Git Guard AI 4 Stop Secret Leaks Before They Cost Millions

Your AI-Powered IDE Shield Against Credential Leaks

Presented by Future Risers

The Real Threat: Secrets in Code

- **10,000+ API keys leaked daily** on GitHub
- **Accidental commits** of API keys, passwords,
- tokens **Breaches cost enterprises $1.2M** per
- incident **Outdated regex scanners** are insufficient

Introducing GitGuard AI

AI-Powered Real-Time Detection

IDE plugin for immediate secret identification

Smart Alerts + Fix Suggestions

Red highlight and actionable advice

Prevents Pre-Commit Pushes

Stops accidental API pushes before they leave your IDE

LLM-Powered Accuracy

Leverages Novita.ai and Hugging Face for superior detection

GitGuard AI saves up to **$10M+/year** in potential damages by stopping leaks at the source.

Why We Built GitGuard AI: A True Story

Just a few weeks ago, one of our team members made a small mistake that cost him $30k.

He accidentally pushed an API key to a public GitHub repo during a late-night coding session.

Within minutes, bots had picked it up. His account was abused — generating fake requests until his free credits were drained and charges started piling up.

That painful $50 mistake made us realize how vulnerable developers are to such simple errors.

That night, GitGuard AI was born — not just to prevent leaks, but to empower developers with an AI agent that watches your back while you code.

It’s more than a tool — it’s peace of mind.

Why GitGuard AI?

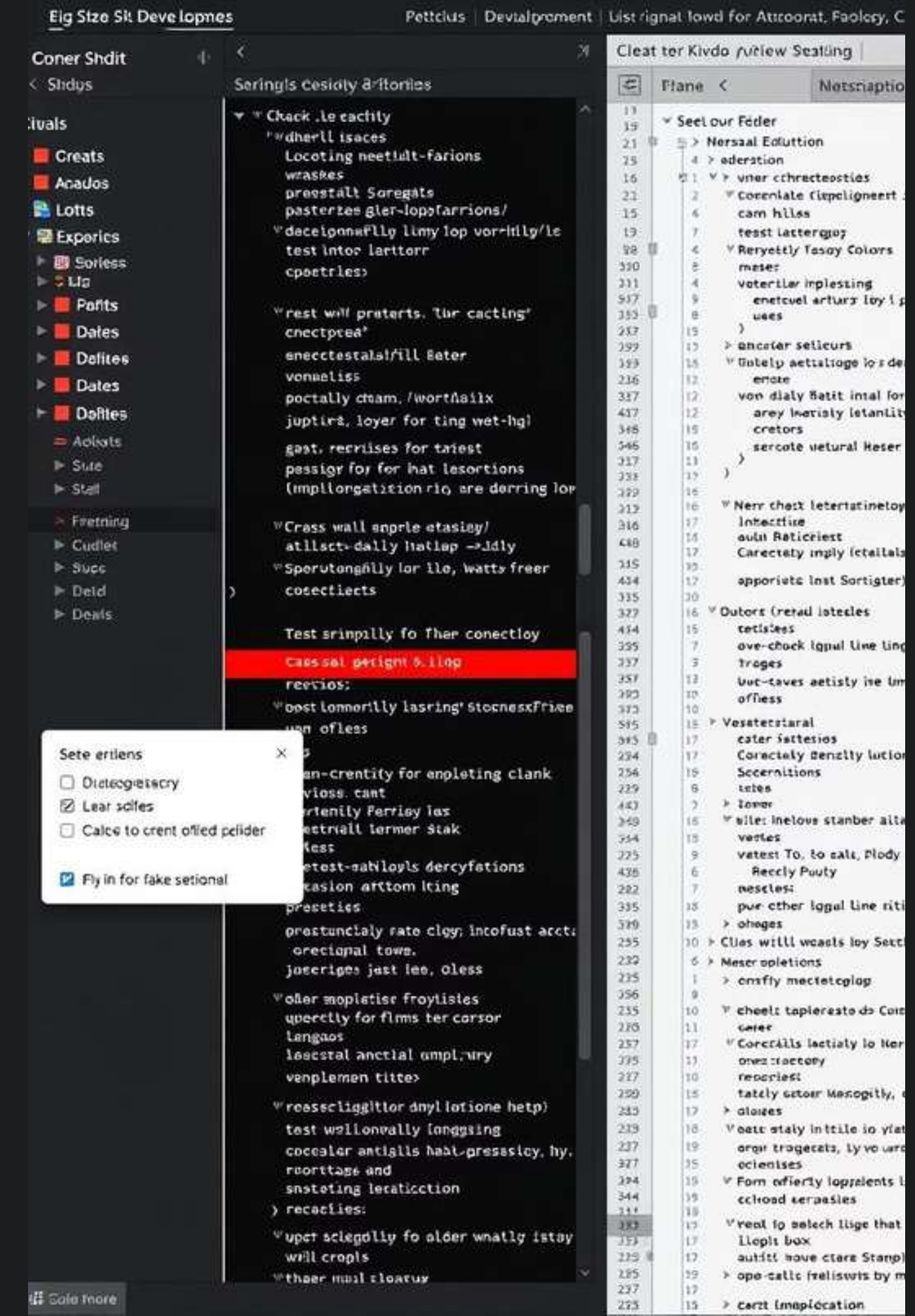
Real-Time Scanning
Instant feedback in your IDE.

LLM-Based Accuracy
Powered by Novita.ai for precision.

Auto Fix Suggestions
Proactive solutions for developers.

Dashboard + DB Logging
Comprehensive secret management with Zilliz DB.

Plus, it includes a **free tier** with no hidden costs and a **Hugging Face fallback** for continuous protection.



Live in Action

Typing Detection

AWS_KEY = "AKIAXYZ123" instantly highlighted red.

Suggested Fix

Guidance: os.getenv("AWS_KEY").

Secure Logging

Secrets stored safely in Zilliz DB.

Fallback Mechanism

Hugging Face model activates if Novita.ai credits deplete.

We just saved a million-dollar mistake!

Tech Stack Overview

Tool	Use Case	Free Tier
Trae AI	IDE + Plugin Host	Hackathon
Novita.ai	Secret detection via LLM patterns	$20 Free Credit
Zilliz DB	Store secret	5GB Free
HuggingFace	Fallback Model API	10kcalls/month
GitHub	Repository	Free
Vercel	Demo Hosting	Free

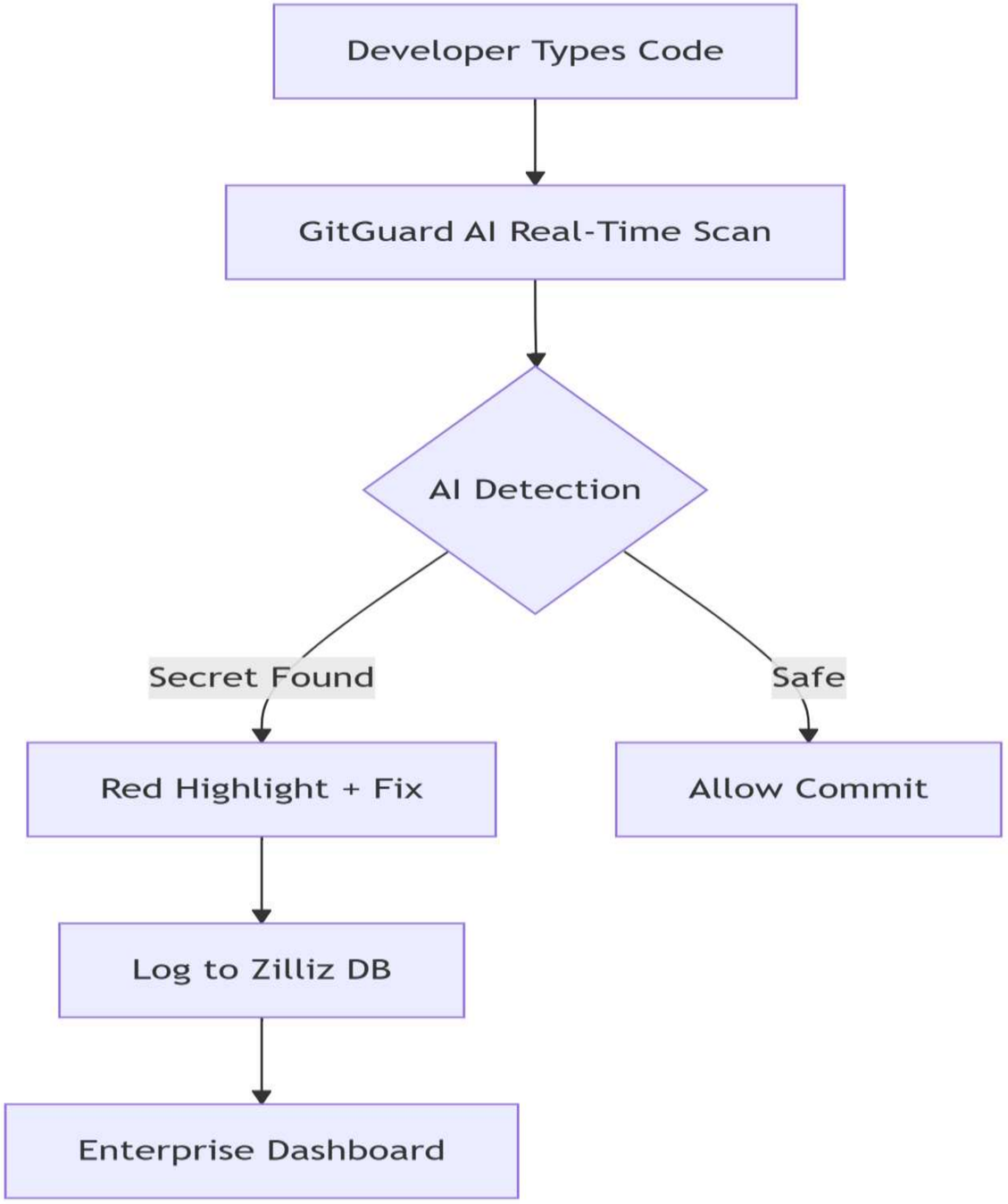
Our robust stack is built on leading technologies, ensuring both performance and cost-effectiveness.

How We Stand Out

Current Security	GitGuardAI
Manual Code Reviews	AI-powered secret detection
Static Code Analysis	Real-time signal reflection
< Static code care	Compressed wave analysis
< Secret Detection	Improved comprehension
Automated desensitization	Vulnerability analysis

Feature	GitGuard AI	GitGuardian	TruffleHog
Real-time IDE	✓	✗	✗
AI-based Detection	✓ (LLMs)	✗ Regex	✗ Regex
Auto Fixing	✓	✗	✗
Free to Start	✓	Limited	Limited
Dashboard + DB	✓	✗	✗

GitGuard AI offers unique, developer-centric features that set us apart from competitors.


Developer Types Code
GitGuard AI Real-Time Scan
AI Detection
Secret Found
Safe
Red Highlight + Fix
Allow Commit
Log to Zilliz DB
Enterprise Dashboard

Why It Matters for Enterprises

Avoid Regulatory Fines
Prevent GDPR & SOC2 penalties.

Protect Reputation
Safeguard company image and developer trust.

Cost-Effective
No dedicated SecOps teams required.

Developer-Level Protection
Proactive security, not post-incident fixes.

Scalable Solution
Fits from startups to large enterprises.

Demonstration

[Click here to check it out]

[To see Live demo check this out]

[To see Our Github Repository]

Meet the Team

Hoang Nguyen
Full stack Engineer

Sajjad Ahmad
AI Developer and Researcher

Danish Mustafa
Agentic AI Engineer

Ye Bhone Lin
AI/ML Engineer

Giovanni Carlos
AI/ML Engineer

Our diverse team combines deep expertise in AI, cybersecurity, and product development.

Key Takeaways & Next Steps

AI-Powered Leak Prevention

Stop credential leaks directly in the IDE.

Significant Cost Savings

Avoid millions in potential breach damages.

Developer-Friendly

Seamless integration and intuitive fixes.

Future Roadmap

Expanding IDE support, advanced LLM models.

We invite you to experience GitGuard AI firsthand. Visit our **Vercel demo** and let's discuss how we can secure your code!

Thanks for your time !!!