# Wavestone Cyber Benchmark

***2025 Edition***

## What is the market maturity?

June 2025

WAVESTONE

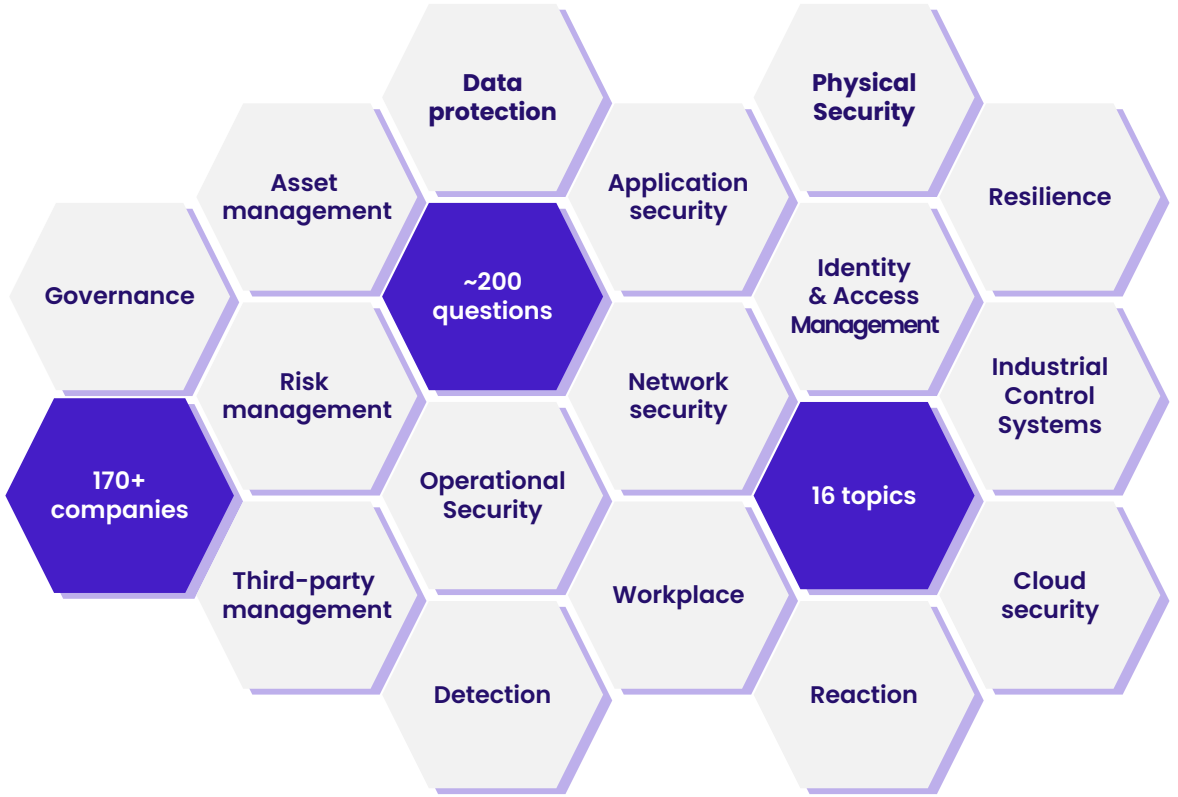
# **Wavestone Cyber Benchmark**: an in-depth analysis of the level of cybersecurity maturity

Based on NIST Cybersecurity framework and ISO 27001/2, the **W-CyberBenchmark,** our **360 assessment approach, goes further** and provides:

A comprehensive approach with an **organizational** and a **technology** maturity **assessment**

An assessment that takes into account the **complexity of organizations** that have different entities with different maturity levels

A benchmark vision: **170+ Wavestone customers** have already completed the assessment over the past years, presenting more than 7 millions employees



# How mature are large organizations?

**Large organizations***

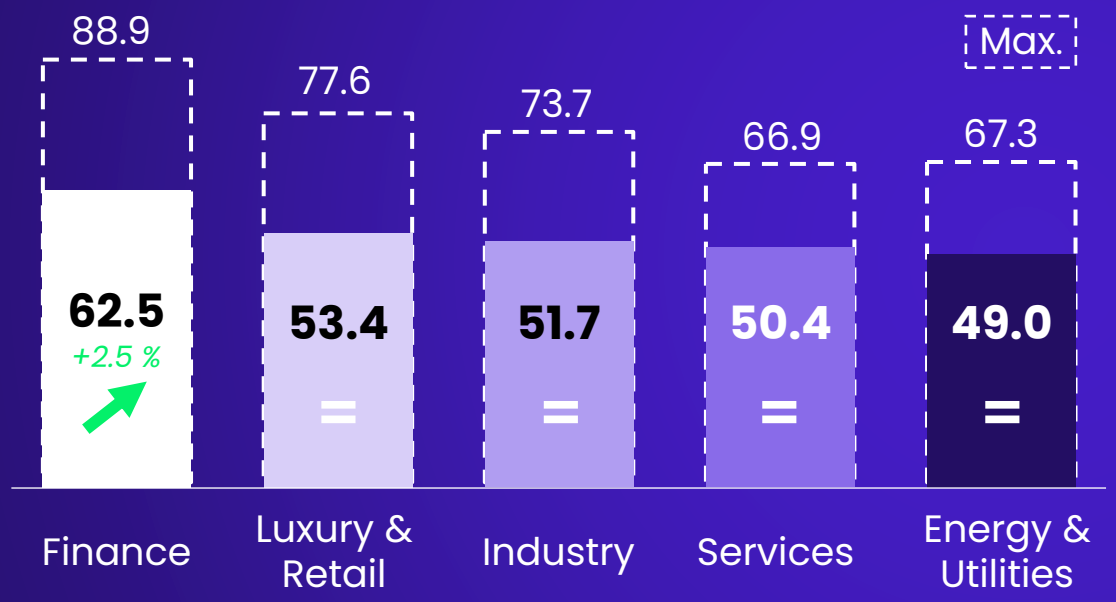
**54**

**/100**

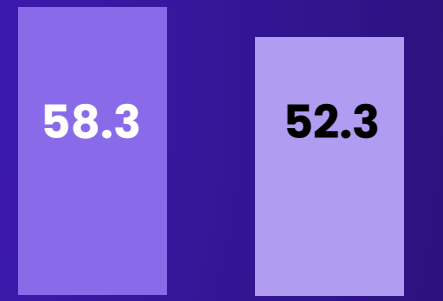
Overall maturity for large organizations is still increasing **(+1 point since 2024),** but the pace is slowing down

*Companies with a turnover over $1B (100+ org.)

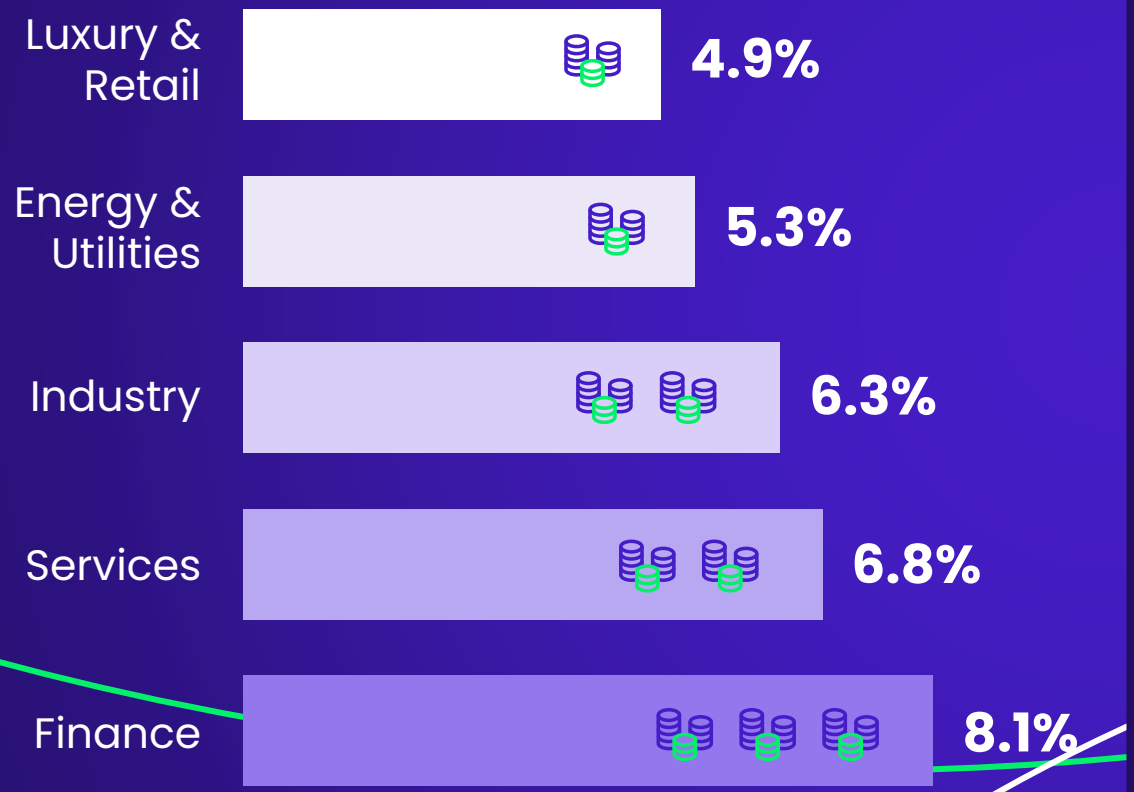
## **Financial sector** is **well ahead** in overall maturity




## **Regulations** have a **major impact** on maturity



# Cybersecurity spending remains mostly stable in large organizations




## Average IT budget percentage dedicated to cybersecurity*

**6.4%**

*2024 : 6,6%*

**Range**

| First quartile | Last quartile |
|---|---|
| **3.0%** | **8.1%** |

**Taking into account that budget percentages can vary a lot depending on previous investments and current build VS run balance*

**Companies with a turnover over $1B (100+ org.)*

# Cyber teams are still growing

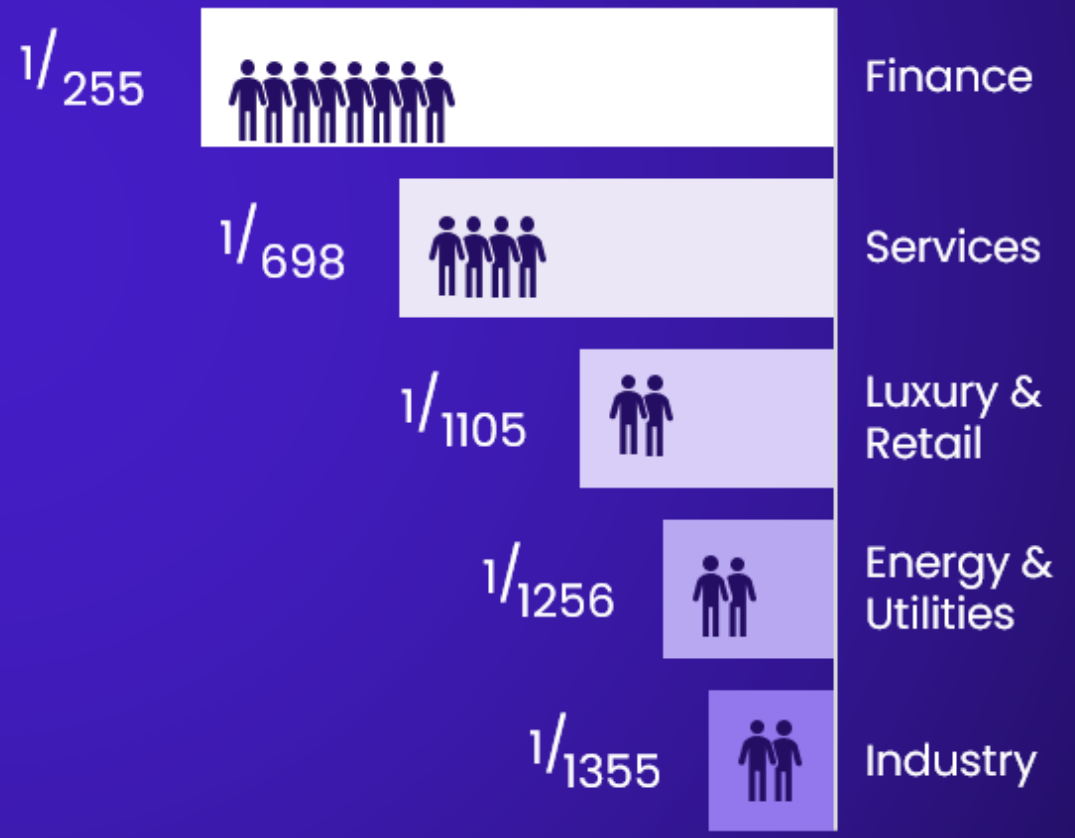
**Average FTE**
**dedicated to cybersecurity**
per employee in large organizations*

**1/1016**

*+7% vs 2024*

*2024 : 1/1086*

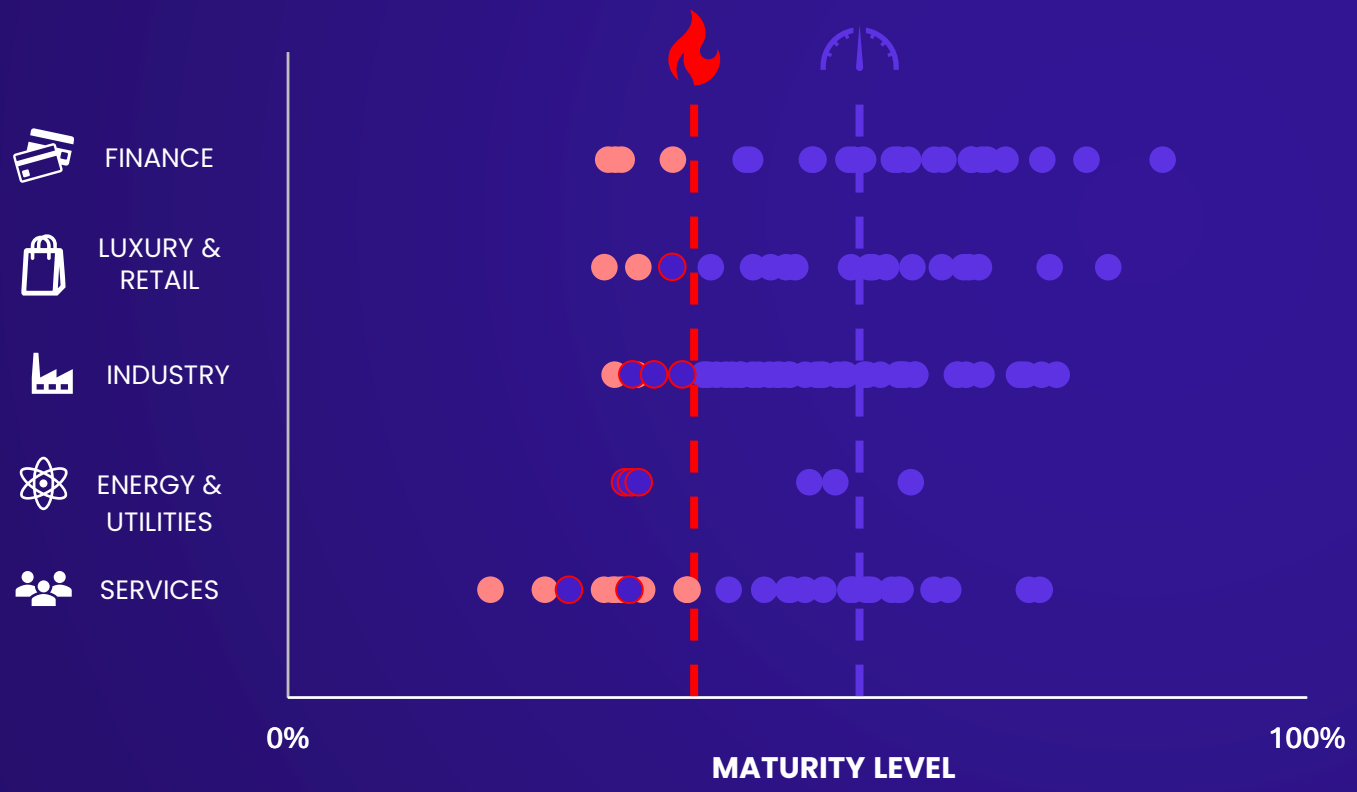
## Sector differences remain significant




*Companies with a turnover over $1B (100+ org.)

# How does the market stand against the latest cyberattacks?

Based on the latest **cyberattacks managed by CERT-Wavestone**, we have selected 29 anti-ransomware measures and assessed our customers' maturity on (attack entry point protection, crisis management, backups, red button…)




**56%**

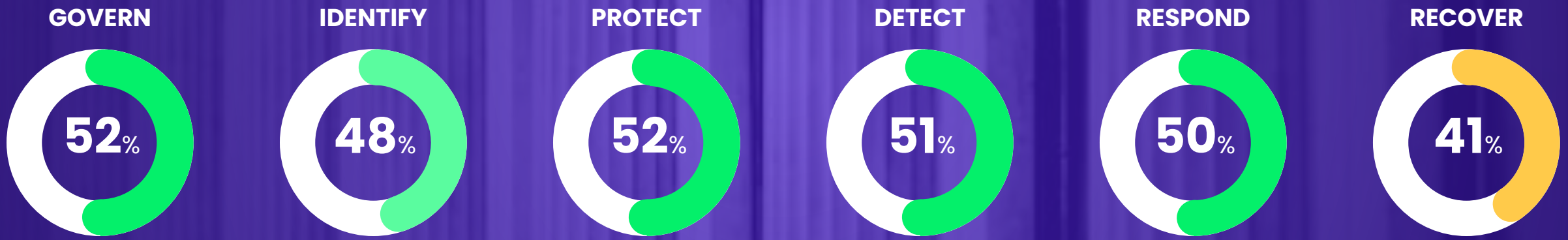
ANTI-RANSOMWARE MATURITY OF **LARGE ORGANIZATIONS*** AND ONLY A FEW IN CRITICAL SITUATION (DARK RED)

**36%** (-18%)

OF **MEDIUM AND SMALL ORGANIZATIONS** CONSIDERED TO BE IN A **CRITICAL SITUATION**

**Companies with a turnover over $1B (100+ org.)*

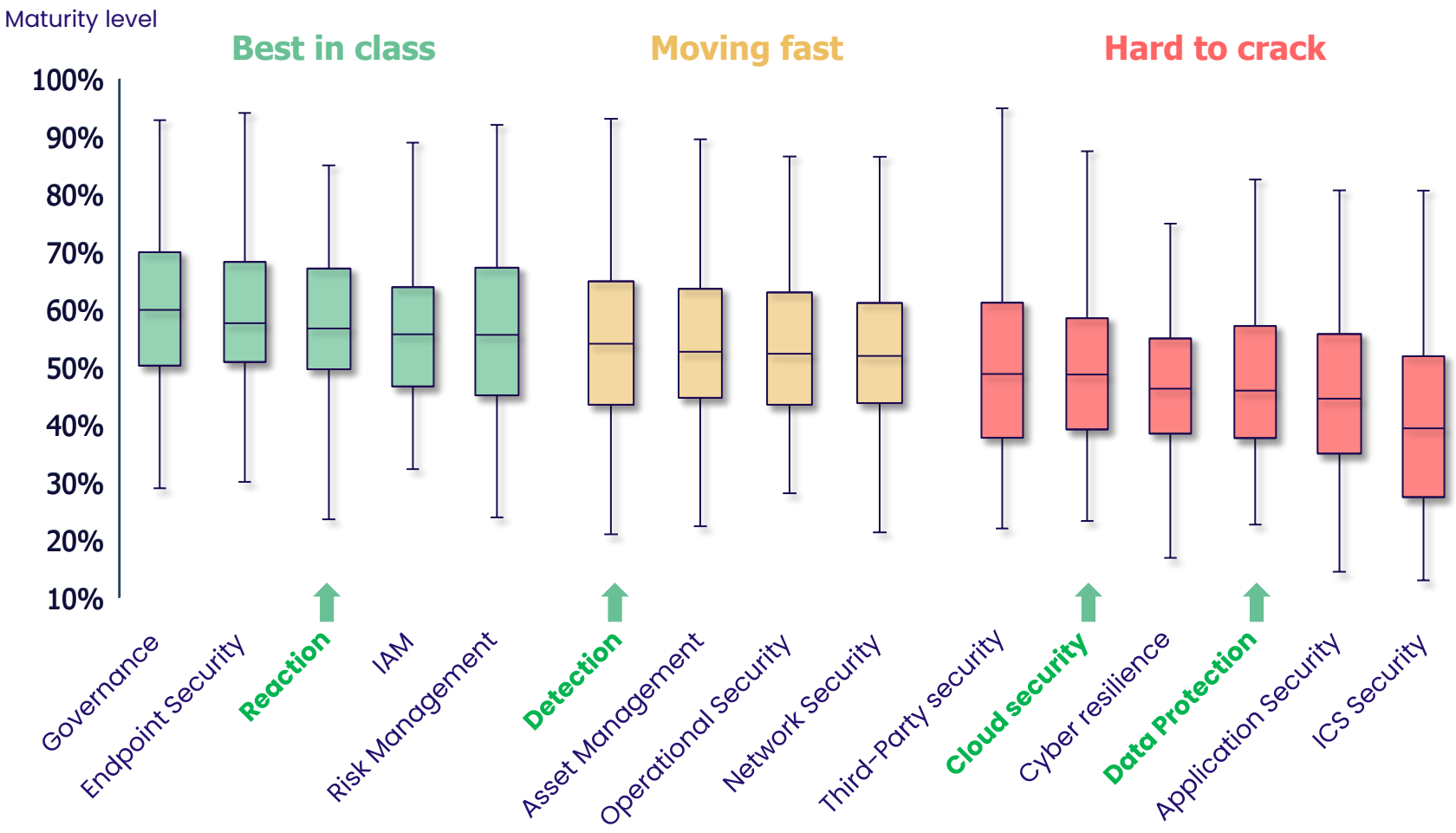
# What is the market **MATURITY** in adopting the new **NIST Cybersecurity** Framework?




The **high consistency** across the **NIST CSF 2.0 pillars** highlights the **significant cybersecurity investments** made in recent years. The only exception is the "**Recover**" pillar, which lags behind in **crisis management** and **resilience capabilities**—though the **financial sector stands out** with a higher maturity level (52%)

# Global overview on cyber topics

Large organizations' performance on key cyber topics in our 2025 CyberBenchmark




**Legend**

↑ Topic that advanced in importance from last year

**Box plot view of maturity score for every topic:** Minimum / 1st quartile / Median / 3rd quartile / Maximum

**Reaction**
Incident response capabilities have shown measurable improvement **(+3%)** primarily driven by enhanced coordination between business units and strengthened crisis preparedness measures.

**Detection**
Detection capabilities continue to improve **(+4%)** demonstrating increased efficiency particularly within large organizations. Significant progress has been observed in monitoring critical environments (e.g., Active Directory) and log coverage has expanded although business log analysis remains a complex challenge.

**Cloud**
Cloud security has improved **(+3%)** supported by more secure deployment practices particularly through CI/CD pipelines and reinforced control over administrator privileges via automated review mechanisms.

**Data protection**
Data protection has also advanced **(+4%)** over the past year. Organizations are actively monitoring for potential data leaks on the internet and are enhancing personal data safeguards to align with international regulatory frameworks such as GDPR resulting in improved coverage and compliance.

# *What* **TO EXPECT** in the years to come?

Current maturity:


5 key topics from 2025

*With a specific sample of 20 organizations

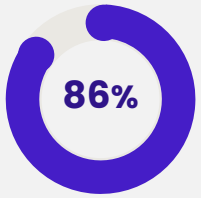
# Detection: a constantly evolving challenge


Maturity of **detection** capabilities by **large organizations** rose significantly (**+4%** compared to **2024**)*

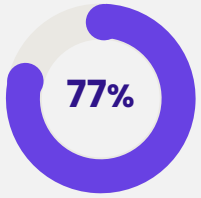
Percentage of large organizations that have implemented each specific practice:

## A Solid Foundation


Configure rules to **trigger alerts** in case of **abnormal activity**

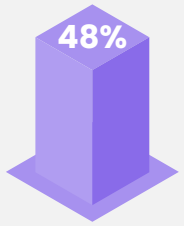



**Collect** and **analyze infrastructure** logs




**Regularly** analyze the configuration of **Active Directory** (AD)

## Ongoing Challenges




**Collect** and **analyze business** application logs


Create **custom detection** scenarios to identify advanced threats

**... taking into account the arrival of AI solutions**

**Companies with a turnover over $1B (100+ org.)*

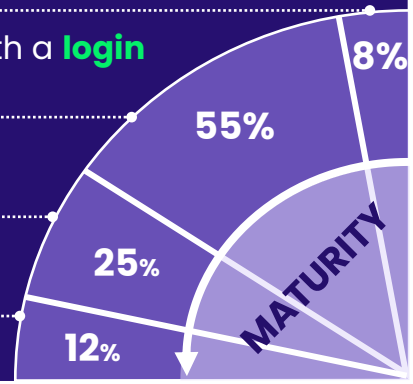
# Cloud security: steady increase

**51%**

**Cloud security** continues to make progress in **2025**, reaching a maturity of **51%** among large organizations (**+3%** compared to **2024**)*

## Cloud administration

- Cloud console accessible **from anywhere** with a **login and password**
- **Multi-factor authentication** (MFA) for administration accounts
- Administrators must connect through a **bastion**
- **No admin** or **Just-in-Time** admin




## Roles & responsibilities

**70%** of large organizations have a Cloud security manager

**37%** of large organizations have clearly defined roles & responsibilities with Cloud Providers

## Opportunities and challenges

**CSPM** (Cloud Security Posture Management) solutions and the challenge of **scaling up and putting the responsibility outside cyber teams**

**CNAPP** (Cloud-Native Application Protection Platform) solutions and the challenge of **converging existing security tools**

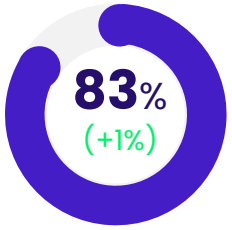
**Cloud Erasure resilience scenario** and the challenge of **rebuilding a Cloud IS** from scratch

**Companies with a turnover over $1B (100+ org.)*

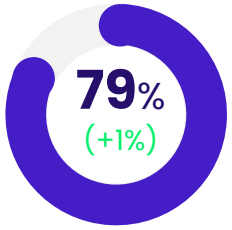
# Cyber Resilience: a strategic ambition still hard to achieve


Cyber resilience remains a **complex subject** (**+1.5%** compared to 2024, except in **Finance +3.5%** based on the same sample than last year)*, as **few organizations** are truly prepared to maintain their business in the event of a **major attack**

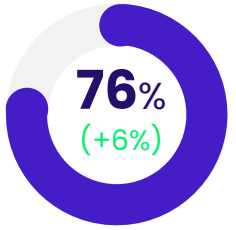
Percentage of large organizations that have implemented each specific practice:




are covered by a **cyber insurance policy**

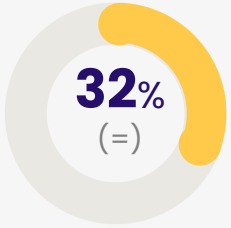



**conduct crisis management exercises** at least every two years

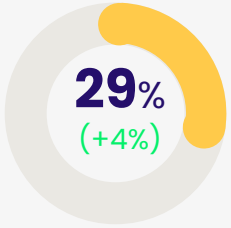



regularly conduct **restoration tests** in accordance with their backup policy

## Despite the progress, certain areas still need strengthening




deploy **degraded mode processes** tailored to users and critical functions



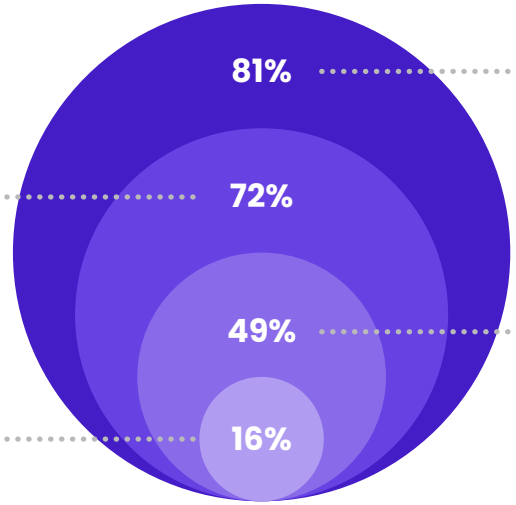

assess **dependencies across each business chain** at a global level

**Companies with a turnover over $1B (100+ org.)*

# Data Protection: stronger controls, safer futures

**48%** Data protection has become a **strategic priority** for organizations (**+4%** compared to 2024)* which reflects **growing awareness of information security risks** and **artificial intelligence needs**

Percentage of large organizations that have implemented each specific practice:




**Automatically monitor** known **attacker sites** to check for **data leaks**

**Encrypt specific personal data** in addition to transport-level encryption

Deploy data **discovery tools** or enforce **automatic classification** upon **document creation**

**Classify all unstructured sensitive data**

Main challenges to be overcome with the arrivals of AI solutions?


**Deployment of mechanisms to detect non-compliance**


**Implementation of a DLP solution with advanced, customized static rules**


**Deployment of a dedicated team for information security data sanitization**

*Companies with a turnover over $1B (100+ org.)*

# Securing a critical asset: artificial intelligence

Based on 20 large organizations, here is a **deep-dive on how organizations are acting to secure AI use cases**

## AI governance and risk identification is already a thing …

64%

Have an **AI security policy**

67%

Give clear **go/no go decision at AI project risk** review

60%

Identified a team to assess **AI projects compliance**

40%

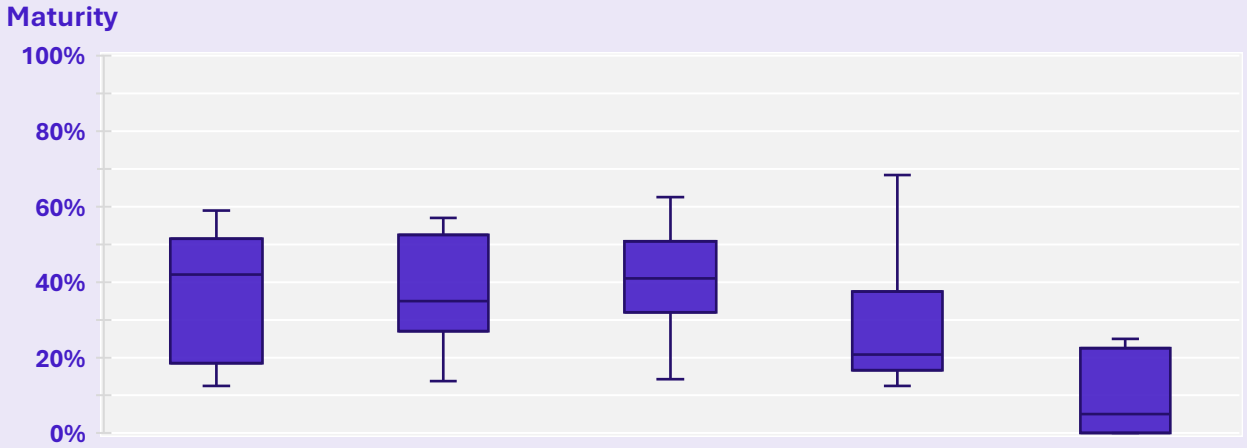
40% of clients **adapted their Third-Party assessment** methodology for AI vendors

7%

Have established measures and adapted **tooling to detect and defend** against **malicious prompts** and other **identified threats**

## …but the journey has just started for complete maturity

| GOVERN | IDENTIFY | PROTECT | DETECT | RESPOND |
|---|---|---|---|---|
| 39% | 39% | 40% | 29% | 9% |




There is no '**Recover**' pillar, as there is no **dedicated recovery specialization for AI.**

# NIS 2: How mature is the market with French security requirements ?

Large organizations*
**80.3%**

**Large organizations** achieve **80% maturity** in relation to the **NIS 2 French draft framework**

## Everyone will have to work, even those who were the most mature

**0**

**Organization 100% compliant with NIS 2** French draft requirements

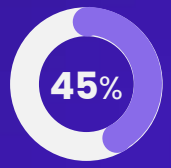
A large majority of clients must make **significant efforts**, mainly **due to the scope expansion**

## Building on NIS 2: Key Priorities for Organizations

- Enhance **Third Party Risk Management**
- Ensure **Resilience**
- Strengthen **Asset management**
- Meet **Administration requirements**

## Main hard-to-crack topics

**Systems secure maintenance**




maintain a **centralized CMDB**

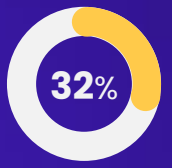
**Third-party management**


regularly **audit their critical suppliers**

**Administrative IT systems**


set up **dedicated admin workstations**

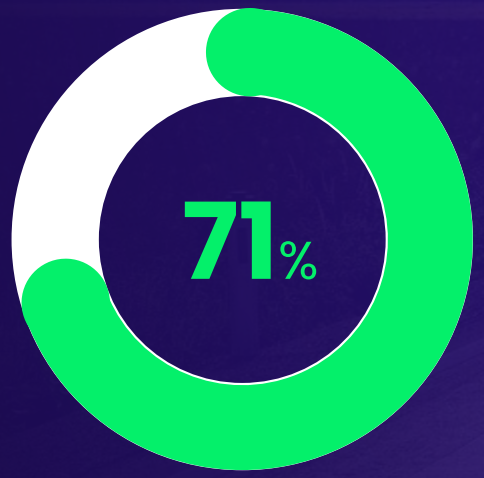
**Crisis management and BCP/DRP**




test **major scenarios on the most critical functions**

# *The need to address* **emerging** *and* ***innovative*** *topics*

Many companies are **starting to reach a high level** of maturity against the international standards




Average maturity score of TOP 10 companies in our cyber benchmark

## A need to cover the new and innovative topics

- Quantum Cryptographic
- *AI security*
- Just-in-time / Just enough
- API based
- Quantification
- Security Data Hub
- Culture change
- Digital twin
- *AI for cyber*
- Plateformization

## Introduction of a new maturity level for pioneers

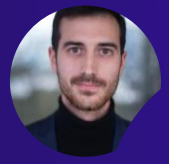
**Levels 1 to 4**
(NIST based)


**Level 5**
Pioneer level

# Wavestone Cyber Benchmark

## *2025 Edition*


**Gérôme BILLOIS, Partner**
gerome.billois@wavestone.com



**Enzo ALLAIN, Senior Consultant**
enzo.allain@wavestone.com

**Théo SEROLE, Consultant**
theo.serole@wavestone.com


WAVESTONE