CASE STUDY

senhasegura

Leading PAM, simply. For you.
senhasegura.com

Largest Latam E-Commerce

(1,6 U$ BILLION REVENUE)

Enabled DevSecOps at largest LATAM e-commerce company

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.

Solution

Integrate senhasegura to DevOps pipeline with gitlab, kubernetes to scan discovery applications, access keys hardcoded and rotate it during deploy.

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

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.**

+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.

Request a trial demonstration and discover the benefits of senhasegura for your company!

Request a Demo