segura

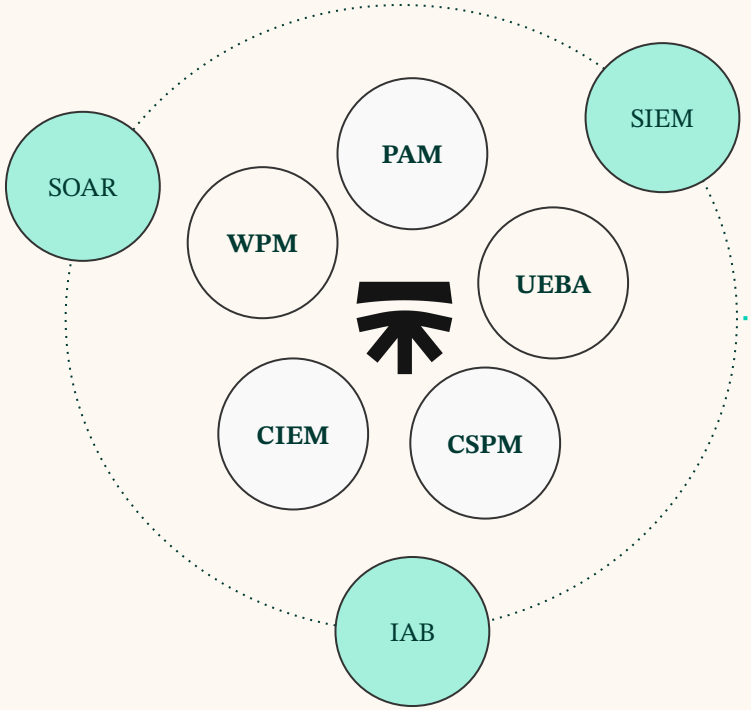
Gartner Peer Insights Customers' Choice 2025

Segura's Unified Vision for Identity Threat Detection & Response (ITDR)

Vendor Briefing

Our Vision on ITDR

Our Vision on ITDR



Zero Trust

User-Centric

Identity Threat Detection and Response

Our Vision on ITDR

Unified Visibility

Native integration in a single platform.

Behavioral anomalies, and misconfigurations.

Continuous Verification

Adaptive Threat Detection

Real-time adaptive controls

Automated Response

Integration with 3rd party tools for real-time remediation

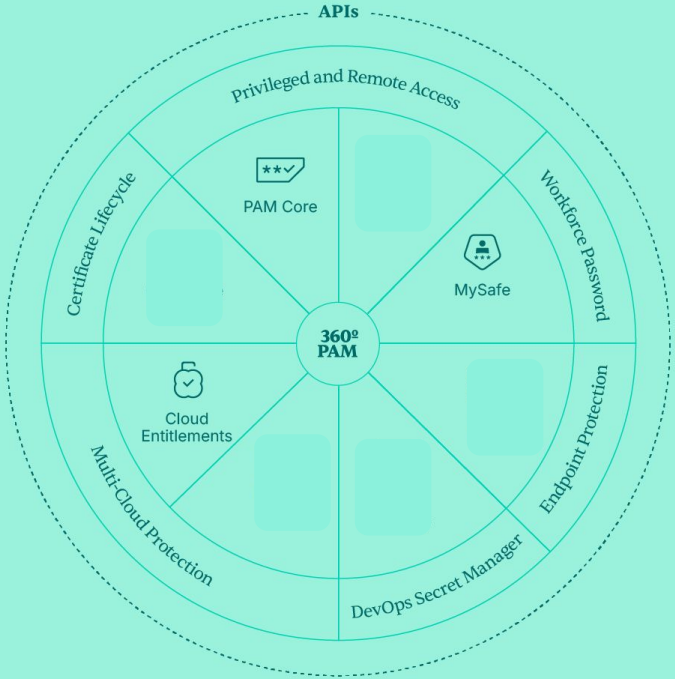
Trigger for incident response via API.

Cloud-Ready Governance

Cloud entitlements and attack path visualization

Detection and remediation of misconfigured cloud permissions.

Our Vision on ITDR



SaaS | Hybrid | On-premises

Our Vision on ITDR

PAM Core

Segura PAM Core
1,882 customers

MySafe

Segura MySafe
108 customers

Cloud
Entitlements

Segura Cloud Entitlements
195 customers

segura

Our Vision on ITDR

PAM Core

Segura PAM Core
1,882 customers

Breakdown

Region	
LATAM	**52%**
EMEA	**27%**
North America	**11%**
APAC	**10%**

Size	
Small	**51%**
Midsize	**39%**
Corporate	**4%**
Enterprise	**6%**

Deployment Model	
Subscription	**34%**
Perpetual	**50%**
SaaS	**16%**

segura®

Our Vision on ITDR

MySafe

Segura MySafe
108 customers

Breakdown

Region	
LATAM	**73%**
EMEA	**11%**
North America	**16%**
APAC	**0%**

Size	
Small	**35%**
Midsize	**42%**
Corporate	**14%**
Enterprise	**9%**

Deployment Model	
Subscription	**73%**
Perpetual	**0%**
SaaS	**27%**

segura

Our Vision on Machine Identity Management

Cloud Entitlements

Segura Cloud Entitlements
195 customers

Breakdown

Region	
LATAM	**60%**
EMEA	**18%**
North America	**12%**
APAC	**16%**

Size	
Small	**0%**
Midsize	**69%**
Corporate	**19%**
Enterprise	**12%**

segura

Demonstration Scenario

Demonstration Scenario

Identity Threat Detection and Response

1. Real-time User Block with SOAR Integration
2. Continuous authentication with Adaptive MFA
3. Cloud Risk Detection and Remediation
4. Breached Password Detection with Dark Web Integration

segura

Vendor Briefing Machine Identity

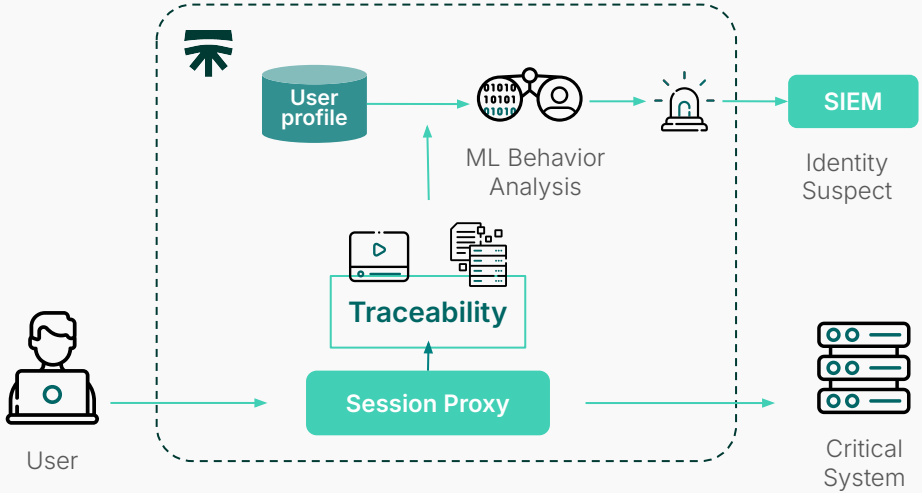
ITDR Use Cases

segura

Use Cases

Real-time User Block with SOAR Integration

Automated privilege revocation triggered by alerts from SOAR platforms.



Problem

Security teams face delays revoking access for compromised accounts due to disconnected tools and manual workflows.

Solution

Segura's API integrates with SOAR platforms to automate user blocking and session termination in real time.

Impact

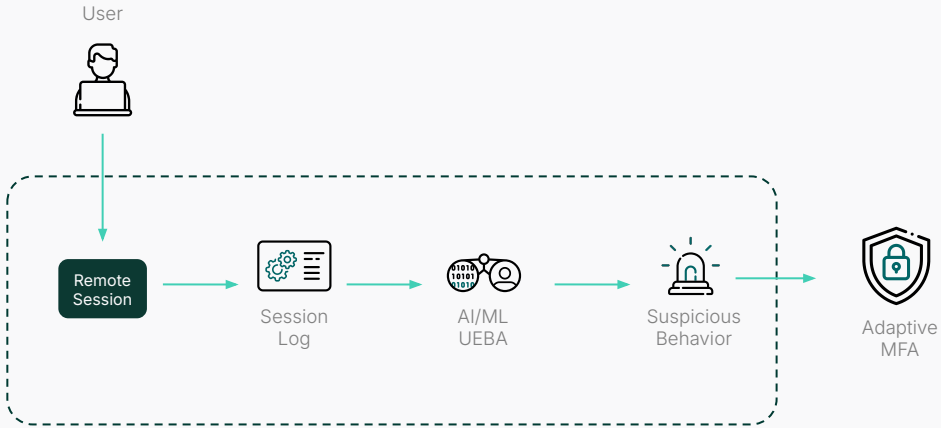
Reduces attacker dwell time from hours to seconds, improves SOC efficiency, and enables compliant, audit-ready remediation.

segura®

Modules & Cases

Adaptive MFA Triggered by UEBA Anomalies

Segura® can monitor user behavior in real time to instantly identify suspect behaviors and revalidate identity during active privileged sessions.



Problem

Although PAM solution provides accountability, malicious actors may gain credential access.

Solution

Segura® implements a real time monitoring user behavior to automatically detect and stop privilege abuse during behavior deviation.

Impact

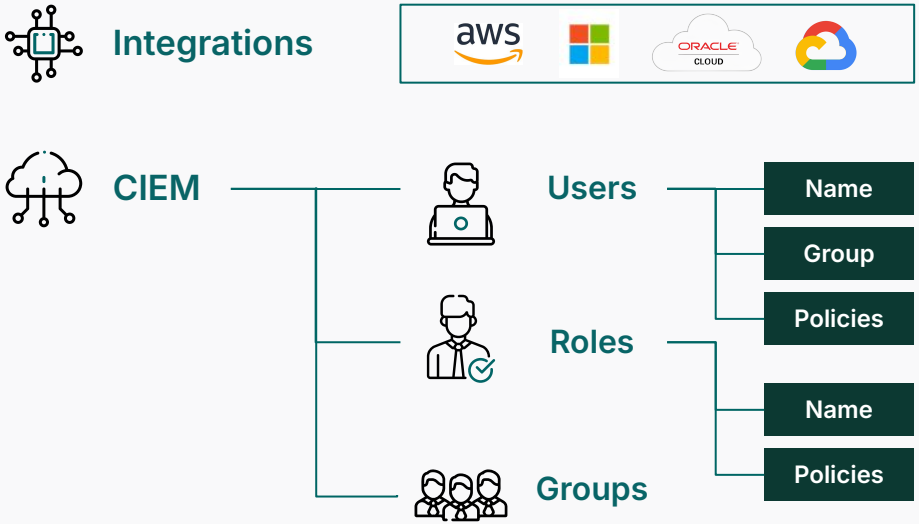
Enable companies to detect malicious acts in real-time, allowing then to reduce the response time. Also inhibit frauds, since frauds can be detected online more effectively than through offline audit.

segura®

Use Cases

Remediation of Risky Machine Identities with CIEM

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



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

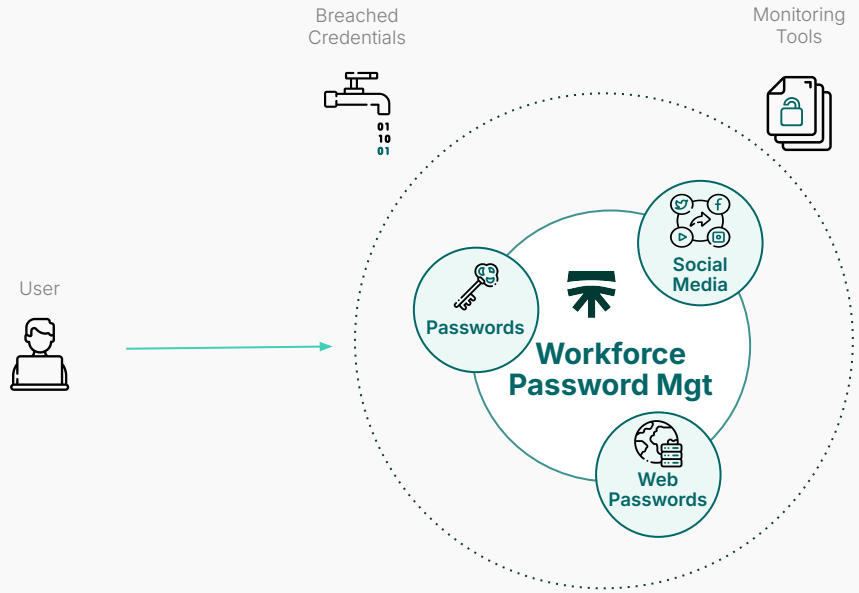
Proactive threat detection and remediation, reducing the likelihood of security incidents and providing comprehensive visibility and control over machine identities.

segura

Modules & Cases

Breached Password Detection

Segura® MySafe prevents account takeovers by monitoring dark web leaks and responding to compromised credentials.



Problem

Organizations struggle to detect and respond to leaked credentials on the dark web before attackers exploit them.

Solution

Segura integrates with breach monitoring tools to trigger forced password resets and session blocks upon detection.

Impact

Reduced account takeover risks, elimination of password reuse vulnerabilities, and compliance with proactive defense standards.

Customer Cases

Bell

Client under NDA

Situation

- Bell Canada needed a secure and efficient method for managing and sharing credentials across departments and with external partners.
- Credential sharing with third parties, such as contractors and partner companies, was often handled through informal and insecure methods.
- Lack of visibility and accountability in shared password usage created compliance and operational risks.

North American Telecom

Leading Telecommunications Provider in Canada

Company with revenues of more than USD 18 billion.

Problem

Shared credentials lacked proper monitoring, which increased the risk of unauthorized access and data breaches.

Shared passwords were prone to mishandling, exposing Bell Canada to potential data leaks and compliance violations.

Solution

MySafe provided a unified platform for managing and securely sharing credentials with individuals, groups, and external partners.

Comprehensive logging of who accessed or modified credentials and when, ensuring full visibility and accountability.

Results

All credentials for shared accounts and external access were securely managed and monitored.

Reduced risk of leaks or breaches.

Teams and external partners accessed shared resources securely and efficiently, enhancing productivity.

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.

2nd Biggest payroll database in the world

Brazilian Gov Data Processor **reduced over 97% of unauthorized access**

Client under NDA

Situation

- Multi region distributes;
- 3 huge data center with more than 6K devices to store and process critical social security;
- Payroll data from more than 90 million Brazilian citizens;
- Fixed local password;
- Indiscriminate privileged access from almost any IT device;
- No privileged access recording.

Problem

Shared secrets caused malicious user to act without accountability;

It was impossible to define a security perimeter;

Did not allow security accountability and didn't inhibit attackers;

Their simple authentication method made it easy to impersonate another person.

Solution

We've isolated devices access with secure gw with high availability and disaster recovery;

We recorded all sessions with Segura®'s cluster security gateway with multi factor authentication trough hardware certificate token;

With our user behavior mechanist integrated to SIEM and access integrated to ITSM tool alert behavior deviation

Automated password rotation job avoid password sharing.

Results

+96% Reduction of local static passwords;

+1.1K users lost direct access to infrastructure;

+300 privileged sessions recorded and stored per day;

+Real time user behavior integrated to SIEM (IBM);

Customer could eliminate more than 97% of unauthorized access.

Large Medical Diagnose Company

220+ service centers with 10.000+ employees

GrupoFleury

Client under NDA

Situation

- Healthcare giant processes 75 million clinical exams per year
- Complex infrastructure
  - 2,000 unmanaged devices
  - 1,500 critical servers
  - 500 databases
- 1,500 local domain credentials unmanaged and unprotected
- Configuration files and code contained hardcoded unprotected credentials

Problem

Ransomware attacks causes data loss and downtime, which affects its operation and business continuity;

Unmanaged privileged credentials and lack of traceability increase detection and response time for security incidents;

Client was victim of a ransomware attack, which affected its systems and stopped exam delivery for seven days;

No visibility of actions performed through privileged credentials.

Solution

500 people use Segura® in the organization to perform privileged access on critical assets;

Segura® was implemented in only 3 days on a 3-node High Availability/Disaster Recovery architecture using a Cloud deployment architecture;

Segura®'s best-in-class Discovery feature allowed the scan, discovery and onboard of devices in less than 6 hours
- 1.500 servers
- 100 network assets and workstations;

User Behavior is used to stop any access from unknown origin;

Integration with SIEM for real time alert sending.

Results

100% privileged credentials are now managed through Segura®, allowing full traceability of actions performed in the environment;

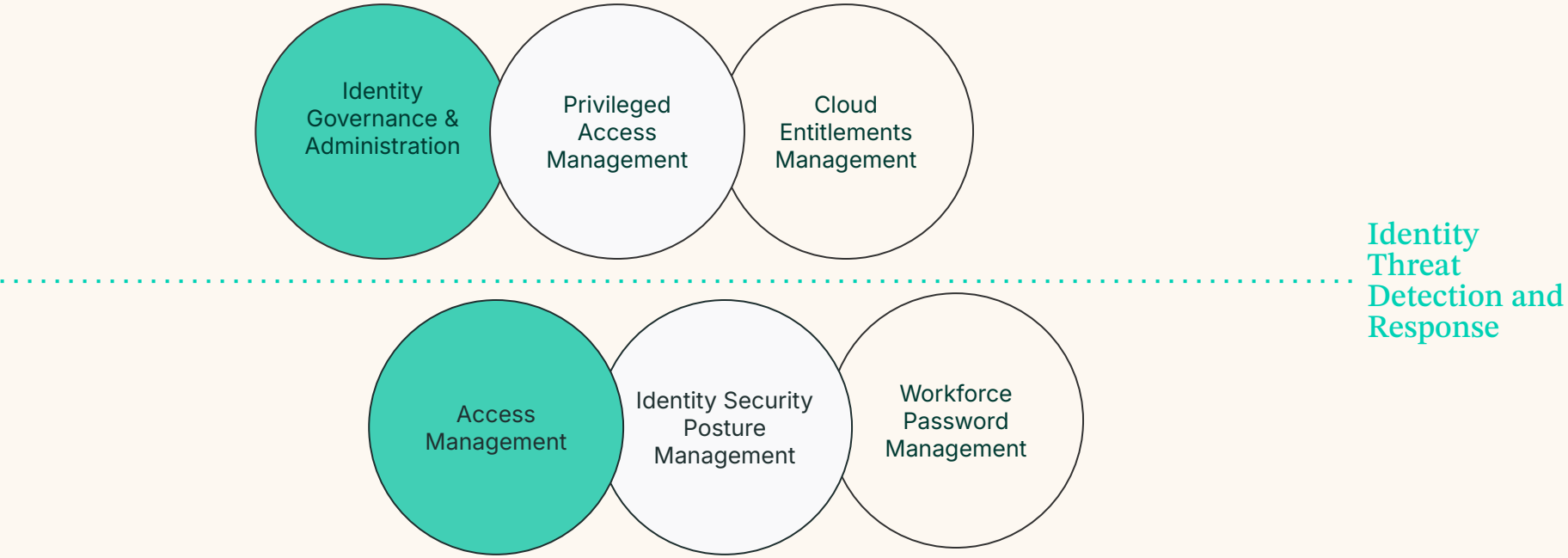
All privileged access is blocked from outside of the PAM solution and is allowed only through Segura® ;

MFA, segregation of access and tiered environment delivers maximum level of security;

Minimum recovery time of the environment.

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 (ITDR)	Attack Path for GCP and Azure	Continuous Identification 2.0	MFA for Privilege Elevation Contextual Access Control	Identity Data Lake for Analytics & Reporting

segura

Summary

Identity Threat Detection and Response

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

Segura's Unified Vision for Identity Threat Detection & Response (ITDR)

Vendor Briefing