Open-Source Release: May 2026

Perplexity Bumblebee

A Deep-Dive into the Internal Dev System Security Shield

github.com/perplexityai/bumblebee | Read-Only Supply-Chain Scanner

What Is Perplexity Bumblebee?

A Shield Against Supply-Chain Risks

Modern software risks are shifting. Hackers now target developer laptops—filled with package lockfiles, editor extensions, and agent configurations—before their malicious code ever hits production.

- **Developer Endpoint Protection:** Designed primarily to audit endpoints and local environments against dangerous components.
- **Strictly Read-Only:** Reads manifests and lockfiles directly. Never executes hazardous tools like `npm install` or lifecycle scripts.
- **Ultra-Fast Audits:** Built completely in Go, featuring zero non-standard library dependencies for maximum fleet safety.

Three Powerful Scan Profiles

Baseline Profile

Routine daily checks targeting standard global installation directories, browser extensions, language environments, and active editor plugins. Seamlessly scheduled via MDM.

Project Profile

Targeted repository scans mapped to active workspace folders like `~/code` or `~/src` to parse locally cached dependencies and package configurations.

Deep Profile

High-verbosity sweep configured for active incident response, allowing threat hunters to seek out exact file hashes or dangerous version strings globally.

Unmatched Ecosystem Coverage

Language & AI Ecosystems

Bumblebee performs direct metadata scanning of popular package managers and Model Context Protocol configurations:

Package Managers: Complete audit support for `npm`, `pnpm`, `Yarn`, `Bun`, `PyPI`, `Go` modules, `RubyGems`, and `Composer`.

AI Agent Configurations: Scans Model Context Protocol (MCP) server profiles dynamically used by LLM integrations.

Editor & Browser Extensions

Vulnerabilities often hide inside developer browser configurations or malicious IDE extension environments:

Developer Editors: Audits plugins inside VS Code, Cursor, Windsurf, and VSCodium configurations.

Web Browsers: Scans extensions across Chromium-based tools (Chrome, Comet, Brave, Arc, Edge) and Firefox.

Addressing The Endpoint Security Gap

Capability Matrix	SBOM & Repo Scanners	Traditional EDR Products	Perplexity Bumblebee
Primary Core Target	Build artifacts & GitHub repositories	Active system processes & networks	Local workspace files & metadata
Extension Auditing	✗ None	✗ Process-only detection	✓ Browser & IDE Extensions
Execution Threat Risk	⚠ Safe (scans remote code)	⚠ High overhead agent	✓ 100% Read-only parsed files
AI Agent Tool Coverage	✗ None	✗ None	✓ Full MCP Profile Checks

Interactive Threat Workflows

Bumblebee + Computer

When a new vulnerability surfaces, Perplexity's Computer drafts threat catalog updates. The community reviews and merges, while Bumblebee instantly scans fleets for exposure.

- **Zero-Trust Engine:** Eliminates execution-based supply-chain attacks.
- **NDJSON Output:** Feeds directly into SIEM or local telemetry dashboards.

Official Resources & Sources

Access the documentation and open-source platform details directly:

Read Announcement Blog

Inspect GitHub Repository