Segura® Certificate Manager
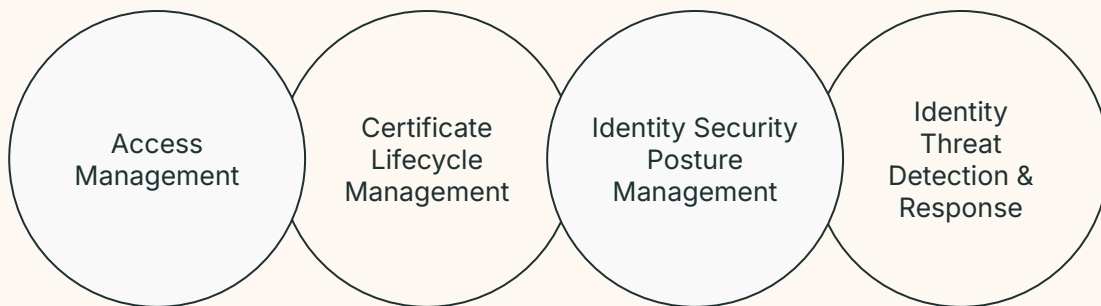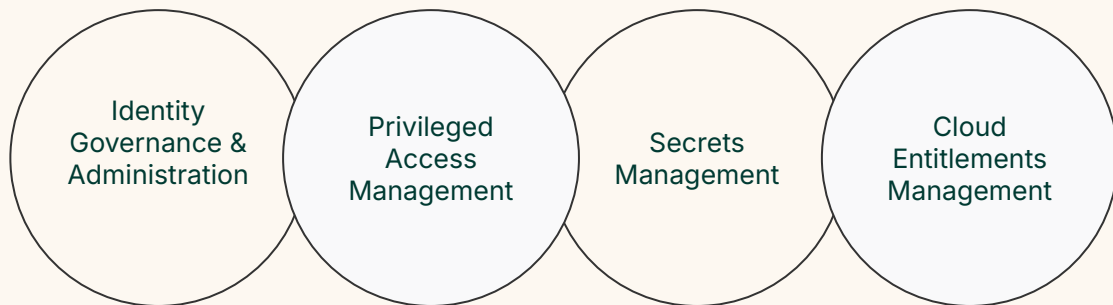
Abril
2025

Our Vision on Machine Identity Management

Our Vision on Machine Identity Management

Identity Governance & Administration

Privileged Access Management

Secrets Management

Cloud Entitlements Management

Machine Identity Management

Access Management

Certificate Lifecycle Management

Identity Security Posture Management

Identity Threat Detection & Response

Our Vision on Machine Identity Management

Discover

→

Govern

→

Automate

→

Management

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

Best Practices
Ownership
Policy Enforcement
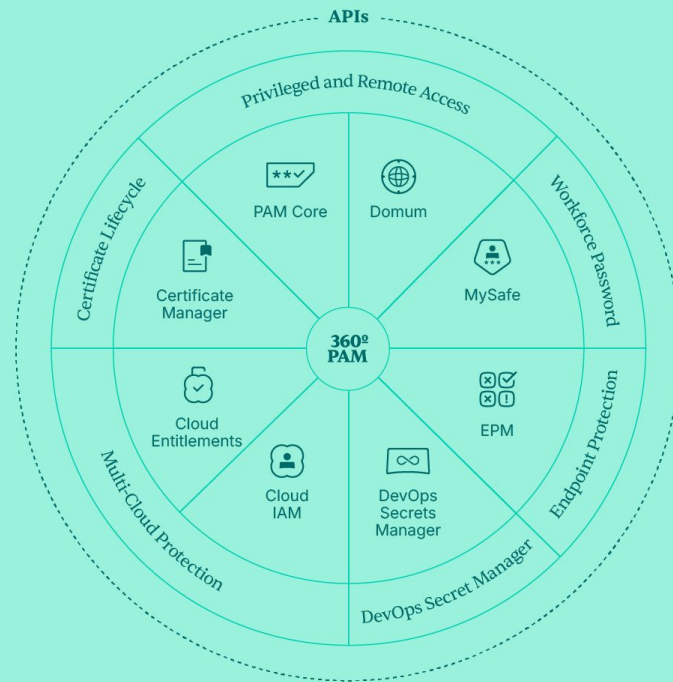Access Control
Traceability
Access Review
Compliance

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

Enhance Security
Hygiene
Least Privilege
Cleanup
Security Posture
ITDR & Behavior

# Our Vision on Machine Identity Management

SaaS | Hybrid | On-premises

segura®

segura.security

Certificate Lifecycle Management

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

Automatize the Management of digital certificates

DISCOVERY · ALERTS DUE DATES · PUBLISH · RENEW
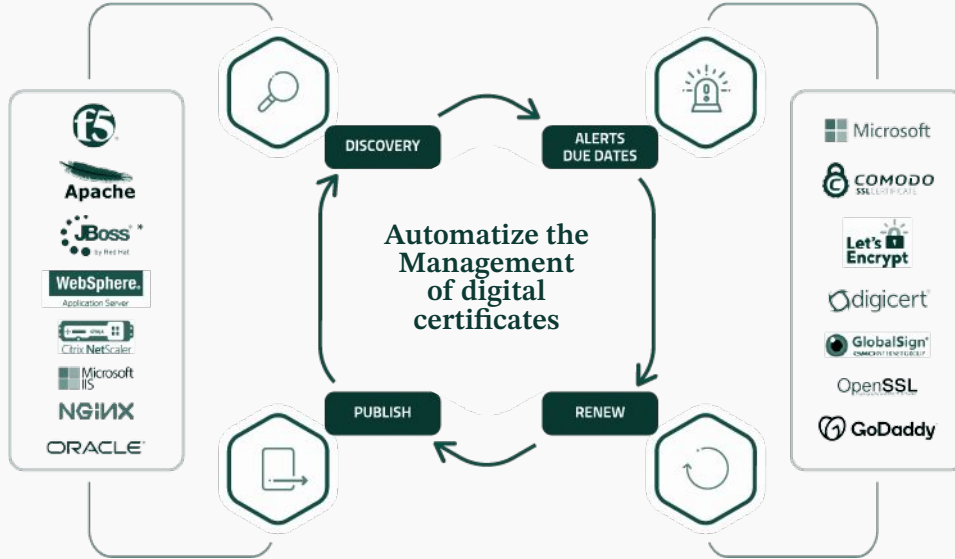
Problem

Control certificate usage, expiration and security requirements.

Solution

Throughout the PAM integration process, Segura® manages the entire certificate lifecycle, from discovery through expiration to automatic renewal and republishing.

Impact

Reduce business outages and bring efficiency and security to higher standards.

Customer Cases

![SF FIRE CREDIT UNION logo]

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.

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.

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 European Telecom

Serves over 110k customers in over 3,200 cities

Telefonica

Client under NDA

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.

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

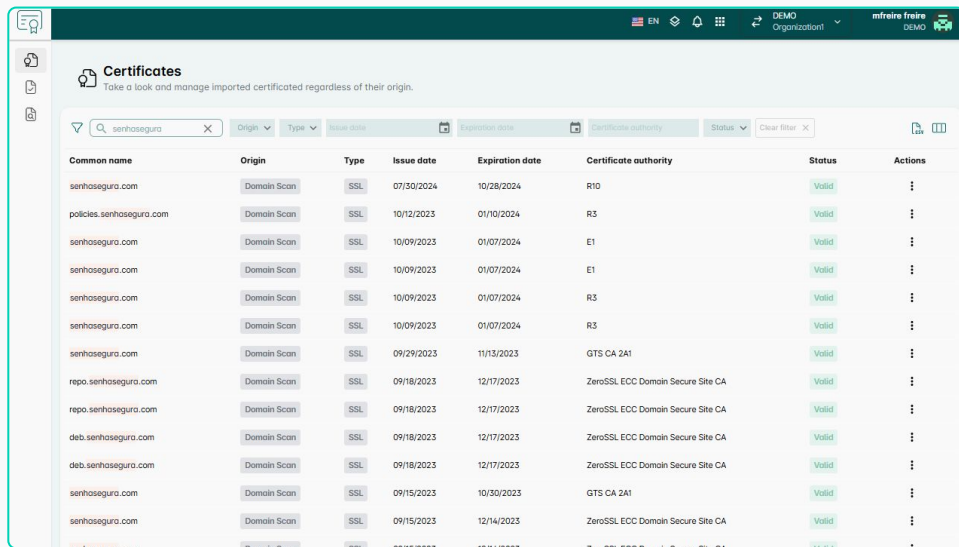Greater visibility and governance, increased security levels, and improved regulatory compliance with security standards.

🎋 segura®

Roadmap

Manage personal certificates on the workstation

Support Auto Enrollment Protocol

New CLM

Cloud-native certificate management with domain discovery, automated alerts, and full audit tracking for security and compliance.

Build With Us
This first version will be available for free for Early Adopters that wants to Build With Us. Request Participation Here.

segura®

Domain Discovery
Monitors domains and automatically imports all associated public certificates.

Notifications
Alerts users about expirations and critical certificate events.

Dashboard
Provides a unified, real-time view of certificate status, alerts, and domain insights, enabling quick and proactive management.

Auditing
Logs all certificate activities for compliance and security oversight.

SaaS
Eliminates the need for on-premise infrastructure, offering automatic updates, scalability, and secure, cloud-based certificate management accessible from anywhere.

Segura® Certificate Manager

Vendor Briefing