segura®

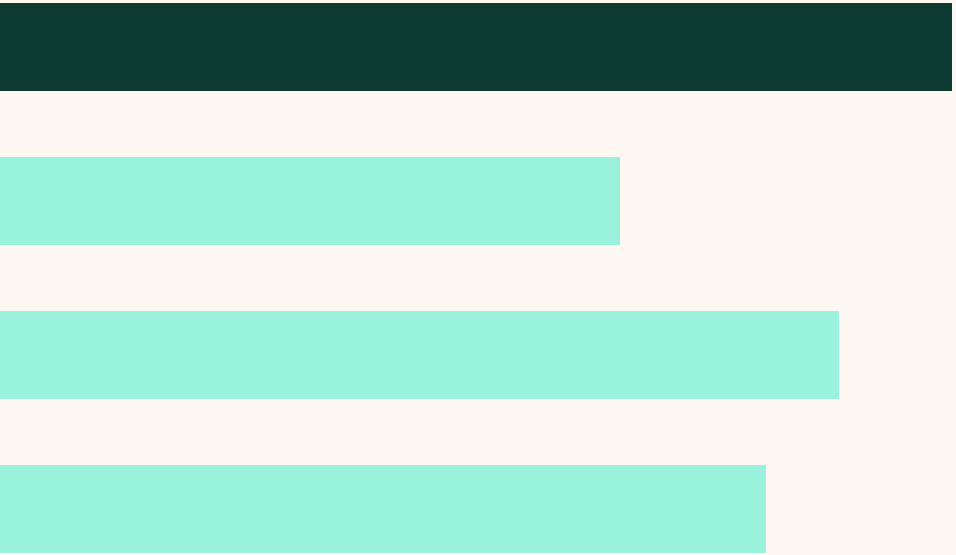
Gartner Peer Insights Customers' Choice 2025™

Segura® Cloud Entitlements

Vendor Briefing

Abril
2025

Table of contents



99%

of security breaches in cloud environments are the customer's responsibility, mainly due to misconfigurations.

76% of organizations use at least du Cloud Service Providers (CSPs).

33% of identity violations are related to compromised privileged credentials.

Source: Gartner

That’s a lot to manage, huh?

18,438
16,685

AWS has more than **18,000 IAM permissions** and more than 16,000 API methods to be managed.

20,144
650

Azure has over **20.000 known actions** in the Azure RBAC service and more than **650 integrated functions** provided by Azure.

11,004
1,820

Google Cloud has more than **11.000 actions** available on IAM and more than **1.800 predefined functions.**

Source: permissions.cloud

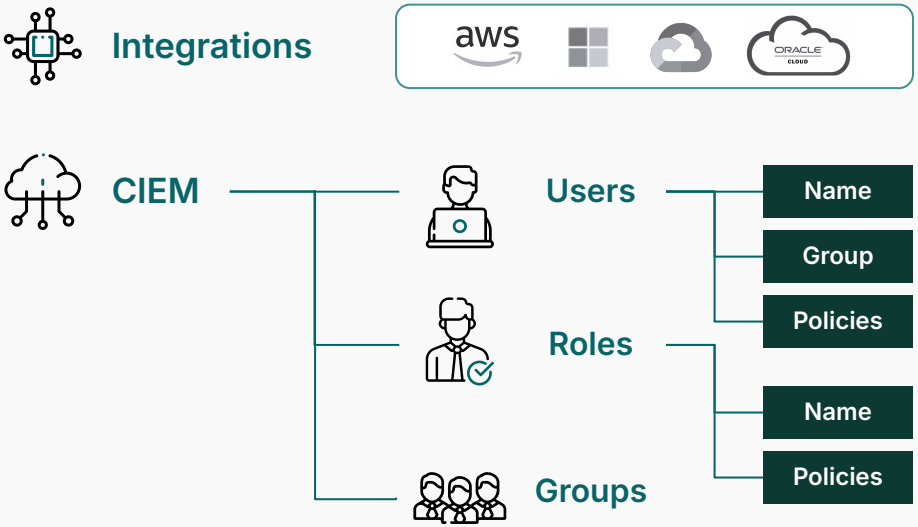
What are the Challenges in Cloud Environments?

- Greater Attack Surface
- Excessive Permissions on Identities
- Lack of Visibility
- Greater Complexity introduce vulnerabilities
- Sanctions from Data Protection laws

How to overcome these challenges?

Cloud Infrastructure Entitlements Management

Through Segura® Cloud Entitlements, it is possible for administrators to determine what applications and resources are critical, offering an elastic policy analysis.



Problem

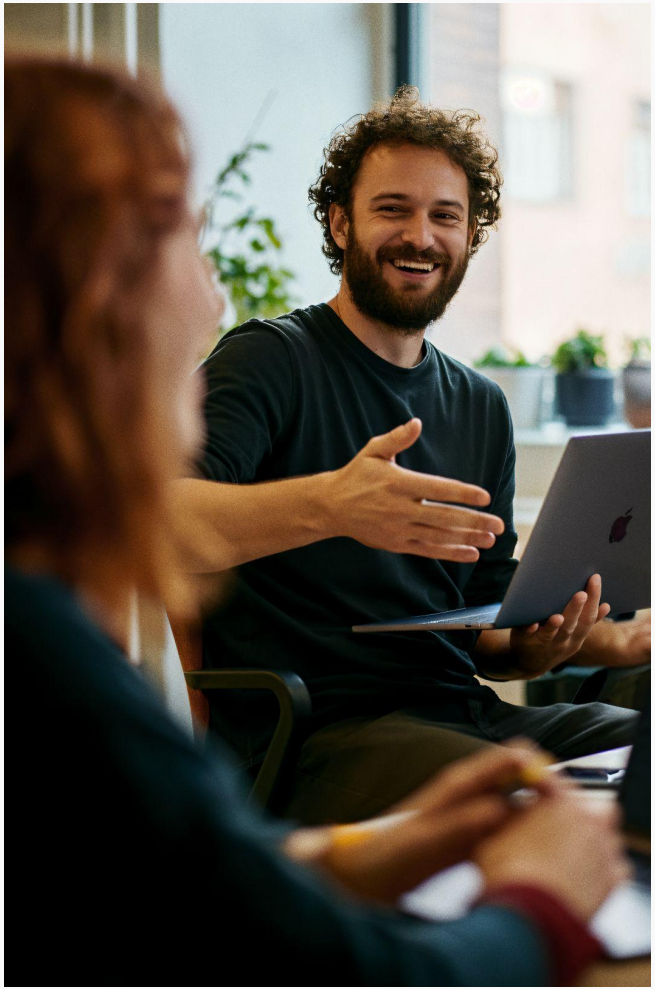
Admins need to provide access to assets according to business reality, based on CSP's best practice guides to multi-cloud environments

Solution

Segura® allows workflow based on access groups, making it possible to segregate policies for users that are in multiple access groups at the same time. Yet, you can segregate entire groups at once using system parameters segregation

Impact

Entities' privileges managed automatically according to real use, with granted non used accesses automatically removed. This reduces risks and increase governance to best practices



Build With Us

Build With Us is a collaborative program that invites partners, customers, and cybersecurity professionals interested in directly contributing to the development and improvement of our solutions.

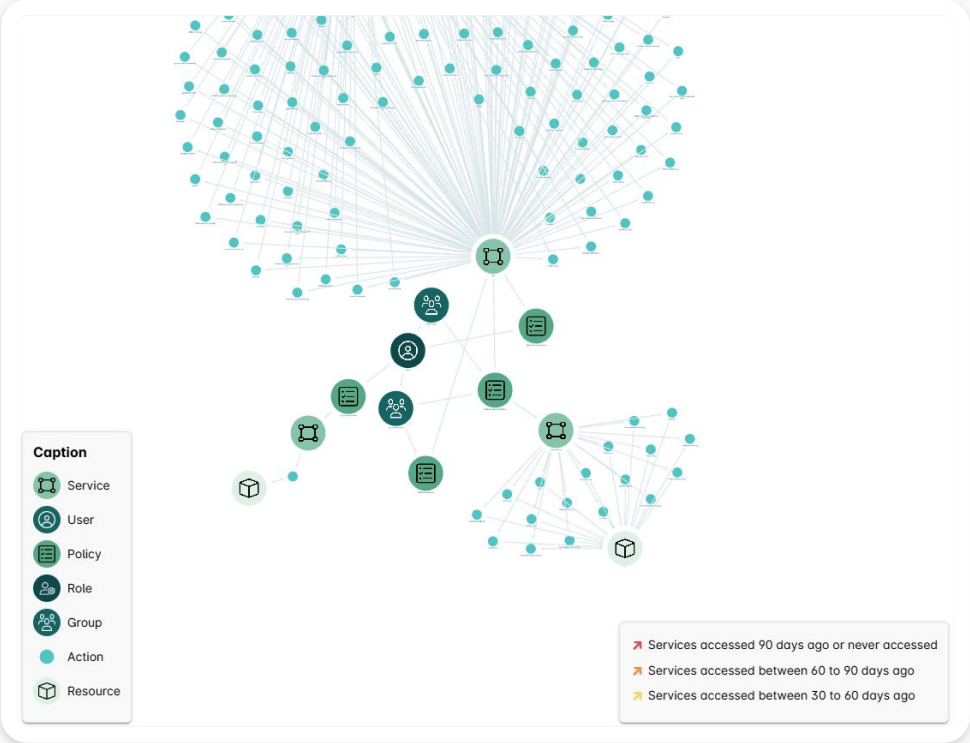
By joining Segura's *Build With Us*, users will gain early access to new products and features, as well as the opportunity to interact with our product team and help shape the solutions that define the future of the global cybersecurity industry.

Main Capabilities

segura

Cloud Entitlements

Access Path of Identities



Granular visibility into the access path of each identity (users, applications, roles) to resources across multi-cloud environments.

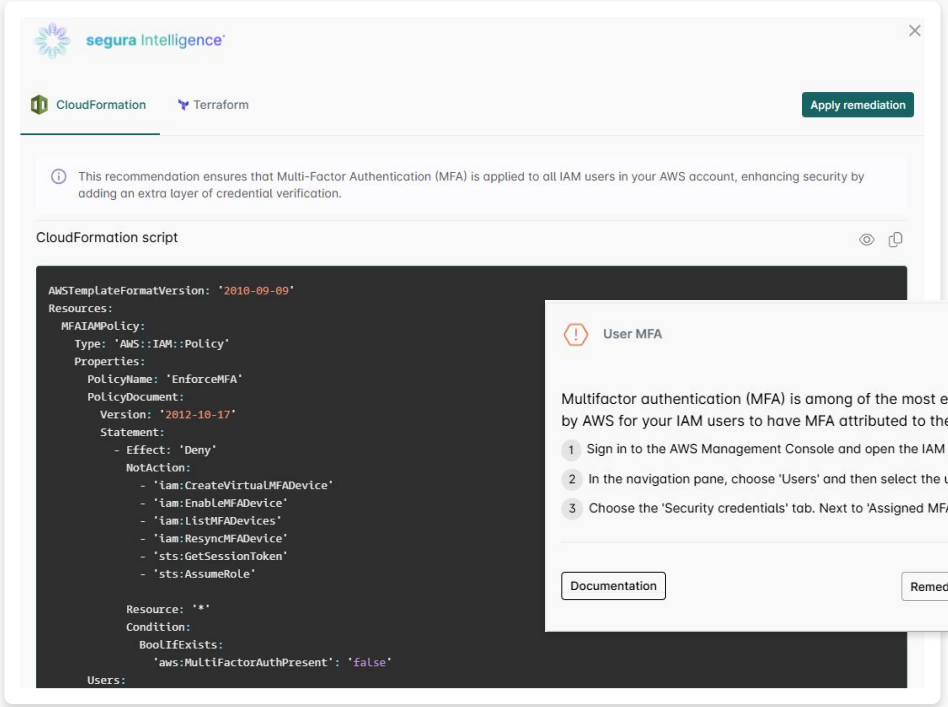
The Access Path feature of Cloud Entitlements allows **tracking and visualizing the permissions and relationships** that enable access in these environments.

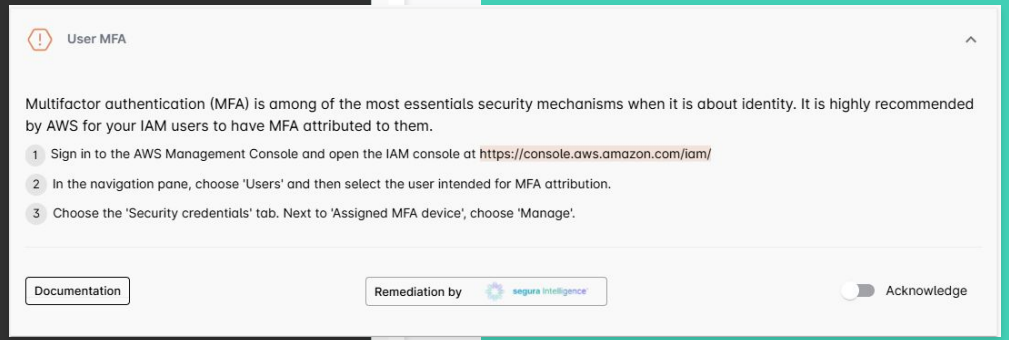
Reduces the time required to **identify over-permissioned configurations**, while also supporting the enforcement of the principle of least privilege.

segura

Cloud Entitlements

Generative AI for Remediation



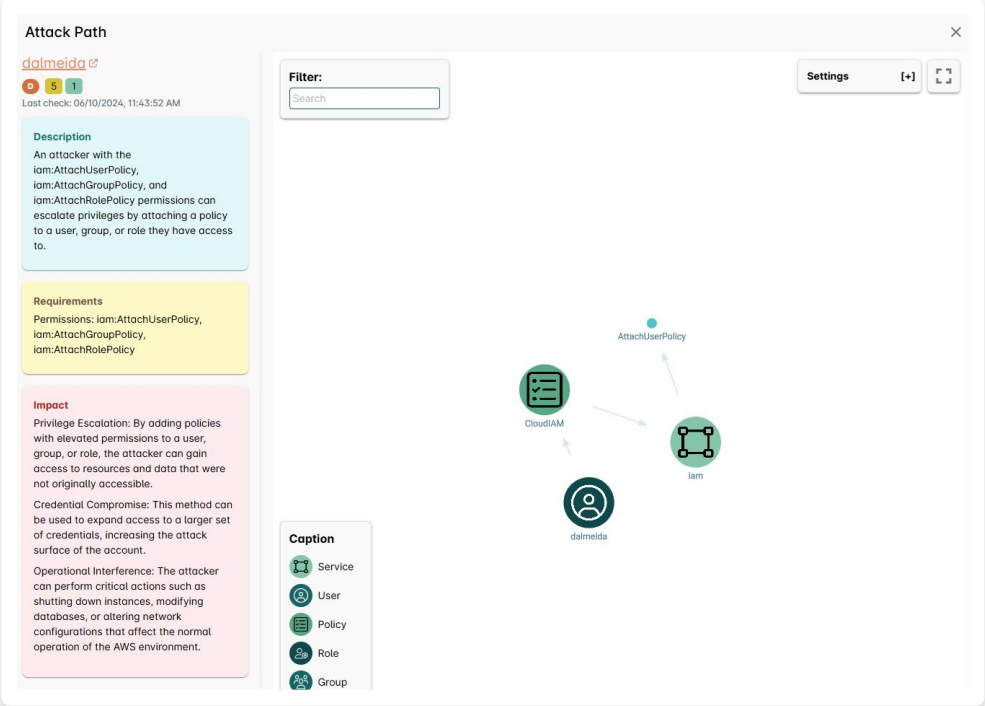


Segura Intelligence, our Generative AI-powered engine, helps **remediate misconfigurations through Infrastructure as Code (IaC) scripts.**

segura

Cloud Entitlements

Identity-based Access Path



Graphical visualization of attack paths that identities can take in cloud environments based on their current permissions.

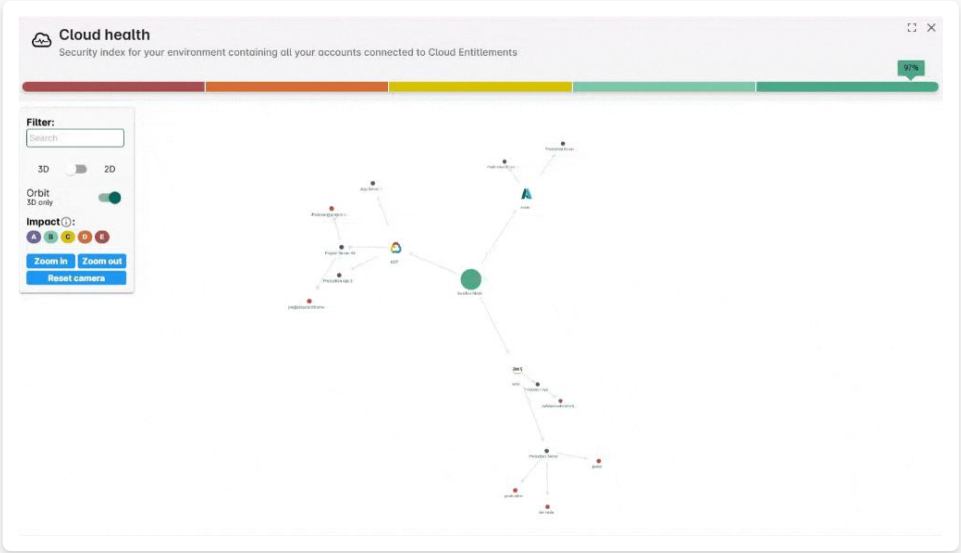
The Attack Path feature offered by Cloud Entitlements simulates attack scenarios, **revealing vulnerabilities and risk exposures** that could be exploited by malicious actors.

It helps drive proactive measures to **enhance the security of the environment.**

segura

Cloud Entitlements

Multi-Cloud Health Score



Unified and quantitative assessment of multi-cloud security posture with the Cloud Health feature of Cloud Entitlements.

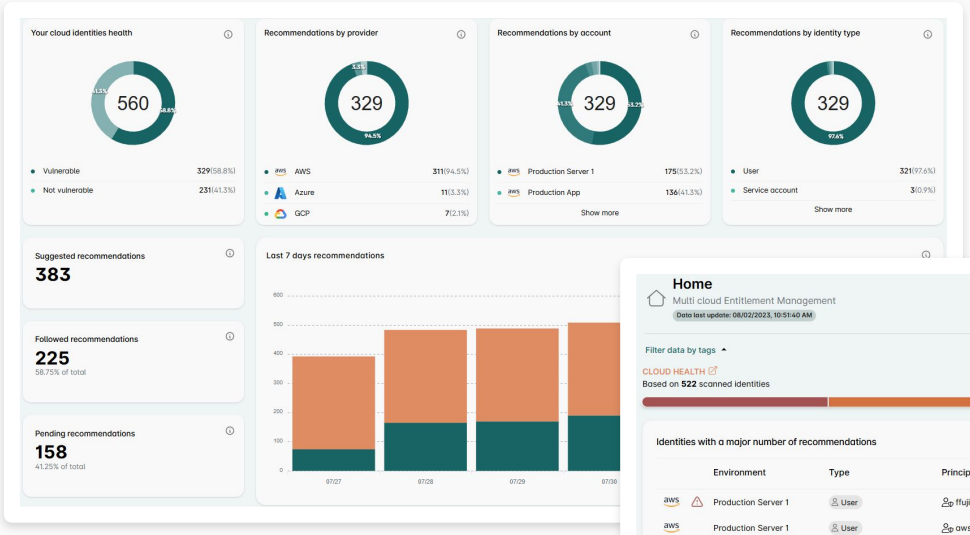
Through a comprehensive analysis of identity and access configurations, Cloud Health generates a health score (as a percentage), providing a **clear view of the security posture** and identifying areas that require immediate attention.

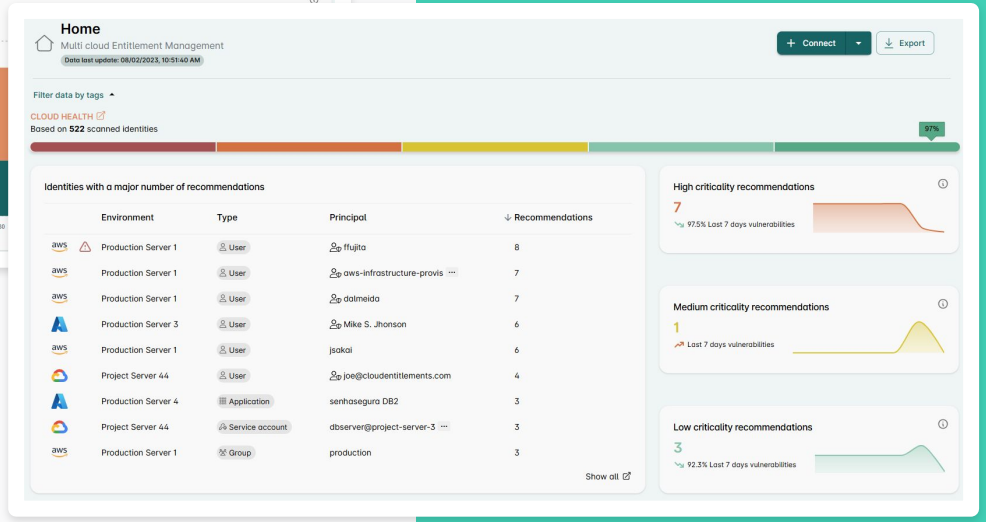
Risk mitigation and enhanced compliance.

segura

Cloud Entitlements

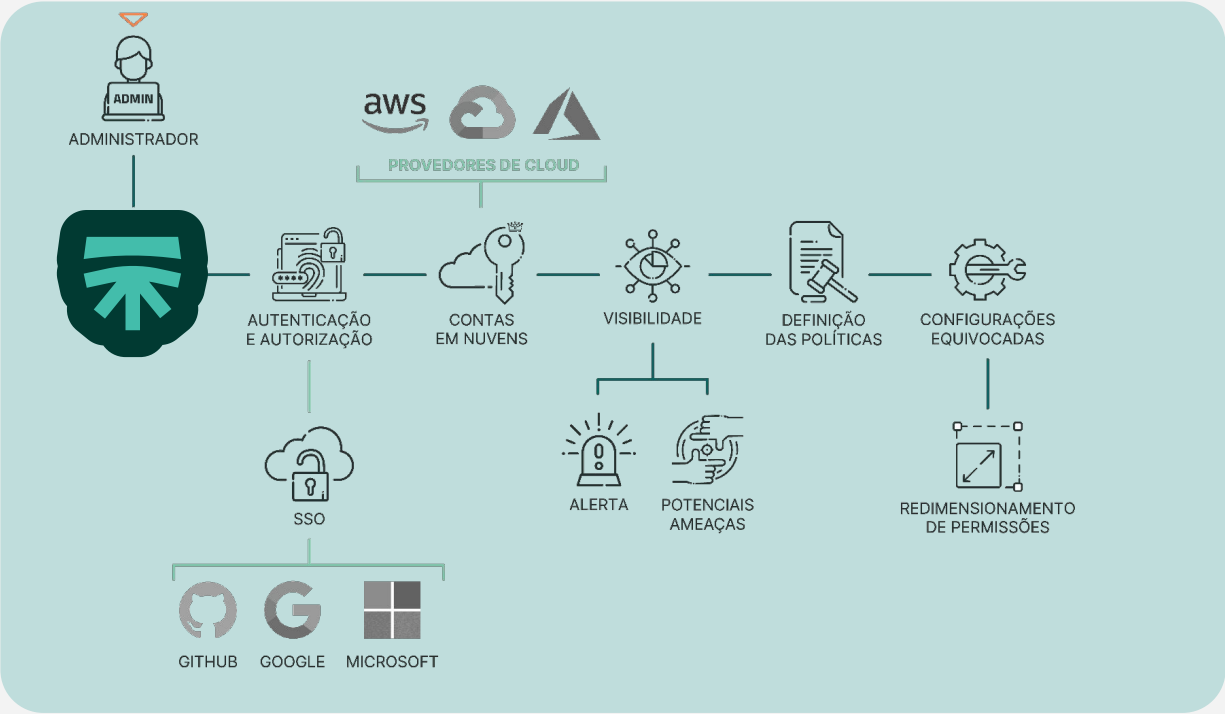
Unified Dashboard





Comprehensive graphical dashboards for **maximum visibility and traceability** of cloud configurations.

How it works?


ADMIN
ADMINISTRADOR
aws
PROVEDORES DE CLOUD
AUTENTICAÇÃO
E AUTORIZAÇÃO
CONTAS
EM NUVENS
VISIBILIDADE
DEFINIÇÃO
DAS POLÍTICAS
CONFIGURAÇÕES
EQUIVOCADAS
SSO
ALERTA
POTENCIAIS
AMEAÇAS
REDIMENSIONAMENTO
DE PERMISSÕES
GITHUB
GOOGLE
MICROSOFT

With Segura Cloud Entitlements, companies take control of their Cloud Security!

Full Visibility

Comprehensive view of all access and privileges across cloud providers. Easily identify unnecessary access, reducing the attack surface and improving detection and response times.

Agility Without Compromising Security

Implement robust policies without impacting business speed and flexibility. Enforcing the Principle of Least Privilege ensures users have access only to the resources they need, when they need them.

Unified and Efficient Governance

Centralized access management across cloud environments, simplifying administration and ensuring consistent enforcement of security policies.

Risk Reduction and Regulatory Compliance

Lower risk of violations, data breaches, and other security incidents. Automate compliance with standards such as SOX, PCI-DSS, ISO 27001, and data privacy regulations like GDPR and LGPD.

Why Segura® Cloud Entitlements?

1. Recognized and industry-awarded User Experience (UX)
2. Fully Customized Criticality Levels
3. Access path visualization
4. Collaborative Licensing Model with no cost to Users

Vendor Briefing Cloud Entitlements

Customer Cases

Telefónica

Client under NDA

Global European Telecom

Serves over 110k customers in over 3,200 cities

Situation

- Telefonica is navigating complexities in its IT infrastructure due to rapid digital transformation.
- The company manages numerous applications, services, and microservices.
- This complex operations rely on thousands of machine identities, deployed across multiple environments:
  - API keys
  - Access tokens
  - SSL certificates

Problem

Lack of Visibility of machine credentials;

Non-compliance with industry regulations like NIST CSF and challenges in auditing credentials;

Manually managing secrets across CI/CD pipelines and cloud services was time-consuming and error-prone, causing deployment delays and increased operational costs.

Solution

Segura®'s integrated approach addresses these challenges through our MIM framework;

DevOps Secrets Manager automates secrets management and dynamic provisioning;

Automation of the entire lifecycle of SSL/TLS certificates, including issuance, renewal, and deployment to maintain secure communications;

Cloud Entitlements provided visibility into machine identity risks and enforced governance policies.

Results

Enhanced security posture;

Compliance with cybersecurity requirements;

Operational efficiency through reducing manual workloads and streamlining processes;

Reduced risk exposure and benefits from scalable solutions that support growth, ensuring robust and consistent management of machine identities.

Client under NDA

Situation

- This client faced significant challenges in managing their Google Cloud Platform (GCP) credentials.
- Developers had the freedom to create credentials with the permissions they deemed necessary, without adhering to the principle of least privilege.
- There was uncontrolled proliferation of credentials with broad permissions (basic roles), posing a potential security risk.

Large Wholesale Company with $5 Billion in Revenue

Over 95,000 employees across 102 stores and 7 distribution centers

Problem

Identifying and managing credentials with excessive privileges was time-consuming and labor-intensive.

The security team had to manually inspect each GCP project to discover which users had Basic Roles, and then remove or adjust the respective permissions.

This process was not only inefficient but also error-prone, leaving the company vulnerable to security threats and potential violations.

Solution

Deployment of Segura® Cloud Entitlements to resolve this critical issue.

Implementation of a filter in Cloud Entitlements to automatically consolidate and display all identities across all GCP projects that had Basic Roles, providing a complete and real-time view of credentials with excessive privileges.

Simplification of the credential management and protection process across the GCP environment.

Results

Improved operational efficiency. The client enhanced overall visibility and control over GCP permissions.

Identification and mitigation of permissions issues, ensuring credentials followed the principle of least privilege.

Reduced time spent auditing credential permissions.

A secure cloud environment, mitigating potential risks and aligning with best practices in cloud security.

Greater Cloud Adoption

The migration to multi-cloud environments has increased the challenges and complexity of managing identities, roles, and permissions in these environments.

Cloud Entitlements

Segura Cloud Entitlements enables centralized discovery, management, and traceability of privileges across multi-cloud environments.

Maximum Security and Compliance

Greater visibility and governance, increased security levels, and improved regulatory compliance with security standards.

segura®

Gartner Peer Insights Customers' Choice 2025™

Segura® Cloud Entitlements

Vendor Briefing

Abril
2025