GuardOn : Shifting Kubernetes Compliance Left with Developers-First Guardrails
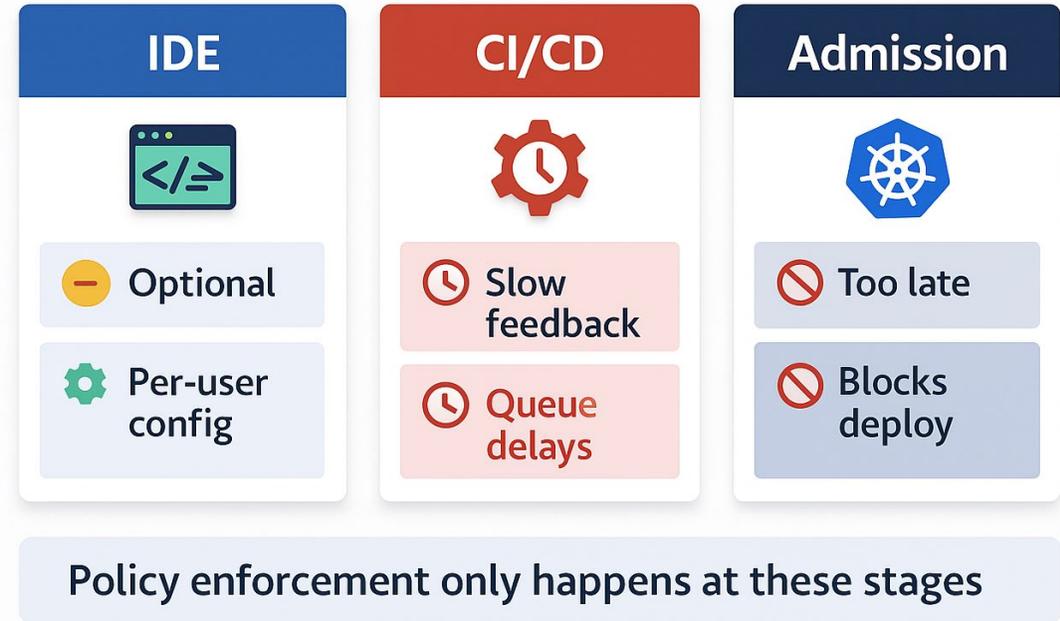
Sajal Nigam

Senior Application Engineer

- Declarative YAML complexity

- Security-sensitive defaults

- Misconfigurations > CVEs

The Problem: **Misconfigurations Are Still Escaping**

Feedback Comes Too Late

Write Code → Commit → ⚙ CI → Deploy → Incident

⚠ **Privileged Container**
Unlimited root access

⚠ **Missing Resource Limits**
Crash risk to other Pods
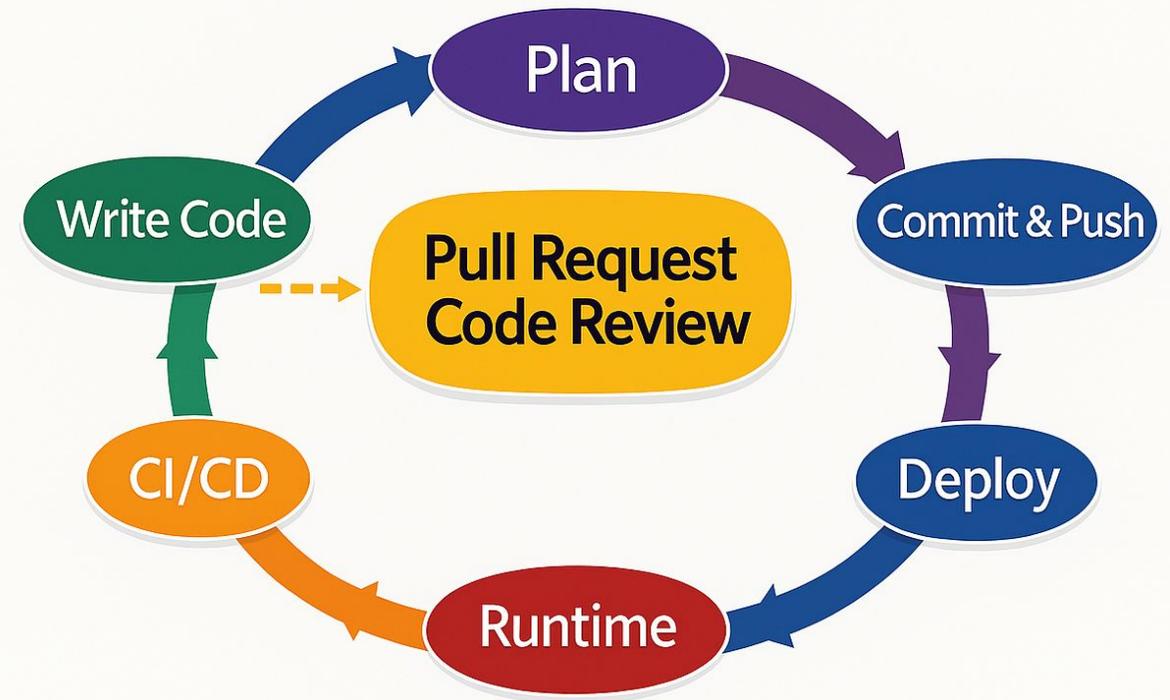
⚠ **Invalid API Version**
Outdated and deprecated
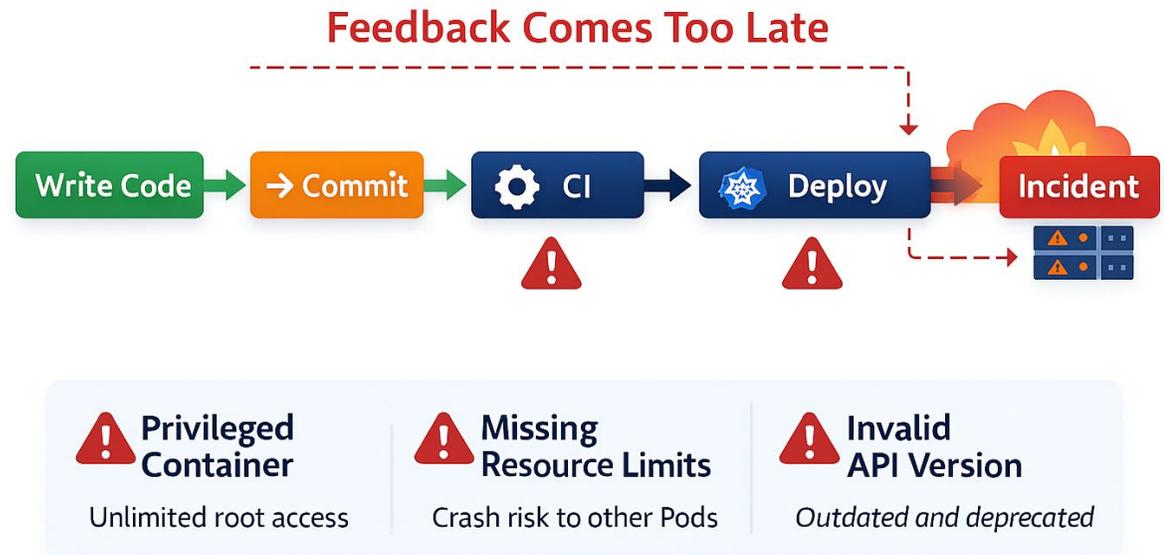
- IDE linters (edit-time)

- CLI & pre-commit (commit-time)

- CI/CD (pipeline-time)

- Admission controllers (deploy-time)

Why Existing Tools Are Not Enough

IDE	CI/CD	Admission
⊖ Optional	🕒 Slow feedback	🚫 Too late
⚙ Per-user config	🕒 Queue delays	🚫 Blocks deploy

Policy enforcement only happens at these stages

- Pull Request review

- Mandatory, collaborative, audited

The Missing Enforcement Point: PR Review

Policy Enforcement Across SDLC

- Edit → Commit → Review → Pipeline → Admission

- GuardOn = Review-Time

Review-Time — GuardOn — Client-Side Browser Extension

Save-Time — IDE-PLUGIN — Individual Config

Build-Time — CI SCANNER — Pipeline Gate

Deploy-Time — ADMISSION CONTROLLER — Cluster Policy

Run-Time — RUNTIME — Pod / Node Enforcement

⚠ Privileged: true

❌ Memory Limits Missing
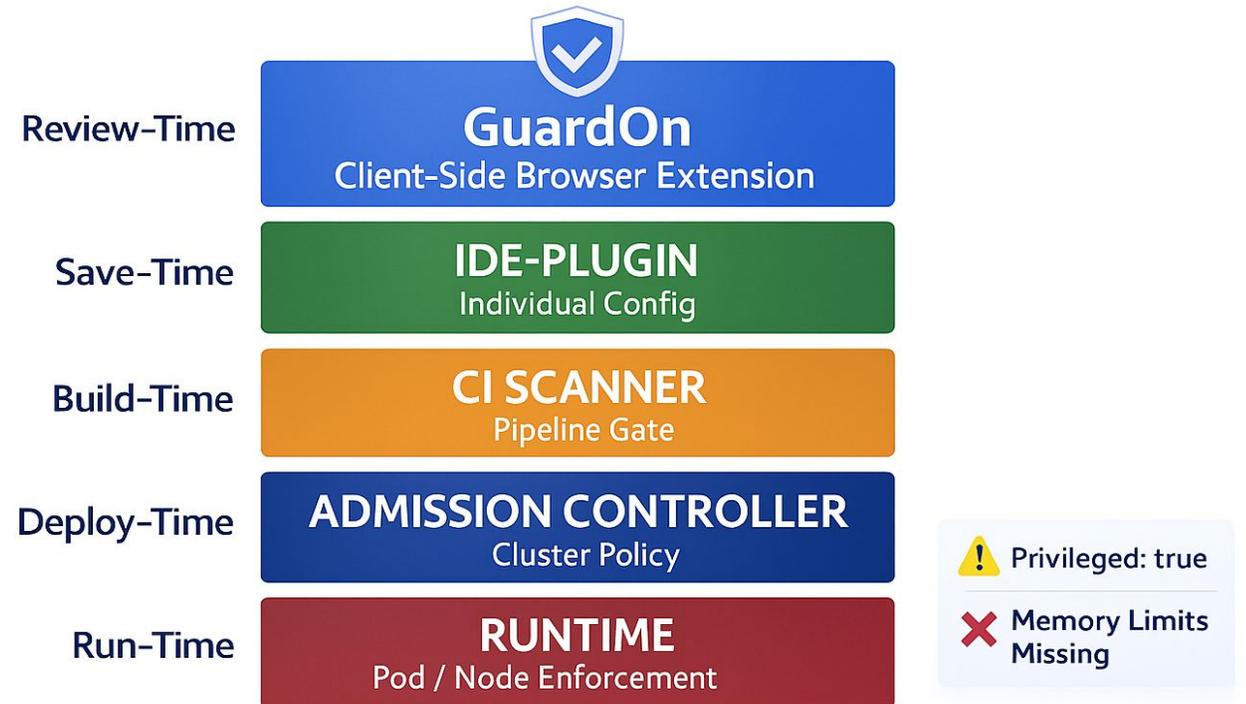
Defense in Depth, GuardOn adds an ealier layer

Why Review-Time Enforcement Matters?

- Zero infrastructure

- Zero drift

- Reviewer-visible
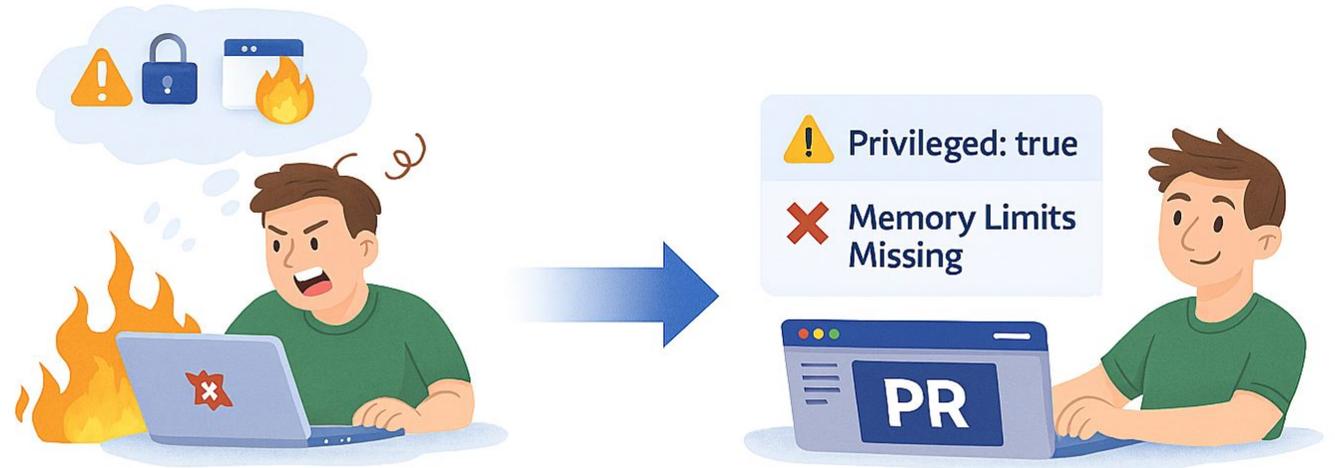
Before GuardOn
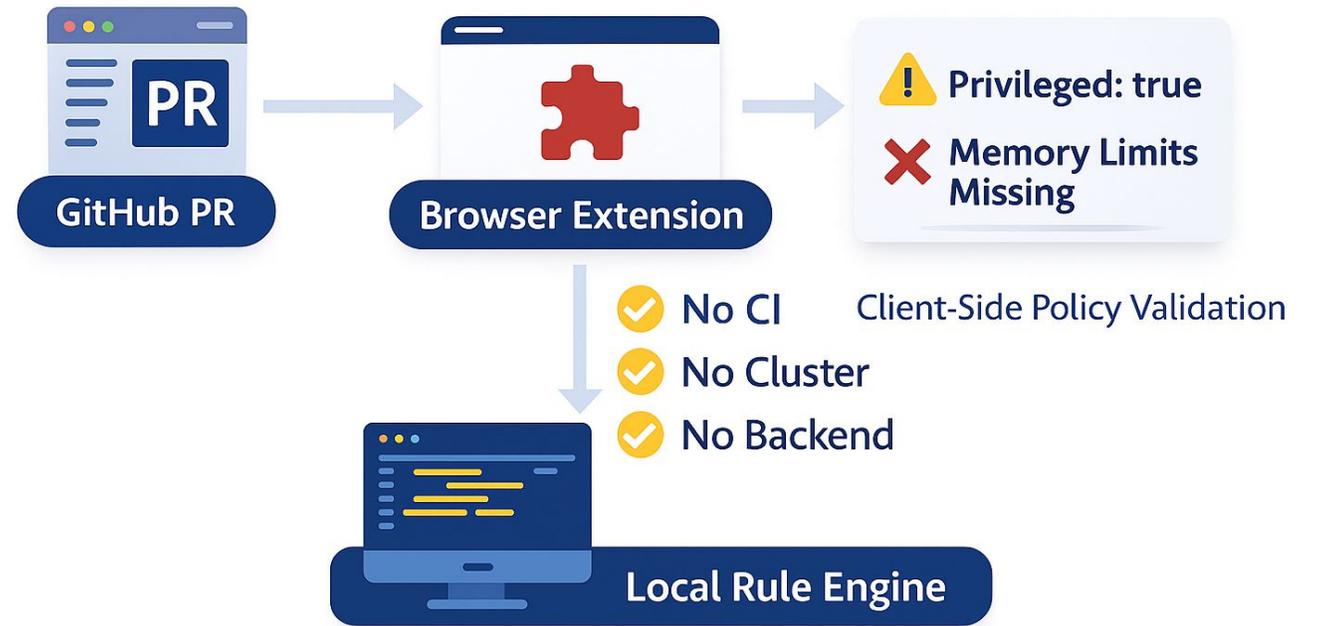
Misconfigurations detected late, during PR merge

With GuardOn

Misconfigurations validated early, during review

- Policy-as-Code inside PRs

- Browser-resident

- No cluster or CI required

GuardOn: Core Idea

GitHub PR → Browser Extension → Privileged: true / Memory Limits Missing

Client-Side Policy Validation

✓ No CI
✓ No Cluster
✓ No Backend

Local Rule Engine

- Content Script

- Background Service Worker

- Core Rule Engine

Client-Side Architecture

Browser Environment

Content Scripts (YAML Extraction)

yaml

Core Rule Engine

Policy Store

- Kyverno
- OPA
- OpenAPI / CRD
- CEL (*future*)

⚠ Privileged: true

❌ Memory Limits Missing
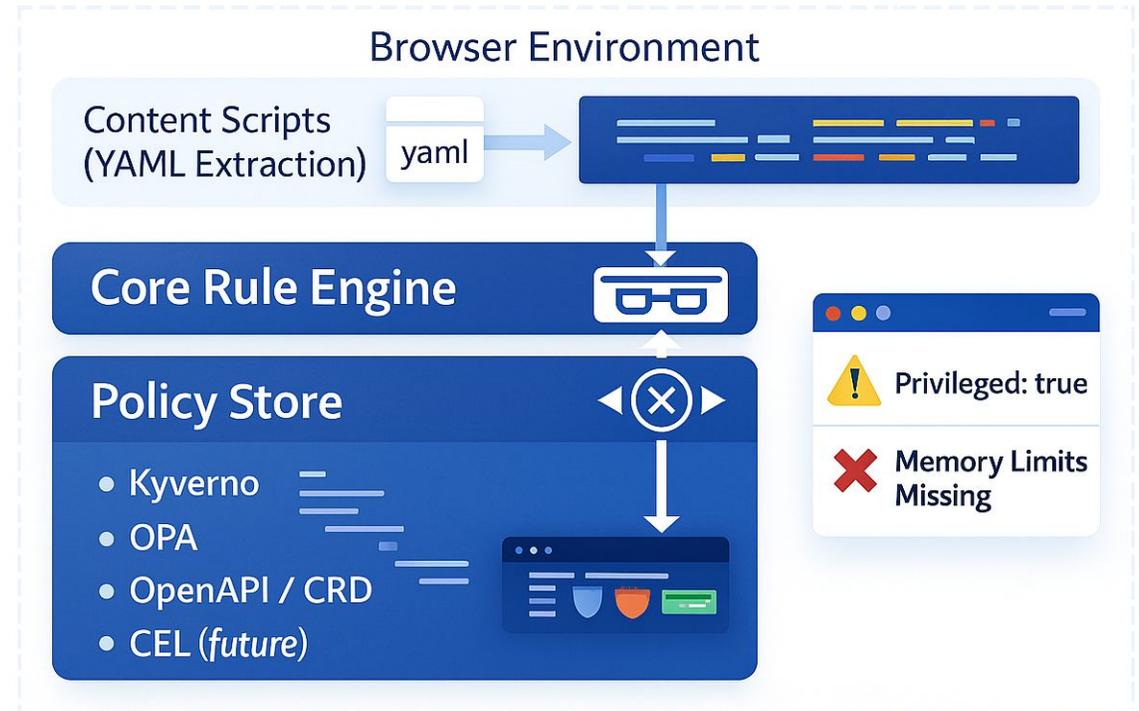
Easy Policy Reuse
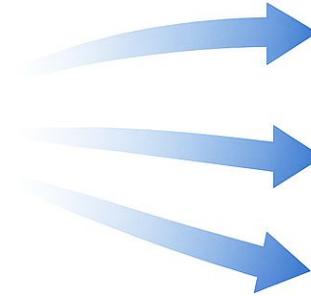
- Native rules

- Kyverno validation import

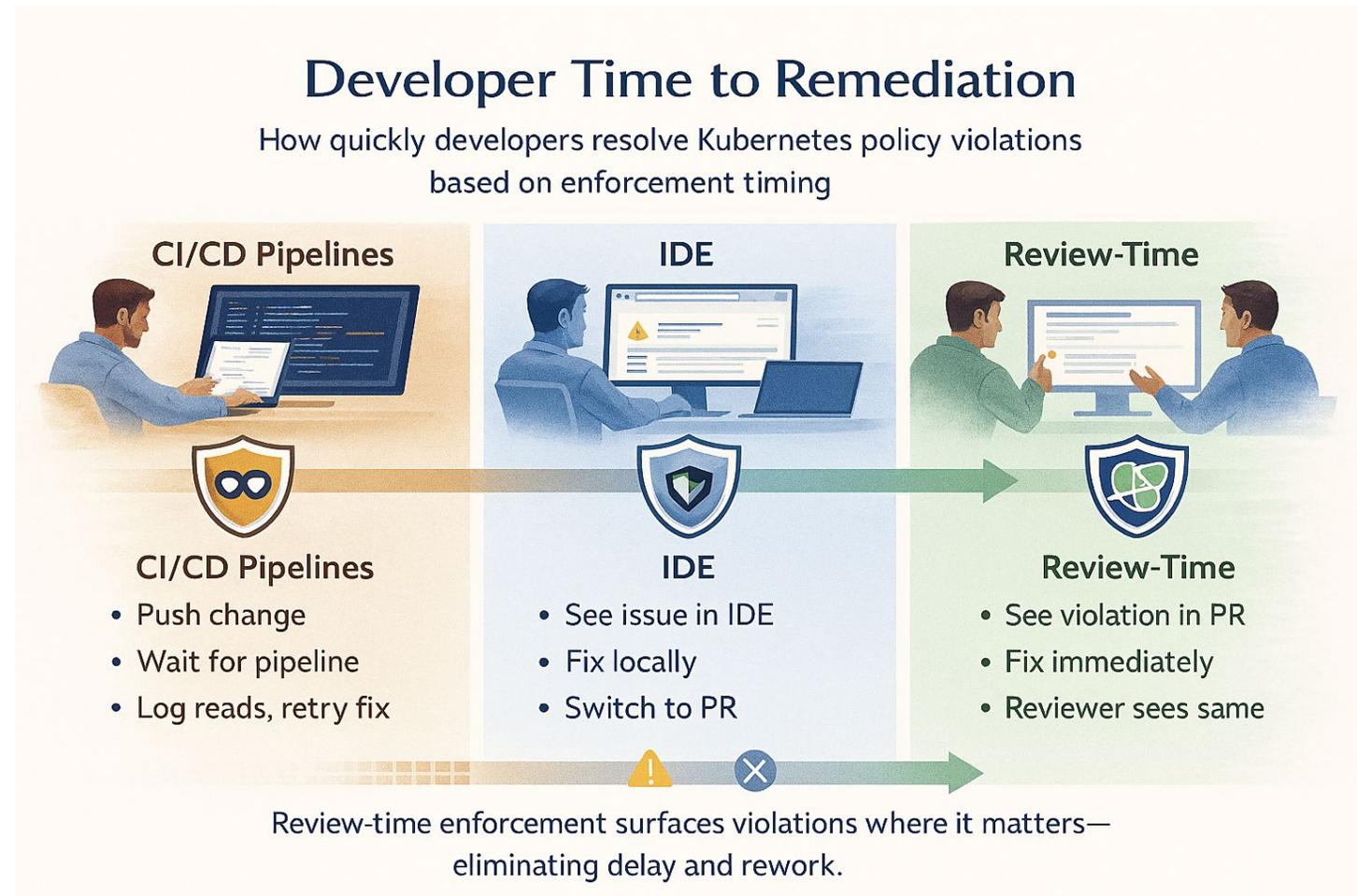- OPA/Rego (subset)

Existing Policies

No Reinventing the Wheel

Deterministic Rule Engine

No ambiguous rules: the same result, every time

- Schema-aware

- Stateless predicates

- Parallel execution

```
reject: all
- rule: must have labels
  validate:
    - kubettl.kubernetes.io/labels
    - required: true
```

Always Pass

Always Fail

Deterministic Rules

- Seconds instead of minutes

- Reduced cognitive load

Developer Time to Remediation

How quickly developers resolve Kubernetes policy violations based on enforcement timing

CI/CD Pipelines	IDE	Review-Time

CI/CD Pipelines
- Push change
- Wait for pipeline
- Log reads, retry fix

IDE
- See issue in IDE
- Fix locally
- Switch to PR

Review-Time
- See violation in PR
- Fix immediately
- Reviewer sees same

Review-time enforcement surfaces violations where it matters—eliminating delay and rework.

Limitations

GuardOn has current limitations that help prioritize future improvements.

Org-Wide Coverage

Only apptied in GitHub, Gitl.ab

Policy Granularity

Per branch exceptions not yet available

Custom Resources

Scenarios requiring domain-specifie logic

chromewebstore.google.com/detail/guardon——developer-first/jhhegdmiakbocegfcfjngkodicpjkgpb

chrome web store

Search extensions and themes

Discover   **Extensions**   Themes

Guardon — Developer-First Kubernetes Governance

Add to Chrome

5.0 ★ (1 rating) ⓘ   < Share

Extension   Developer Tools   Mature content   3 users

Overview

Guardon validates Kubernetes YAML files in GitHub/GitLab against configurable Guardon checks.

A lightweight browser extension that validates Kubernetes YAML files in real time against common security and compliance guardrails

Enterprise Concerns

- Per-user rule upload does not scale

Risk Exposure

Misconfigurationes increase the attack surface

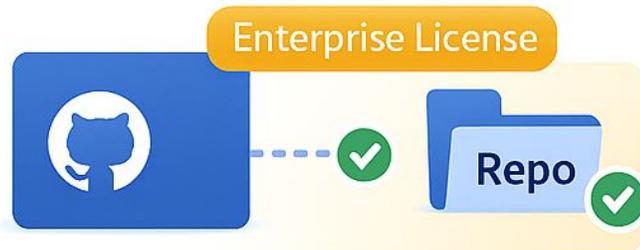**Supply Chain Security**

Weak code can leak dependencies

Regulatory Compliance

Strict rules dictate secure configurations

Enterprise vs Community Version

ENTERPRISE

- ✔ Centrally Defined Policies
- ✔ Org-Wide Enforcement
- ✔ Audit & Traceability

Enterprise License

Repo

COMMUNITY

- ✔ User-Defined Policies
- ✔ Single-Repo Usage
- ✔ Basic Issue Tracking

Repo

PR

Free / Open Source

Two Flavors of GuardOn Tailored to Your Needs

Call to Action

- Try GuardOn

Guardon — Developer-First Kubernetes Governance

5.0 ★ (1 rating) ⓘ   ⤷ Share

Extension   Developer Tools   Mature content   5 users

KUBERNETES GUARDRAILS

Secure Your YAMLs: Guardrails for Kubernetes Made Simple