TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

TeleTrusT-Konferenz 2025

Berlin, 02.07.2025

Angriff ist die beste Verteidigung in der Cloud

Nils Karn, Mitigant

Cloud Attacks Are Increasing Rapidly

- **80% of companies** have encountered an increase in the frequency of cloud attacks.
- **99% of the cloud incidents** through 2025 happen due to cloud misconfigurations by the cloud customers
- Cloud ransomware attacks **increase by 13%** in the past 5 years
- Average total cost of a cloud data breach is **USD 4.35 million**

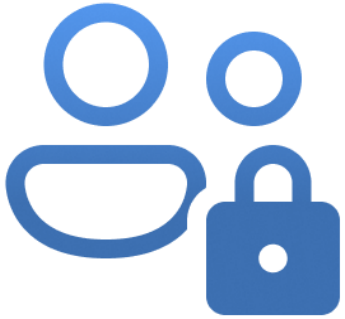
https://www.scworld.com/brief/massive-aws-access-key-database-leveraged-in-ransomware-campaign
https://www.sentinelone.com/cybersecurity-101/cloud-security/cloud-security-statistics/
https://www.gartner.com/smarterwithgartner/is-the-cloud-secure
IBM Cost of Data Breach Report 2025

How Would You Know If …

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Cloud Incident Response Playbooks

Cloud Security Mechanisms



Security Team

Security Tools

Will Work Effectively to Protect Your Cloud & AI From Cyber Threats?

Cyber Resilience Is The New Norm In The Cloud

The ability to **prevent, withstand, and recover** from cyber incidents while the system continues delivering the expected outcomes

Cyberattacks can lead to **service downtime, lost revenue, reputational harm, penalties**, high recovery cost, and more

Organizations need to ensure that the services and resources hosted in the cloud will be available with **minimum disruptions to continue normal operations**

Why Cyber Resilience Is Important for Cloud Security

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

1 Cyber resilience can be used to measure the organization's **cybersecurity maturity and business resilience level**

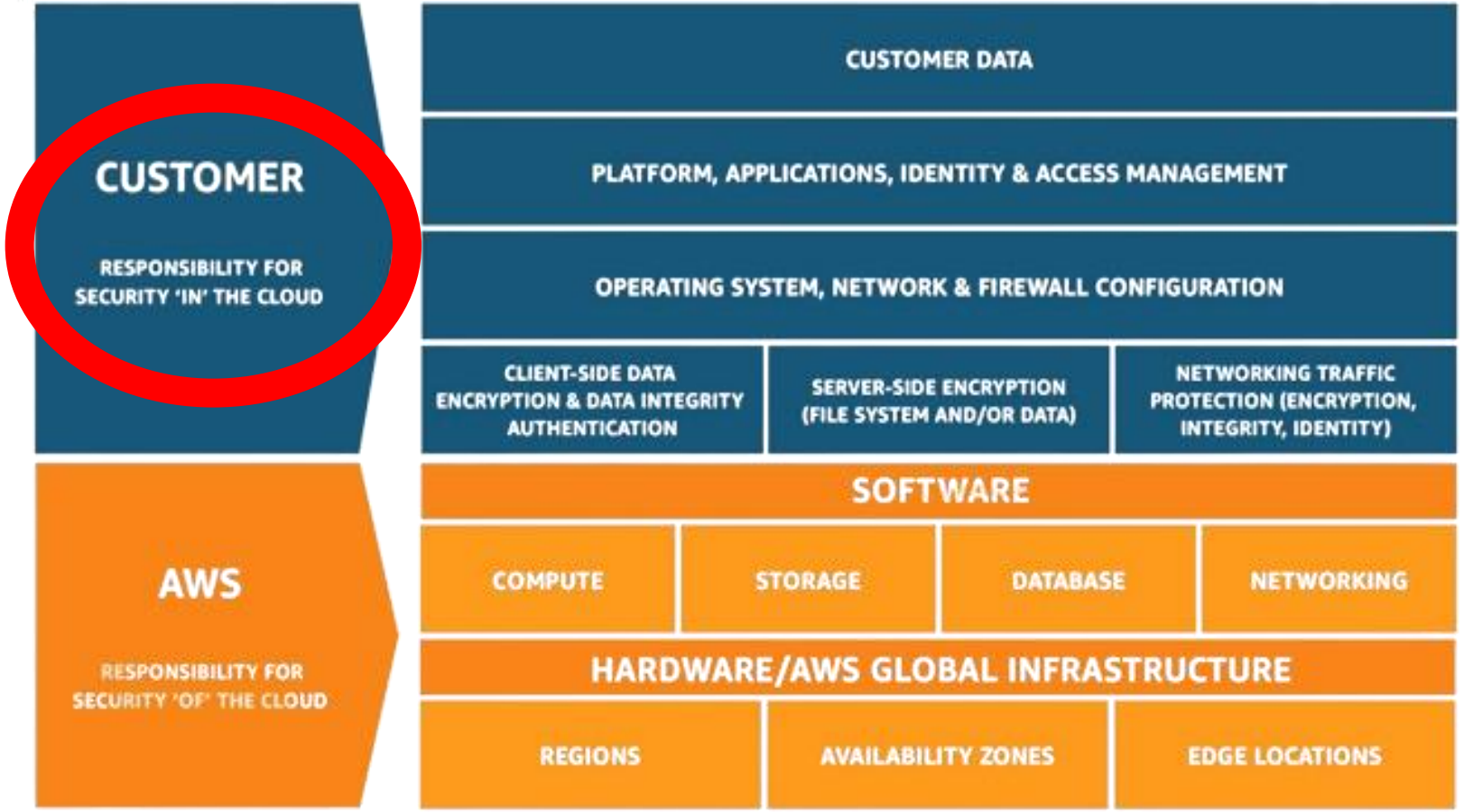
2 Many organizations focus on cloud attack preventions, but **few tries to be better prepared for potential cyber threats** targeting the cloud

3 Without comprehensive cyber resilience strategy, organizations will be **unable to effectively detect, respond, and recover to cloud attacks,** thus potentially making worse impacts to the organizations and their clouds (e.g., longer recovery time, bigger recovery costs, etc)

4 Several **challenges of cyber resilience adoption** within organizations:

- Limited resources (manpowers, budgets, knowledge)
- Lack of awareness of cloud security responsibilities

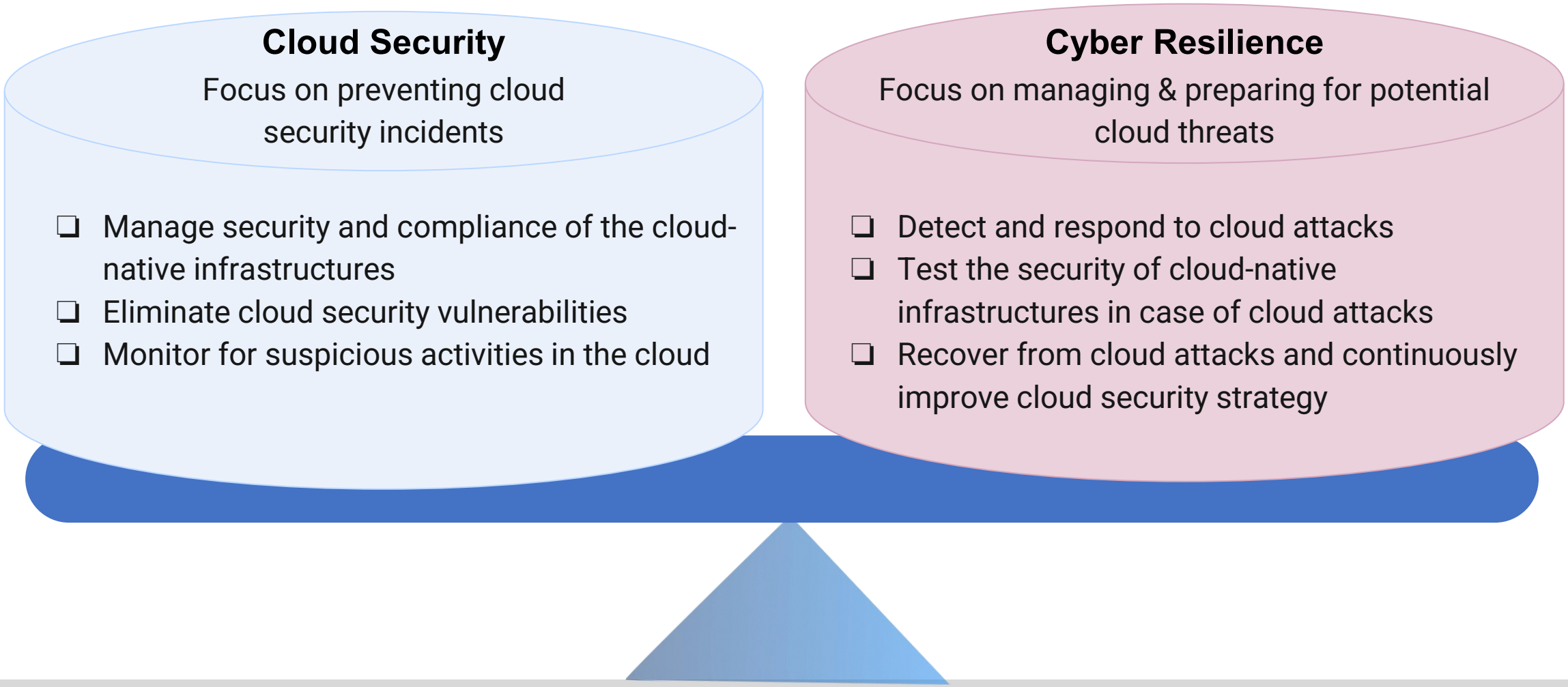
Who Is Responsible When Cloud Attack Happens?



https://aws.amazon.com/compliance/shared-responsibility-model/

The Importance of Cloud Security & Cyber Resilience Balance

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.



Push For Cyber Resilience (In Cloud)

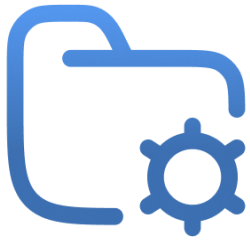
- To ensure organizations are resilient against emerging cyber threats rapidly increasing and evolving over the years, cyber resilience are being pushed through **regulations and best practices**, such as:
  - EU Network and Information Security (NIS2) Directive
  - EU Digital Operational Resilience Act (DORA)
  - MITRE ATT&CK framework
- Cyber resilience strategy needs to be implemented additional to the existing cloud security strategy ensuring **complete protection against cyber threats**

Cyber Resilience’s Aspects Cloud Infrastructure Should Have

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Cloud Backup

Cloud Security Incident Playbooks



Attack Surface Management

Threat Detection and Response

Forensic and Recovery

Attacking Your Cloud To Improve Cyber Resilience Posture

1

Understand Your Cloud Security Posture

- ❑ Identify important assets and stakeholders within your clouds (cloud resources, running services, etc)
- ❑ Execute threat assessments to identify potential risks, threat actors, and attack surfaces
- ❑ Run cloud security assessments to identify security vulnerabilities within your clouds (misconfigurations, compliance violations)

2

Implement Strategies for Cloud Security & Cyber Resilience

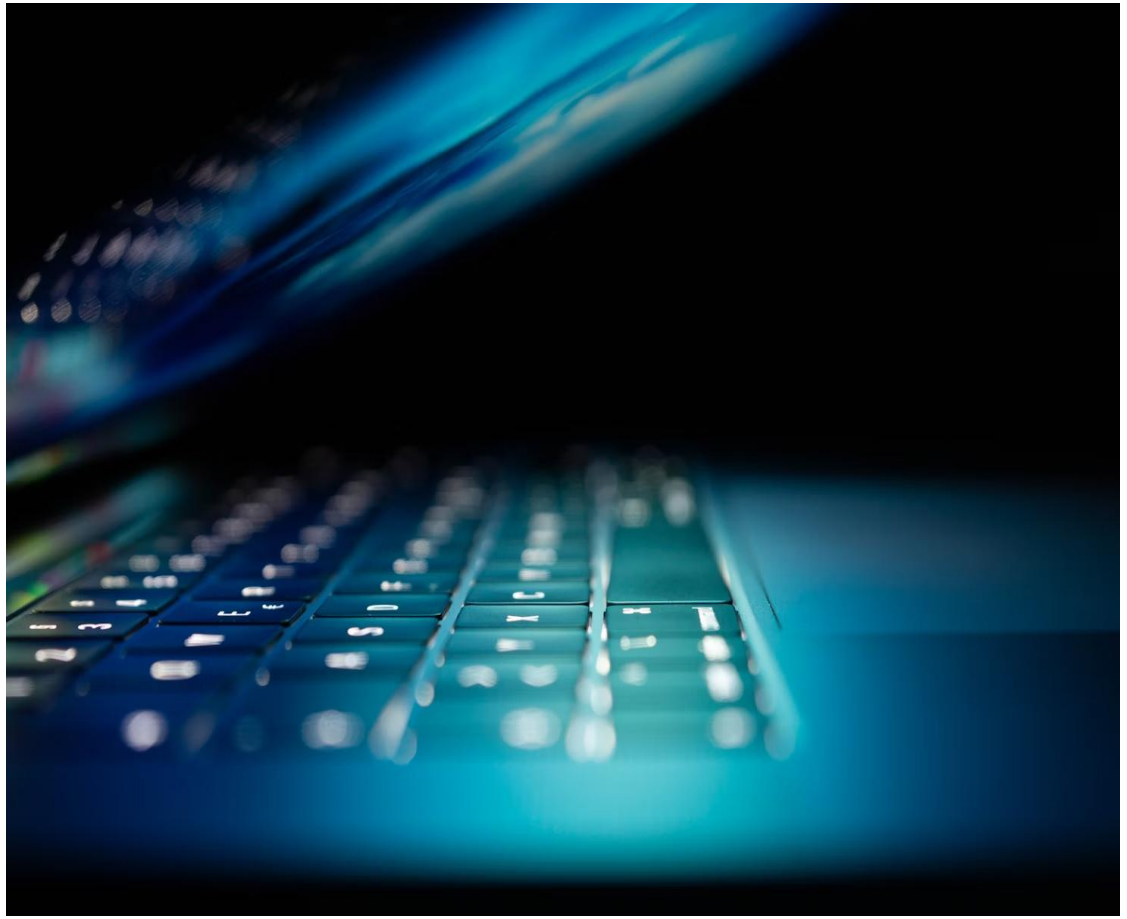
- ❏ Secure cloud infrastructures based on the latest cloud security posture and threat assessments
- ❏ Create strategies to securely manage the cloud based on the organization's requirements and to respond to potential cloud threats
- ❏ Monitor the implementation of cloud security and cyber resilience strategies

Attacking Your Cloud To Improve Cyber Resilience Posture

3

Validate Cloud Security & Cyber Resilience Strategies

- ❏ Execute cloud penetration test to identify potential threat vectors, attack paths, and vulnerable entry points
- ❏ Run security gamedays to ensure the cloud, the security team, and implemented strategies work effectively when the potential cloud threats happen
- ❏ Continuously improve the implemented strategies by detecting and remediating security blind spots and gaps based on the test results



Benefits of “Attacking” Your Cloud

Measure the readiness of the organizations for potential threats targeting the cloud (i.e., security teams, tools, and strategies)

Verify the effectiveness of cloud security and cyber resilience strategies (e.g, incident playbooks, backups)

Discover security blindspots and gaps within the cloud security strategy implementations

Improve your cloud security & cyber resilience posture and better prepared for potential threats

Danke für Ihre Aufmerksamkeit

Nils Karn

Chief Executive Officer

nils@mitigant.io

(+49) 331 971 83 007