segura®

Gartner Peer Insights Customers' Choice 2025™

End-to-End Machine Identity Management with Segura®

Vendor Briefing

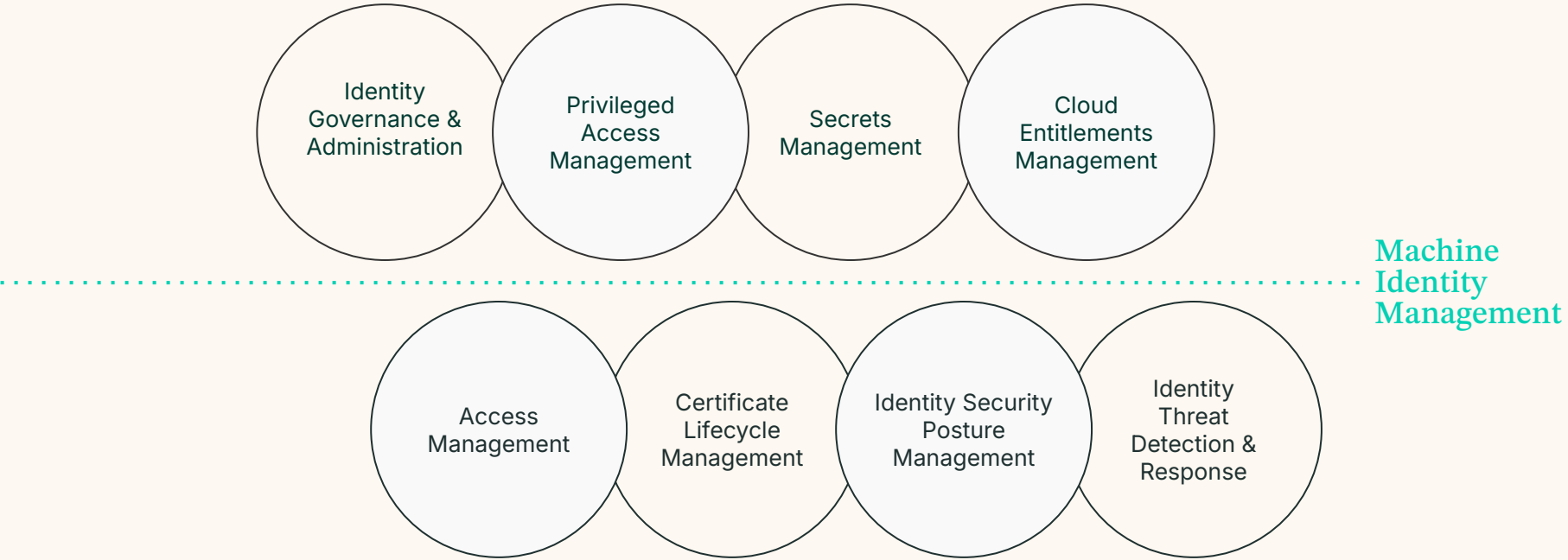
Abril
2025

Table of contents

Vendor Briefing Machine Identity

Our Vision on Machine Identity Management

Our Vision on Machine Identity Management



Our Vision on Machine Identity Management

Discover

We find them in
- Servers
- Containers
- DevOps Pipelines
- Cloud Workloads
- Source Code

Govern

Best Practices
- Ownership
- Policy Enforcement
- Access Control
- Traceability
- Access Review
- Compliance

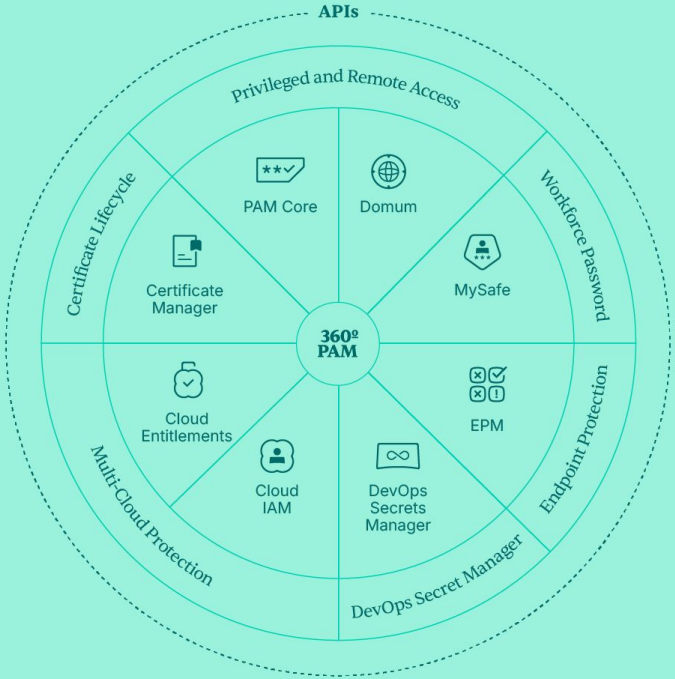
Automate

Orchestrate
- Just-In-Time
- Provisioning
- Deprovisioning
- Integrations
- Secret Rotation
- Certificates

Management

Enhance Security
- Hygiene
- Least Privilege
- Cleanup
- Security Posture
- ITDR & Behavior

Our Vision on Machine Identity Management



SaaS | Hybrid | On-premises

Demonstration Scenario

Global European Telecom

Serves over 110k customers in over 3,200 cities

Telefónica

Client under NDA

THE 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.

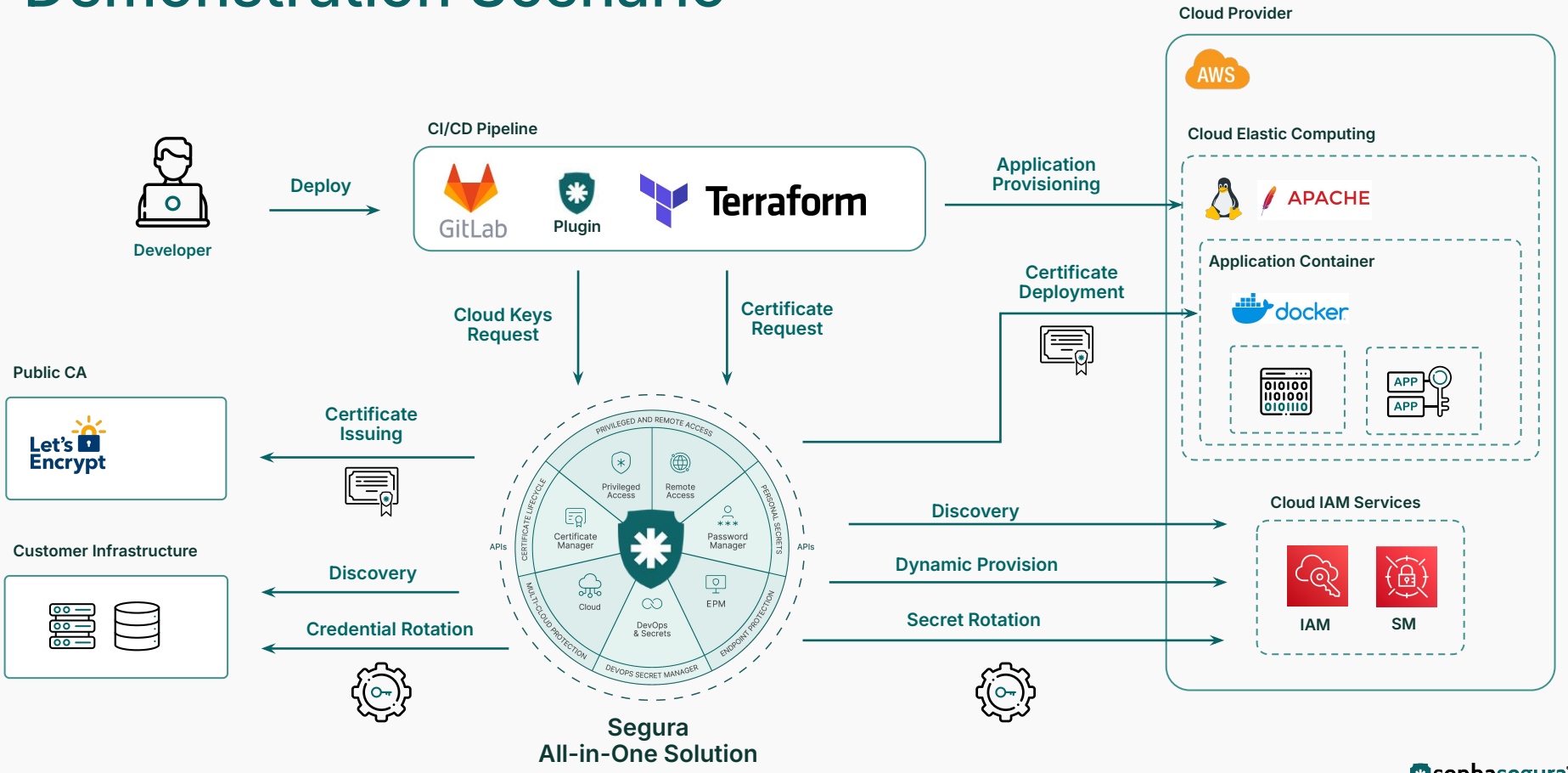
Reduced risk exposure and benefits from scalable solutions that support growth, ensuring robust and consistent management of machine identities.

segura

Demonstration Scenario

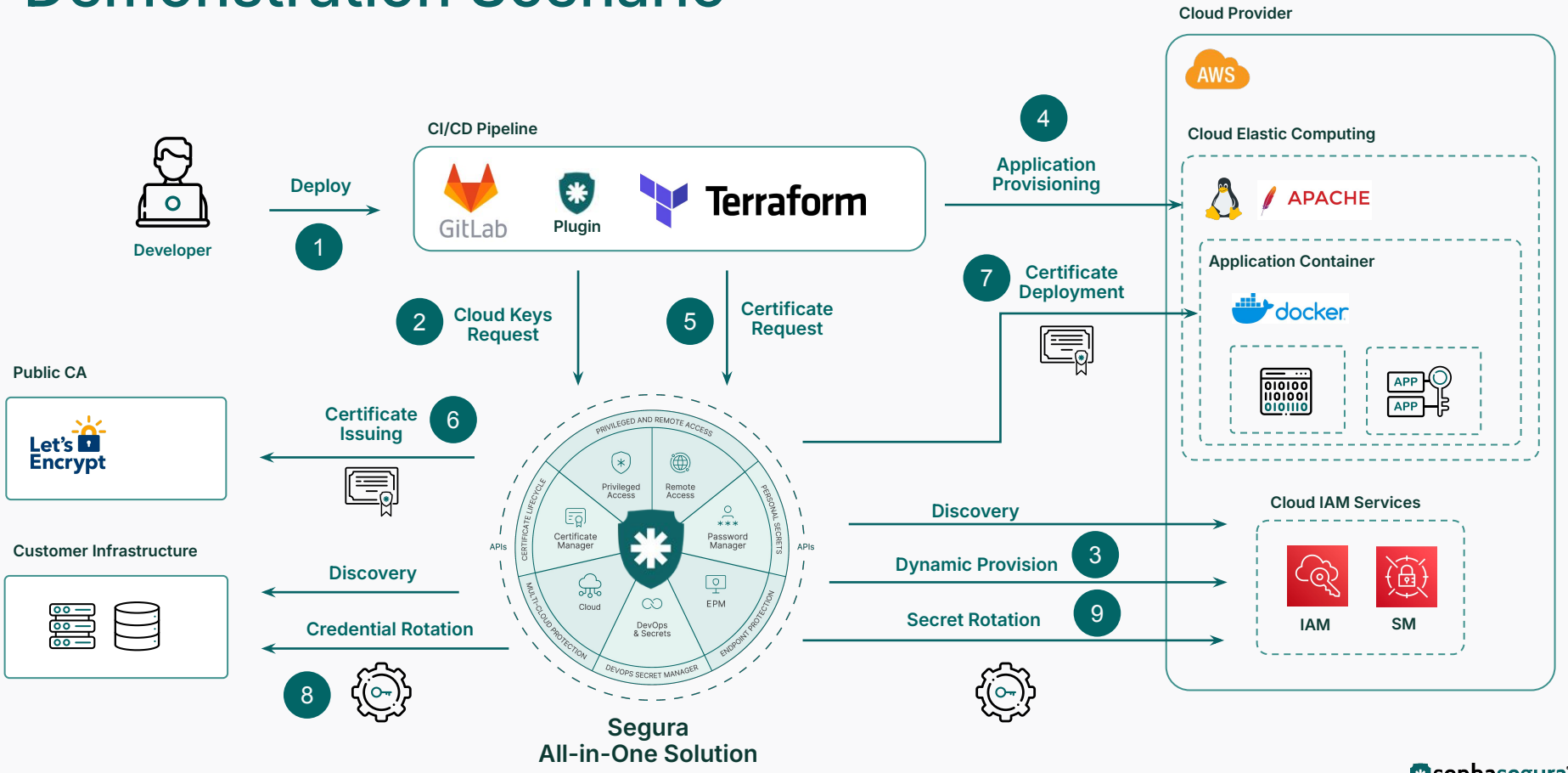
segura®

Demonstration Scenario



senhasegura

Demonstration Scenario



senhasegura

Vendor Briefing Machine Identity

MIM Use Cases

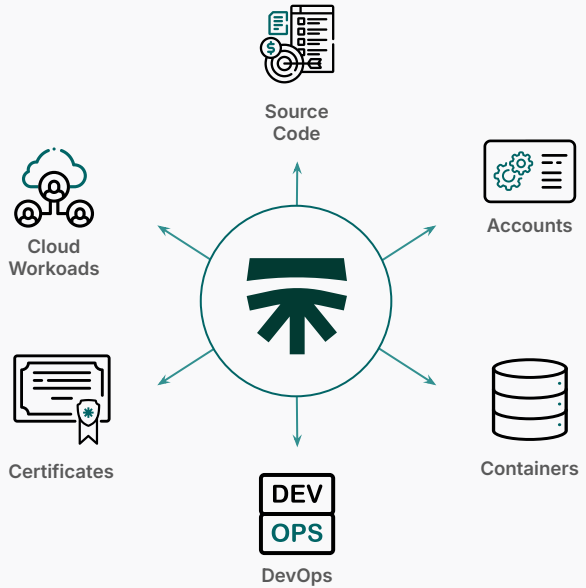
segura

Use Cases

Discover

Discovery of Machine Credentials

Segura® provides a comprehensive solution to discover and inventory machine credentials, enhancing security and compliance.



Problem

Organizations lack full visibility into their machine credentials due to complex IT environments, leading to security vulnerabilities and compliance issues.

Solution

Segura offers comprehensive discovery capabilities to uncover and inventory machine credentials across the entire IT landscape.

Impact

Enhanced security posture with full visibility of machine credentials.

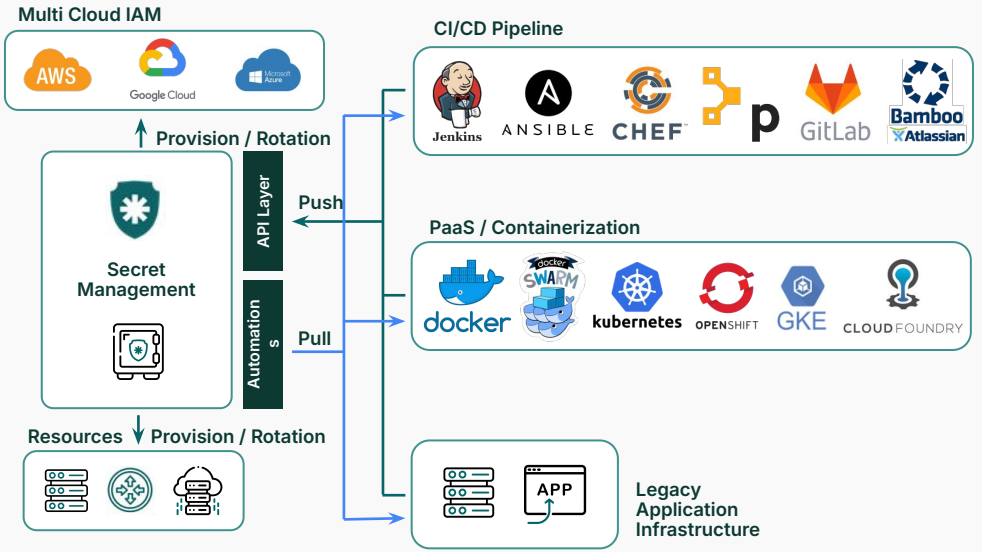
segura

Use Cases

Govern Automate

Integration With CI/CD

Segura® can manage secrets across heterogeneous environments in order to guarantee visibility, security and granularity access by applications.



Problem

In secure software development and deployment pipelines, consistent and secure management of secrets is often overlooked, risking credential leakage and access violations.

Solution

Segura provides seamless integration with CI/CD tools, ensuring secure management of secrets throughout the development lifecycle, while enforcing best practices in DevOps environments.

Impact

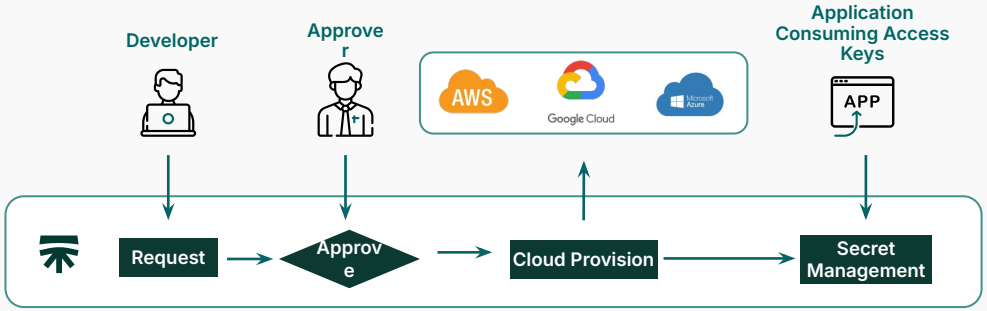
Secure and efficient DevOps processes for accelerated deployment cycles without compromising security.

segura®

Use Cases

Dynamic Secrets Provisioning with TTL

Segura® controls the creation process of key access to main IaaS providers, avoiding unnecessary keys to be created and implementing governance requirements.



Problem

In fast changing cloud environments, managing secrets for applications and services dynamically and securely leads to static and vulnerable credentials.

Solution

Segura's DSM and Cloud IAM provide dynamic provisioning of secrets, ensuring that credentials are governed without manual intervention.

Impact

Increased agility and security in cloud environments with on-demand credential provision for minimized risk.

segura®

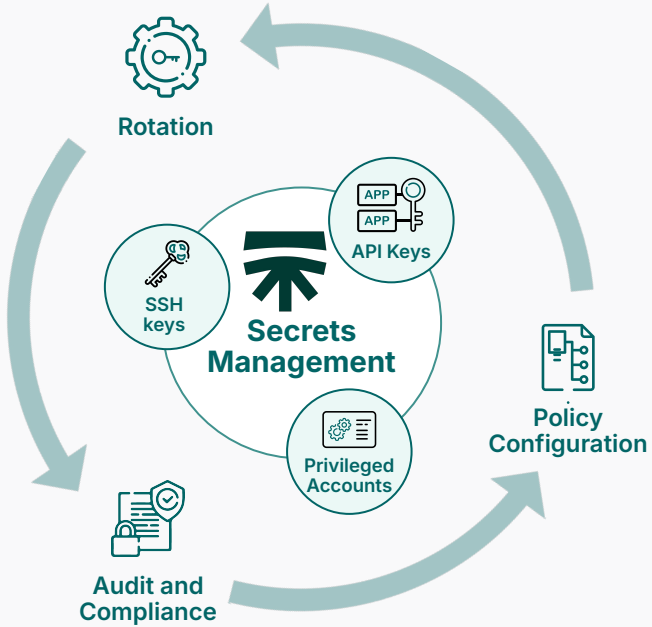
Use Cases

Rotation with secrets (PAM Credentials)

Automate

Secure

Automated rotation of PAM credentials with **Segura®** reduces security risks associated with static credentials.



Problem

Static privileged credentials are vulnerable to compromise, making manual rotation error-prone and inefficient.

Solution

Segura automates credential rotations for consistent updates and management.

Impact

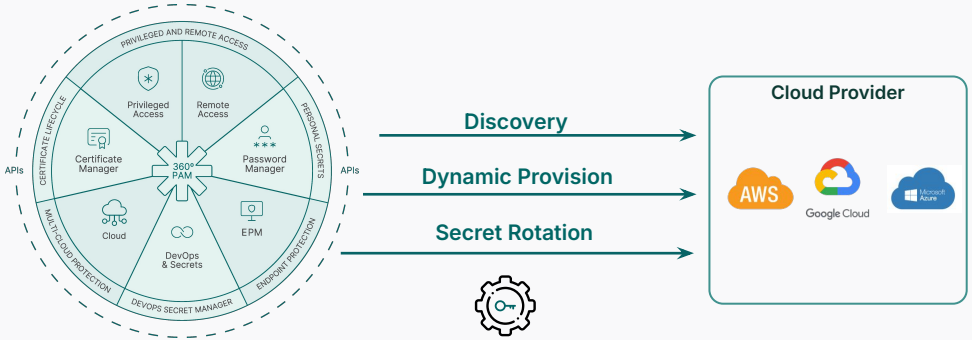
Improved security by reducing exposure risks, enhances operational efficiency, and compliance with minimal manual intervention.

segura

Use Cases

Secrets Manager with AWS Secrets Manager and Automation

Segura can manage the entire SSH keys lifecycle, provisioning, discovering, monitoring e rotating keys on the infrastructure.



Problem

Managing secrets in hybrid environments with multiple CSPs can become cumbersome, leading to potential security gaps.

Solution

By integrating seamlessly with CSPs, **Segura** provides a unified approach to secrets management, leveraging automation to maintain consistency and security across platforms.

Impact

Reduced risk of exposure through automated secrets rotation and access controls.

segura

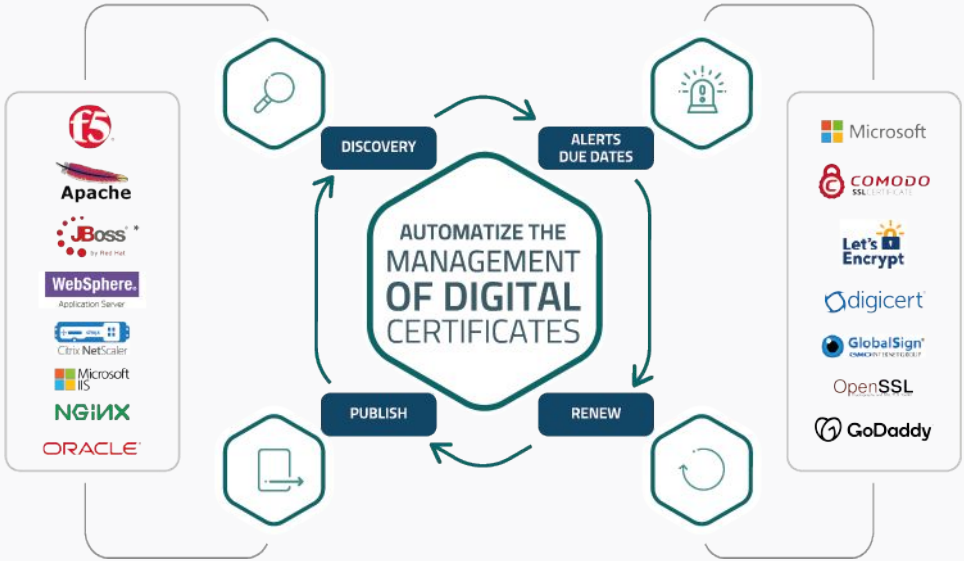
Use Cases

Automated Certificate Management

Automate

Secure

Segura can manage the entire certificate lifecycle from certificate generation to publish in order to increase security and efficiency.



Problem

Managing the lifecycle of digital certificates can be complex and error-prone, leading to potential outages and security breaches

Solution

Segura offers a centralized approach to certificate management, automating the publishing and renewal processes to ensure certificates are always up-to-date and valid.

Impact

Streamlined operations with less manual intervention and reduced chance for human error.

segura®

Use Cases

Visibility of Risks in MIM

Discover

Secure

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

Integrations

CIEM

- Users
  - Name
  - Group
  - Policies
- Roles
  - Name
  - Policies
- Groups

Problem

It is challenging to identify and manage risks associated with machine identities, as these can be numerous and complex.

Solution

Segura Cloud Entitlements provides insights into machine identity behaviors, helping organizations identify potential risks and vulnerabilities through comprehensive monitoring and analytics.

Impact

Proactive threat detection and remediation, reducing the likelihood of security incidents and providing comprehensive visibility and control over machine identities.

Customer Cases

North American Credit Union

Named one of America's Best Credit Unions in 2024

Financial Institution with more than USD 1.7 billion in assets.

Client under NDA

Situation

- SF Fire Credit Union faced challenges in managing the lifecycle of their SSL/TLS certificates across a diverse IT environment;
- There are over 200 certificates in use throughout the environment;
- Certificates were managed manually, which risked service disruptions due to expired certificates.

Problem

Manual management of certificates lead to potential security vulnerabilities and compliance issues;

Expired certificates could result in service outages, impacting customer trust and operational integrity.

Solution

Segura® Certificate Manager automates certificate issuance, renewal, and deployment.

The solution acts as a centralized repository for all certificates.

Automated alerts and policy-based management ensured that certificates were maintained according to organizational and regulatory standards.

Results

Improved security by preventing service interruptions due to expired certificates;

Increased operational efficiency, reducing the manual workload on IT staff;

Enhanced visibility and control over certificates facilitated better compliance, supporting the customer's regulatory responsibilities.

Global Restaurant Chain

Presence in more than 100 countries.

Segura® helped protecting more than 1,242 restaurants.

Client under NDA

Situation

- Dynamic DevOps environment heavily reliant on microservices.
- They faced challenges managing machine identities because many of these services utilized static credentials.
- This practice created security vulnerabilities and operational complexities, given the scale and speed at which their infrastructure evolved.

Problem

The use of static credentials in microservices made the system susceptible to unauthorized access and data breaches.

Developers were reluctant to refactor existing code to integrate more secure credential management practices, as it required significant operational effort and time.

This led to inconsistent security practices and complicated the maintenance of a secure and efficient environment.

Solution

Integration of External Secrets Operator within corporate Kubernetes clusters.

Automated credential management and rotation, enabling customer microservices to securely access dynamic secrets without requiring any code modifications.

Automation of the entire credential lifecycle, ensuring credentials remains secure and up-to-date.

Results

Enhanced security by successfully transitioning from static credentials to dynamic secrets, reducing the risk of unauthorized access.

Improved operational efficiency, as developers no longer needed to alter code to adhere to secure practices.

Consistent and robust security framework.

Client under NDA

Situation

- DevOps Pipeline (CI/CD) with thousands of secret hard-coded keys
- +200 Admin developers operating the Pipeline with DevOps systems
- 4K cloud permanent servers
- 20K ephemeral cloud servers
- +2K of hardcoded access keys with indiscriminate usage
- Indiscriminate privileged access to cloud servers with no traceability

Largest LATAM e-commerce

(1,6 U$ BILLION REVENUE)

Enabled DevSecOps at largest LATAM e-commerce company.

Problem

Shared secrets caused malicious user to act without accountability:

Changes made without accountability caused more operational errors and allowed malicious activities to contribute with data leakage and unavailability;

Company couldn't control access proliferation and also not guarantee security governance.

Solution

Integrate Segura® to DevOps pipeline with gitlab, kubernetes to scan discovery applications, access keys hardcoded and rotate it during deploy;

Integrate Segura® to AWS and GCP to automatically identify ephemeral servers and manage credential and record sessions trough AD authorization.

Results

100% Applications and AWS secret keys mapped;

+40% of AWS unnecessary users were deleted reducing the attack surface and therefore the risks;

+80% Admin access recorded and audited;

Customer was able to accelerate their DevSecOps initiative.

ATACADÃO

Client under NDA

Situation

- This customer faced significant challenges in managing their GCP credentials.
- Developers had the freedom to create credentials with the necessary permissions as they deemed fit, without adhering to the principle of least privilege.
- There was an uncontrolled proliferation of credentials with extensive permissions (Basic Roles), posing a potential security risk.

Global wholesale company

More than USD 30 billion in revenue

Over 60,000 employees spread across more than 100 stores and 7 DCs.

Problem

Identifying and managing over-privileged credentials was time-consuming and cumbersome.

The security team had to manually inspect each GCP project to uncover which users had Basic Roles and then remove or adjust those permissions accordingly.

This process was not only inefficient but also prone to errors and oversight, leaving the company vulnerable to security threats and potential breaches.

Solution

Segura leverages Cloud Entitlements to helps managing entitlements in multiple CSPs, including GCP.

Segura Cloud Entitlements offers a specific filter that consolidates all identities across all connected GCP projects that held any Basic Roles

Comprehensive and real-time view of over-privileged credentials.

Results

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

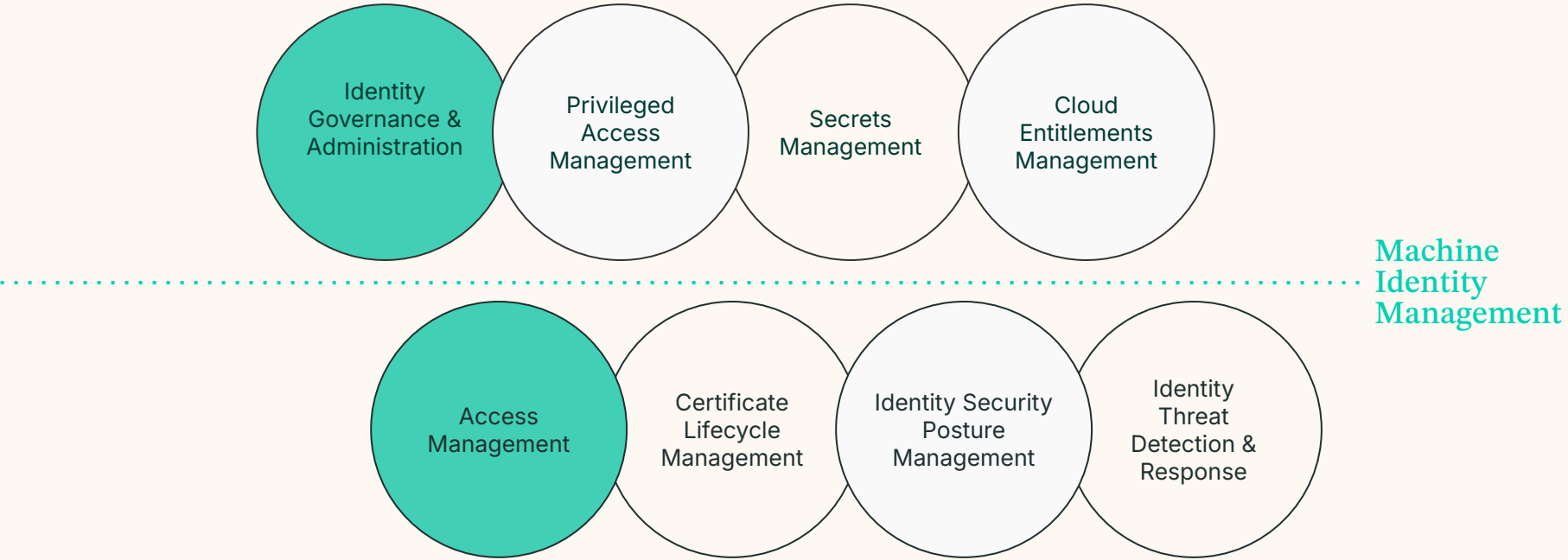
The customer could now identify and address permissions issues, ensuring all credentials adhered to PoLP

Reduction of audit time on credential permissions

Enhanced security of the cloud environment, mitigating potential risks.

Roadmap

Roadmap: Full Converged Identity Solution



Roadmap: Full Converged Identity Solution

	2025/H1	2025/H2	2026	2027
Major	ISPM	IGA	Access Management	Customer IAM
Minor (MIM)	SPIFFE Auth ITDR Protocols	MIM Full Governance Quantum Safe IAM	Cloud PKI Secretless Broker	Full Edge and IoT IAM Identity Data Lake for Analytics & Reporting

segura

Summary

Machine Identity Management

Unified Security Vision

Comprehensive Protection
Enhanced Security Posture
Operational Efficiency

Simplicity

Streamlined Workflows
User-Friendly Interface
Easy Deployment
Centralized Management

segura®

Gartner Peer Insights Customers' Choice 2025™

End-to-End Machine Identity Management with Segura®

Vendor Briefing

Abril
2025