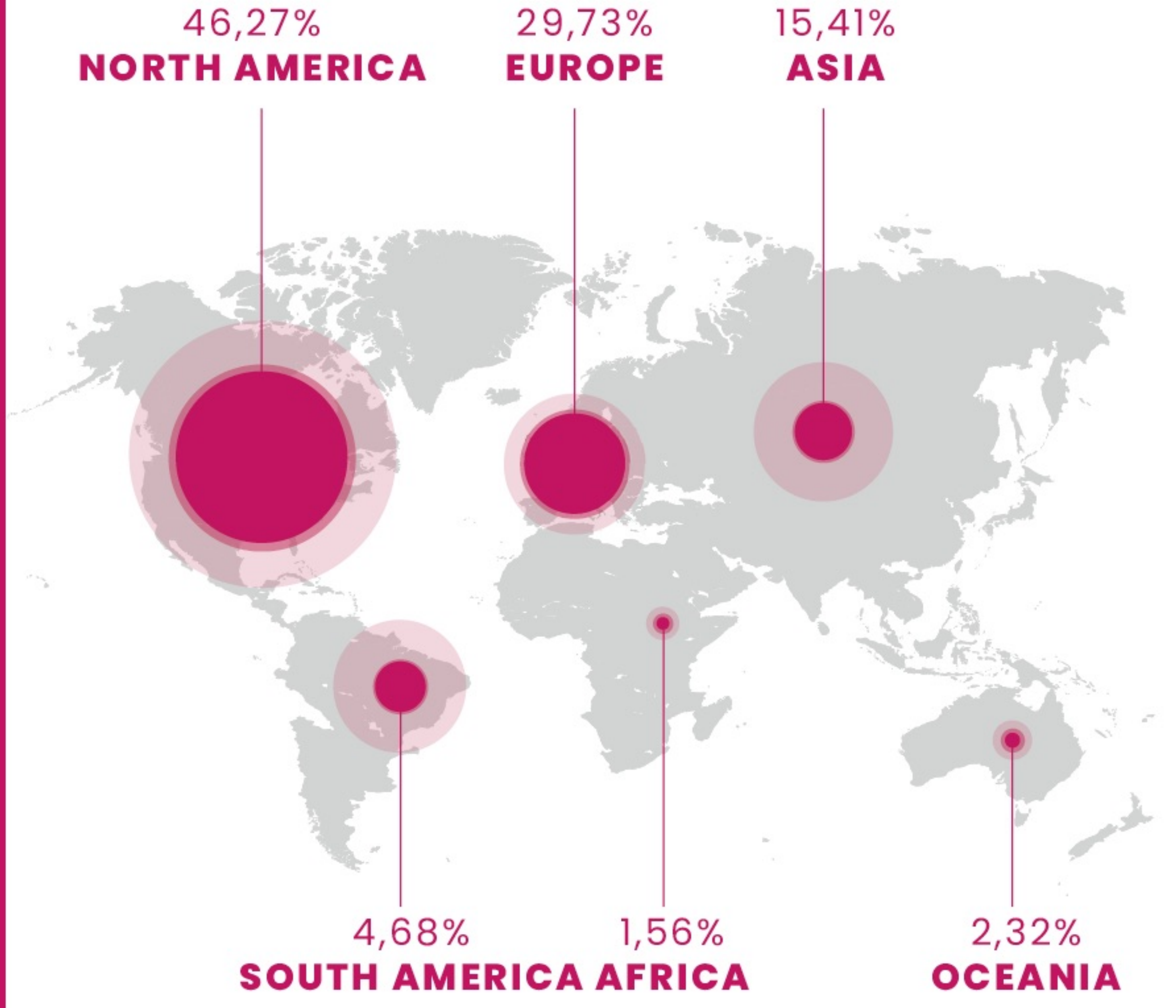
COMPARISON BETWEEN **2022** AND **2021**

- Geographical areas
- Range of employees
- Range of annual revenues
- Ransomware Groups

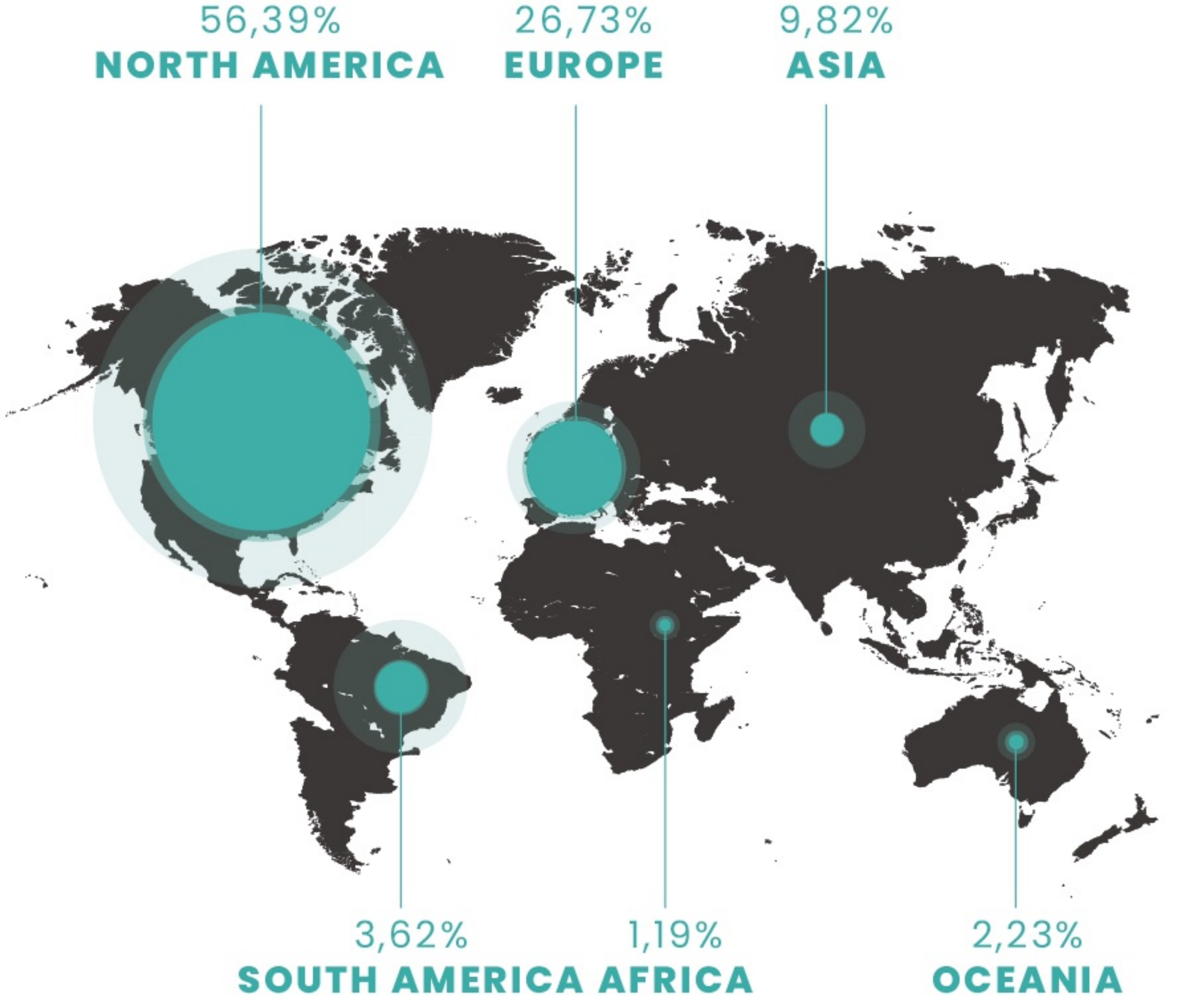
SMEs are the most targeted by ransomware attacks in both 2021 and 2022

Global view by geographical areas

North America is the only region where ransomware attacks **decreased** (-10%).



2022

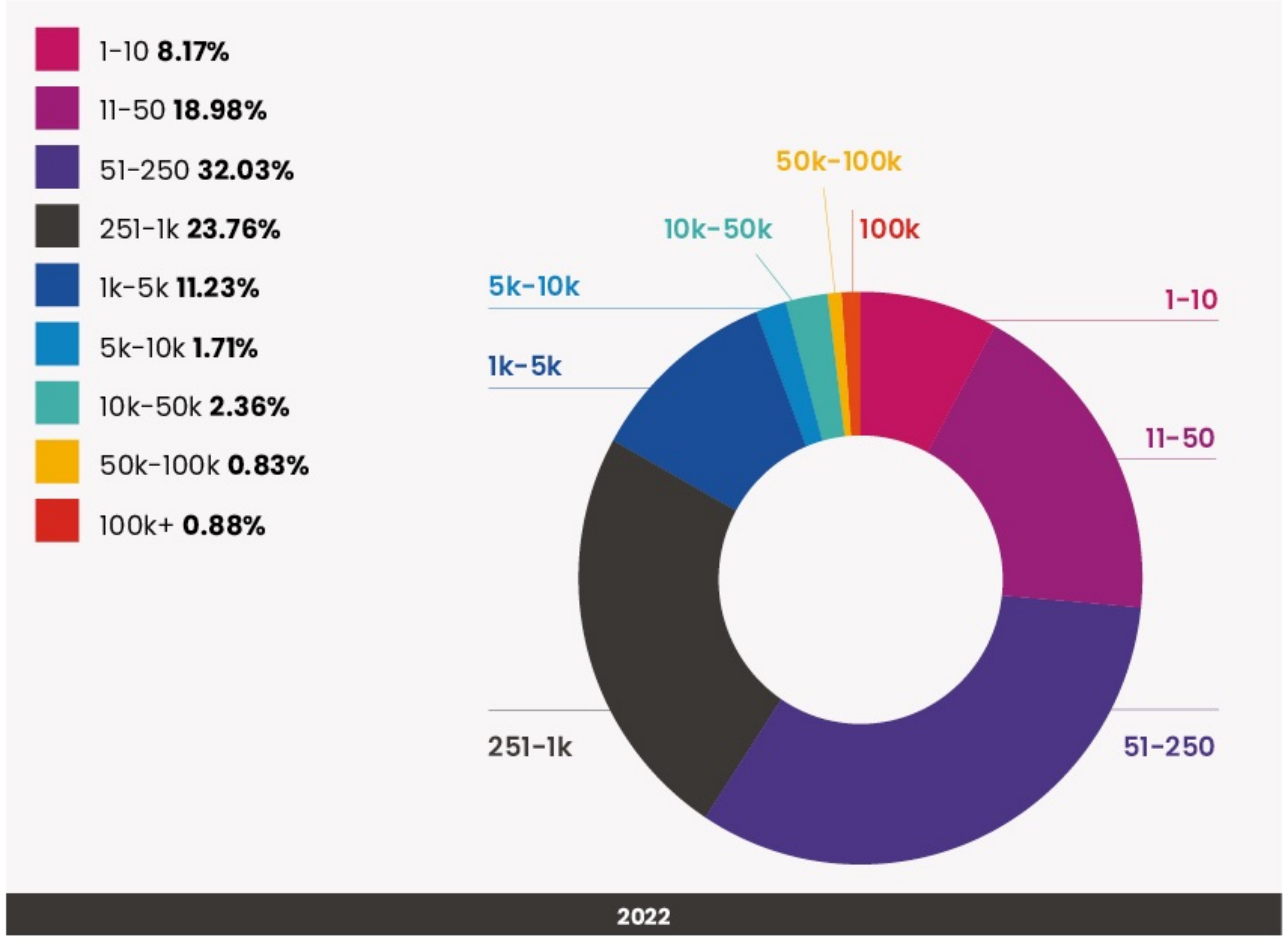


2021

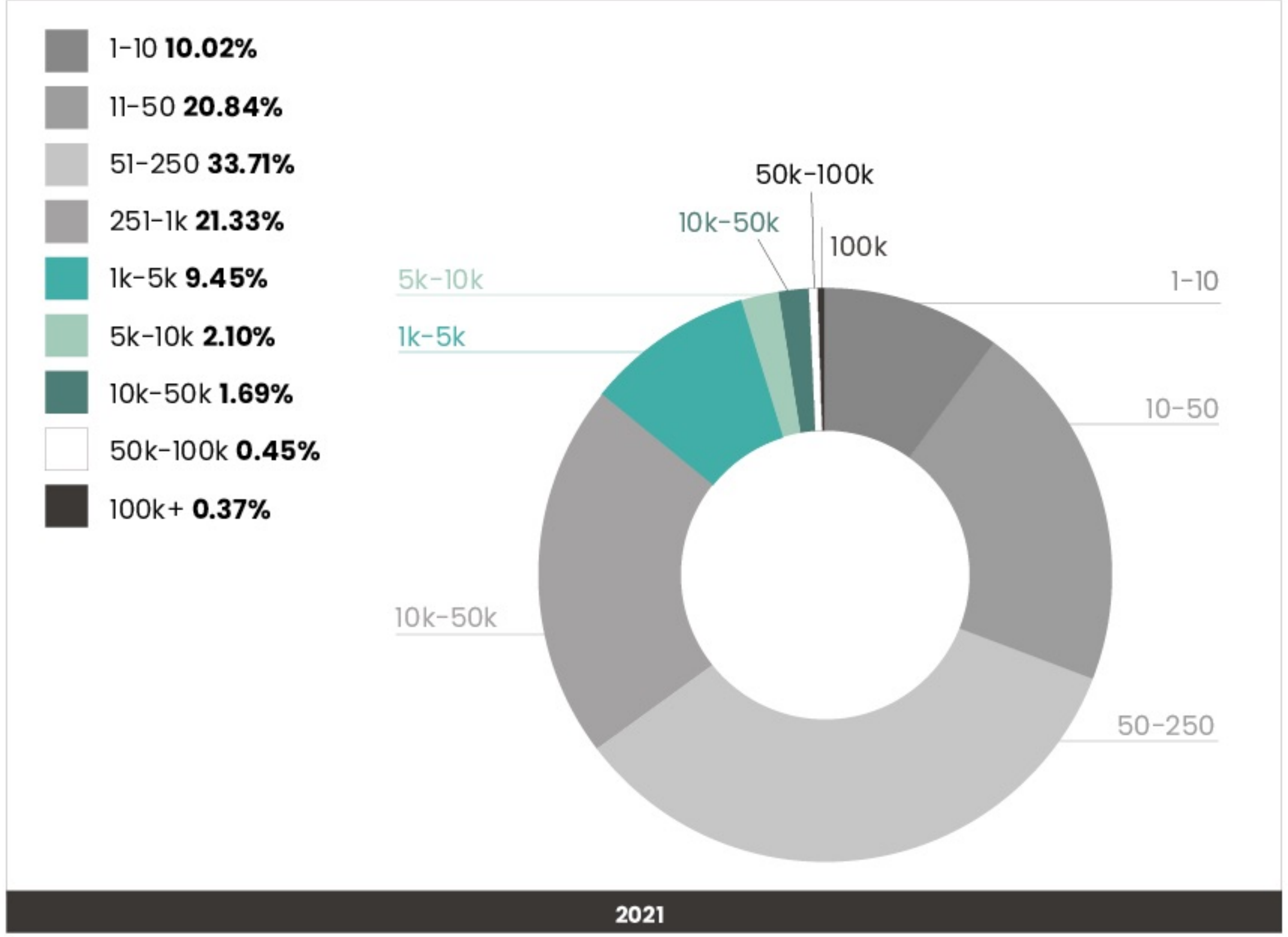
Global view by range of employees

Both in 2021 and 2022 majority of attacks affected organization with **less than 1k employees**.

RANGE OF **EMPLOYEES**



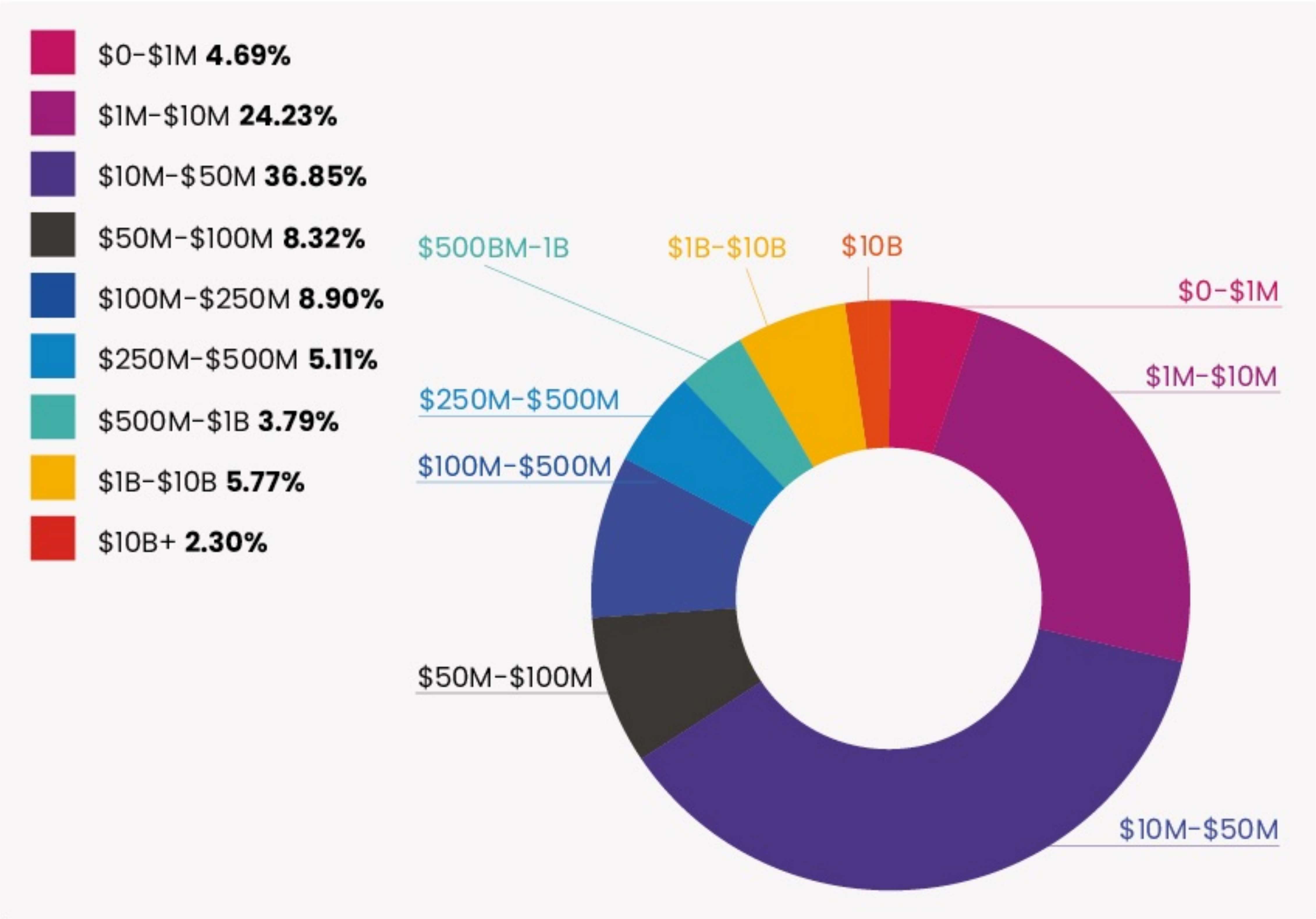
RANGE OF **EMPLOYEES**



Global view by revenues range

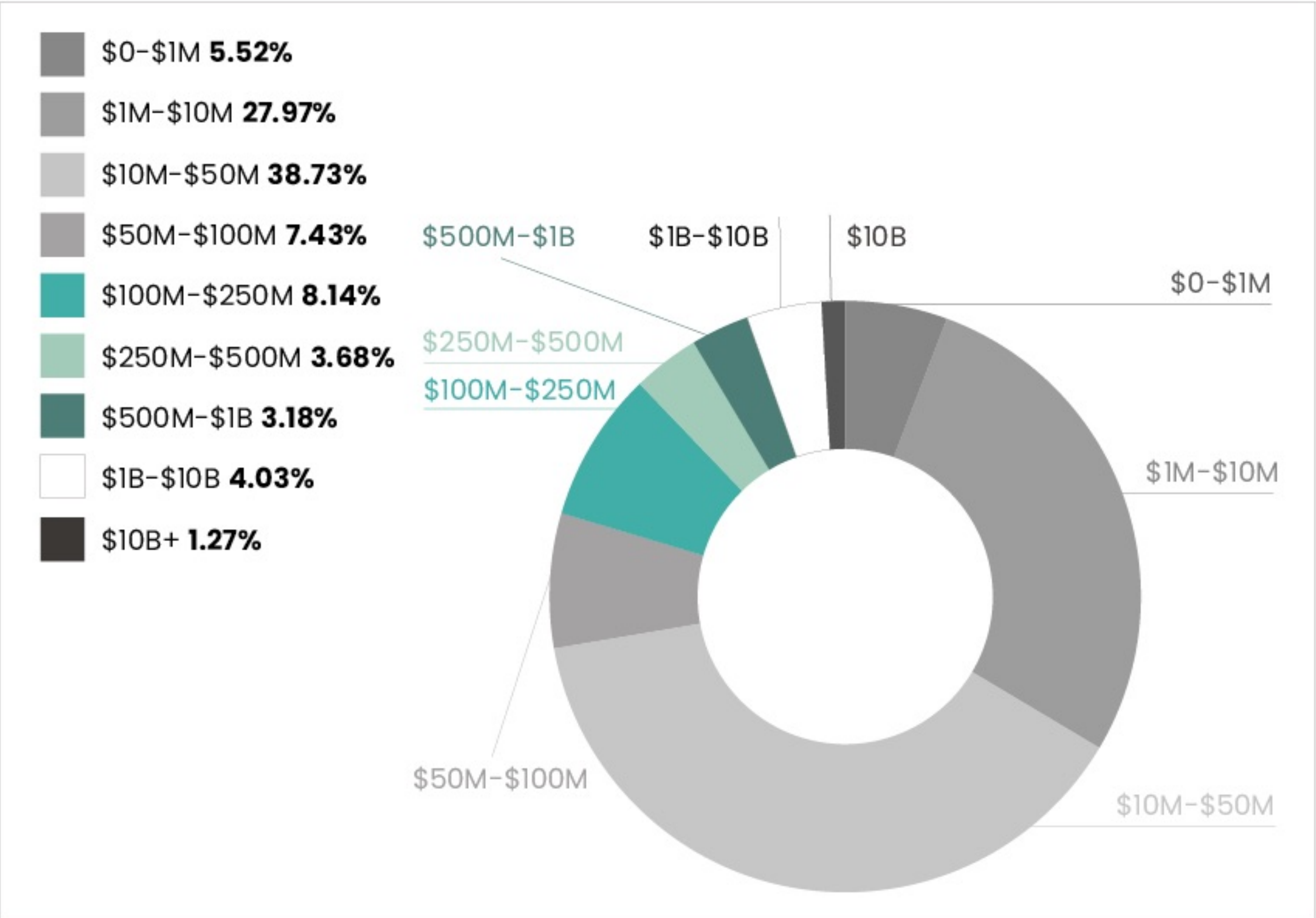
Companies between **1M and 50M** turnover represent about **60% of attacks** both in 2022 and 2021.

RANGE OF **ANNUAL REVENUE**



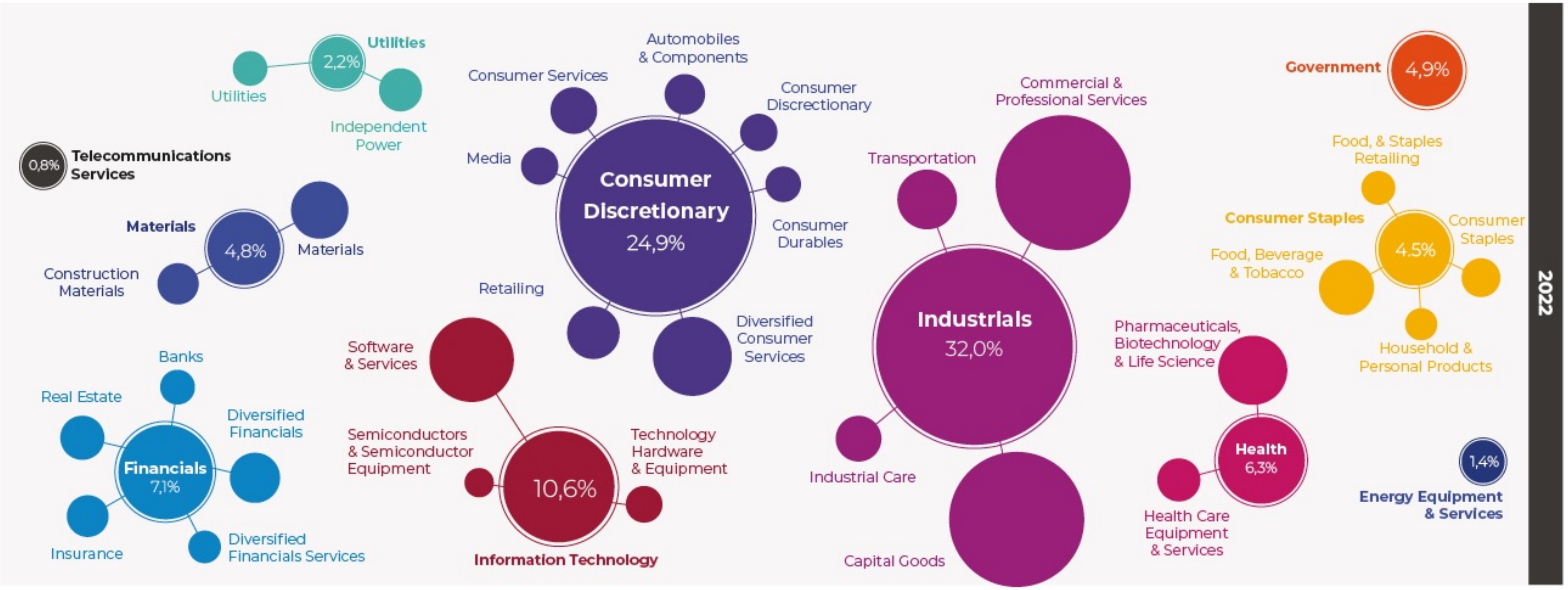
2022

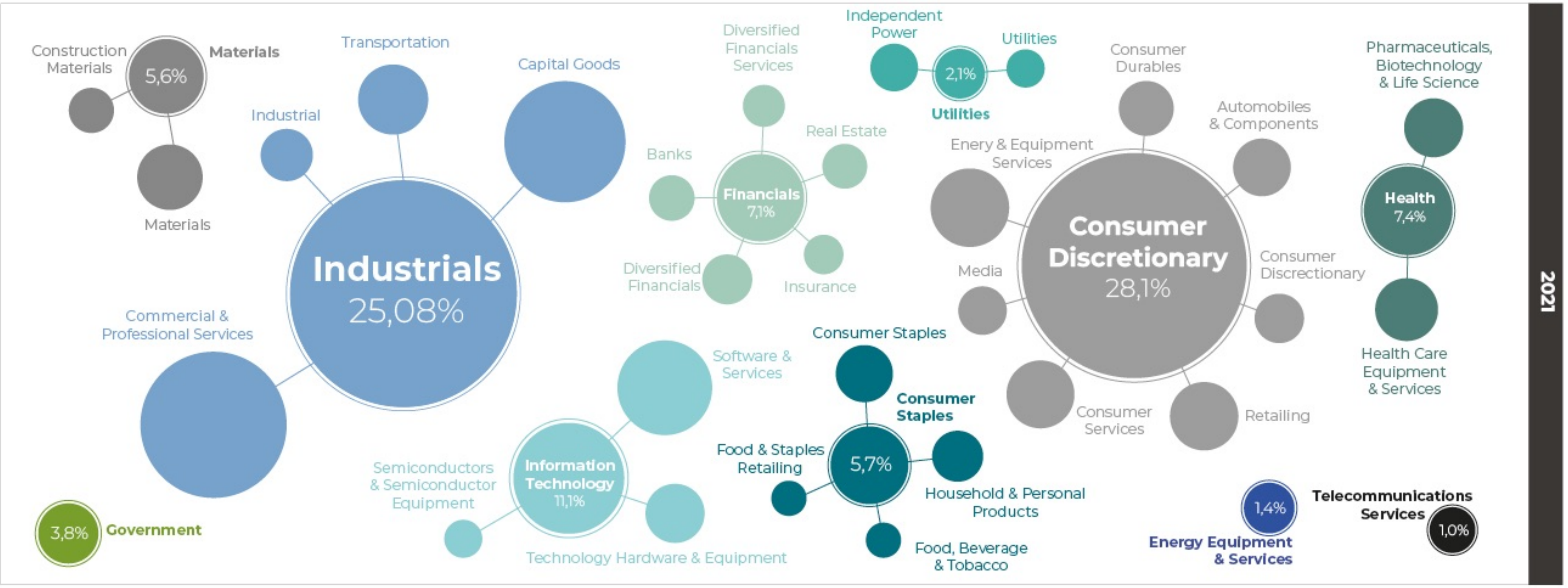
RANGE OF **ANNUAL REVENUE**



2021

Global view of the most affected **sectors**





Global view by Ransomware Groups

Number of **Ransomware Groups increased from 52 to 66** (+26%) and 30 groups of 2021 are still in 2022 (**55%**).

Lockbit	**29,36**
BlackCat	**8,62**
Conti	**6,16**
Black Basta	5,62
Hive	4,83
Karakurt	4,61
Vice Society	3,78
BianLian	2,41
Royal	2,16
Quantum	2,05
AvosLocker	1,83
BlackByte	1,76
AgainstTheWest	1,62
LV ransomware	1,65
Cuba	1,51
Stormous	1,44
Industrial Spy	1,26
Lorenz	1,22
Snatch	1,22
Clop	1,11
Everest	1,11
Ragnar Locker	1,08
KelvinSecurity	1,08
PLAY	1,01
RansomHouse	0,82
z6wkg	0,68
Suncrypt	0,54
VSOP	0,54
Sparta	0,46
Haron	0,46
Anonymous	0,46
Mindware	0,46
Ransomexx	0,43
Endurance	0,43
IceFire	0,39
Revil	0,39
Cryptonicode	0,39
CryptOn	0,32
D0N#T	0,32
Grief	0,28
Yanluowang	0,28
Bl00dy	0,28
Mallox	0,25
SiegedSec	0,25
Pandora	0,25
RedAlert	0,21
LAPSUS$	0,21
Qilin	0,21
Daixin	0,21
LeakTheAnalyst	0,18
Relic	0,18
DataLeak	0,18
Unsafe Security Blog	0,18
Arvin Club	0,14
Payload.bin	0,10
Sabbath	0,10
Moses Staff	0,10
MetaEncrypter	0,07
Black Shadow	0,07
Omega	0,07
Night Sky	0,07
IMM0RTAL$	0,03
Marketo	0,03
Entropy	0,03
Rook	0,03
CoomingProject	0,03
Dark Army	0,03

2022

The **number** of Ransomware Groups **increased from 52 to 66** (+26%).

30 groups of 2021 are still in 2022 (55%).

Conti	**16,64**
Lockbit	**15,08**
Pysa	**7,39**
DoppelPaymer	6,63
Avaddon	5,37
Revil	4,80
Clop	2,91
Grief	2,55
Darkside	2,51
Hive	2,25
Marketo	2,22
Everest	1,92
AvosLocker	1,79
LV ransomware	2,22
Prometheus	1,52
Babuk	1,49
Corporate	1,35
BlackByte	1,32
CoomingProject	1,29
Spook	1,22
Haron	1,12
BlackMatter	1,12
Ragnarok	1,45
Cuba	1,09
Karakurt	1,09
Vice Society	1,06
Payload.bin	0,89
Ransomexx	0,89
Lorenz	0,86
Snatch	0,79
Xing Team	0,72
Netwalker	0,62
Ragnar Locker	0,49
Astro Team	0,49
Moses Staff	0,49
SynACK	0,43
Egregor	0,39
BlackCat	0,33
Sabbath	0,29
Entropy	0,26
Groove	0,26
Quantum	0,26
Suncrypt	0,23
Arvin Club	0,23
Mount Locker	0,19
Rook	0,19
Bonaci	0,19
LockData Auction	0,16
Atomsilo	0,16
N3tw0rm	0,13
Karma	0,09
Bl@ckt0r	0,09
RobinHood	0,09
Black Shadow	0,09

2021

Pysa was in the top 3 in 2021 but the next year disappeared.

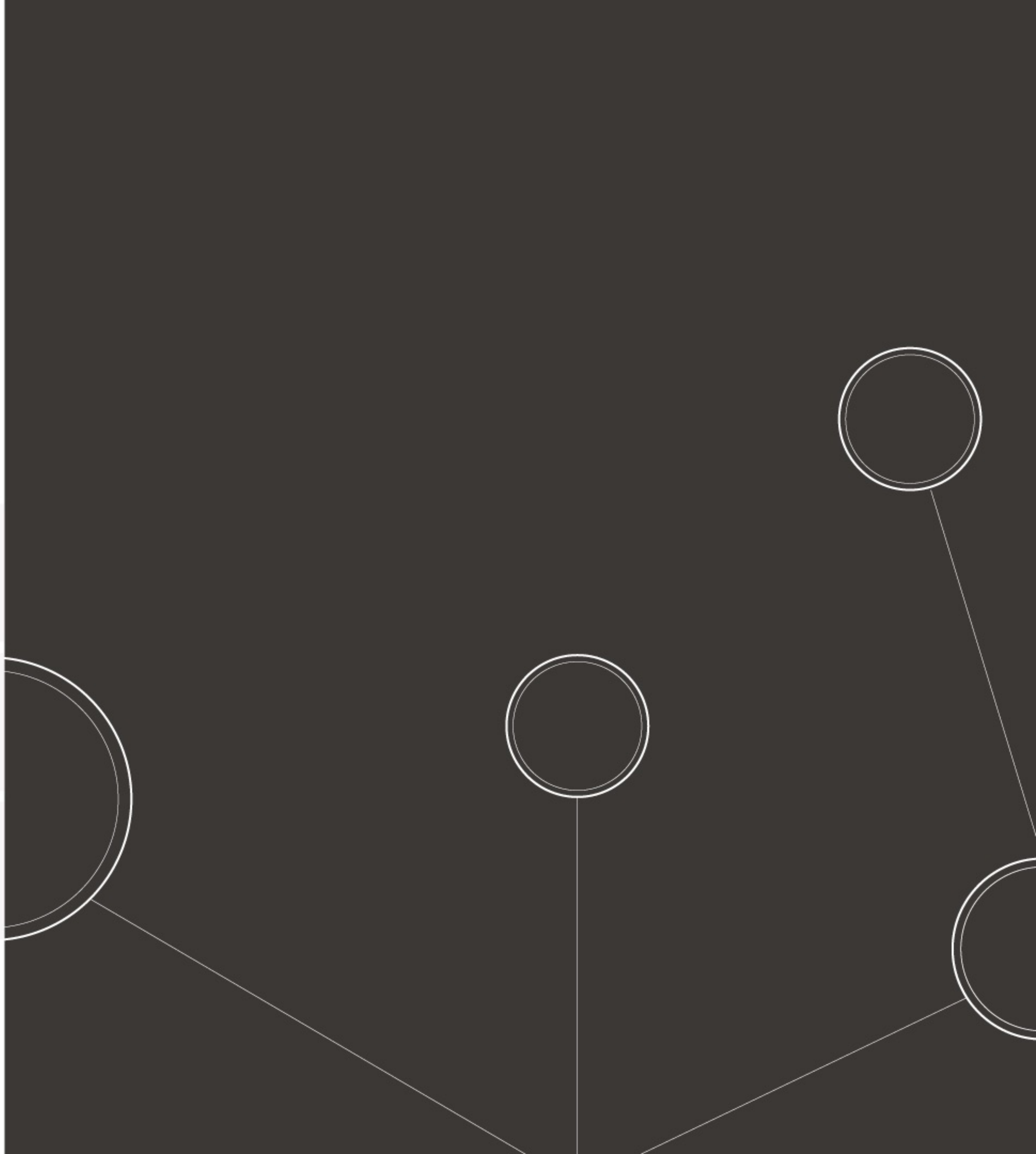
Blackcat in 2022 entered the top 3 (+8%).

Global view of the top three Ransomware Groups

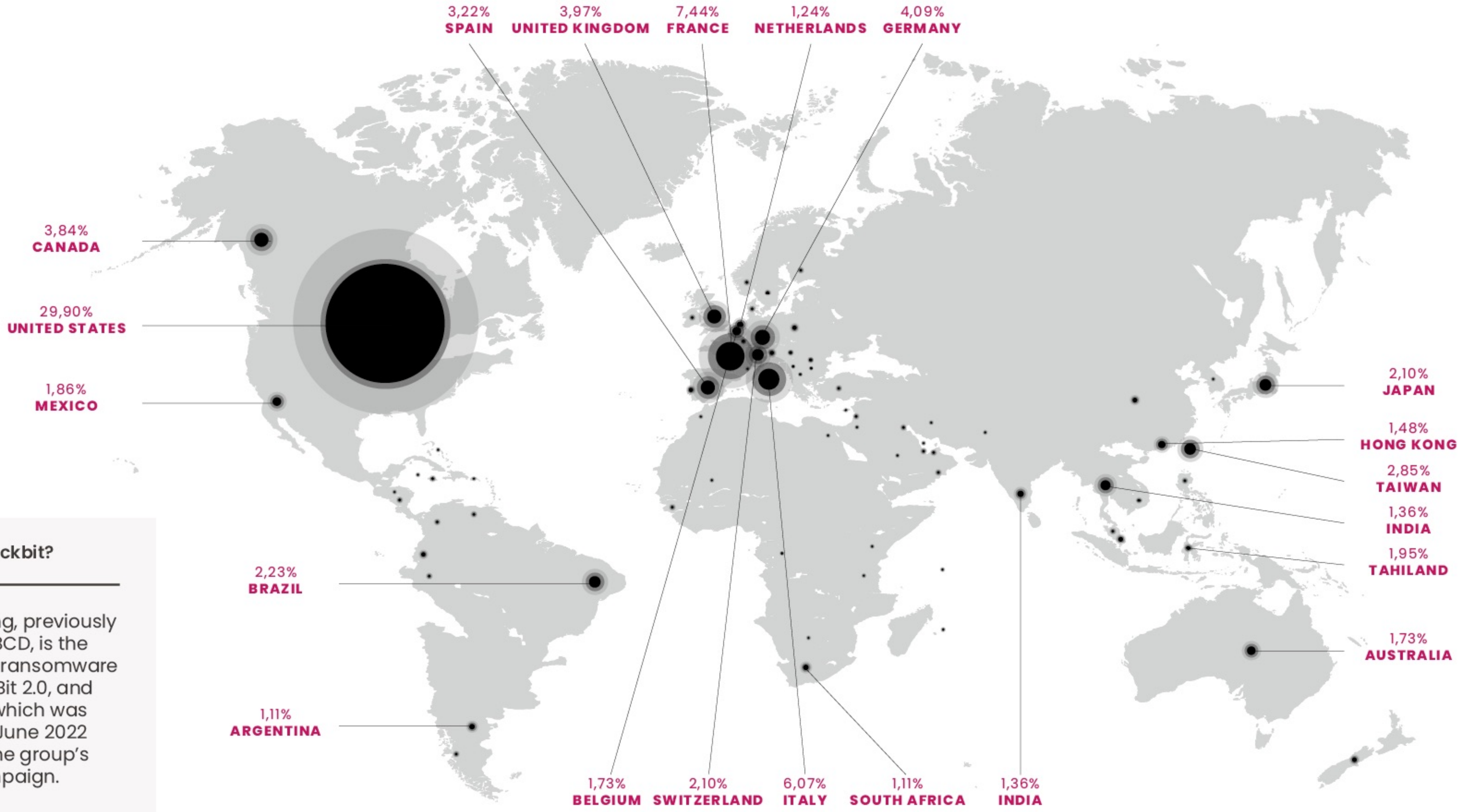
1 LOCKBIT

2 BLACKCAT

3 CONTI



Lockbit: most targeted areas

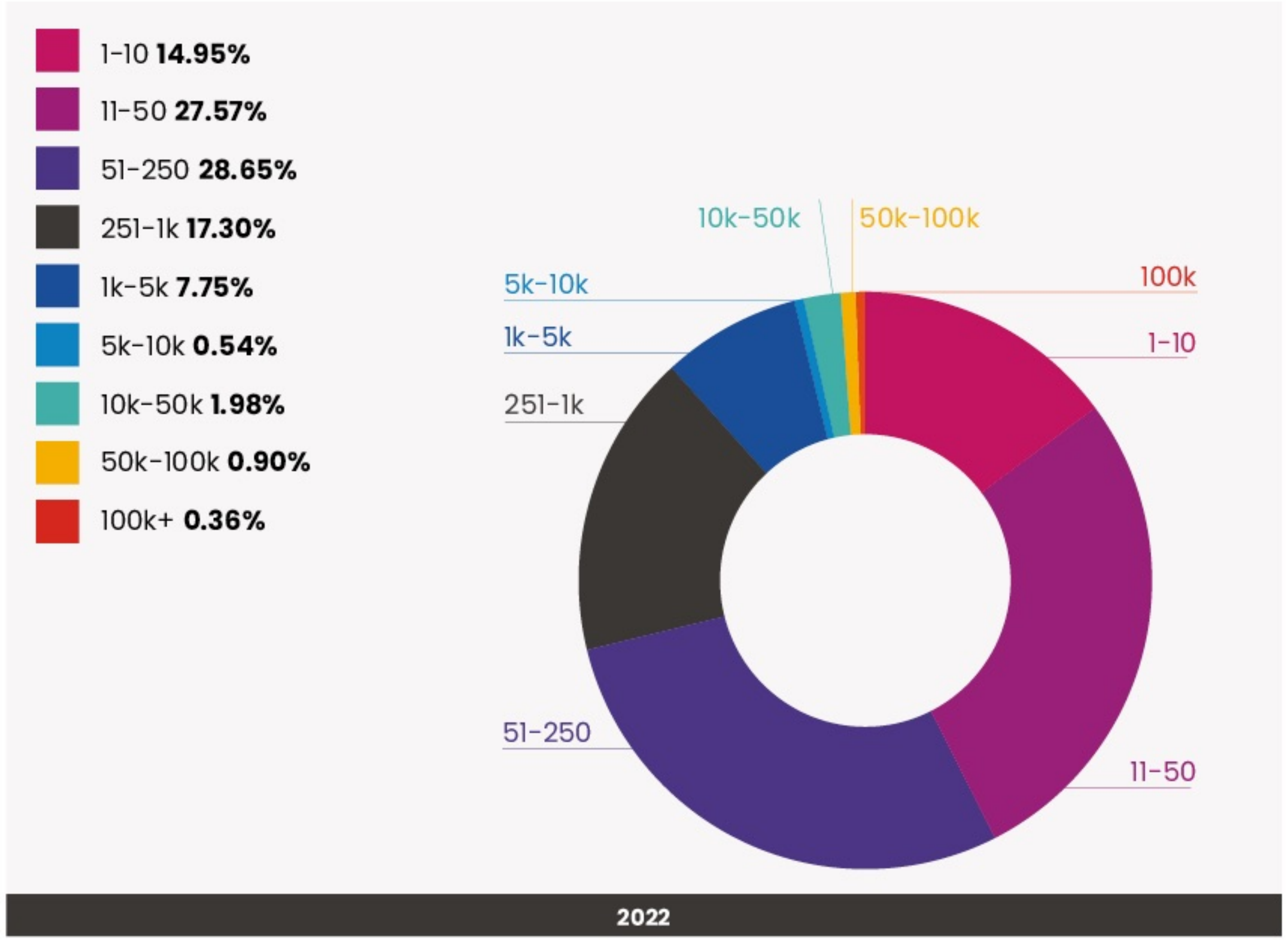


Who's Lockbit?

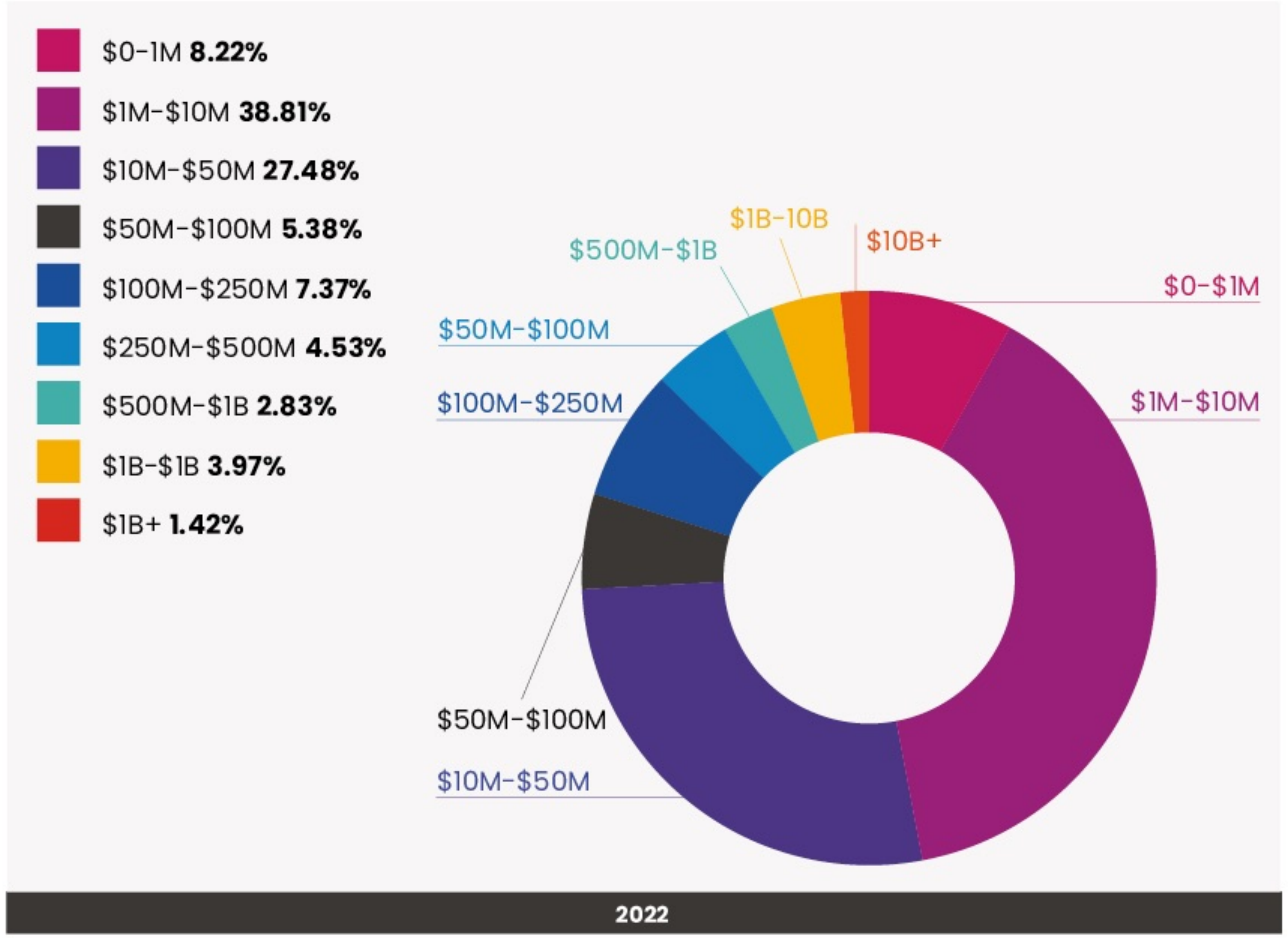
The LockBit gang, previously known as ABCD, is the operator of the ransomware LockBit, LockBit 2.0, and LockBit 3.0, which was released in June 2022 as part of the group's new campaign.

Lockbit: most breached companies

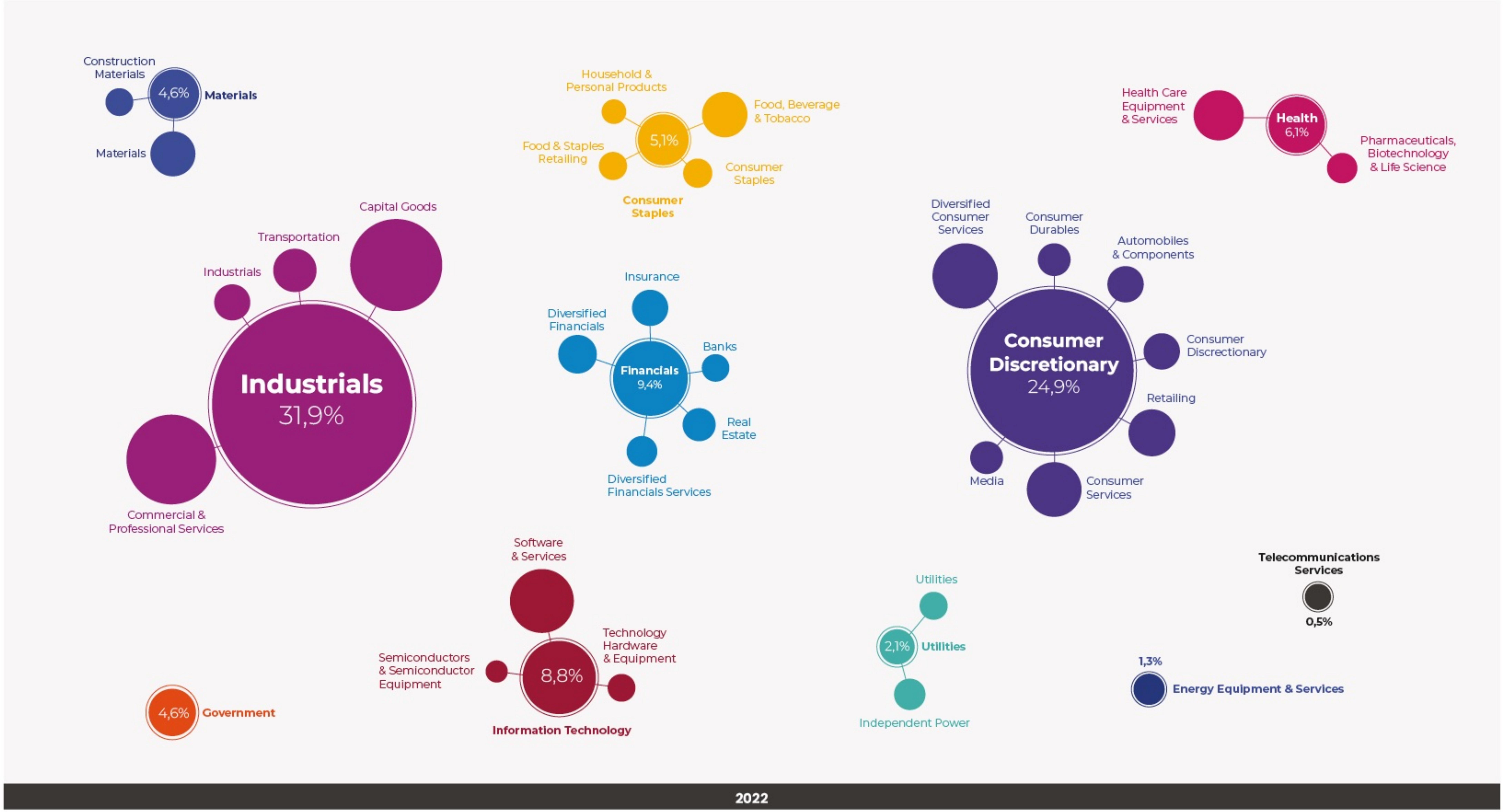
RANGE OF **EMPLOYEES**



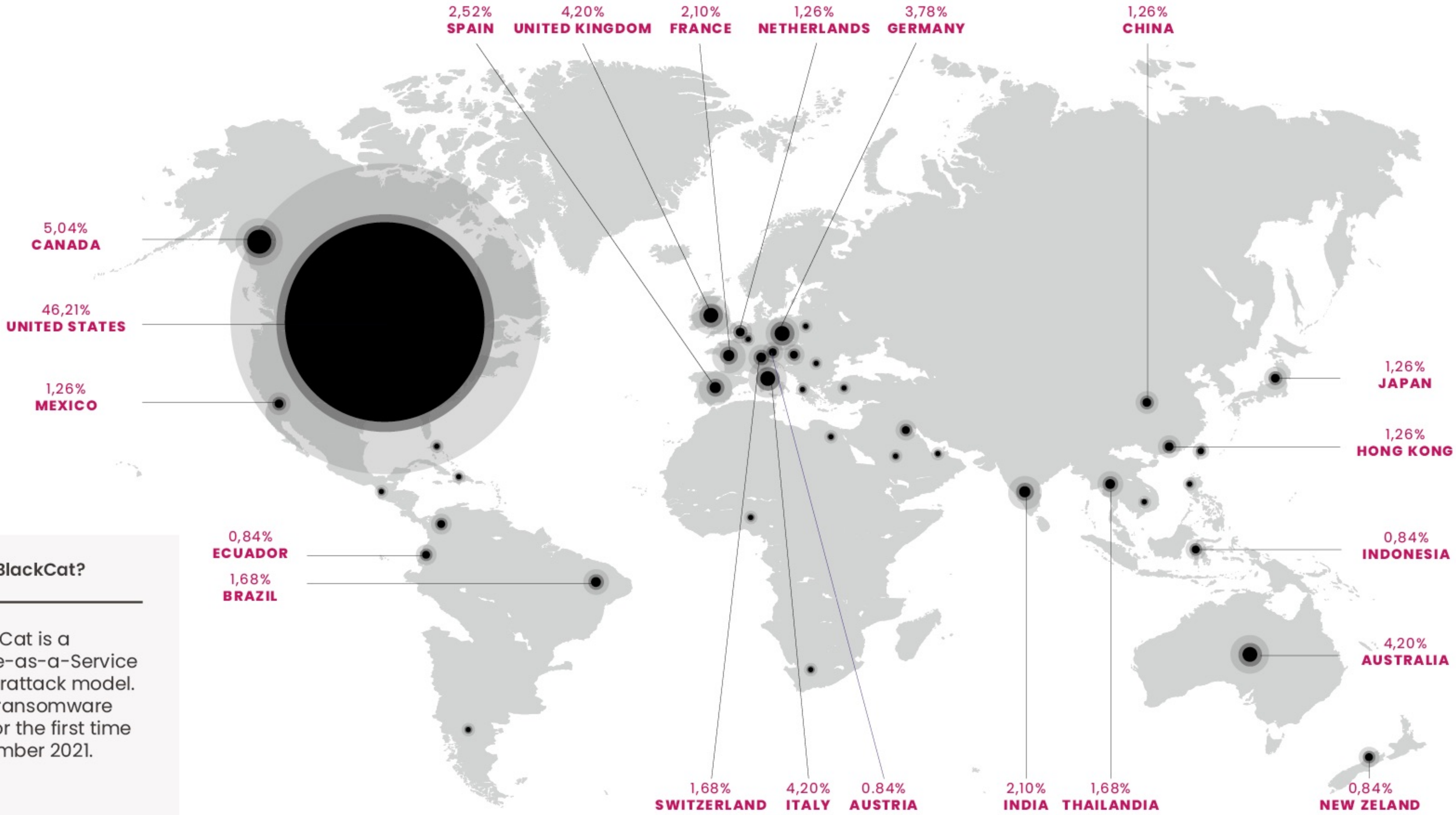
RANGE OF **ANNUAL REVENUE**



Lockbit: most affected sectors



Blackcat: most targeted areas

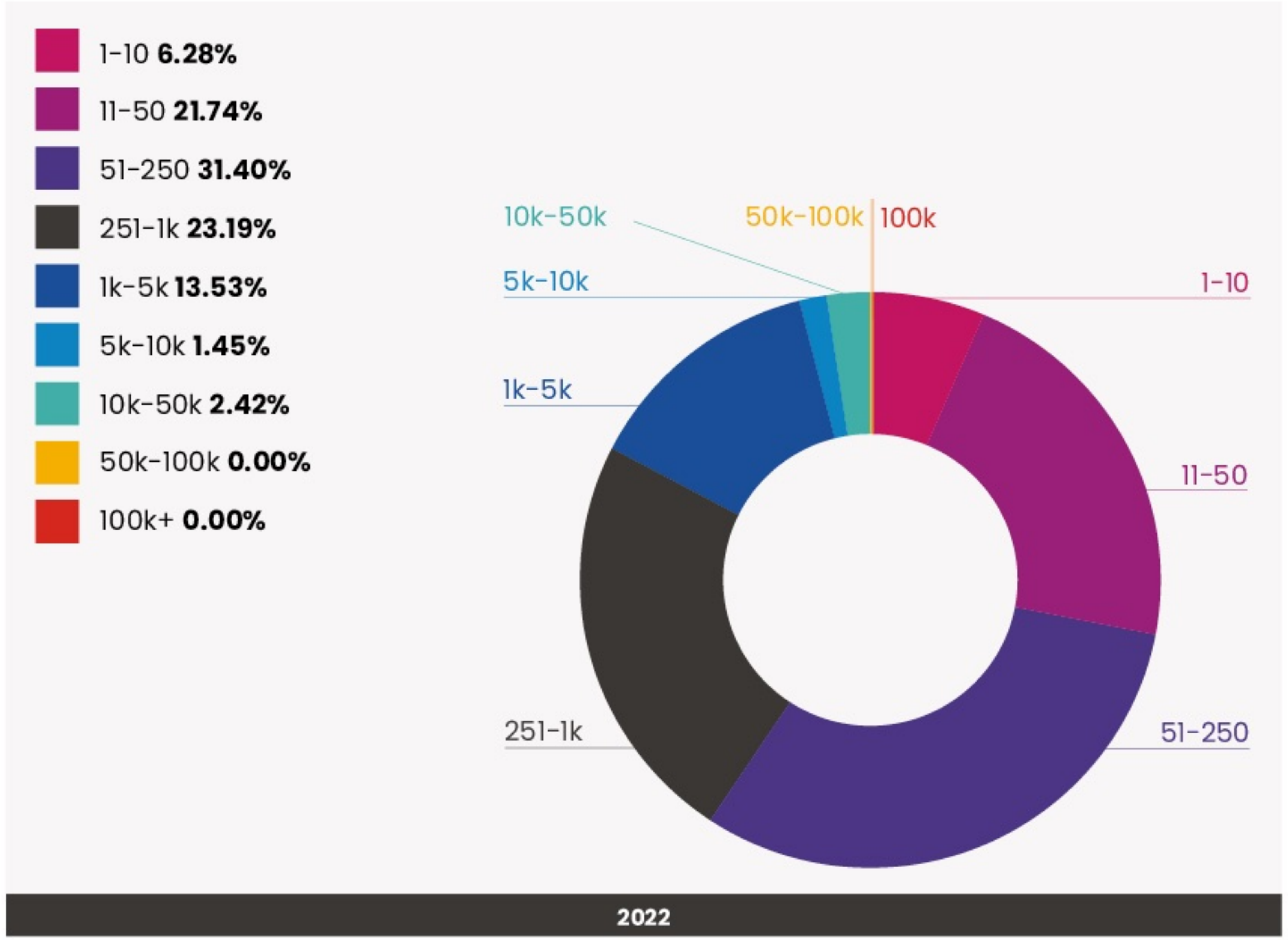


Who's BlackCat?

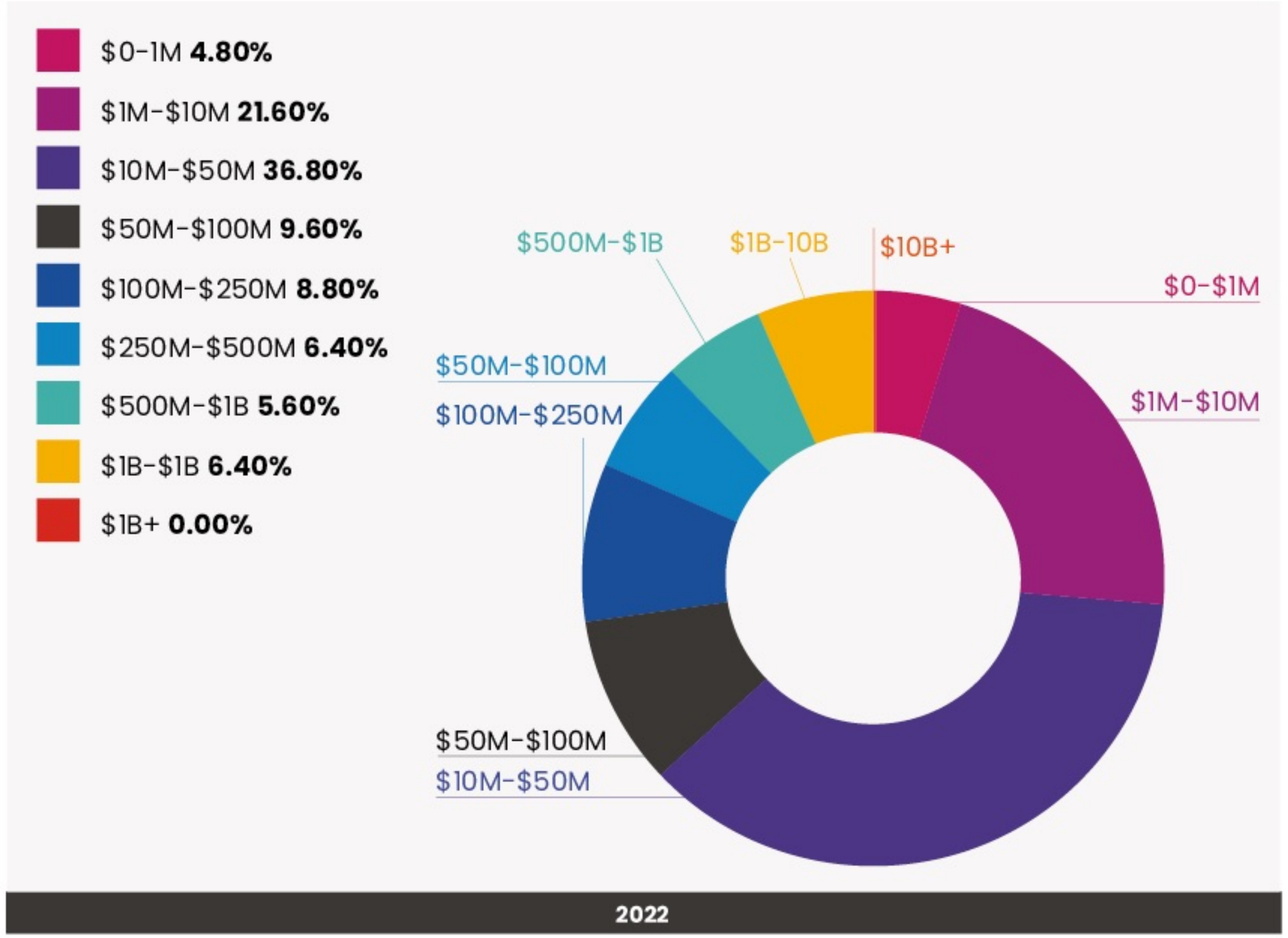
BlackCat is a Ransomware-as-a-Service (RaaS) cyberattack model. BlackCat ransomware appeared for the first time in November 2021.

Blackcat: most breached companies

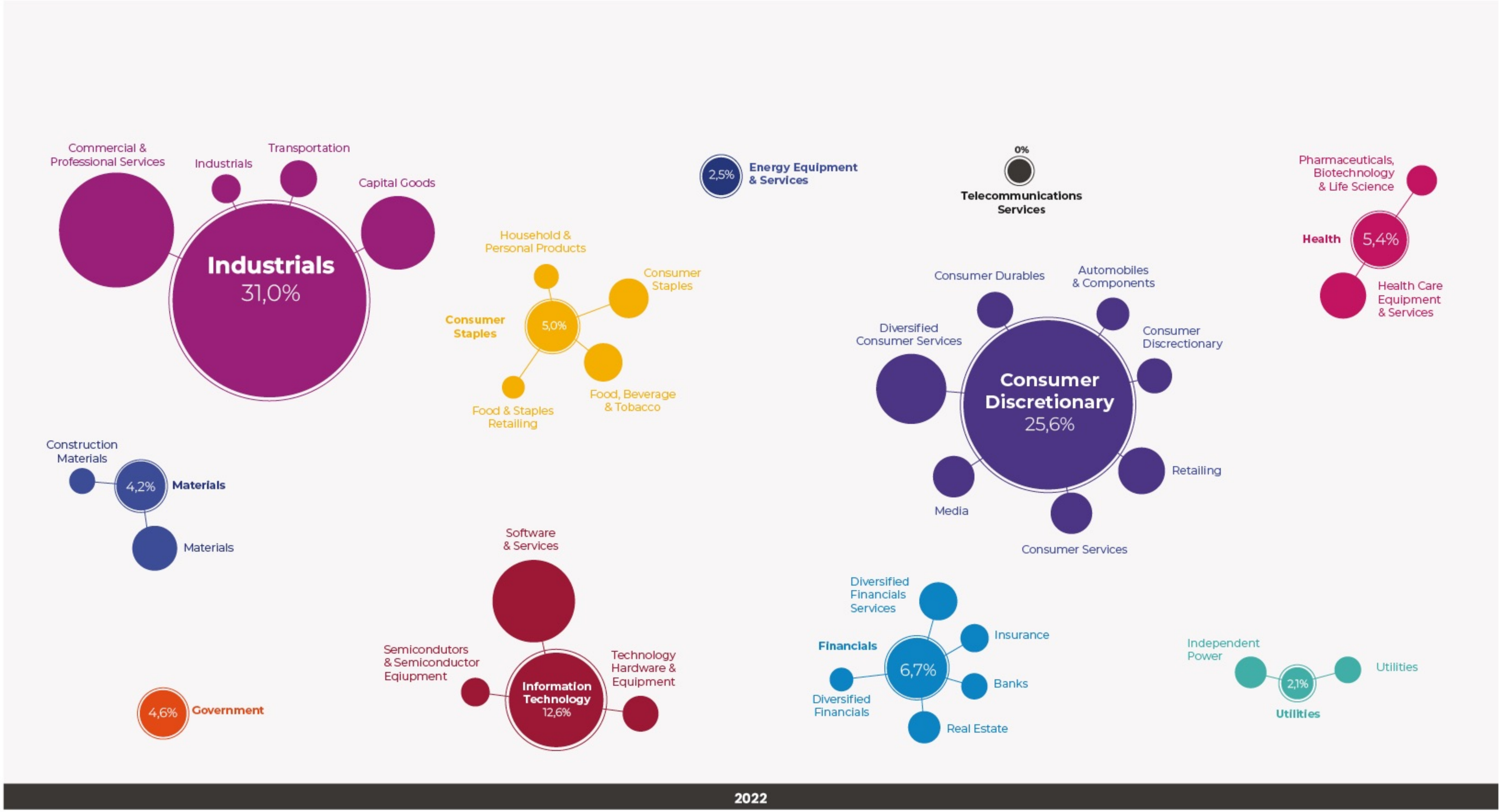
RANGE OF **EMPLOYEES**



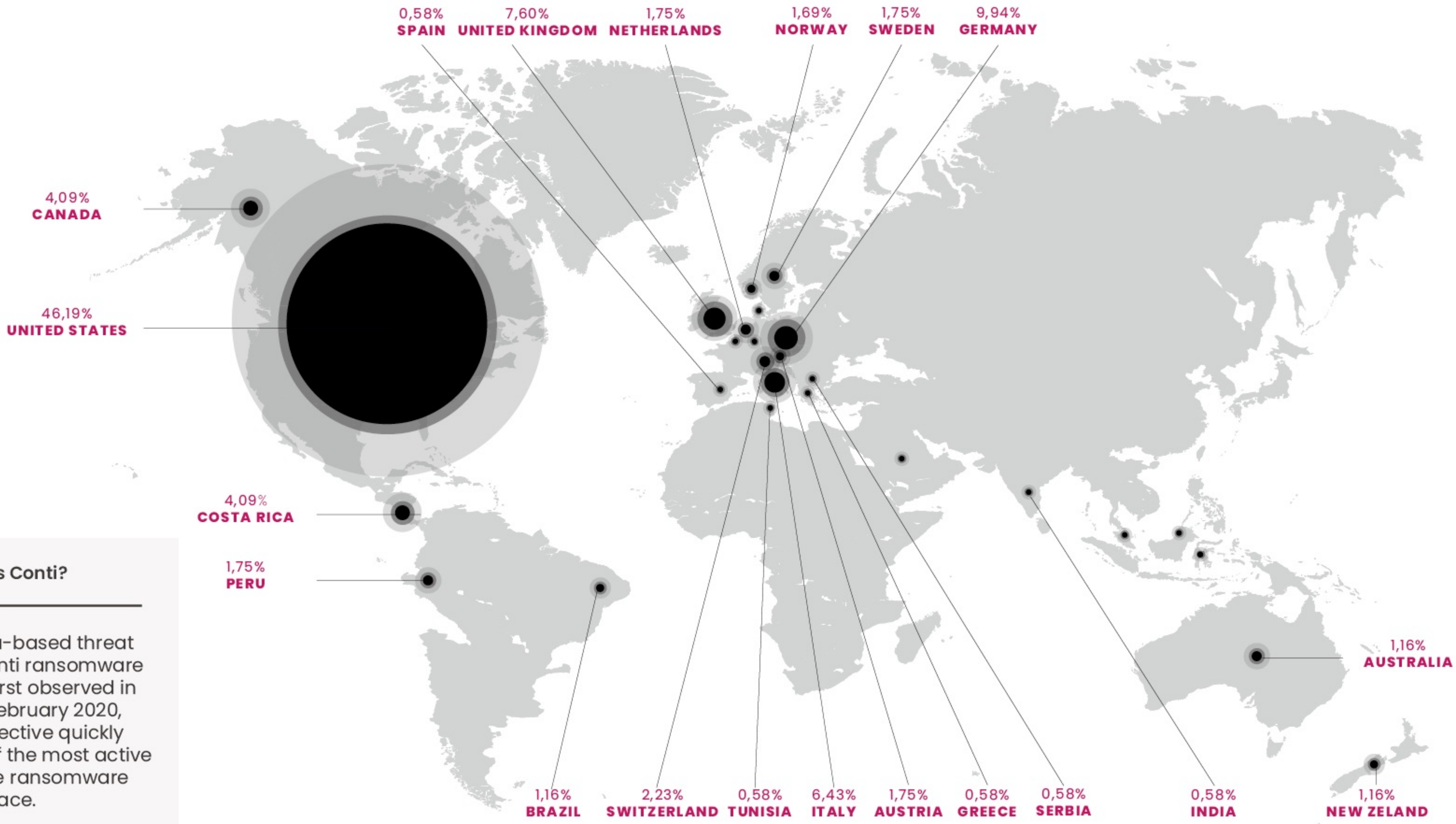
RANGE OF **ANNUAL REVENUE**



Blackcat: most affected sectors



Conti: most targeted areas

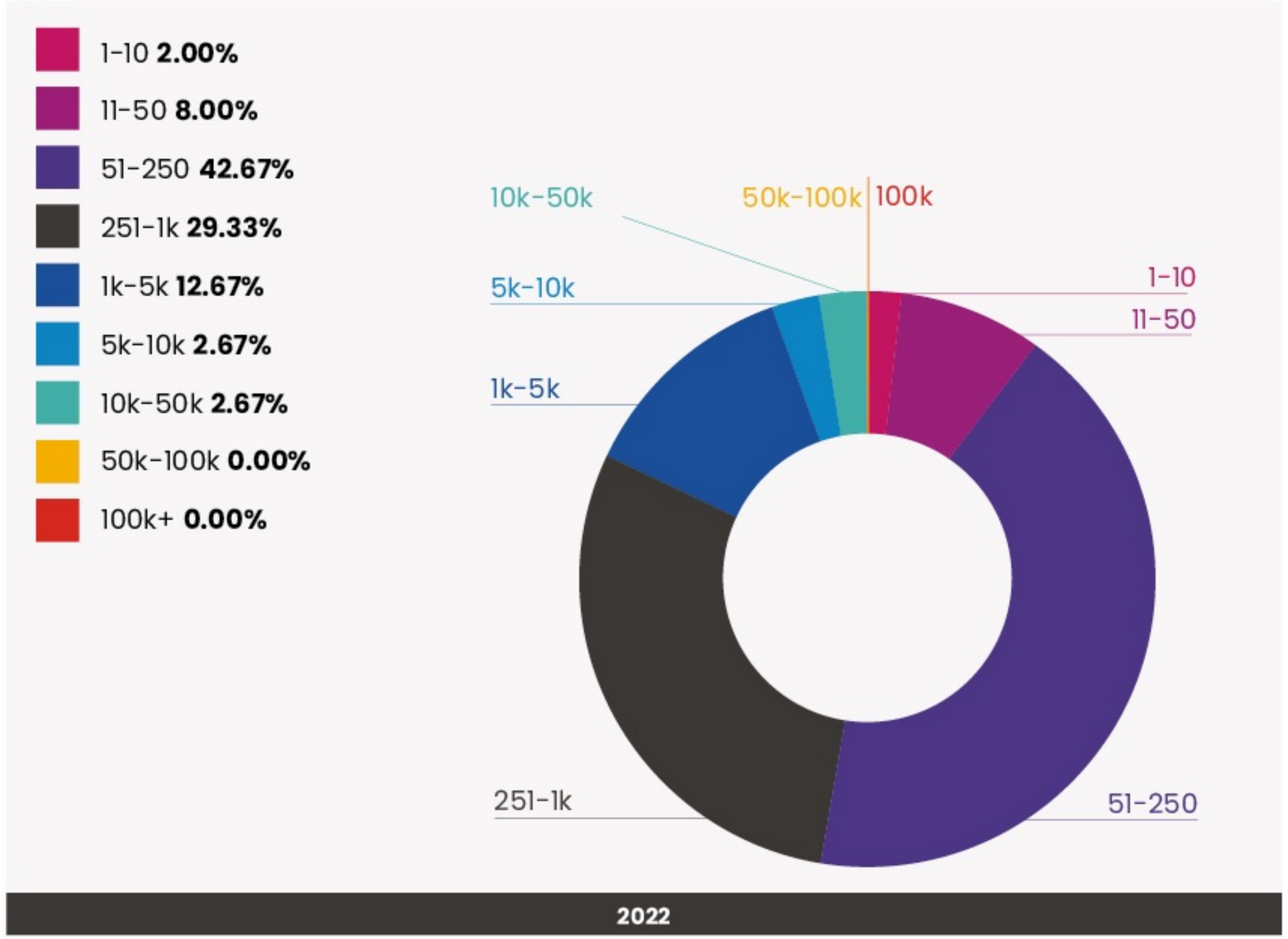


Who's Conti?

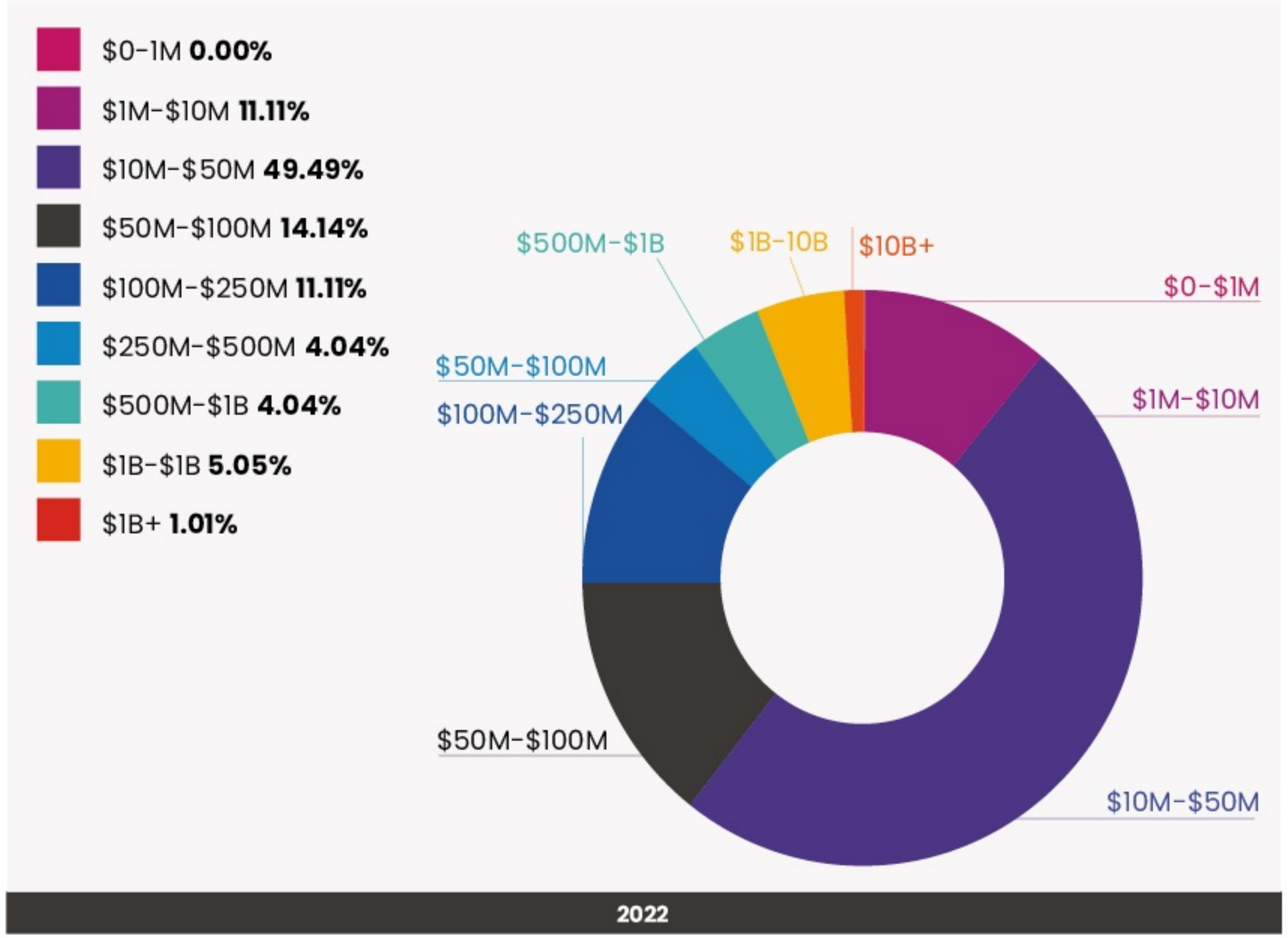
Led by Russia-based threat actors, the Conti ransomware variant was first observed in or around February 2020, and the collective quickly became one of the most active groups in the ransomware space.

Conti: most breached companies

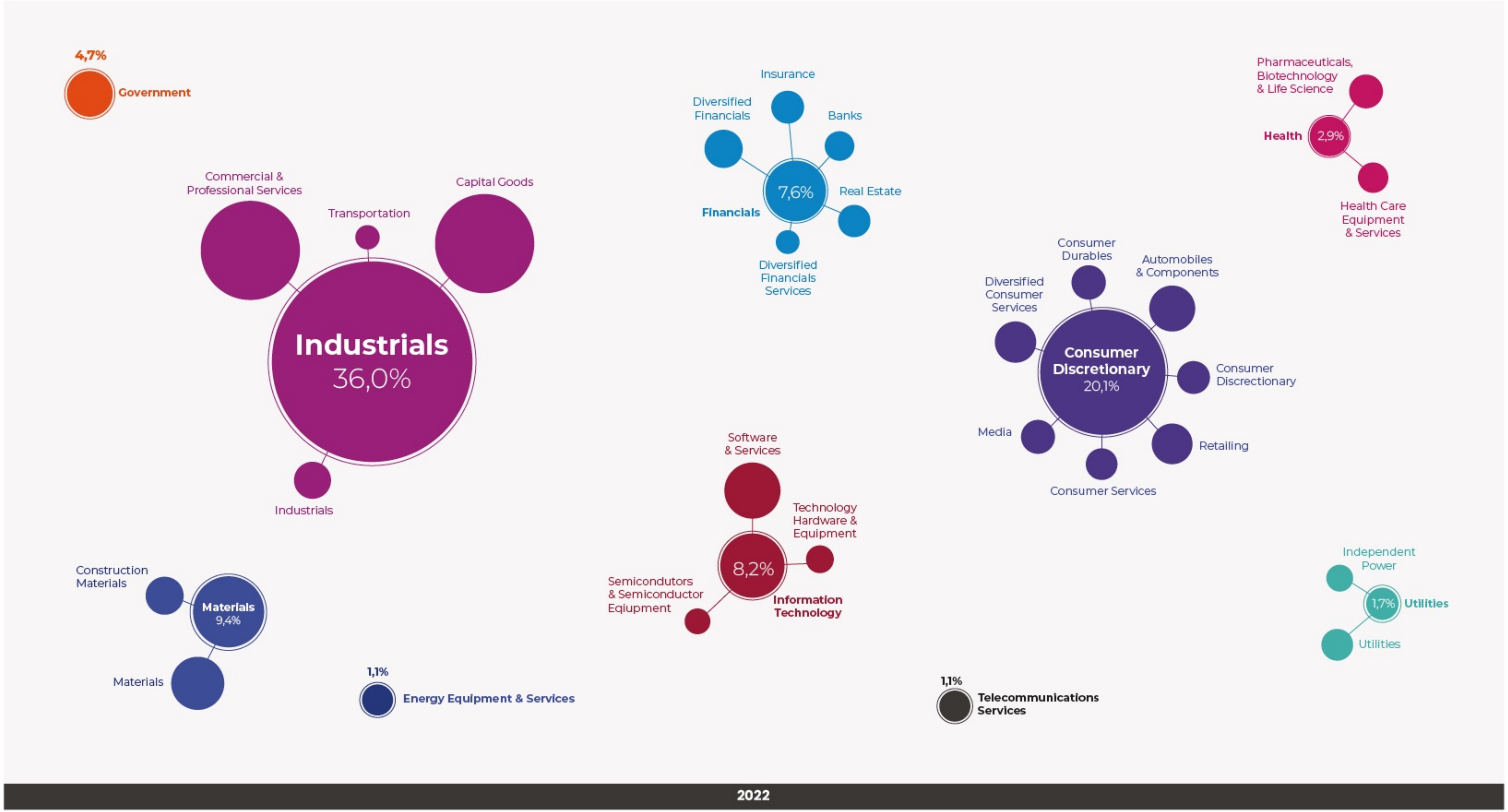
RANGE OF **EMPLOYEES**



RANGE OF **ANNUAL REVENUE**



Conti: most affected sectors



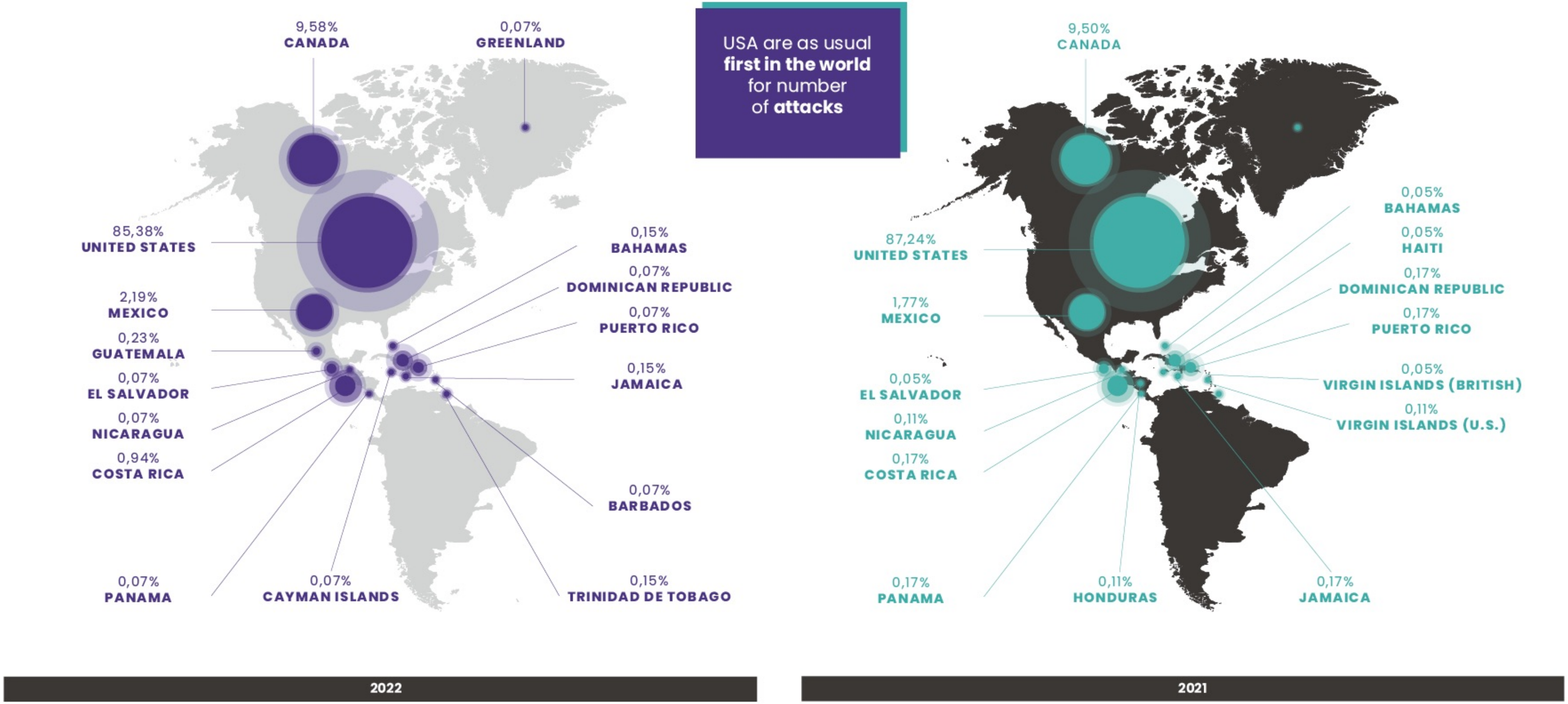
North America view

COMPARISON BETWEEN **2022** AND **2021**

- Geographical areas
- Range of employees
- Range of annual revenues

In 2021 North America was targeted by 48 ransomware groups, which became 57 in 2022

North America view by geographical areas

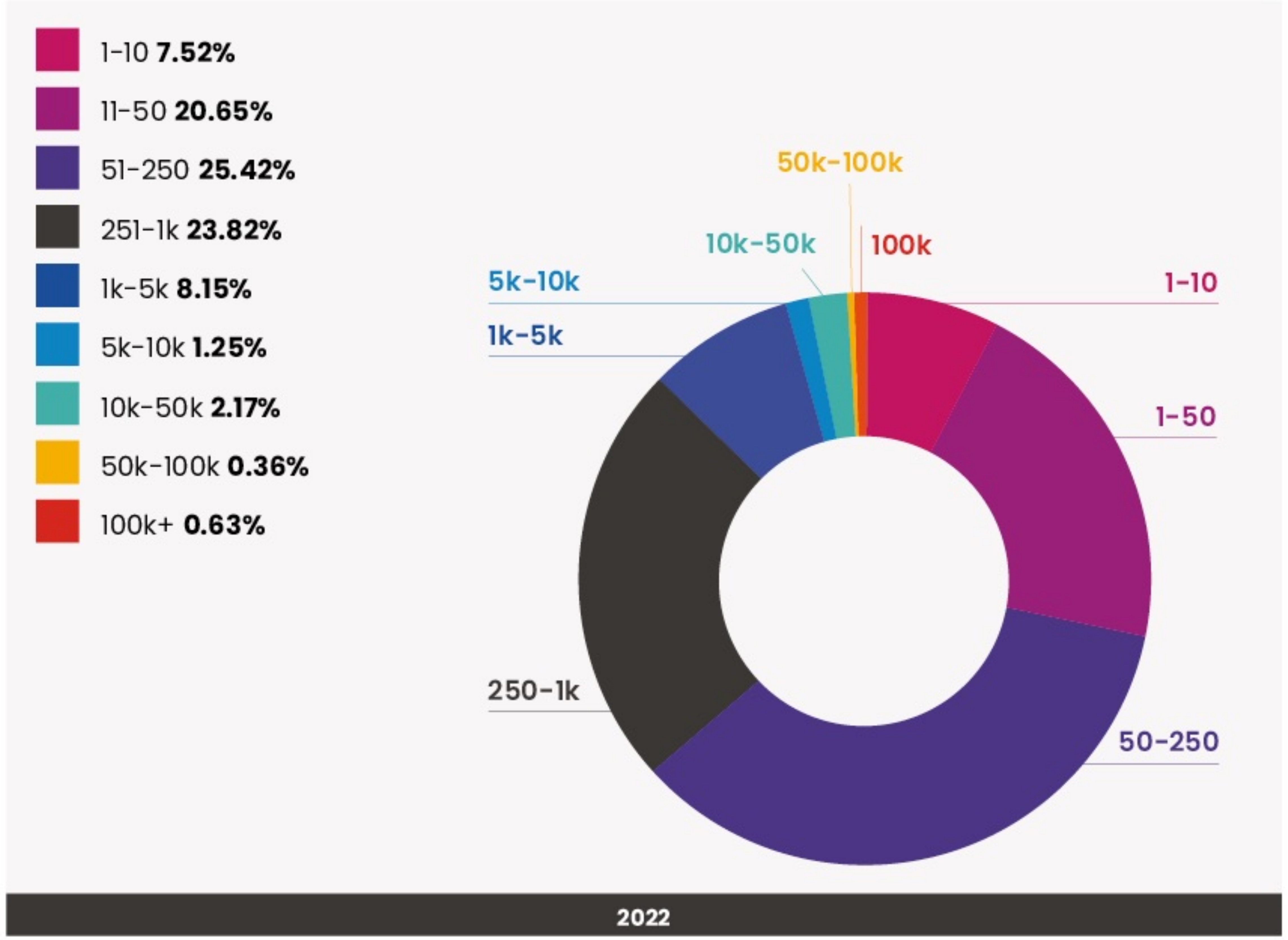


USA are as usual **first in the world** for number of **attacks**

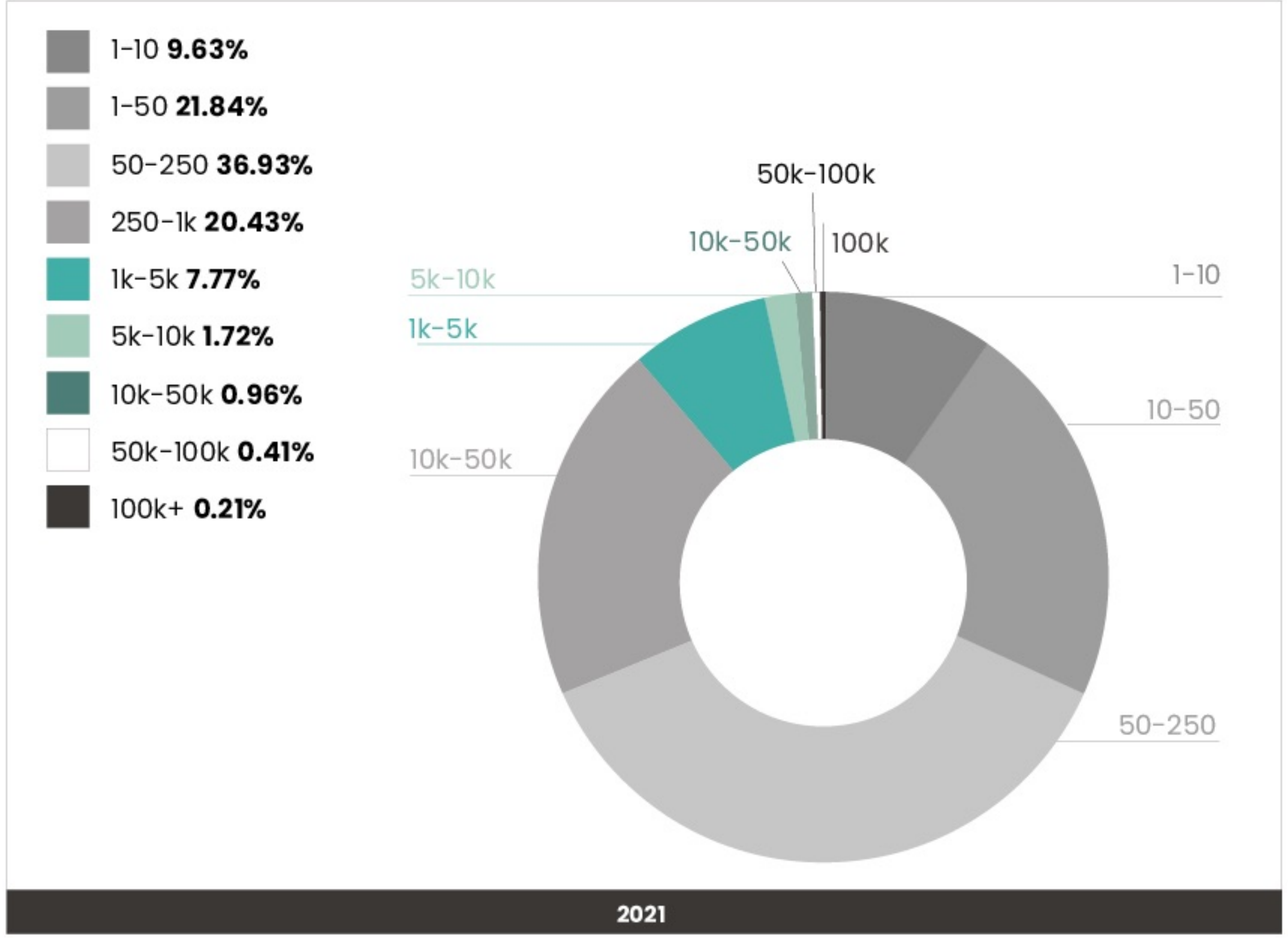
North America view by range of employees

Although North America is the area that **suffered most of attacks**, it is also the one that **recorded the major decrease** (**-10%**).

RANGE OF **EMPLOYEES**



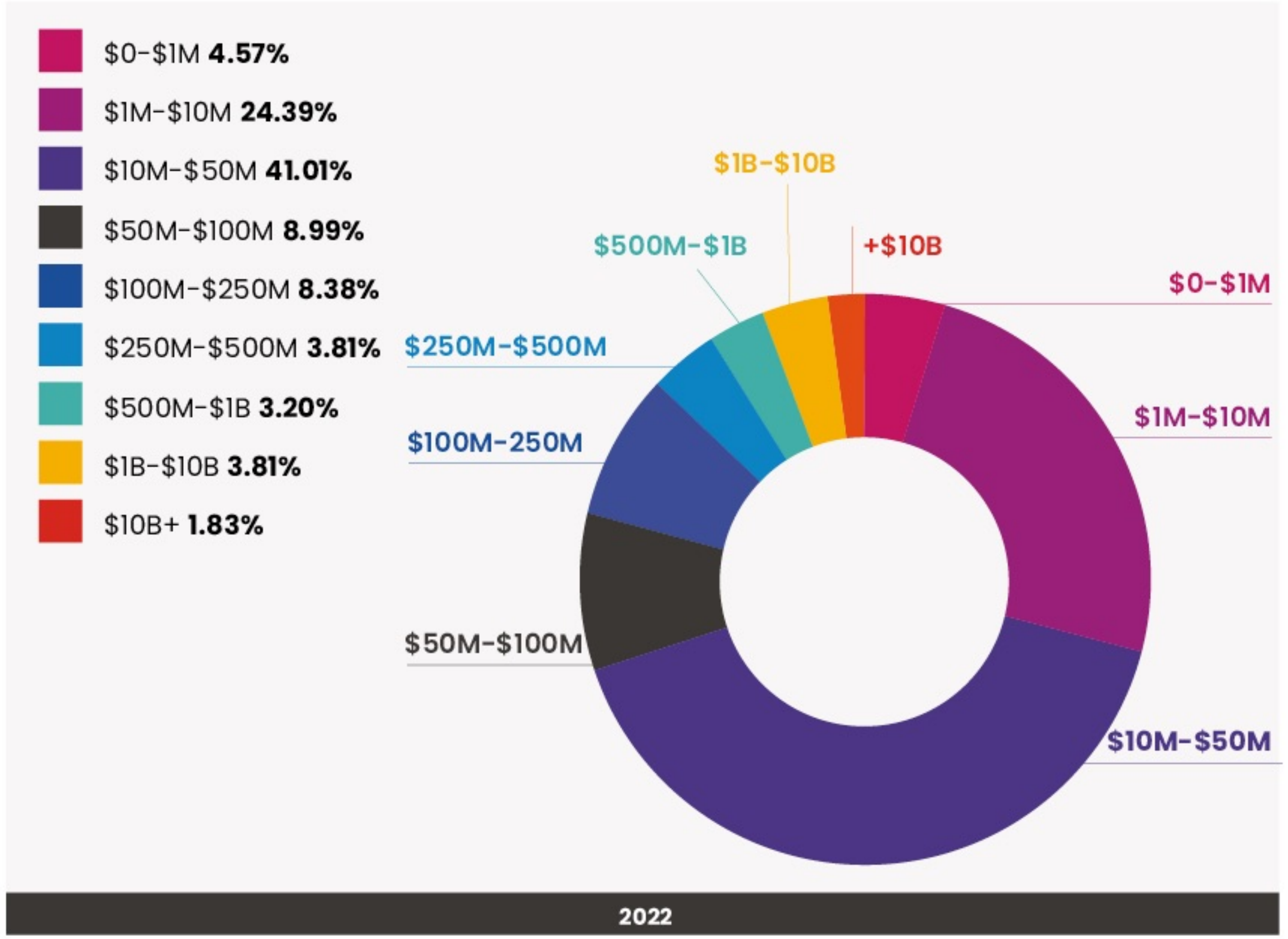
RANGE OF **EMPLOYEES**



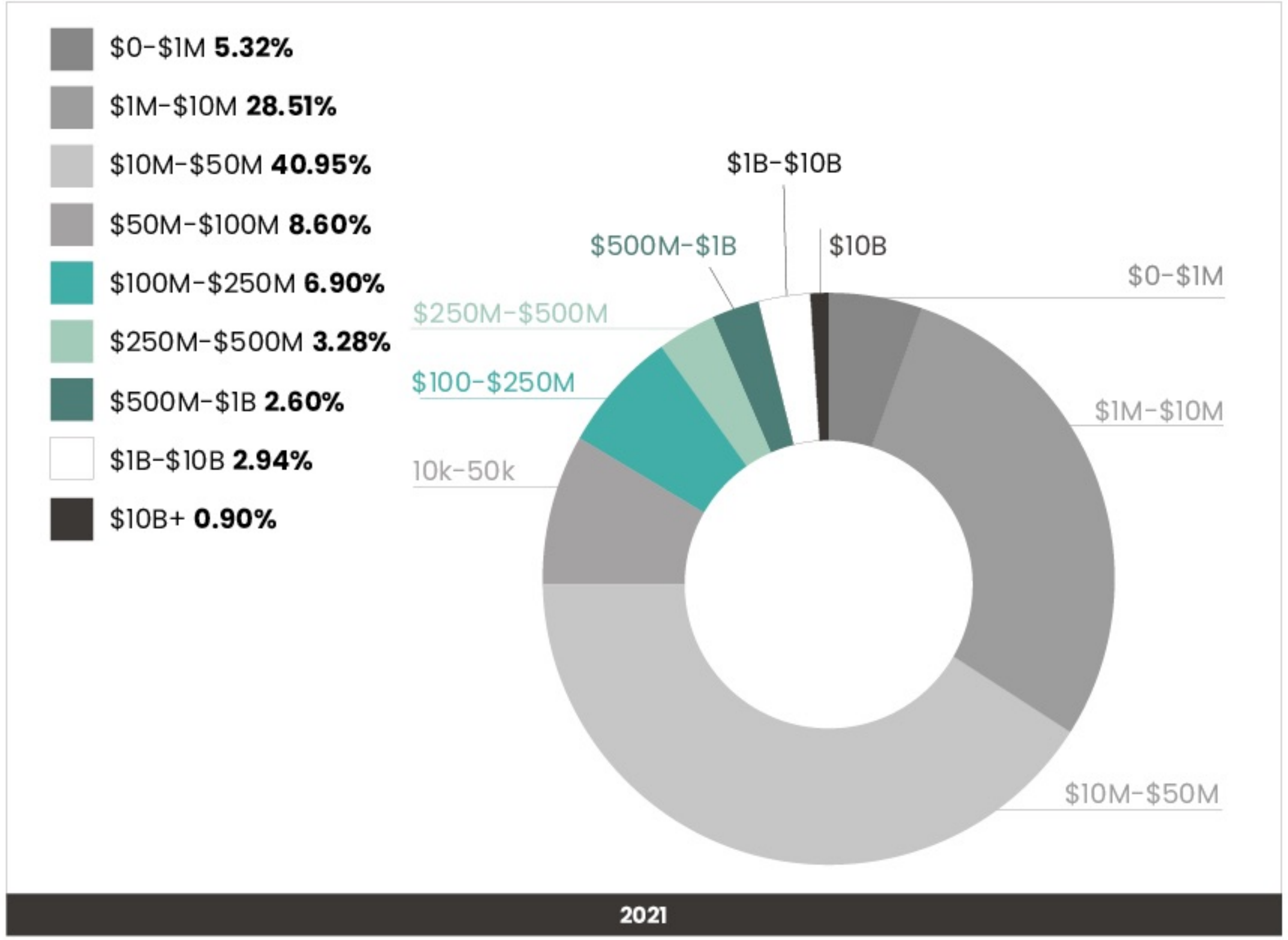
North America view by revenues range

SMEs and in particular companies with **revenues between $0 and $50M** represent 3/4 of the total number of companies affected.

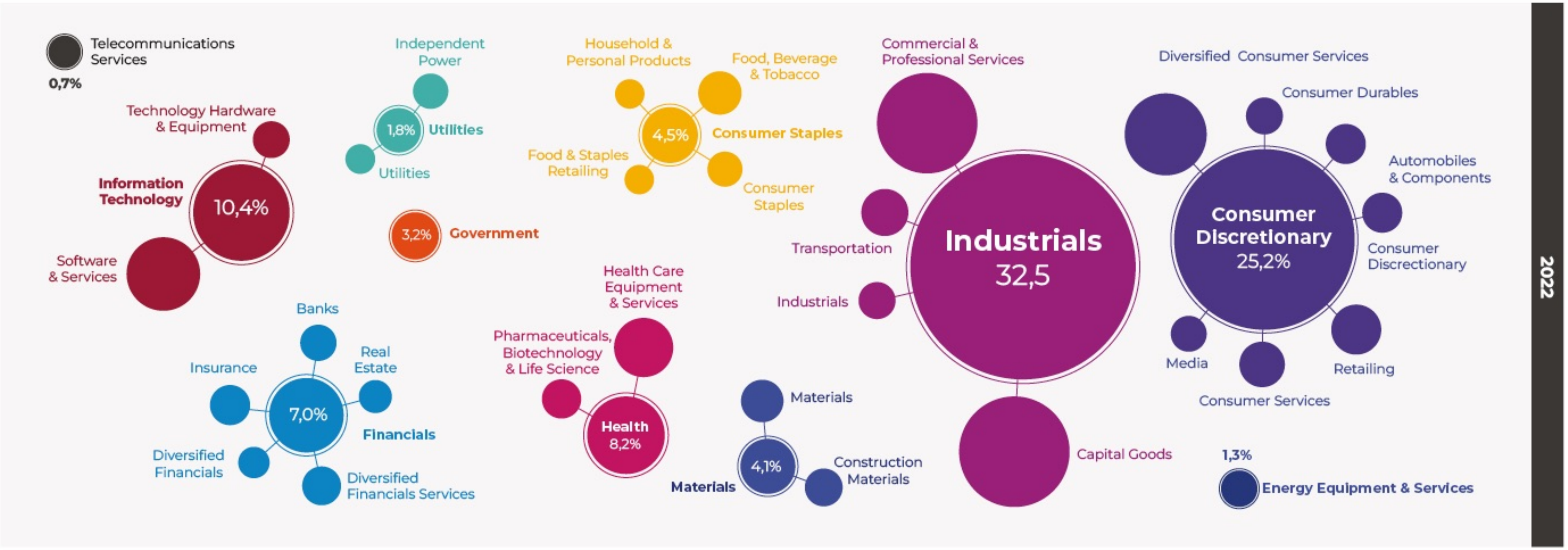
RANGE OF **ANNUAL REVENUE**

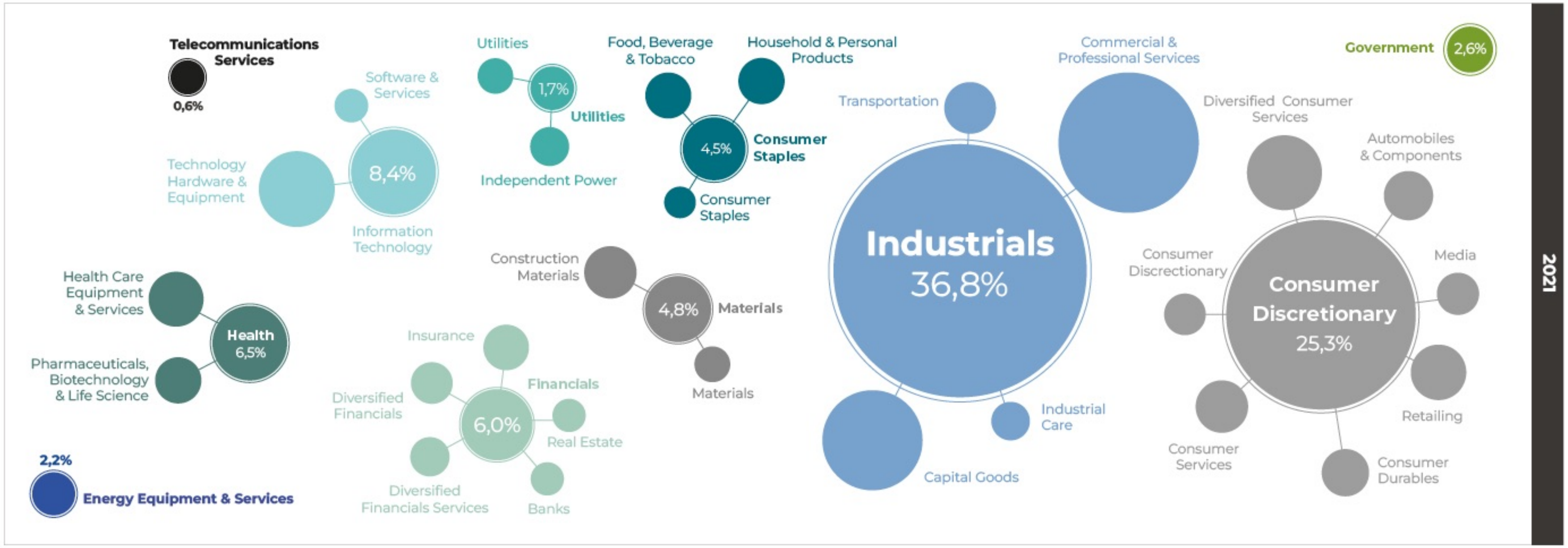


RANGE OF **ANNUAL REVENUE**



North America view of the most affected sectors





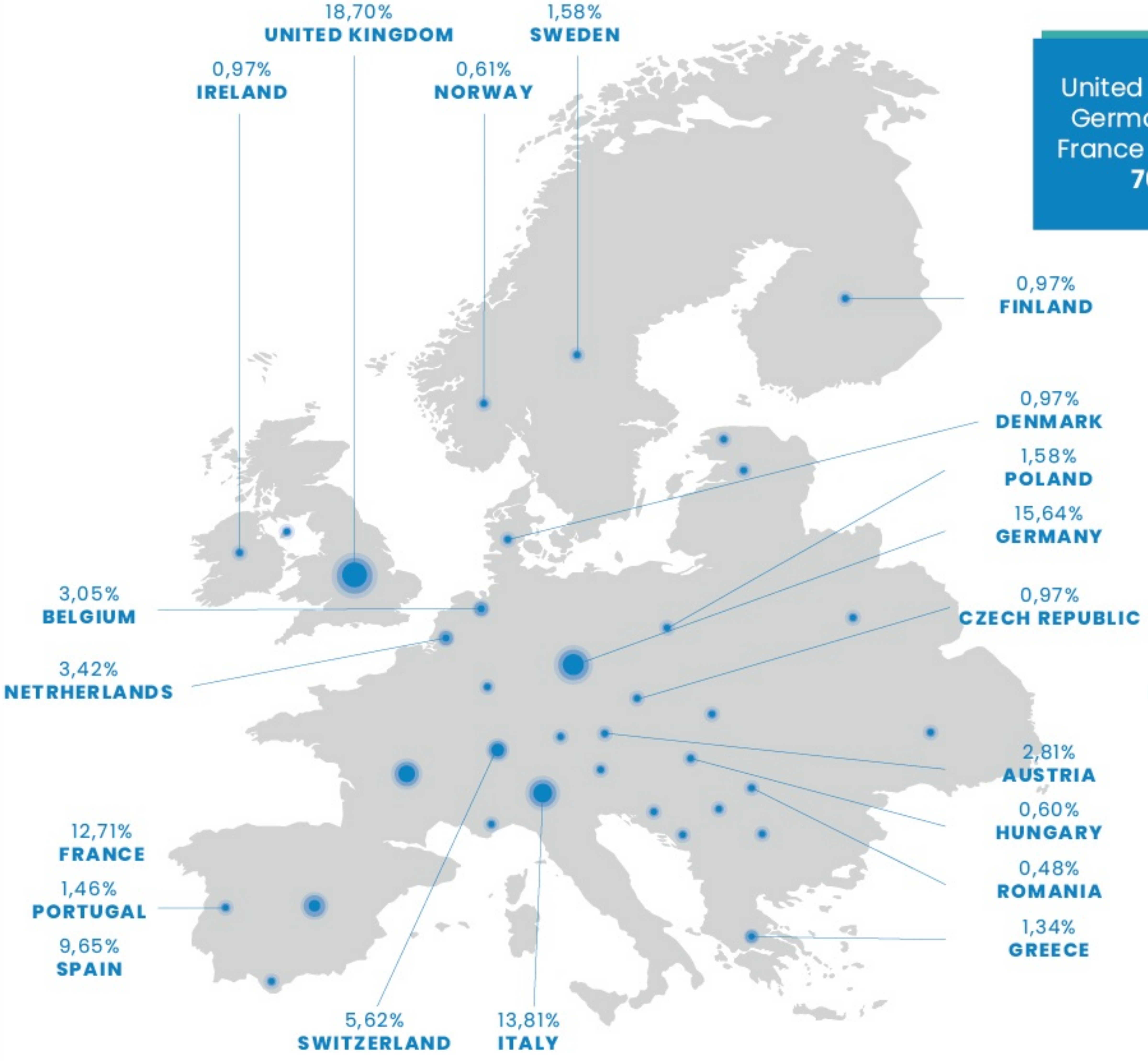
Europe view

COMPARISON BETWEEN **2022** AND **2021**

- Geographical areas
- Range of employees
- Range of annual revenues

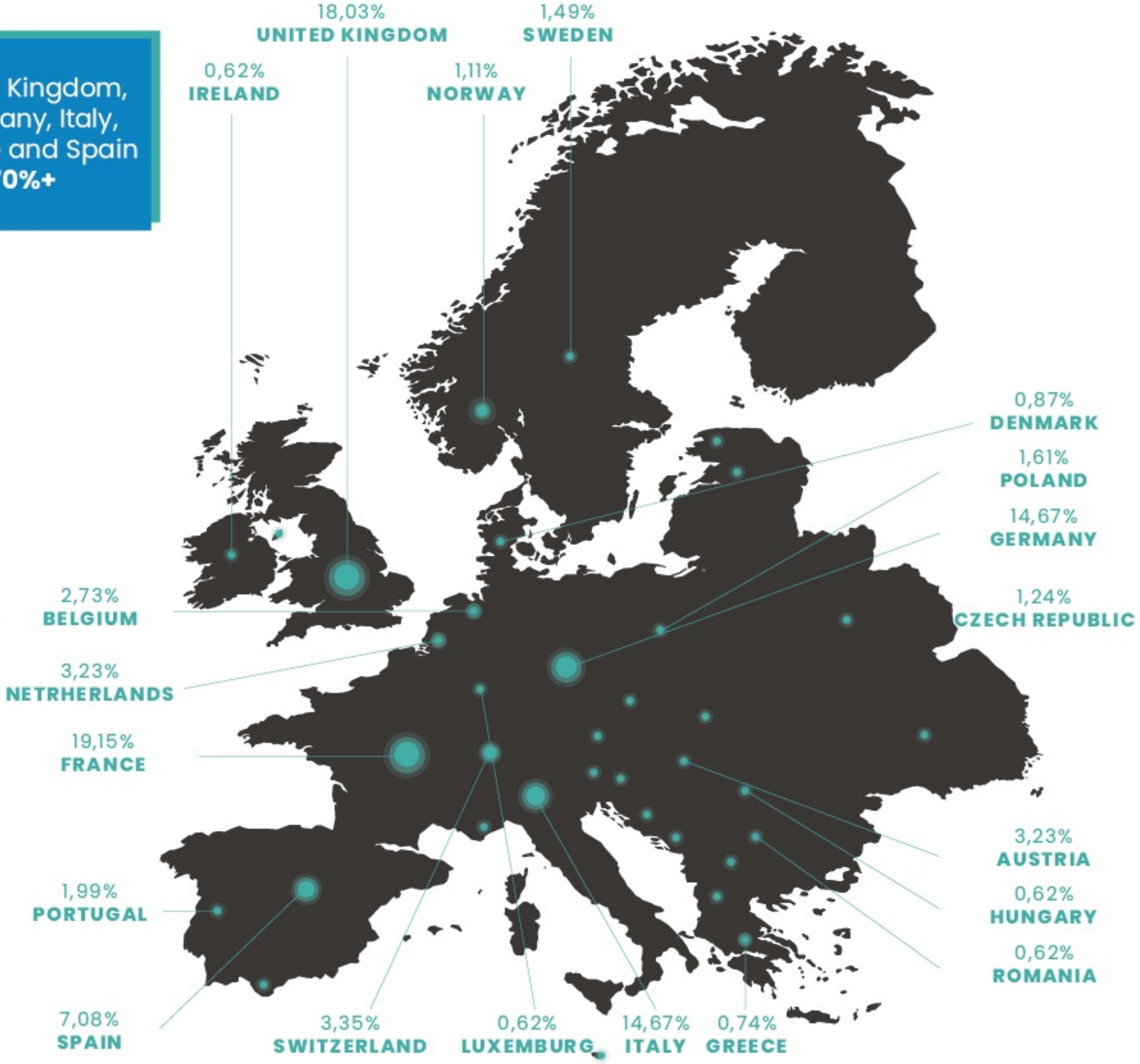
In 2021 Europe was targeted by 48 ransomware groups, which became 51 in 2022

Europe view by geographical areas



2022

United Kingdom, Germany, Italy, France and Spain **70%+**

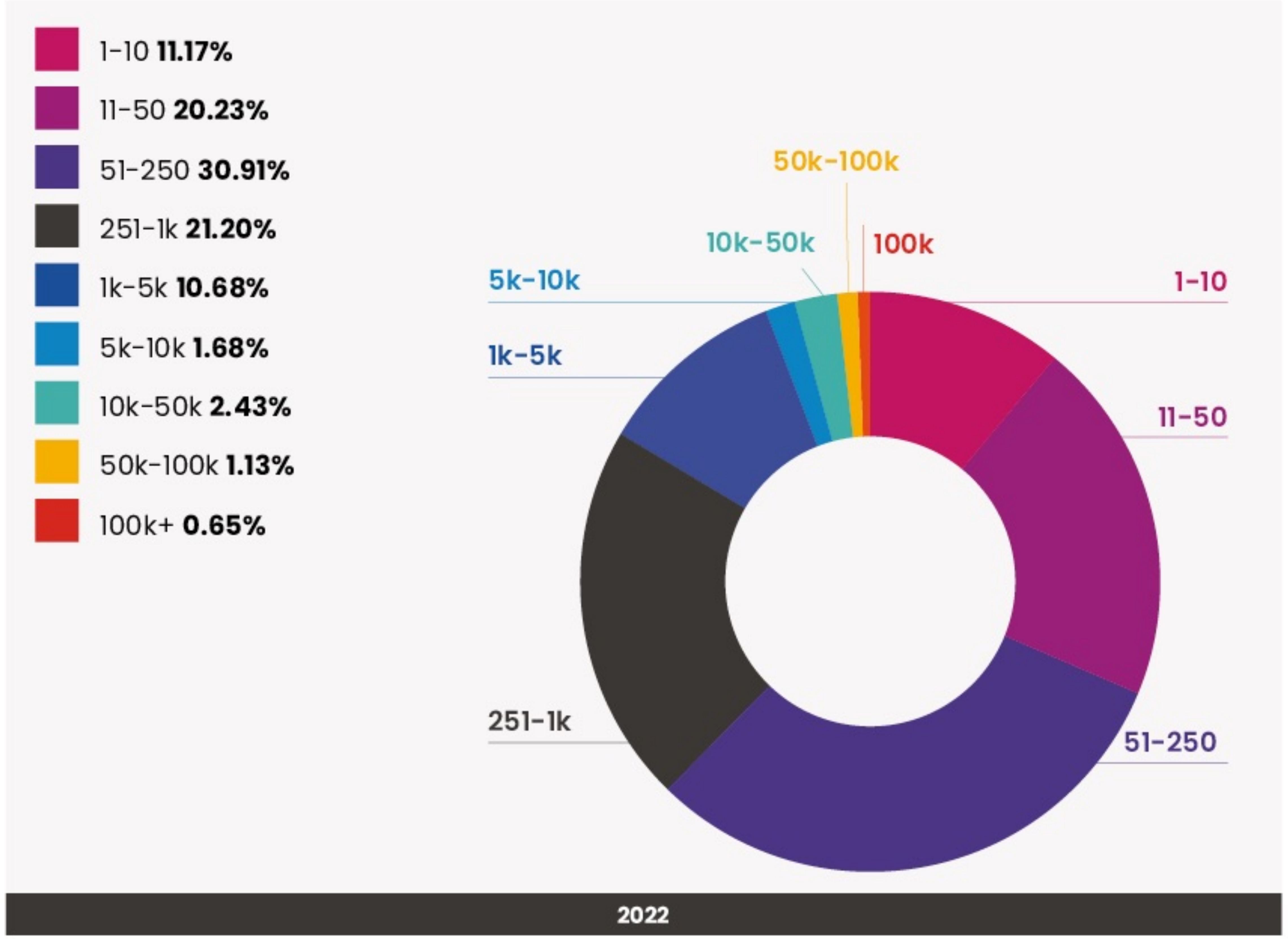


2021

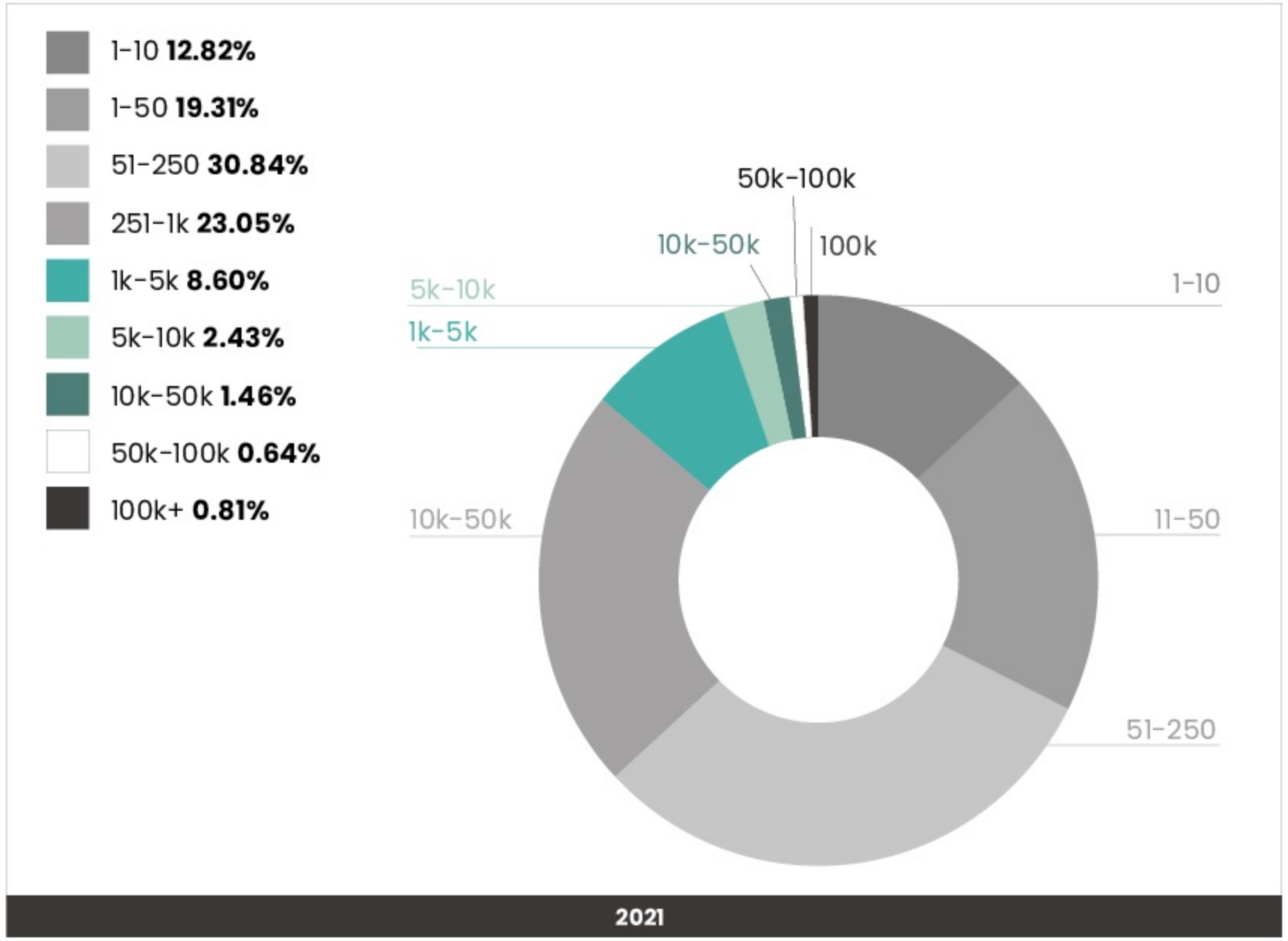
Europe view by range of employees

About 60% of targeted companies in 2021 and 2022 have **less than 250 employees**.

RANGE OF **EMPLOYEES**



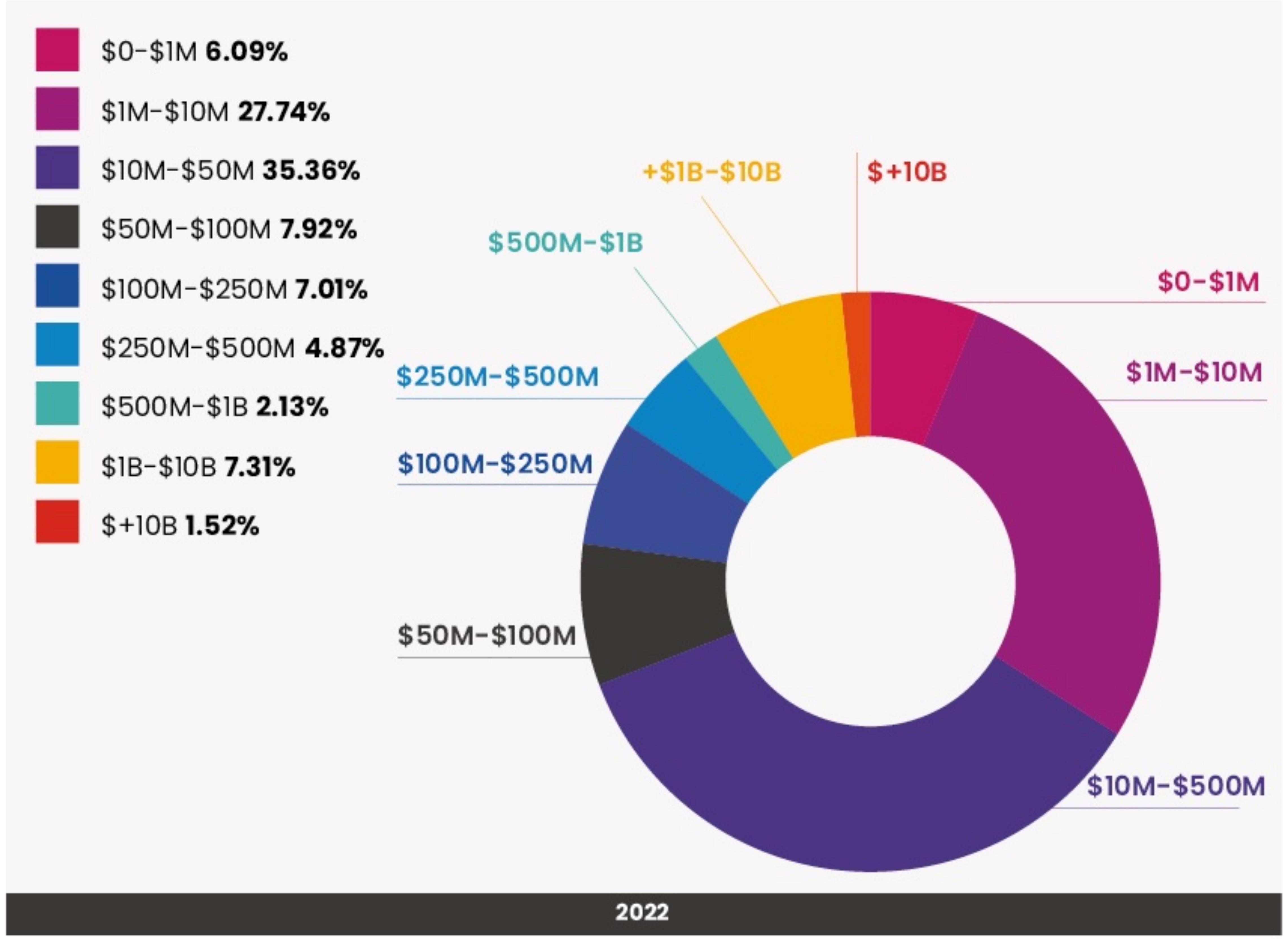
RANGE OF **EMPLOYEES**



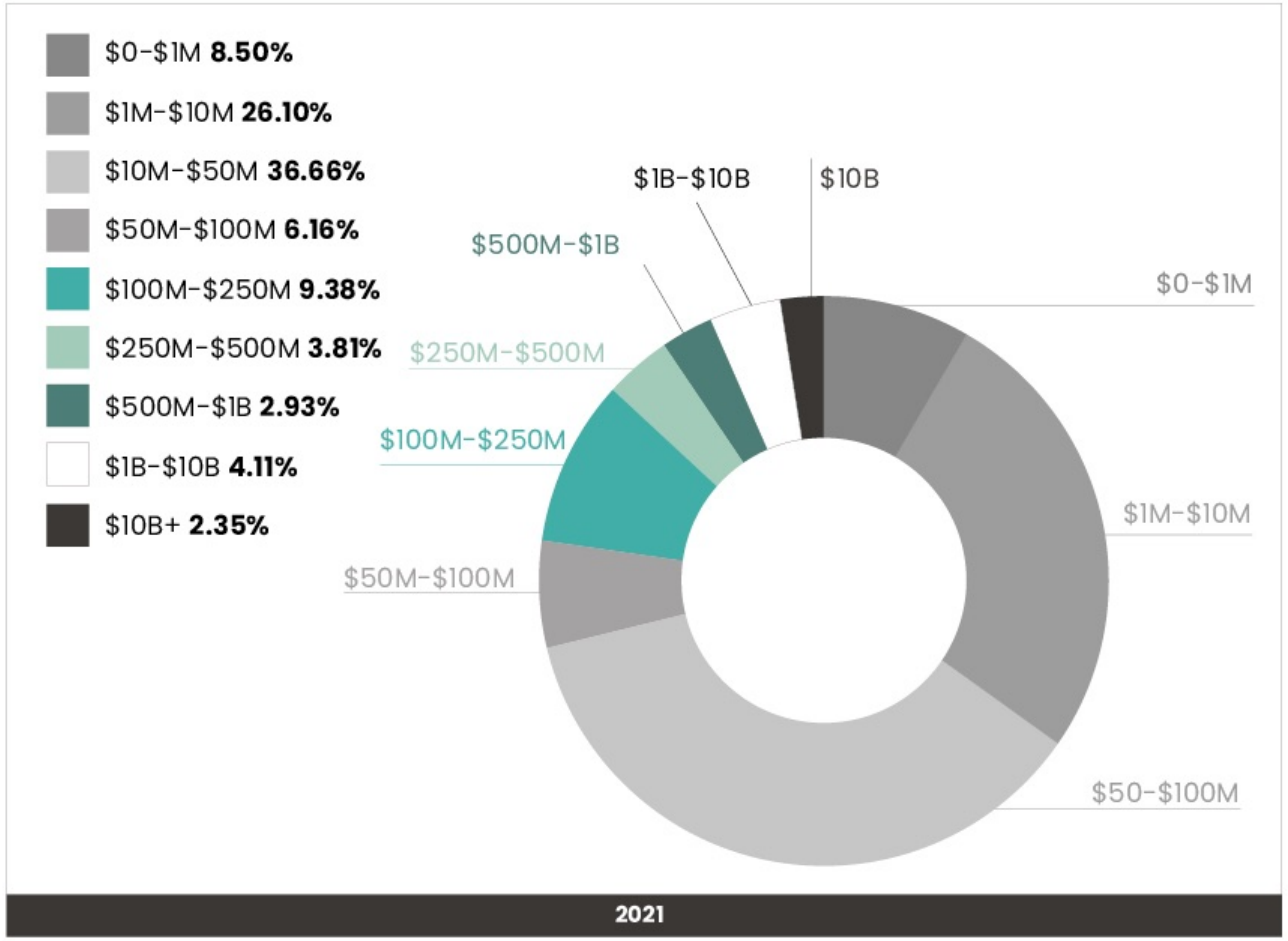
Europe view by revenues range

Companies with **less than 50M in revenues** represent about 70% both in 2021 and in 2022.

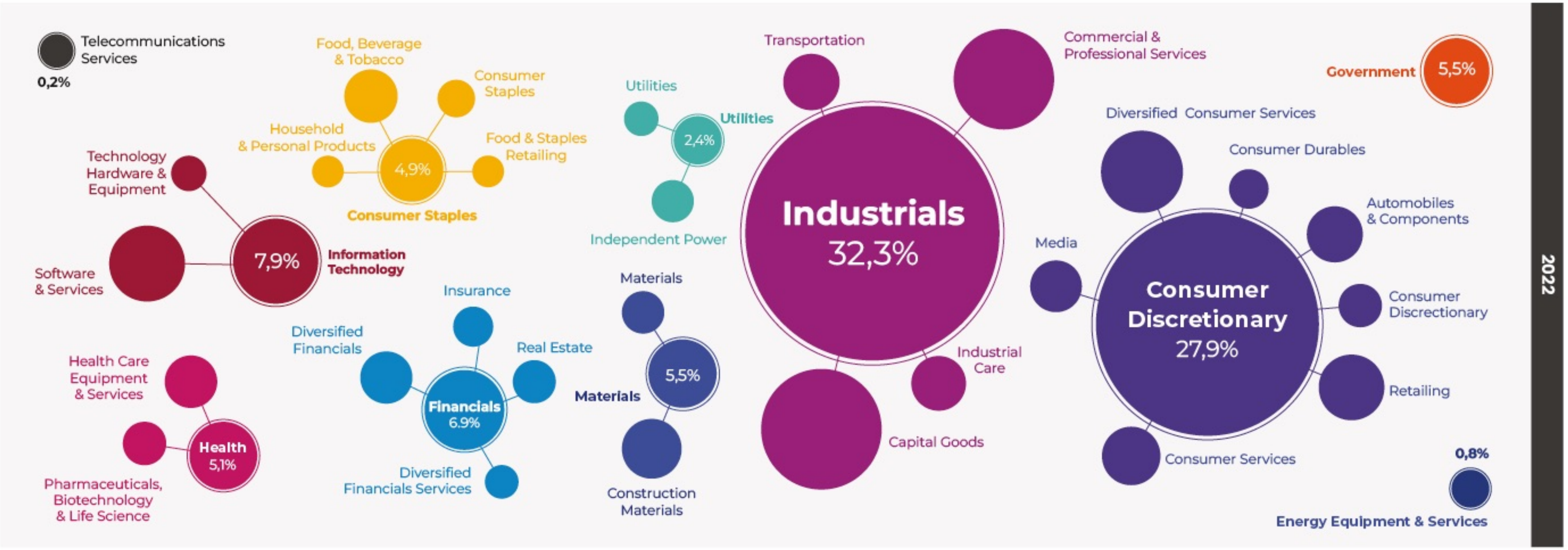
RANGE OF **ANNUAL REVENUE**

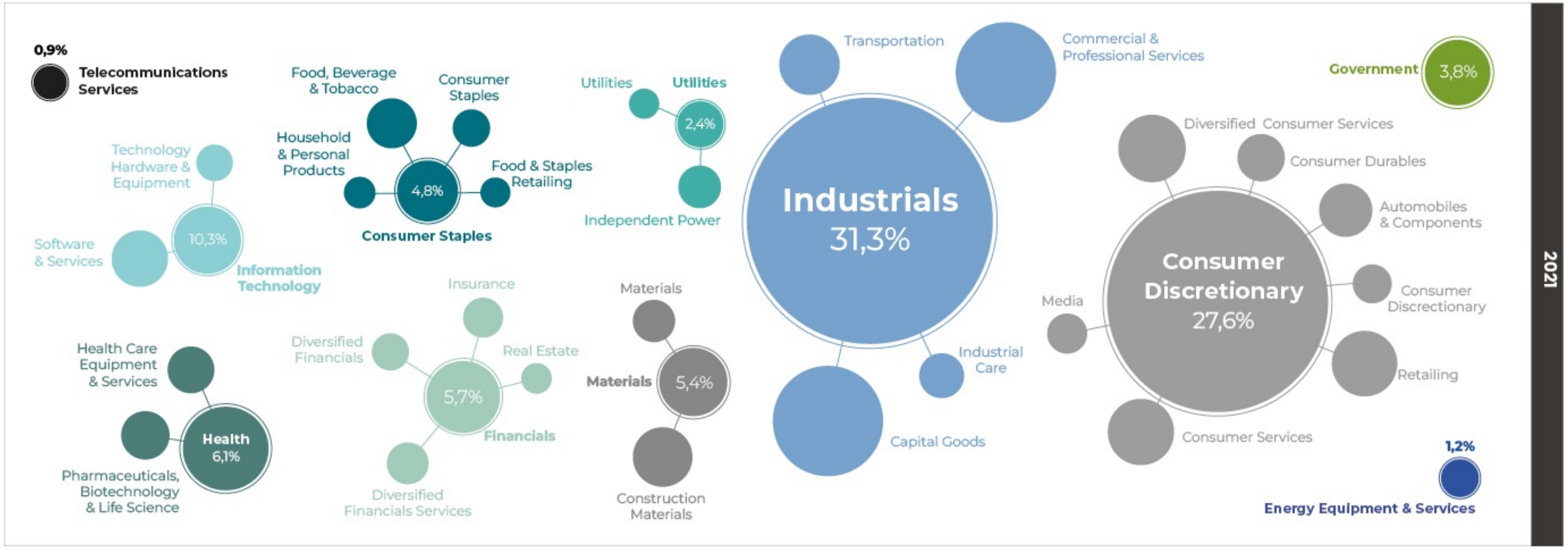


RANGE OF **ANNUAL REVENUE**



Europe view of the most affected sectors





Asia view

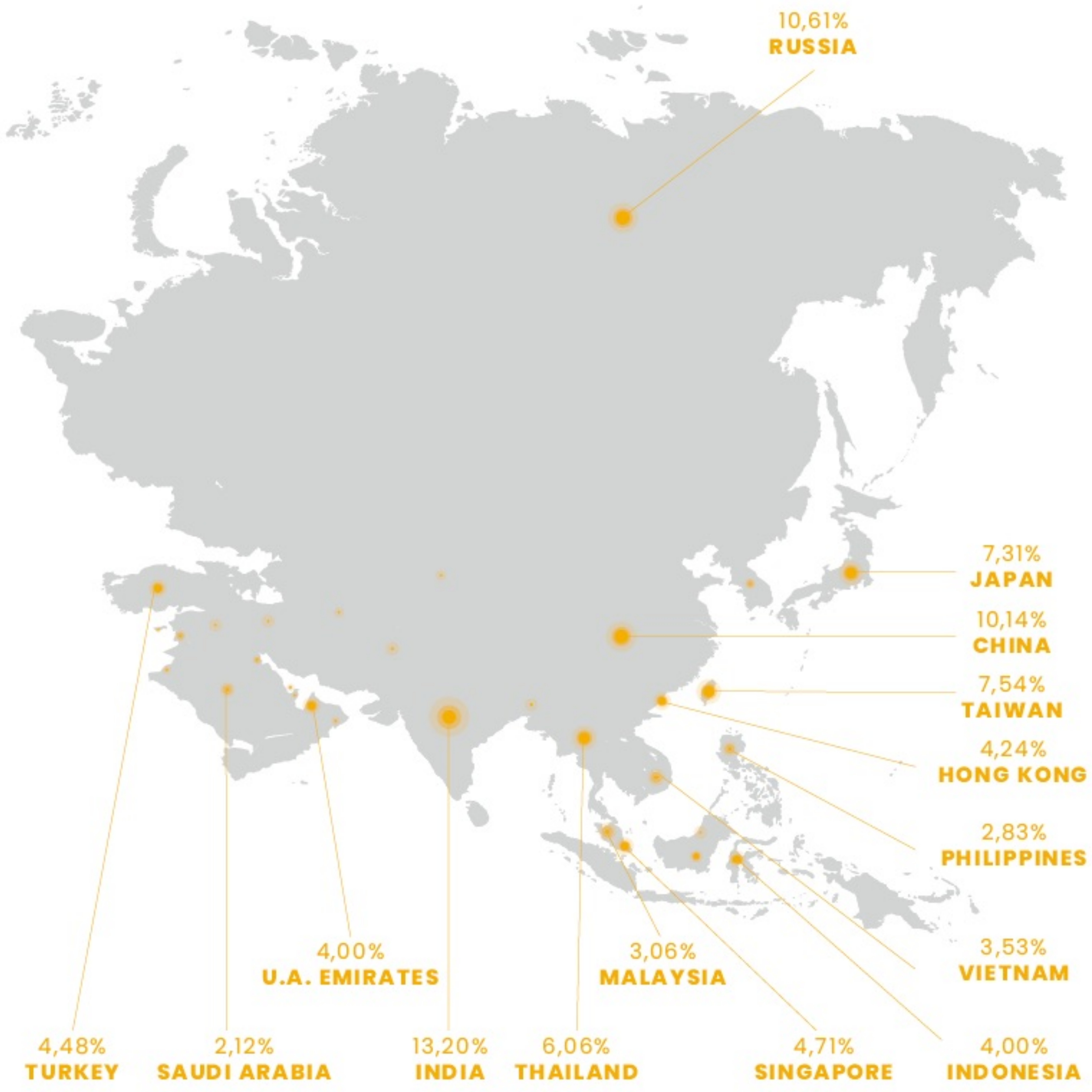
COMPARISON BETWEEN **2022** AND **2021**

- Geographical areas
- Range of employees
- Range of annual revenues

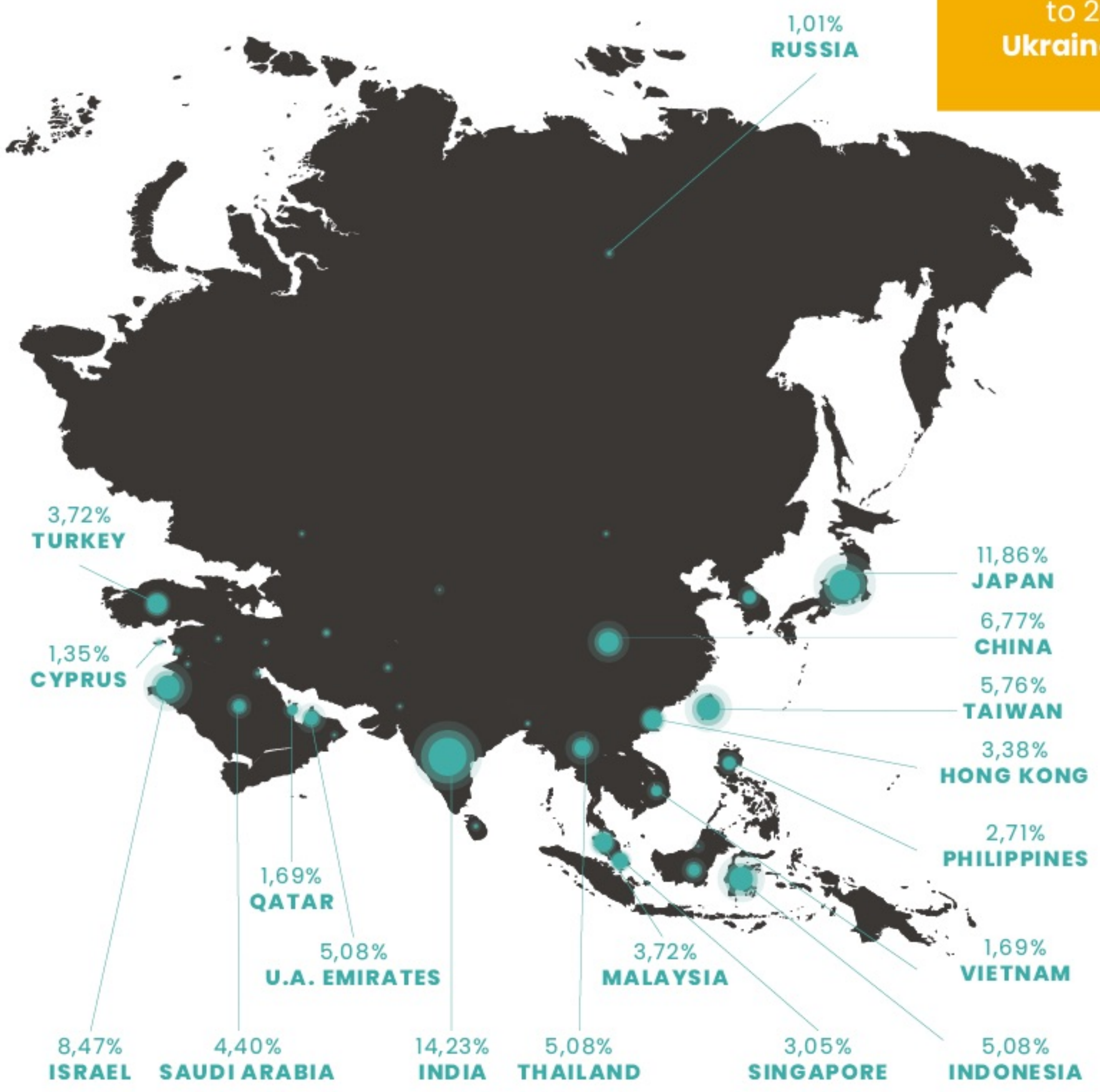
In 2021 Asia was attacked by 45 ransomware groups, which became 51 in 2022

Asia view by geographical areas

Russia recorded **+ 9%** compared to 2021. **Ukraine war?**



2022

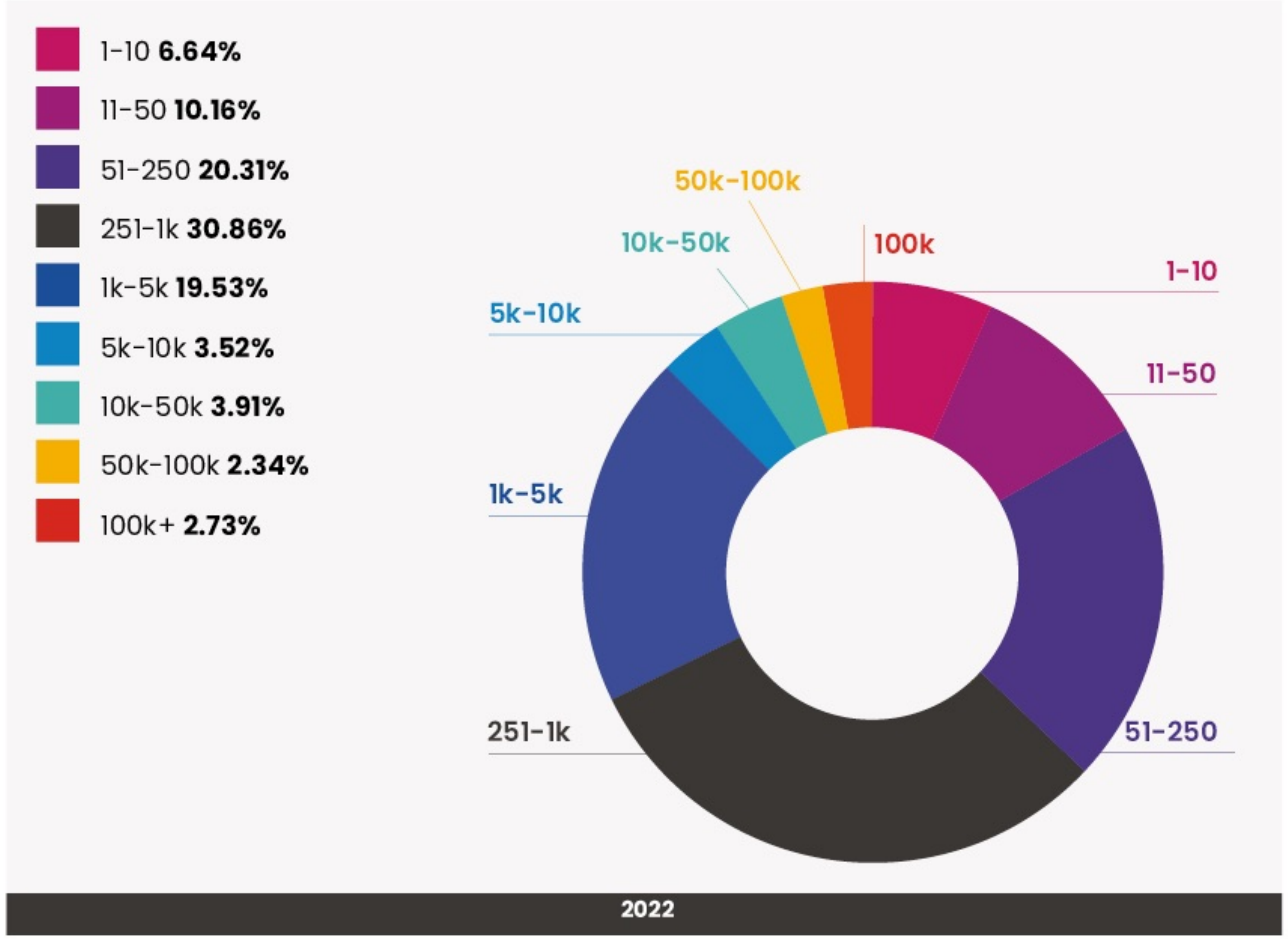


2021

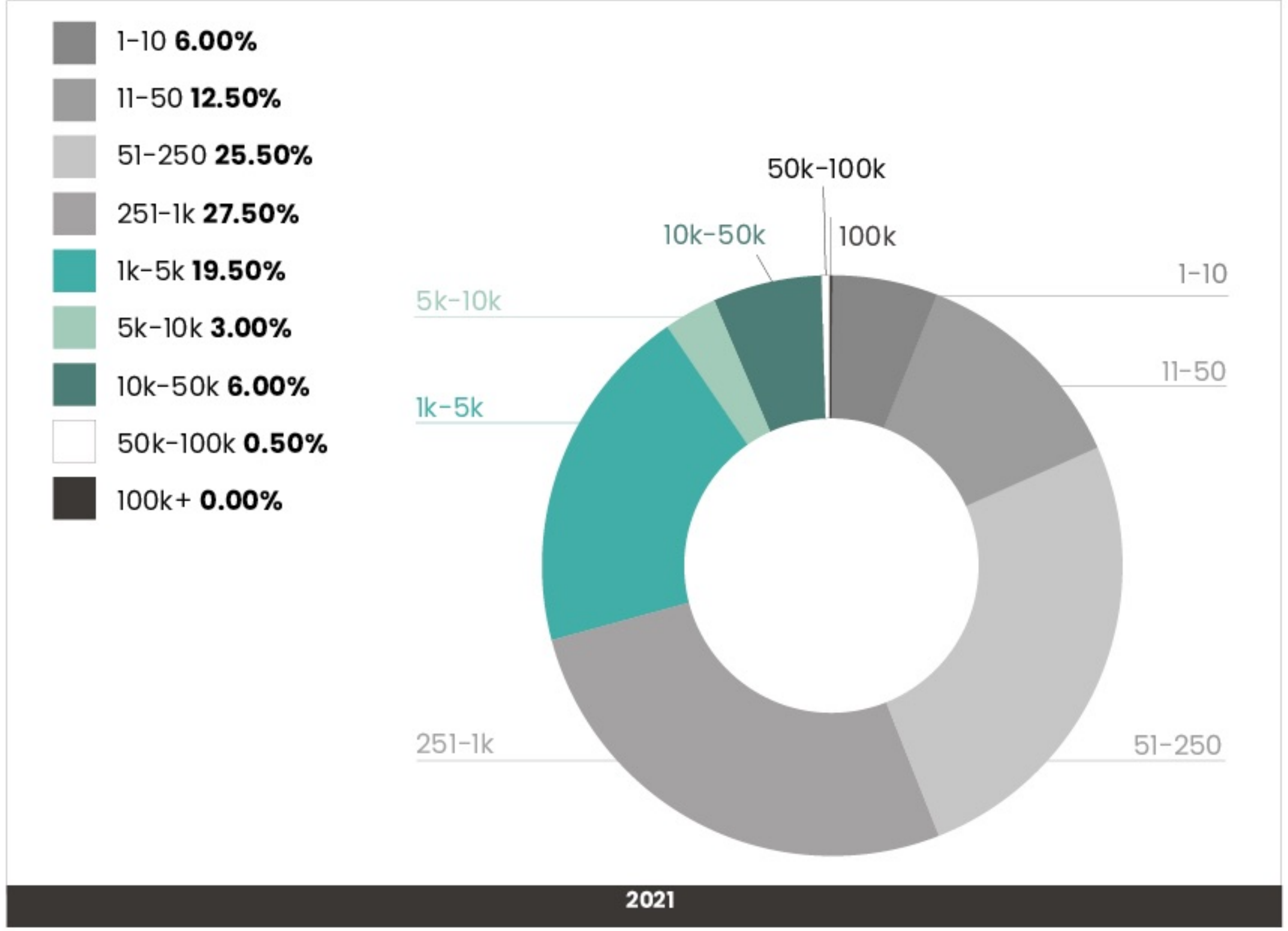
Asia view by range of employees

Attacks on **companies with 50k+ employees** increased **+4.5%** from 2021 to 2022, while companies with **less than 1k employees** decreased **- 3%**.

RANGE OF **EMPLOYEES**



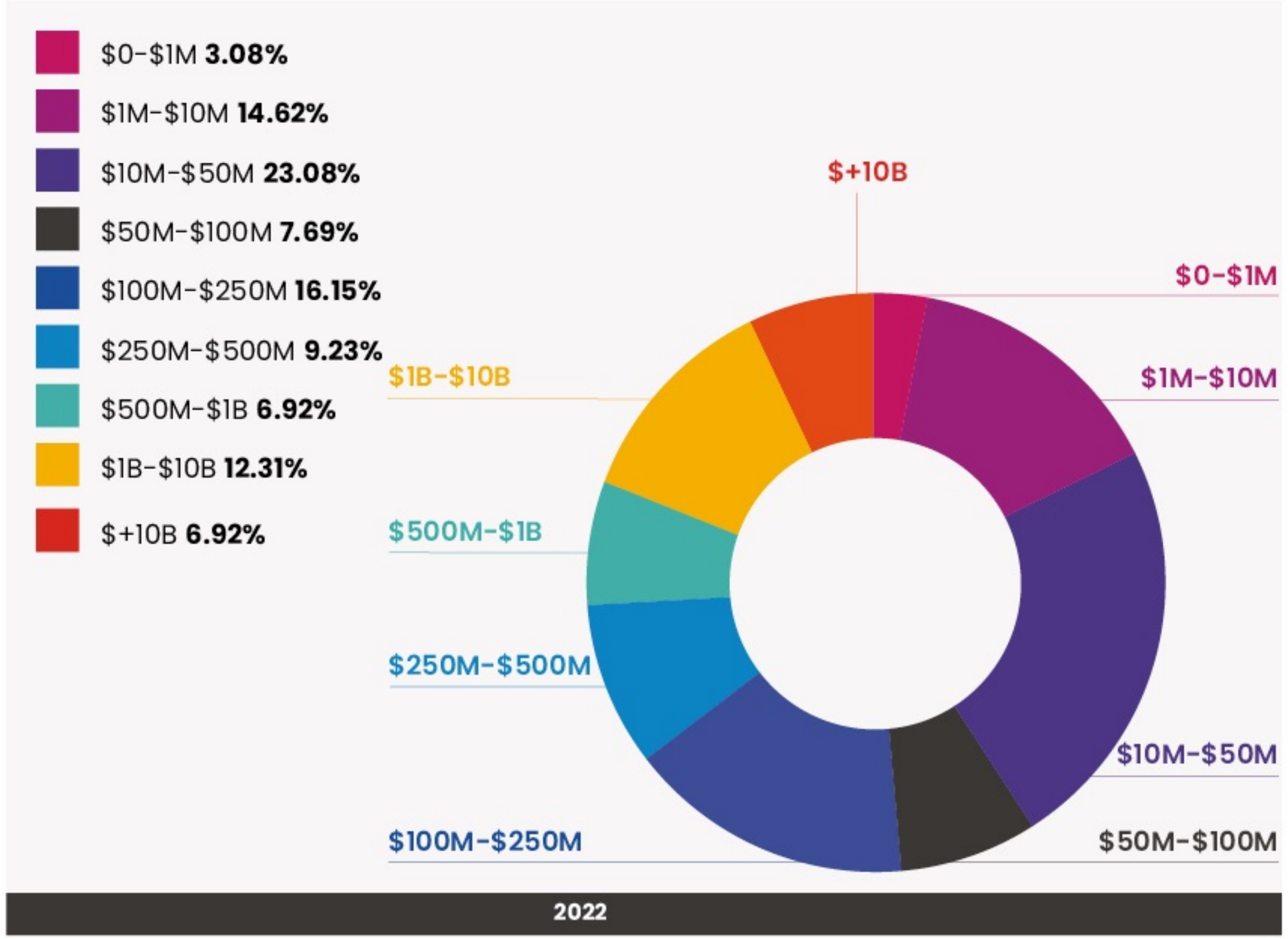
RANGE OF **EMPLOYEES**



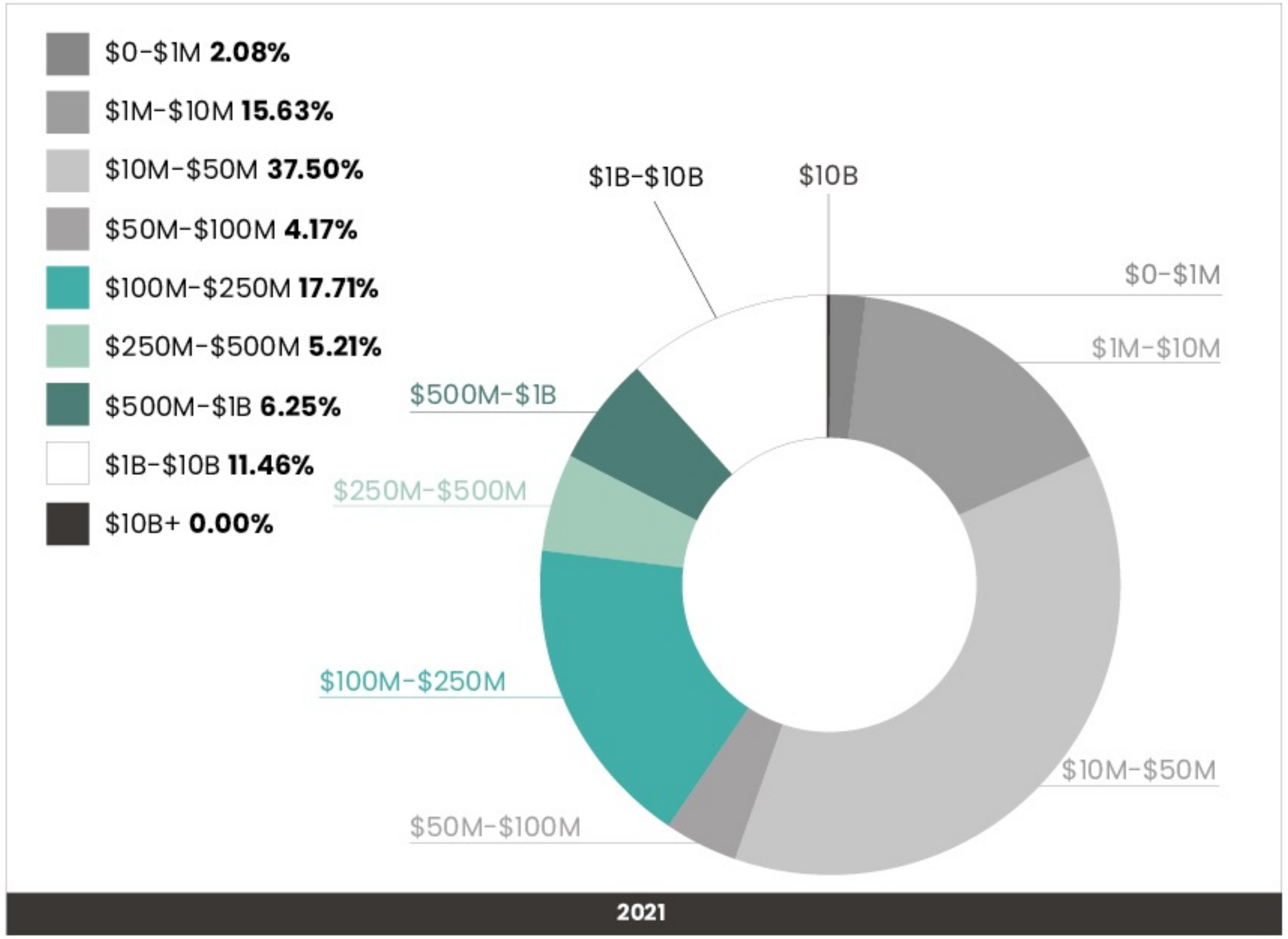
Asia view by revenues range

From 2021 to 2022 attacks **increased 7%** on businesses with **$10B+** in revenue.

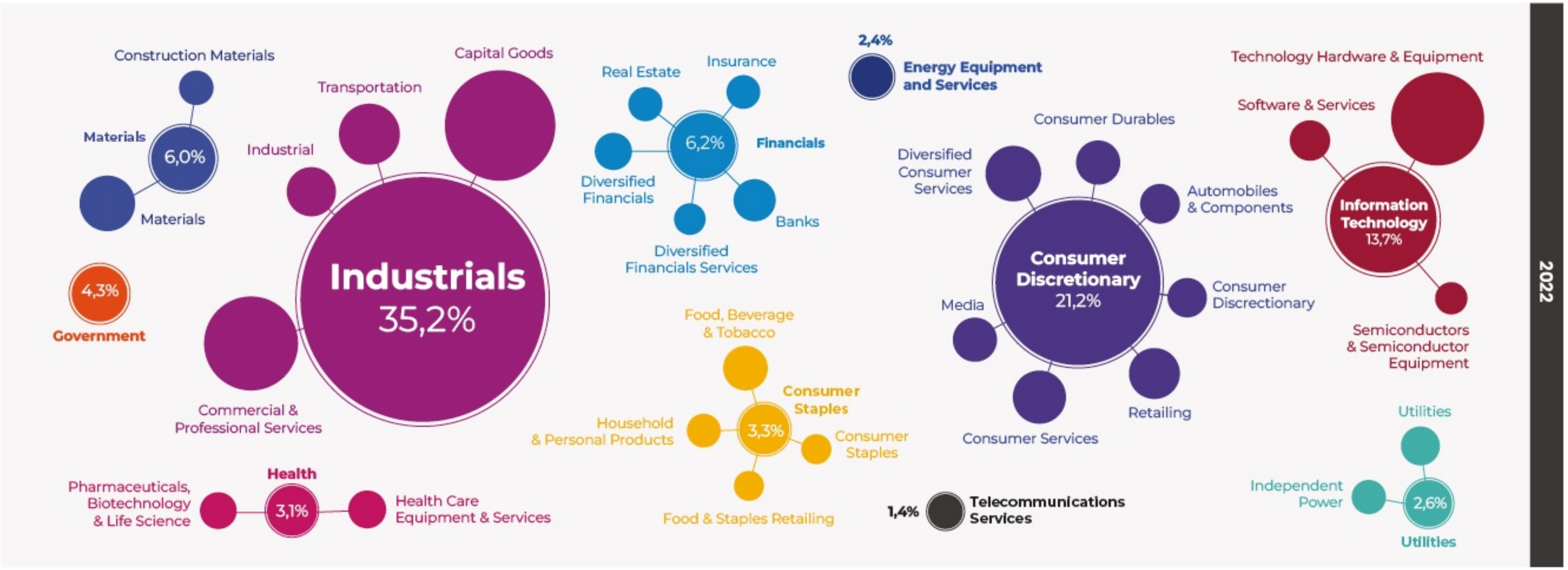
RANGE OF **ANNUAL REVENUE**

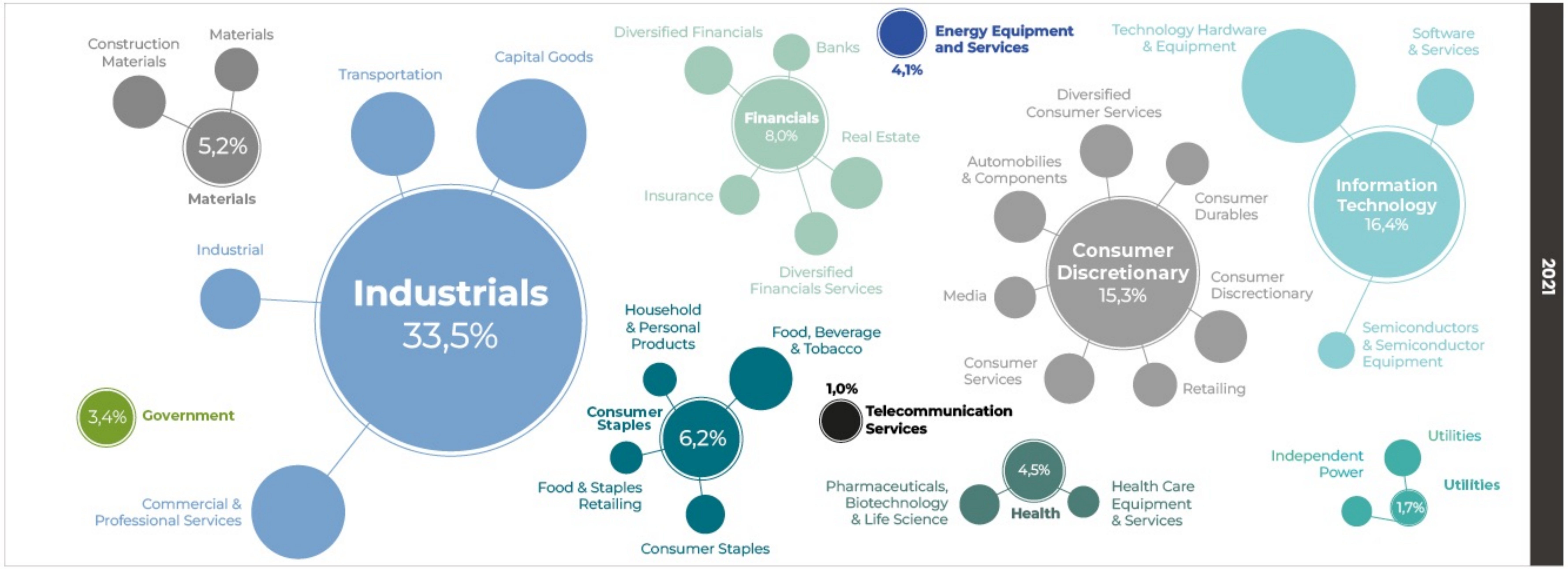


RANGE OF **ANNUAL REVENUE**



Asia view of the most **affected sectors**





Conclusion

CYBER RISK AND CYBER INSURANCE

Insurance companies are also facing challenges when it comes to assessing the cyber risks of their clients, and determining the potential impact of a ransomware attack.
Assessing this impact can be difficult, as it depends on factors such as the type of data encrypted, the systems affected and the organization's ability to recover from the attack.

Overall, **the impact of ransomware on the cyber insurance industry has been significant and continues to be a major concern**.

It is one of the **leading cause of cyber claims** and it's expected that this trend will continue in the future. As the threat landscape continues to evolve, it's crucial for insurance companies and organizations alike to stay informed about the latest trends and developments in the field of ransomware and take appropriate measures to protect themselves.

Ransomware attacks have become a major concern for organizations of all sizes, and they continue to increase in frequency and sophistication. These attacks have a significant impact on businesses, both financially and operationally.

The insurance industry plays an important role in helping organizations mitigate and respond to these risks, and insurance policies that cover cyber-attacks are becoming increasingly important.

However, the insurance industry must also take proactive steps to assess and mitigate cyber risk of their clients. This includes offering solutions such as threat intelligence, incident response planning, cyber security assessments and managed services to help organizations identify and mitigate potential vulnerabilities.

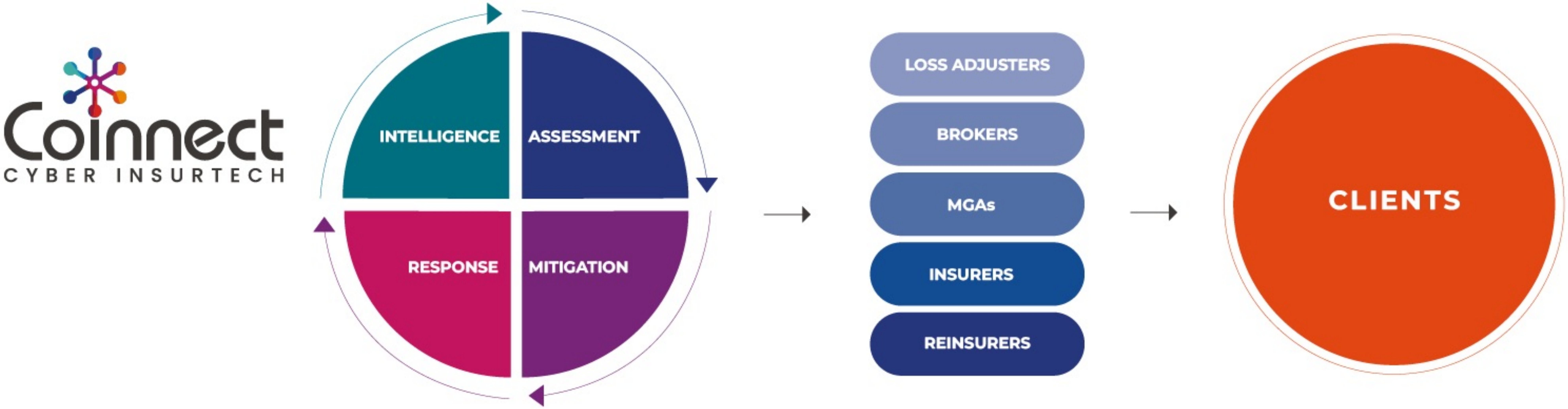
By bundling these **solutions with insurance policies**, the insurance industry can provide a comprehensive approach to cyber risk management, helping to protect organizations from the potentially devastating consequences of a ransomware attack.

It is crucial for the insurance industry to keep pace with the evolving threat landscape in order to provide effective and comprehensive coverage for their clients.

About **Coinnect**

We are a **Cyber Insurtech Company** providing innovative solutions for **Cyber Risk Assessment**, **Mitigation and Response**

100% built for Insurers and to make **Cyber Insurance** a more profitable business



CLOUD PLATFORMS • APIS • TECHNICAL SERVICES

Coinnect Platform

Our **Cyber Insurtech Platform** provides unique capabilities

INTELLIGENCE

- Dark Web **Ransomware Data**
- Open and Closed Sources
- **Data** Breaches
- Exfiltrated **Credentials**
- **Infected Endpoints**
- **Exposed Assets**
- **Vulnerabilities**
- Lookalike **Domains**

ASSESSMENT

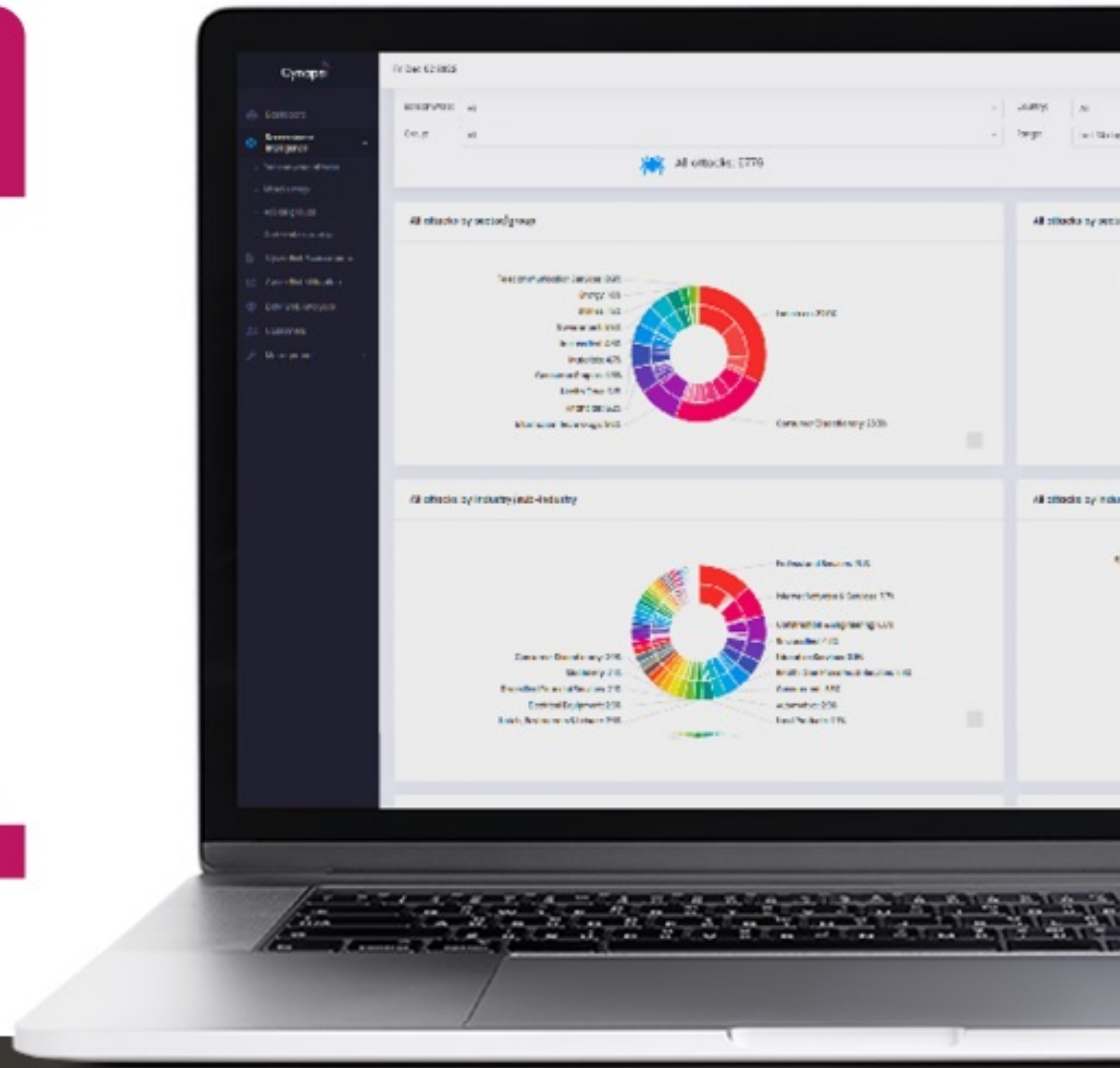
- **Proprietary** Methodology and Algorithms
- Based on **technical evidences**
- **Ransomware Risk** evaluation using exclusive DB
- Risk Indexes and Data in **near real-time**

MITIGATION

- Built to be bundled with **Insurance Policies**
- Proactive risk monitoring and mitigation
- **Easy activation** for clients
- Engineered for SMBs and SMEs

RESPONSE

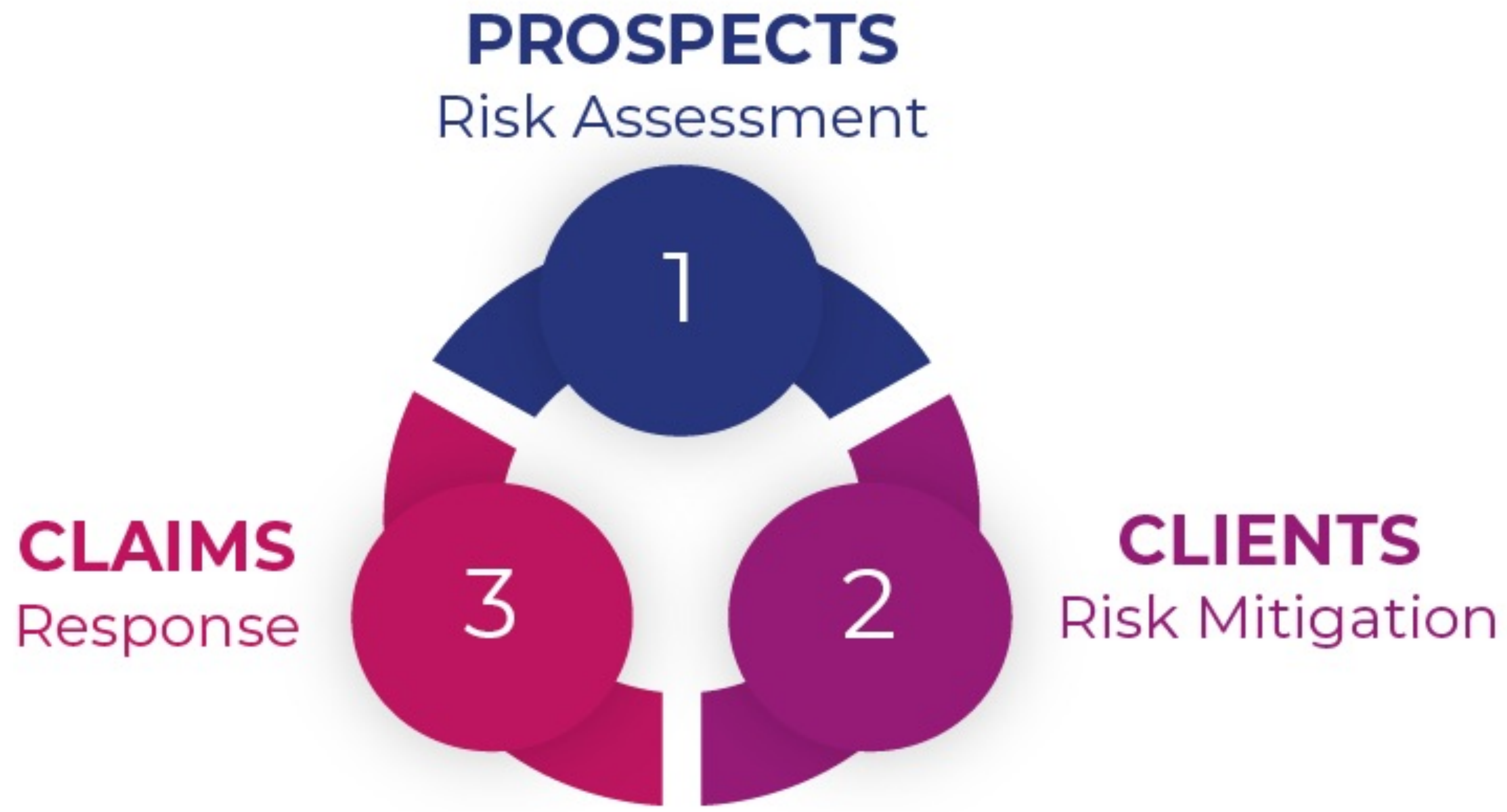
- **Incident Response** for Cyber Claims
- **24x7** Fast response using custom and best of breed integrated tools
- XDR, Compromise Assessment, Data Recovery, Ransomware Support, Forensic



WEB ACCESS AND / OR APIs + SUPPORT AND SERVICES

Why **Coinnect**

Built to support main stages of **Cyber Insurance life cycle**



- Tailored for the specific needs of the SMBs and SMEs insured clients
- Crafted by Cyber Security experts with hands-on experience
- Proprietary Ransomware Data and Intelligence Platform
- Cooperation with Insurance Partners is our sole business model

Coinnect

CYBER INSURTECH

☎ +41 782574125

✉ info@coinnect.io

www.coinnect.io

Via Penate 16
6850 Mendrisio,
Switzerland