



SECRAILS

[Home](#)

[About](#)

[Platform](#)

[Demo](#)

[Page 01](#)

Introduction to Secrails

Build Rails, Not Gates

[Start](#)

hi@secrails.com

-

Copyright © 2025 Secrails all rights reserved

Enterprise-Grade Cloud Security, Made Simple.

**#ACCESSIBLE TO
BUSINESS OF ALL SIZES**



CLOUD SECURE POSTURE MANAGEMENT

Secrails is a Cloud Security Posture Management (CSPM) platform that helps businesses analyze, detect, and remediate misconfigurations and vulnerabilities across multi-cloud environments (AWS, Azure, Google Cloud, Oracle) through continuous monitoring in near real time.

We enable users to track the security posture of their cloud resources by collecting an inventory of cloud assets across regions and providers. Providing full visibility into cloud infrastructure, identifying security gaps, assessing risks, and aligning with compliance frameworks like ISO 27001, GDPR, CIS, NIS2, SOC2, PCI-DSS, HIPAA and more.

Secrails proactively prevents security issues with Policy-as-Code by integrating into CI/CD pipelines to catch misconfigurations before deployment. With advanced threat detection, automated security posture assessments, and real-time reporting, Secrails ensures businesses stay protected, compliant, and resilient against cyber threats.



The problem



<90% of SMBs state that cybersecurity issues would severely impact their business within a week, with 57% risking bankruptcy or closure>

EUROPEAN UNION AGENCY
FOR CIBERSECURITY

**Adapted*



COMPANIES ARE FACING THE **HIGHEST NUMBER** OF DATA BREACHES AND **CYBERATTACKS** IN DECADES.



SMBS FACE ENTERPRISE-LEVEL THREATS BUT **LACK RESOURCES** AND DEAL WITH **CONFUSING PRICING PLANS**.



RAPIDLY **GROWING COMPLIANCE REQUIREMENTS** ARE DIFFICULT TO FOLLOW, ASSESS AND MEET.



EXISTING TOOLS ARE COMPLEX AND DIFFICULT TO USE. ONLY BUILT FOR LARGE ENTERPRISES.



KNOWLEDGE GAPS AS MOST OF THE COMPANIES LACK EXPERT AND DEDICATED SECURITY TEAMS.



The Solution

**CLOUD SECURITY ACCESSIBLE
TO BUSINESS OF ALL SIZE**

**A USER FRIENDLY
ALL-IN-ONE PLATFORM**

EXPLORE IN THE NEXT SLIDES

ADDRESS AND OVERCAME YOUR BUSINESS CLOUD SECURITY CHALLENGES

COMPREHENSIVE PROTECTION AGAINST EVOLVING THREATS

KEEPING UP WITH RAPIDLY CHANGING CYBERSECURITY RISKS IS CHALLENGING. PROTECT YOUR CLOUD ENVIRONMENT WITH CUTTING-EDGE SECURITY MECHANISMS THAT ADAPT TO EMERGING THREATS.

SIMPLIFIED COMPLIANCE FOR COMPLEX REGULATIONS

NAVIGATING DYNAMIC SECURITY REGULATIONS CAN BE OVERWHELMING. ENSURE SEAMLESS ALIGNMENT WITH INTERNATIONAL STANDARDS LIKE ISO 27001, GDPR, NIS2, SOC2, CIS, PCI-DSS AND MORE TO STAY AHEAD OF COMPLIANCE REQUIREMENTS.

UNBEATABLE VALUE ACCESSIBLE TO EVERYONE

MOST SECURITY TOOLS ARE BUILT FOR LARGE ENTERPRISES, BUT WE OFFER ENTERPRISE-GRADE PROTECTION DESIGNED TO FIT ANY BUDGET. GAIN ROBUST SECURITY AND COMPLIANCE AT A FRACTION OF THE TRADITIONAL COST.



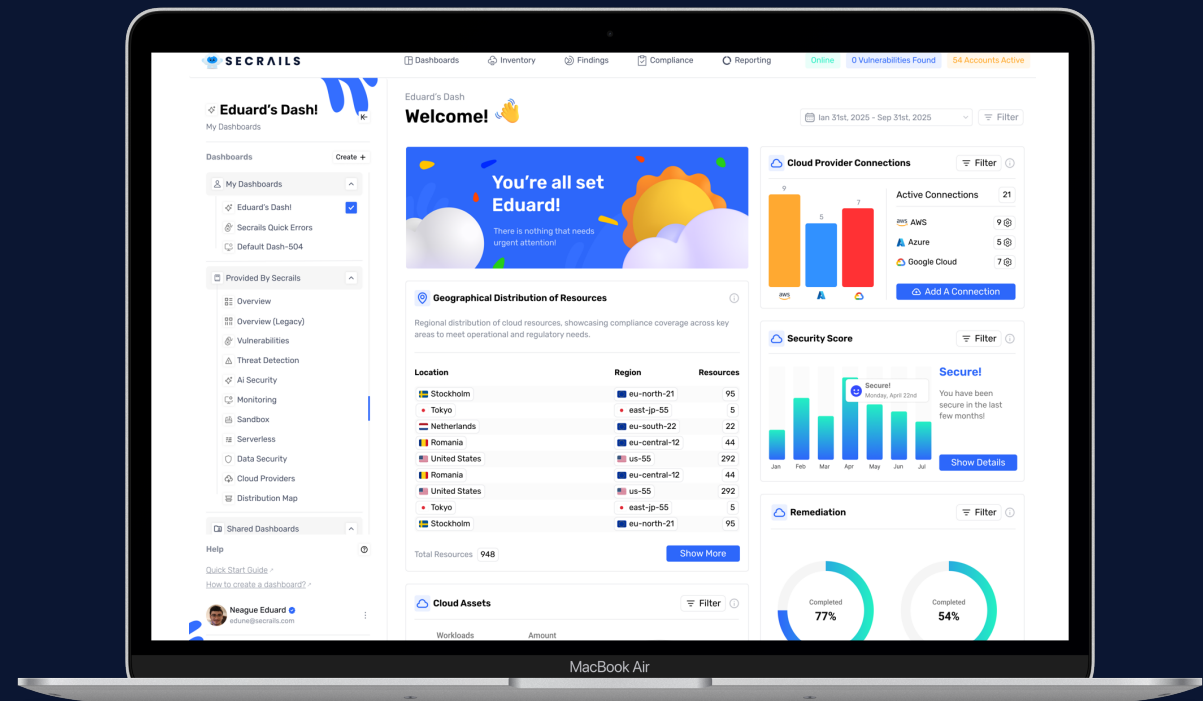
“**A COMPREHENSIVE CLOUD
CYBERSECURITY SOLUTION**”

CLOUD SECURITY**VULNERABILITY MANAGEMENT****CODE SECURITY****COMPLIANCE**

About Secrails

Secrails is a cybersecurity solutions provider specializing in end-to-end application security for modern cloud infrastructures. By combining automated threat detection, compliance monitoring, and streamlined remediation workflows, Secrails empowers organizations to identify vulnerabilities and misconfigurations faster, maintain regulatory compliance, and protect critical data in an ever-evolving cyber landscape.

Discover Our Platform



EXPLORE OUR FUNCTIONALITIES IN THE NEXT SLIDES



MULTICLOUD



DASHBOARDS



INVENTORY



FINDINGS



COMPLIANCE



REPORTING



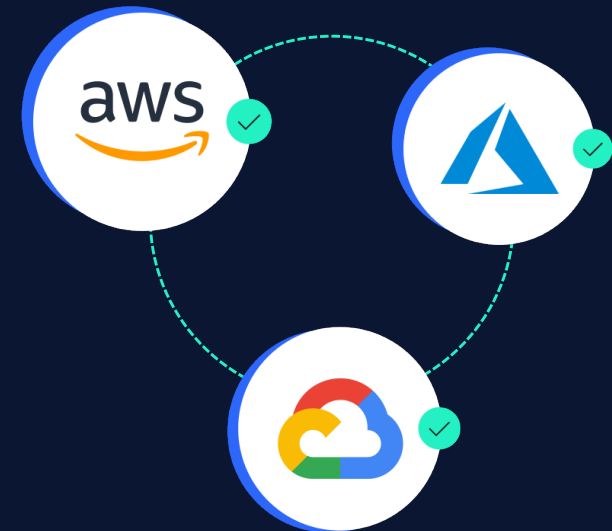
MULTI-CLOUD MULTI-REGION INTEGRATION



Seamlessly integrate with any provider across all regions, ensuring comprehensive asset visibility for proactive security management.

AWS, MS Azure, Google Cloud

...and more



DASHBOARD

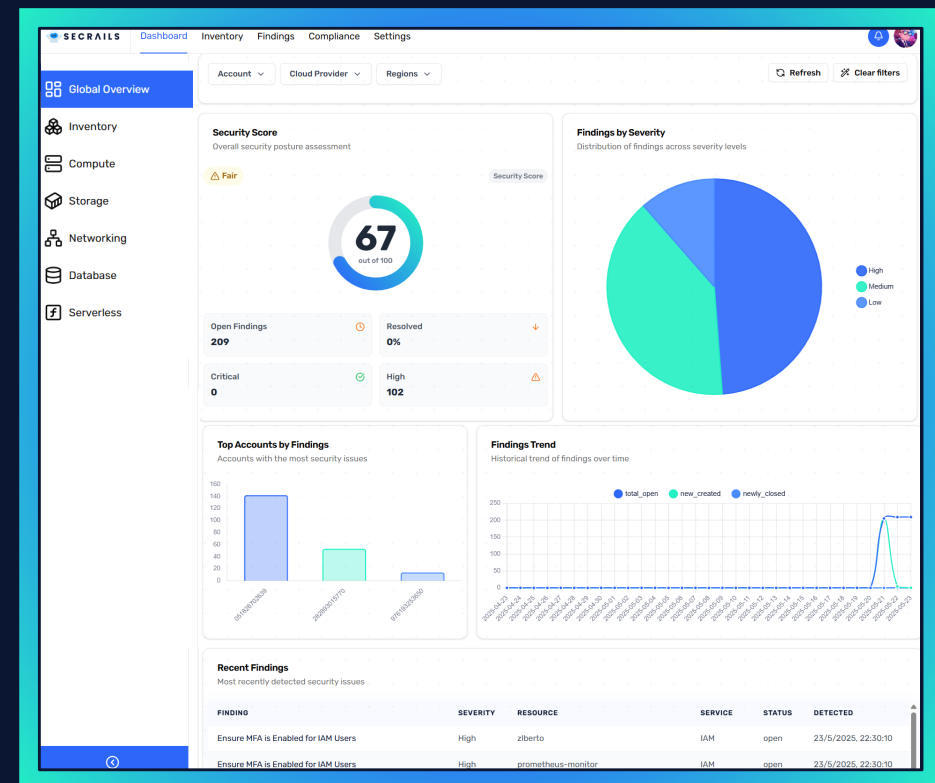


UNIFIED SECURITY, INFORMATION AT A GLANCE

Gain near real-time visibility into your entire cloud security posture. Monitor misconfigurations, compliance status, risk trends, and assets across all environments — all from a single, intuitive dashboard.

Security Score

Get an **instant overview** with our platform about your security posture. Quickly understand your cloud security posture with a **single, easy-to-read score**.



INVENTORY



You can't protect
what you can't see

Centralized asset
management providing
full visibility of cloud
resources to enhance
security and control.

The screenshot shows the 'Inventory Dashboard' interface. At the top, there's a search bar and several filter dropdowns: 'Accounts', 'Service Providers', 'Regions', 'Resource Types', and 'Service Names'. Below the filters, there's a 'Clear Filters' button and a '10 Results' indicator. The main content is a table with the following columns: 'Resource Type', 'Resources Count', 'Accounts', and 'Type'. The table lists several AWS resources:

Resource Type	Resources Count	Accounts	Type
AWS::ACM::Certificate Security & Compliance	2	2 Accounts	aws
DynamoDB Table Databases	8	2 Accounts	aws
EC2 Instance Compute	2	2 Accounts	aws
EC2 Security Group Networking & Content Delivery	13	2 Accounts	aws
EC2 Subnet Networking & Content Delivery	12	2 Accounts	aws
EC2 VPC	3	2 Accounts	aws

FINDINGS



IDENTIFY, PRIORITIZE, REMEDIATE

Our platform applies security rules aligned with the most important compliance frameworks to detect misconfigurations that could lead to vulnerabilities. Ensuring your resources are configured according to best security practices with over +1000 rules.

Type of finding

By identifying and addressing different types of findings, **organizations** can significantly **reduce their security risks**, improve compliance, and enhance the overall integrity of their cloud environment.



Severity

Our platform categorizes cloud security findings by severity, from low to critical, enabling teams to **prioritize high-risk vulnerabilities** and address the most urgent security threats first. This ensures prompt remediation and **minimizes potential risks** to your cloud environment.

Remediation Guidance


For every finding, our platform provides clear remediation steps, enabling teams to **take action immediately** and reduce potential security breaches before they occur.



[Inventory](#) [Findings](#) [Settings](#)

































Cloud Security Posture Management

Accounts ▾ Regions ▾ Service Providers ▾ Severities ▾

 Clear Filters

10 Results  

Finding Type (Control)	Total Issues	Risks	Severity
 EC2 Instances Should Require IMDSv2 Compute Security	1 	1 Accounts	  
 EC2 Instances Should Have Detailed Monitoring Enabled Compute Security, Monitoring and Logging, Operational Security	1 	1 Accounts	  
 EC2 Instances Should Not Be Assigned Public IP Addresses Compute Security, Network Security	1 	1 Accounts	  
 Lambda Functions Should Set Reserved Concurrency Compute Security, Operational Security, Cost Management and Optimization	18 	1 Accounts	  
 Lambda Functions Should Use a Dead-Letter Queue for Asynchronous Invocations Compute Security, Operational Security, Reliability	18 	1 Accounts	  
 Lambda Function Settings Check Compute Security, Configuration Management	18 	1 Accounts	  

Load More

COMPLIANCE



STAY ON TOP OF REGULATIONS, PROVE COMPLIANCE IN REAL TIME

Elevate your organization's ability to meet regulatory requirements, industry specific standards and security best practices by centralizing, automating, and scaling compliance across multiple frameworks—all in one streamlined solution.



Audit Readiness

Maintain up-to-date records of security policies, incident response procedures, and system configurations. Easily export compliance status and relevant documentation to expedite audit processes and reduce disruptions.

Customer and Stakeholder Confidence

Reassure customers, investors, and partners with transparent, robust compliance management. Gain a competitive edge in sectors where data privacy and security are paramount.

REPORTING



ACTIONABLE INSIGHTS

Transform raw security data into strategic intelligence and empower decision-makers at every level of your organization. With our Advanced Cloud Security Reporting, you'll translate findings into meaningful action.

Compliance focused

Generate **framework-specific reports** for GDPR, ISO 27001, NIS2 and other regulations. Track progress, pinpoint gaps, and streamline audits with ready-to-present compliance documentation.

Automate

Schedule recurring reports to stay on top of regular security reviews **or generate on-demand** assessments for impromptu audits. Export them in multiple formats—PDF, CSV, XLSX—for effortless sharing and collaboration with reporting line managers, SecOps teams, CISO, CTO and more.

Analytics

Track security **improvements over time** through historical data analysis. Predict potential future vulnerabilities based on current trends and measure the **effectiveness of ongoing security initiatives**.

CNAPP Coming soon!

FROM CODE TO CLOUD, WE SECURE EVERY STEP

Integrating our Cloud Native Application Protection Platform you will cover the full software development lifecycle –secure your infrastructure, containers, and code with confidence in one platform.

Policy as code

Safeguard your **Infrastructure-as-Code** environment by detecting and addressing misconfigurations early, securing each update from the start.

Static Code Analysis

Integrate our platform with your GitHub or GitLab repositories to **detect vulnerabilities** preventing security issues **before they reach production**.

Container Security

Strengthen your containerized environments with in-depth image scanning, pinpointing vulnerabilities early for comprehensive security from development to deployment.

WHAT MAKE US DIFFERENT?



With years of experience in the cloud security industry, I've seen firsthand how small and medium businesses are priced out of essential protections. That's why we've made it our mission to democratize access to powerful innovative cybersecurity solutions—because security should never be out of reach. We offer an enterprise-grade security solution accessible for businesses of all sizes, providing comprehensive protection fully aligned with compliance frameworks.

Alberto Ureña,
Founder of Secrails



ALL-IN-ONE SECURITY SOLUTION

Including integration with multi-cloud environments across all regions, code security, vulnerability management and cloud security.



ENTERPRISE GRADE LEVEL COMPLIANCE

+1,000 compliance rules, ensuring audit-readiness and adherence to key security frameworks like the Fortune 500 companies.



SCALABLE PRICING FOR EVERYONE

Scalable simple pricing designed for SMBs and large enterprises, making cloud security accessible to all.



COMPREHENSIVE CYBERSECURITY

From Code to Cloud. Prevent, detect, remediate, and monitor threats throughout the entire software development lifecycle (SDLC).



Don't wait for a
Cyberattack to
Jeopardize your
business

[Book a demo](#)

Stay Secure,
Stay Compliant,
Stay Ahead

Contact

sebi@secrails.com



<https://secrails.com/>



SECRAILS

[Home](#)

[About](#)

[Platform](#)

[Demo](#)

Page 18

Thank You

hi@secrails.com

-

Copyright © 2025 Secrails all rights reserved