



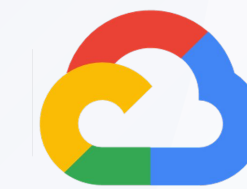
Be Secure. Be Resilient.

Mitigant - Mehr Übersicht und Resilienz in der Sicherheit für öffentliche Cloud-Infrastrukturen



Referent: Nils Karn

Shared Responsibility Model of Public Clouds



Google Cloud

99% of successful cloud attack
possible due to **human errors and
misconfigured cloud resources by 2025.**¹

The Challenge



Complex and Expensive

Managing cloud infrastructure security is complex.
Security experts are hard to find and expensive.



Lack of Visibility

It takes approx. 280 days for companies to detect & respond to data breaches.²



Absence of Resilience

Most cloud security solutions do not enable resiliency against cloud attacks.

2. <https://www.ibm.com/security/digital-assets/cost-data-breach-report/>

The Challenge

TECHNOLOGY > CYBERSECURITY | June 1, 2022 | updated 17 Aug 2022 9:21am

Pegasus Airline breach sees 6.5TB of data left in unsecured AWS bucket

An unsecured cloud data store has left vital information from the airline's software exposed online.



Continuous Security Verification



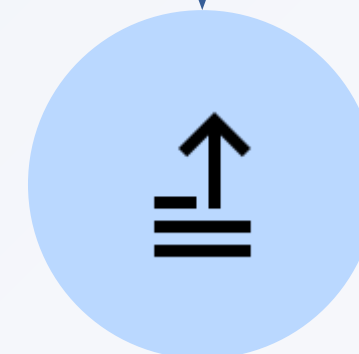
Detect

Discover Security
Issues With **One Click.**



Scan Resources

Scan all available cloud resources and their configurations across all regions



Leverage Rules

Leverages Mitigant's dynamic rules engine to detect security issues in the cloud infrastructure



Detect Changes

The Drift Analysis discovers any changes happening on the cloud infrastructure



Continuously Resolving Security Issues.



Check Compliance

Compliance checks are based on cloud security standards & best practices (e.g. CIS, NIST, PCI-DSS, BSI C5, HIPAA,...)



Solving Security Issues

Detected security problems are solved by guided steps or using command-line interface (CLI).

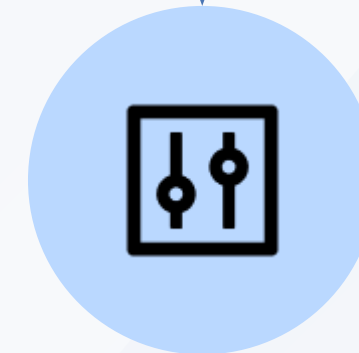


Reconcile Drifts

Once click reconciliation of drift - Secure asset and change management.



Cloud Resilience via Security Chaos Engineering (SCE)



Simulate Attacks

Inject controllable & reversible security faults (chaos) to cloud infrastructure (e.g. Ransomware attack)



Analyze Impact

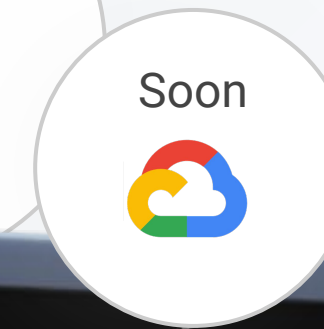
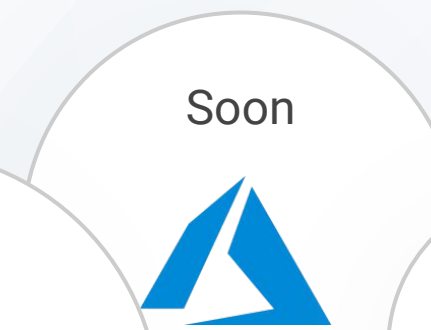
Mitigant analyzes the impact of the attacks and generates a report of countermeasures



Enable Resilience

Continuous application of the SCE and its results enables a hardened security as well as resilience against cloud attacks.

Simplifying security for cloud infrastructure. Ready in minutes.

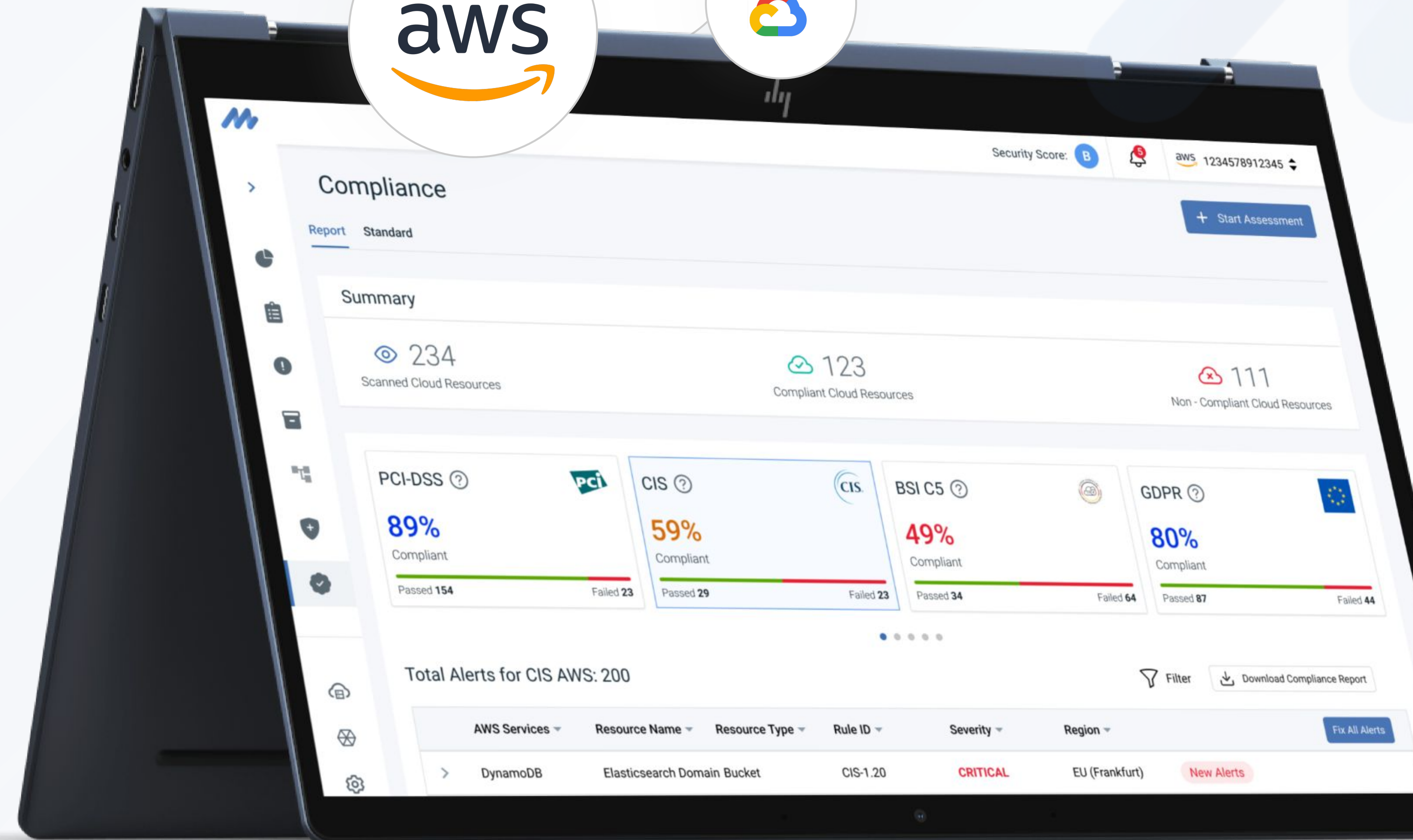


01 **Continuously secured and easy to use.**

Valentin Schipfer (CEO)
White Gloves

02 **The whole process took 10 Minutes.**

Marcel Matzat (DevOps)
Memoresa



The Mitigant Team



Nils Karn
Co-Founder/CEO

- IT Trainer & Consultant at IServ GmbH
- Former Project Coordinator at Hasso Plattner Institute GmbH
- Former ECG (now EXXETA) Project Manager for Shell



Dr. Muhammad Sukmana
Co-Founder/CPO

- Former Doctoral Candidate & Research assistant at Hasso Plattner Institute GmbH
- Former external consultant for SAP Research Project



Kennedy Torkura
Co-Founder/CTO

- Former Senior Cloud Security Researcher at Firebolt and Former Cloud Security Engineer at Mattermost
- External Doctoral Candidate, Hasso Plattner Institute GmbH



Dr. Thomas Fricke
Co-Founder/Advisory Board

- Chief Technology Officer at Endocode AG
- Freelance Senior Expert for Kubernetes Security & SecDevOps



Our investors:



High-Tech Gründerfonds

Brandenburg Kapital

ILB

adesso
ventures

Let's meet in **hall 7** at **booth 242!**

Thank you.

For questions please feel free to
contact Nils:

mail: **nils@mitigant.io**
phone: **(+49) 331 971 83 007**