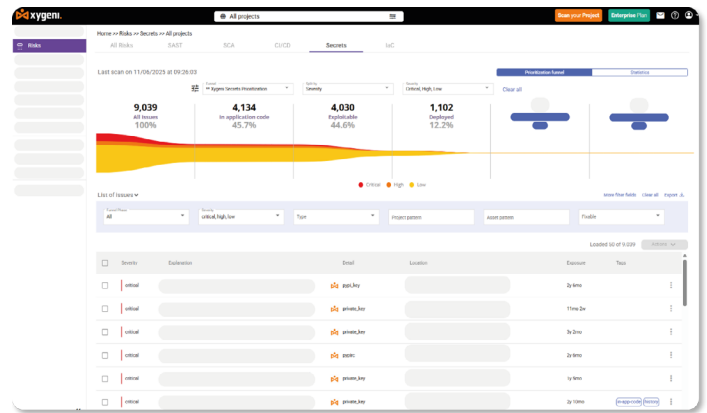


Block Secrets Leakage at All Stages of Development

Xygeni Secrets Security scans every stage of your SDLC to catch exposed credentials before they spread. With an **exploitability based prioritization funnel**, **instant revocation**, and **auto-remediation**, you stay ahead of leaks without slowing down development.



About Company

Xygeni is an **All-in-One Application Security Platform** built to protect every stage of the software development lifecycle. We offer complete control over application risks, a unified security view from code to cloud, and eliminate noise to prioritize risks effectively. Our advanced malware detection and early warning system makes Xygeni a leader in protecting applications from emerging threats, ensuring rapid and secure software delivery.

Xygeni Secrets Security **stops exposed credentials** like API keys, tokens, and passwords **at every stage of the SDLC**. It combines a smart exploitability prioritization funnel, instant revocation, and seamless remediation to secure your workflow without slowing development.

In 2024, GitHub reported over **39 million leaked secrets**, with **23.8 million found in public repositories**. That's a **25 percent increase** from the previous year. Even more concerning, **70 percent of those secrets remained active after exposure**. Detection alone is not enough. Xygeni ensures action happens immediately, keeping secrets protected and teams moving forward.

\$4.88m
was the global
average cost of a
data breach last
year
IBM






Secure Every Code Stage

Scan early. Detect everywhere.

Xygeni **scans every layer of your software development lifecycle to detect hardcoded secrets** before they're pushed, merged, or deployed. From local development to production pipelines, you get full visibility into exposed secrets across files, containers, and repositories.

Whether hidden in a recent commit or buried in Git history, our solution **catches secrets at the source** and blocks them before damage is done.

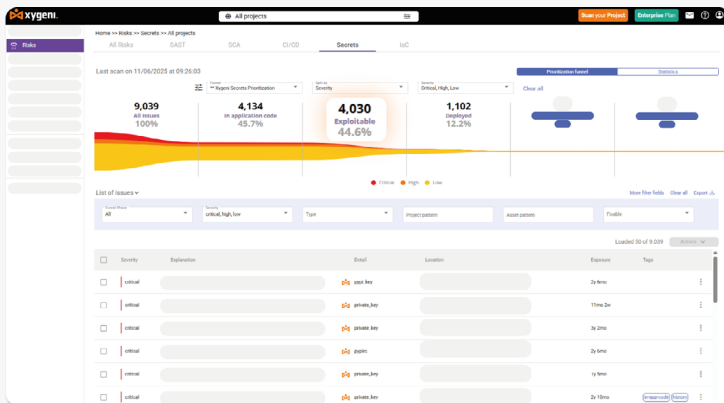
Capabilities Include:

-  **Detection of Committed Secrets** Identify secrets already in your repositories, at both repository and organization level.
-  **Pre-Commit Secret Blocking:** Prevent secrets from being added to your repositories.
-  **Comprehensive Git History Scanning:** Examine your repository's entire git history for hidden secrets.
-  **Secret Validation:** Confirm the validation status of secrets to ensure they grant access or authentication.
-  **Docker images scanning:** Identify secrets in your docker images.

Works with your stack: Language-agnostic. Git-native. Seamless integration with GitHub, GitLab, Bitbucket, Jenkins, and more.

Visibility and Prioritization at Scale

Cut through the noise. Act on what matters.



Xygeni Secrets Security turns raw detection into clear, actionable intelligence. It gives security and engineering teams **full visibility** into where secrets are exposed, how critical they are, and whether they can actually be exploited.

At the core of this process is the **exploitability funnel** a prioritization model that filters findings based on factors like location, frequency, secret type, and validation status. **Verified, active,** and high-impact secrets rise to the top, while duplicates, test values, and inactive items are deprioritized automatically.

What you get:

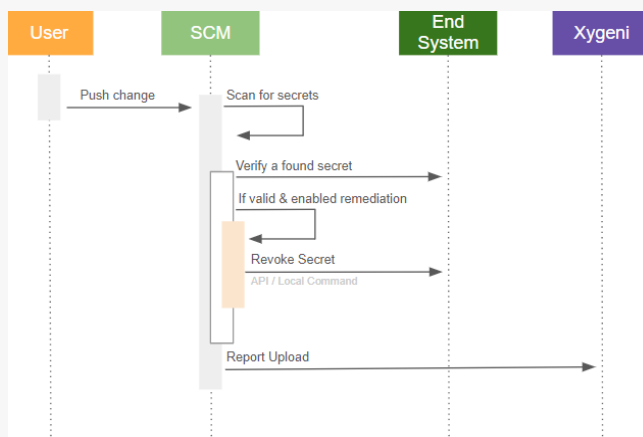
- A **centralized dashboard** to manage secrets across all projects.
- **Funnel-phase filtering:** in-app code, exploitable, deployed, and more.
- **Severity and validation scoring** to surface real threats.
- Clear **differentiation between verified, inactive, or stale secrets.**
- **Custom filters** for faster triage across large repositories.
- **Exportable reports** and **compliance-ready views** for audit and governance

Auto Remediation and Secret Revocation

Stop secret leaks before they escalate

Xygeni doesn't just detect exposed secrets it **revokes them instantly** to reduce risk and prevent misuse. When a hardcoded secret is pushed to a repository, Xygeni verifies its validity and, if remediation is enabled, triggers the appropriate revocation method based on secret type and platform.

Whether it's an AWS key, Google API token, GitLab PAT, or Slack credential, **Xygeni automatically mitigates exposure** using **prebuilt remediation playbooks** all without disrupting development flow.



Key Features:

- **Faster containment:** Revoke live secrets before they're exploited.
- **Automatic threat mitigation:** No human delay, no manual steps.
- **Clear remediation status:** Issues are tagged and tracked as resolved.
- **Adaptable to your environment:** Works across teams, workflows, and services.
- **Clear resolution tracking:** Secrets are tagged as remediated inside the platform

Detect What Others Miss

Xygeni supports 100+ secret types out of the box from API tokens and cloud credentials to webhooks and encrypted keys. Whether embedded in code, configs, containers, or pipelines, our detectors help you catch and manage every kind of secret before it becomes a threat.

1. API Tokens and Keys: GitHub, GitLab, Google API Keys, Azure, Alibaba Cloud, and more.

2. OAuth and Access Tokens: OAuth2 tokens for Facebook, Google, Slack, Atlassian, Bitbucket, etc.

3. Cloud Provider Credentials: AWS, Azure, GCP, IBM Cloud, Tencent Cloud including service account keys.

4. Cryptographic Keys: Private keys in PEM, PPK, and other standard formats.

5. Database and Data Storage Credentials: MySQL, PostgreSQL, Redis, RabbitMQ, LDAP credentials, and more.

6. Webhooks and Embedded Secrets: Slack, Discord, Teams webhooks and high-entropy strings.

7. Miscellaneous Credentials: SSH passwords, SMTP credentials, and secrets in config files like .htpasswd.



End-to-End Secrets Security Across the SDLC

Detect, prevent, and manage exposed credentials across your development pipeline before they become a risk.

- No credit card needed
- Quick setup, instant results

[Start your free trial](#)



Get in touch today!

www.xygeni.io

<https://www.linkedin.com/company/xygeni>

<https://twitter.com/xygeni>