



# Socket

**Protect your code from everyone else's**

# Agenda

Nov 17, 2025

## 1. 1st Hour: Online Session

- a. General Overview
- b. Tooling & Setup - Developer experience
- c. How to Use Socket
- d. Q/A

## 2. 2nd Hour: Continued Deep-Dive

- a. Technical Deep-Dive
- b. Customer Use Cases
- c. Roadmap Session

# Socket General Overview

# Cut through the **noise**. Focus on **real threats**.

## Detect

- ✓ Malicious dependencies
- ✓ Vulnerable dependencies
- ✓ 0-day supply chain attacks
- ✓ Typosquat attacks
- ✓ Dependency hijacking
- ✓ Backdoors
- ✓ High-risk dependencies
- ✓ Malicious install scripts
- ✓ Hidden behavior
- ✓ 70+ signals

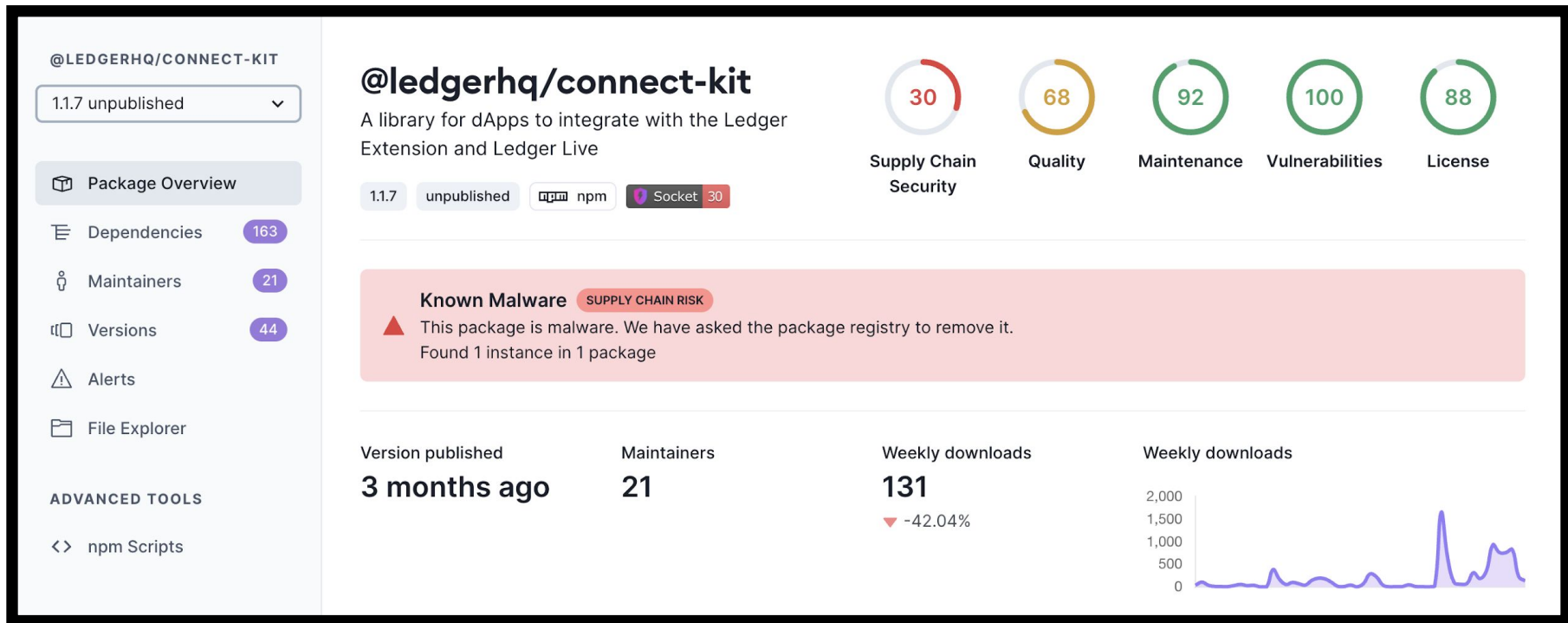
## Prevent & Block

- ✓ CI/CD Integrations (Gitlab)
- ✓ Socket Firewall
- ✓ IDE Extension
- ✓ MCP Plugin
- ✓ Web Extension

## Prioritization

- ✓ Tier 3 – Module Level  
Reachability
- ✓ Tier 2- Real Time Dependency  
Reachability
- ✓ Tier 1 – Function Level  
Reachability from your source

# Understand packages with risk scoring



Socket detects and prevents

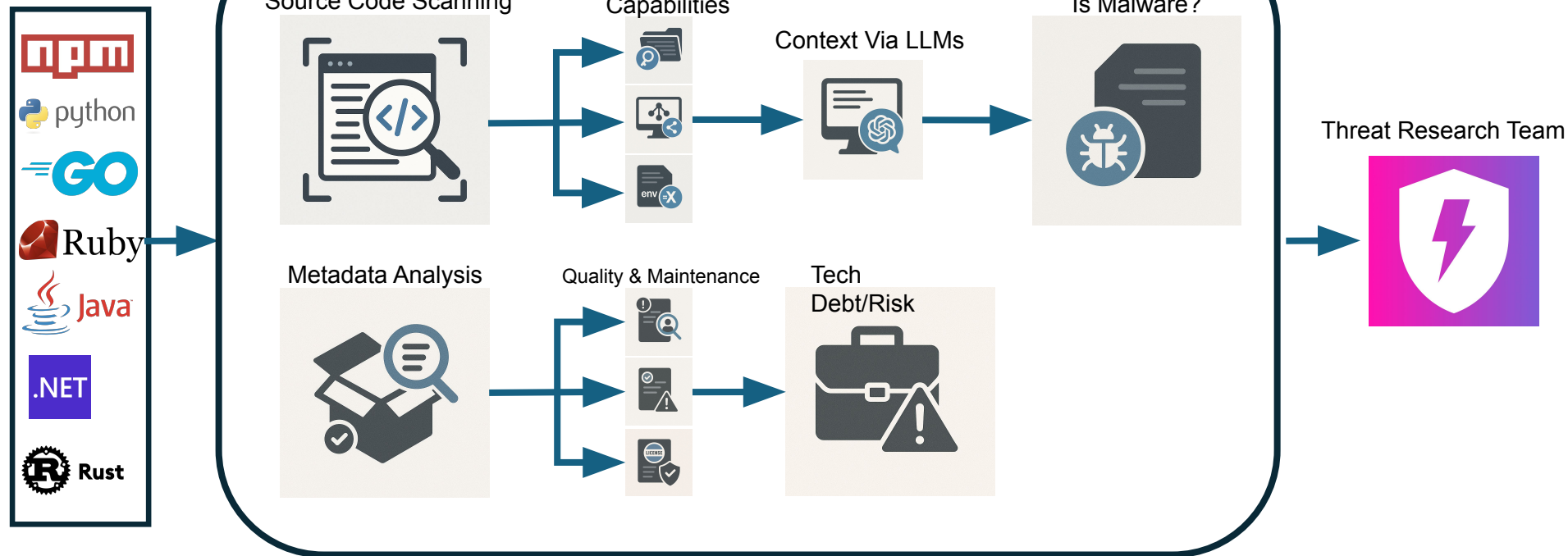
over 1,000

software supply chain attacks every week



# Socket AI Threat Engine

Package Managers



# Get the full picture of open source risk

## Vulnerabilities

- ✓ **Critical CVE**
- ✓ High CVE
- ✓ Medium CVE
- ✓ Low CVE

## Quality issues

- ✓ **Unpopular package**
- ✓ Minified code
- ✓ Bad dependency semver
- ✓ **Wildcard dependency**

## Maintenance risks

- ✓ **Deprecated**
- ✓ **Unmaintained**

## Supply chain risks

- ✓ **Known Malware**
- ✓ **Possible typosquat attack**
- ✓ AI-detected potential malware
- ✓ Git dependency
- ✓ GitHub dependency
- ✓ HTTP dependency
- ✓ **Obfuscated code**
- ✓ **Protestware or potentially unwanted behavior**
- ✓ Telemetry
- ✓ **Unstable ownership**
- ✓ AI-detected potential security risk
- ✓ Native code
- ✓ **Network access**
- ✓ Non-existent author
- ✓ Potential vulnerability

- ✓ **Shell access**
- ✓ Trivial Package
- ✓ **Uses eval**
- ✓ AI-detected potential code anomaly
- ✓ Environment variable access
- ✓ **Filesystem access**
- ✓ High entropy strings
- ✓ **New author**
- ✓ NPM Shrinkwrap
- ✓ **Install scripts**
- ✓ Manifest confusion
- ✓ Debug access
- ✓ **Dynamic require**

## License risks

- ✓ **Explicitly Unlicensed Item**
- ✓ **License Policy Violation**
- ✓ Misc. License Issues
- ✓ Ambiguous License Classifier
- ✓ Copyleft License
- ✓ License exception
- ✓ No License Found
- ✓ Non-permissive License
- ✓ Unidentified License

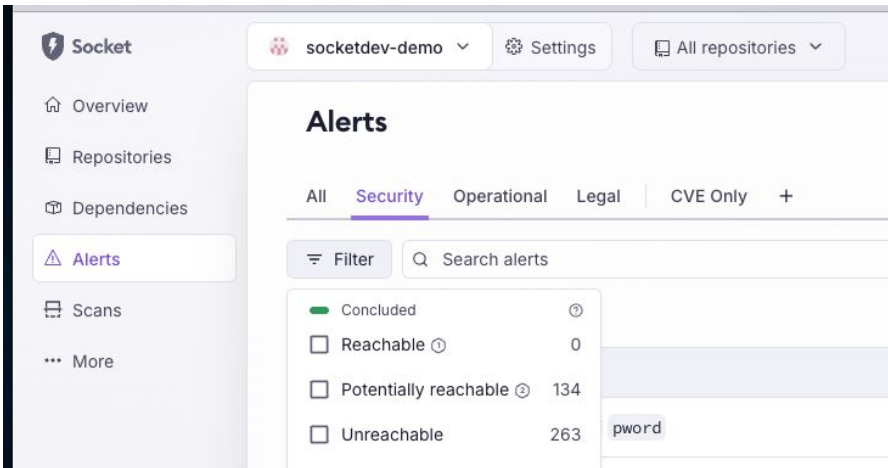
# Reachability

# Tier 3 Reachability

- Works for all Socket Alerts
- Looks for imports that are unused in dependencies
- No special configuration needed
- Has about 35% reduction in alerts

The screenshot displays the Socket Alerts interface. On the left, a sidebar contains navigation links: Overview, Repositories, Dependencies, Alerts (highlighted), Scans, and More. The main content area is titled 'Alerts' and features tabs for All, Security (selected), Operational, Legal, and CVE Only. A 'Filter' button and a search bar are present. A dropdown menu for 'Dependency Use...' shows 'Used' (1052) and 'Unused' (26) options. Below this, two critical CVE alerts are listed: 'Critical CVE: Verification Bypass in npm jsonwebtoken' and 'Critical CVE: Arbitrary Code Execution in npm underscore'. The interface also includes a top navigation bar with 'socketdev-demo', 'Settings', and 'All repositories'.

# Tier 2 Reachability



- Works for CVE Alerts only
- Pre-computed against the Direct Dependencies and their transitive dependencies
- Determines reachability of CVEs for transitive dependencies
- Goes 4 levels deep
- No special configuration needed
- Has about 60% reduction in CVE alerts

# Tier 1 Reachability

- Works for CVE Alerts only
- Utility ran in your environment and does function level reachability from your source code
- Determines reachability of CVEs for Direct and transitive dependencies
- Goes to any depth of transitive resolution
- Creates a Socket Findings file that can be checked in as a Reachability Manifest file that works with the Github App or CLIs
- Has about 90% reduction in CVE alerts

# Web Extension

# Web Extension

- Provides information wherever a supported install command is
- Links to the Socket Package Page
- Useful to see risks inline when searching on the internet

If these commands return version numbers, you're set. If not, download and install Node.js from the [official website](#).

2. **Install the package:** Use npm to install the specific version 4.5.0 of the `@telepo/web-attendant` package by running:

```
bash  
  
npm install @telepo/web-attendant@4.5.0
```

This command will install the package into your project file accordingly.

3. **Verify the package is listed in your package.json under dependencies**

```
json  
  
"dependencies": {  
  "@telepo/web-attendant": "4.5.0",  
  // other dependencies  
}
```

**@telepo/web-attendant@4.5.0**

Known malware  
Uses eval  
Install scripts

**Dependencies**

Socket optimized override available

# GitLab

# Gitlab Pipeline – MR Comments

- Currently, integrates via the Gitlab Pipeline
  - Coming soon is a self hosted Gitlab Application
- Simple workflow that can be added  
(<https://docs.socket.dev/docs/socket-in-your-gitlab-pipeline#/>)
- Two types of comments
  - Dependency Overview
  - Security Issues Comment

# Dependency Overview Comment

- Informational comment
- Provides information on new or updated direct dependencies
- Scores are based on detected Alerts for dependencies

[Compare with previous version](#)

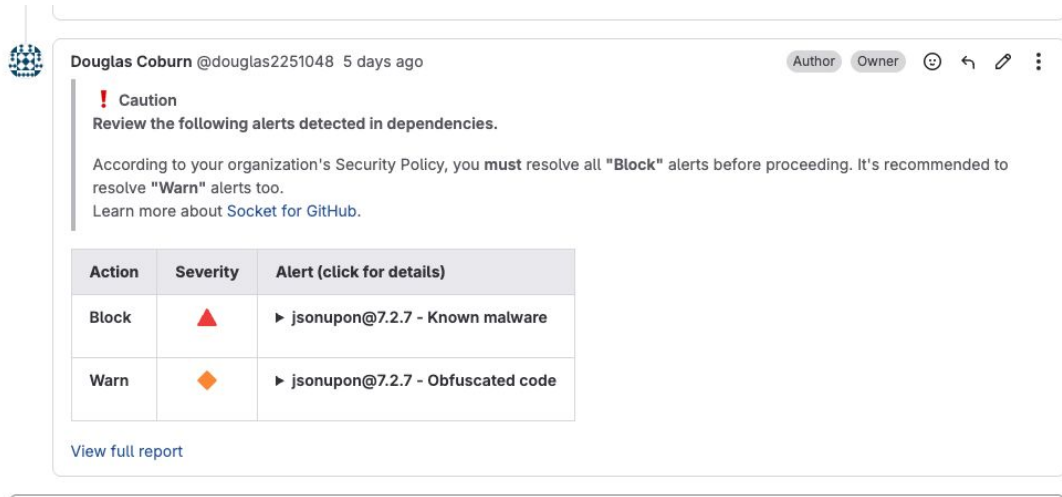
 Douglas Coburn @douglas2251048 5 days ago Author Owner 

## Socket Security: Dependency Overview

Review the following changes in direct dependencies. Learn more about [socket.dev](#)

| Diff                                                                              | Package       | Supply Chain Security                                                               | Vulnerability                                                                       | Quality                                                                             | Maintenance                                                                         | License                                                                             |
|-----------------------------------------------------------------------------------|---------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
|  | jsonupn@7.2.7 |  |  |  |  |  |

# Security Issues Comment



The screenshot shows a GitHub comment by Douglas Coburn (@douglas2251048) from 5 days ago. The comment is a 'Caution' alert regarding security issues in dependencies. It states that according to the organization's Security Policy, all 'Block' alerts must be resolved before proceeding, and it's recommended to resolve 'Warn' alerts too. A link to 'Learn more about Socket for GitHub' is provided. Below the text is a table with two rows of alerts: 'Block' (red triangle) and 'Warn' (orange diamond), both from 'jsonupon@7.2.7'. A 'View full report' link is at the bottom.

Douglas Coburn @douglas2251048 5 days ago

**! Caution**  
Review the following alerts detected in dependencies.

According to your organization's Security Policy, you **must** resolve all "**Block**" alerts before proceeding. It's recommended to resolve "**Warn**" alerts too.  
[Learn more about Socket for GitHub.](#)

| Action | Severity | Alert (click for details)          |
|--------|----------|------------------------------------|
| Block  | ▲        | ▶ jsonupon@7.2.7 - Known malware   |
| Warn   | ◆        | ▶ jsonupon@7.2.7 - Obfuscated code |

[View full report](#)

- Based on configured Security & Legal Policies
- Only new Alerts in that PR will trigger
- Additional details are in drop down
- Block Alerts fail PR Checks
- Warn is informational
- Links to report in Socket

# Socket Pipeline Status

- MR Pipeline will return non-zero if there are New Block Alerts
- In a MR the CLI attempts to do a diff of the head versions versus the current
- Results will be in console output in addition to the MR Comment

```
27 2025-11-11 06:53:23,326: Starting Socket Security CLI version 2.2.27.dev1
28 2025-11-11 06:53:25,897: Push initiated flow
29 2025-11-11 06:53:25,898: Starting comment logic for PR/MR event
30 2025-11-11 06:53:26,011: Total files found: 2
31 2025-11-11 06:53:26,401: Creating new full scan
32 2025-11-11 06:53:26,747: Total time to create new full scan: 0.35
33 2025-11-11 06:53:31,028: Full scans are ready in 0.43 seconds
34 2025-11-11 06:53:31,028: Comparing scans - Head scan ID: 4d4b30dd-4fc4-433b-9ea0-cbaafb281015, New scan ID: a7c23312-25a5-4d87-ad5e-0efc8b6de9da
35 2025-11-11 06:53:31,278: Diff Report Gathered in 0.25 seconds
36 2025-11-11 06:53:31,279: Diff report artifact counts:
37 2025-11-11 06:53:31,279: Added: 1
38 2025-11-11 06:53:31,279: Removed: 0
39 2025-11-11 06:53:31,279: Unchanged: 54
40 2025-11-11 06:53:31,279: Replaced: 0
41 2025-11-11 06:53:31,279: Updated: 0
42 2025-11-11 06:53:35,380: Security issues detected by Socket Security:
43 2025-11-11 06:53:35,380: Diff Url: https://socket.dev/dashboard/org/socketdev-demo/diff/4d4b30dd-4fc4-433b-9ea0-cbaafb281015/a7c23312-25a5-4d87-ad5e-0efc8b6de9da
44 2025-11-11 06:53:35,382:
45 +-----+-----+-----+-----+-----+-----+-----+
46 | Alert      | Package |                               url                               | Introduced by | Manifest File | CI Status |
47 +-----+-----+-----+-----+-----+-----+-----+
48 | Known malware | jsonupon@7.2.7 | https://socket.dev/npm/package/jsonupon/overview/7.2.7 | direct      | package.json | block    |
49 | Obfuscated code | jsonupon@7.2.7 | https://socket.dev/npm/package/jsonupon/overview/7.2.7 | direct      | package.json | warn     |
50 +-----+-----+-----+-----+-----+-----+-----+
51 Cleaning up project directory and file based variables
52 ERROR: Job failed: exit code 1
```

# VS Code Extension

# VS Code Extension

- Can be installed as a normal extension
- Underlines in manifest files detected risks
- <https://marketplace.visualstudio.com/items?itemName=SocketSecurity.vscode-socket-security>

# Socket MCP Server

# MCP Plugin

- Can be added to VS Code, Cursor, or Claude Code
- Can pull Socket Scores to be used in AI Instructions
- <https://socket.dev/blog/introducing-socket-mcp-for-claude-desktop>
- <https://github.com/SocketDev/socket-mcp>

# Socket Python CLI

# Python CLI

- Only supports creating Socket Scans
- Tailored for CI/CD and doing PR comments in Github, Gitlab, etc
- Can generate a license file with attribution
- Can now run reachability analysis
- Very similar to the Github App in how it works in diffing

# Socket NPM CLI



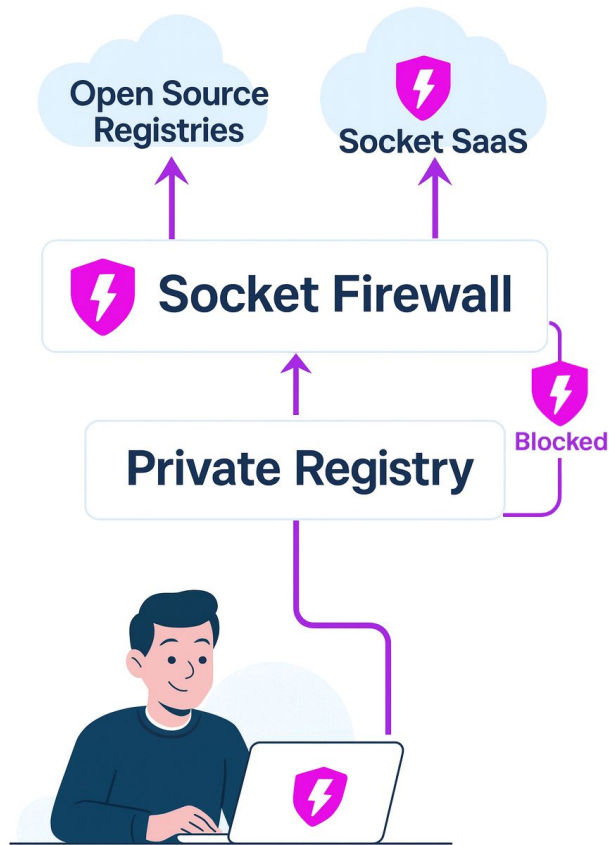
# General NPM CLI

- Wrapper for Socket API
- Provides many different functions like creating scans or CycloneDX SBOM files
- Socket scan create is the preferred method for creating Full Scans
- Supports doing socket scan github to do a one time scan of all repos
- Generally more used for one off scans that don't need diffing

# Socket Firewall

# Socket Firewall

- Has two modes Service & Wrapper mode
- Service Mode
  - Runs as a MITM (Man in the Middle) proxy
  - Has in memory cache and now supports shared cache
- Wrapper mode
  - Runs on individual developer systems to provide protection
- Uses the Socket Security policy to decide Block/Warn configuration



**Clients**  
(CI/CD, IDEs, Developer)      Machines

# Socket Basics

# Socket Basics

- Unifies management and results of Open Source tools to provide
  - SAST
  - Secret Scanning
  - Container Scanning
- SAST Supports same ecosystems as Socket Native
- Once enabled can be configured in Socket dashboard

<https://github.com/SocketDev/socket-basics>



A screenshot of the Socket dashboard interface. The top navigation bar includes "Socket", "socketdev-demo", "Settings", and "All repositories". The left sidebar has a menu with "Overview", "Repositories", "Dependencies", "Alerts", "Scans", and "More". The main content area is titled "Scan" and shows a list of alerts for "socket-basics" on "10/17/2023, 12:59:40 AM". The alerts are categorized by priority: High priority (Critical CVE, High CVE), Medium priority (Dockerfile issues), and Low priority (Medium CVE, License Policy Violation). Each alert includes a description, severity, and action links. Below the alerts, there's a section for "Socket Basics" with a toggle for "SAST Languages" and a grid of language-specific scanning options (Python, JavaScript/TypeScript, GoLang, Java, PHP, Ruby, NETCore, C, C++, Kotlin, Scala, Swift, Rust, Elixir) with individual enable/disable toggles. At the bottom, there are links for "SAST Rules Configuration", "Secret Scanning", "Container &amp; Dockerfile Scanning", "External CVE Scanning", and "Socket Tier 1".

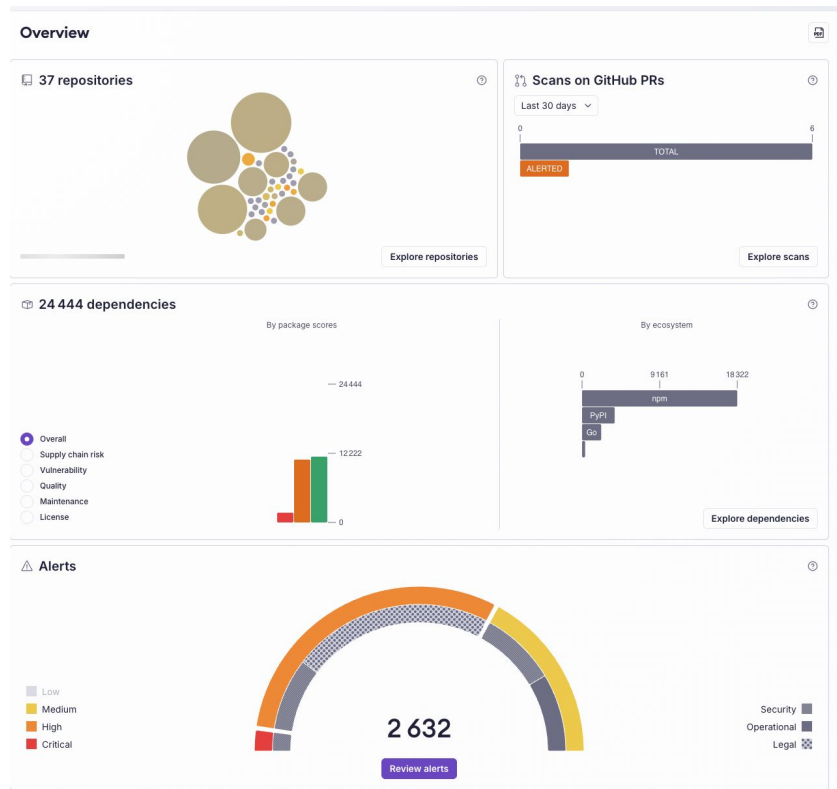
# Socket Dashboard

# Socket Dashboard

- Overview
- Alerts
- Repositories
- Dependencies
- Scans
- Telemetry
- Threat Feed

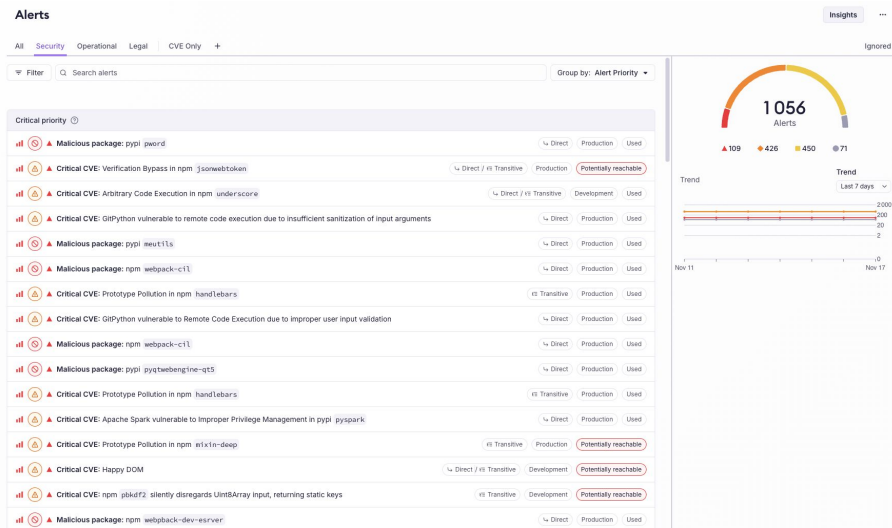
# Overview

- Summarization of results of Socket Org
- Can be filtered by Repository
- Able to drill into different data points
- Is populated by scans from the default branch



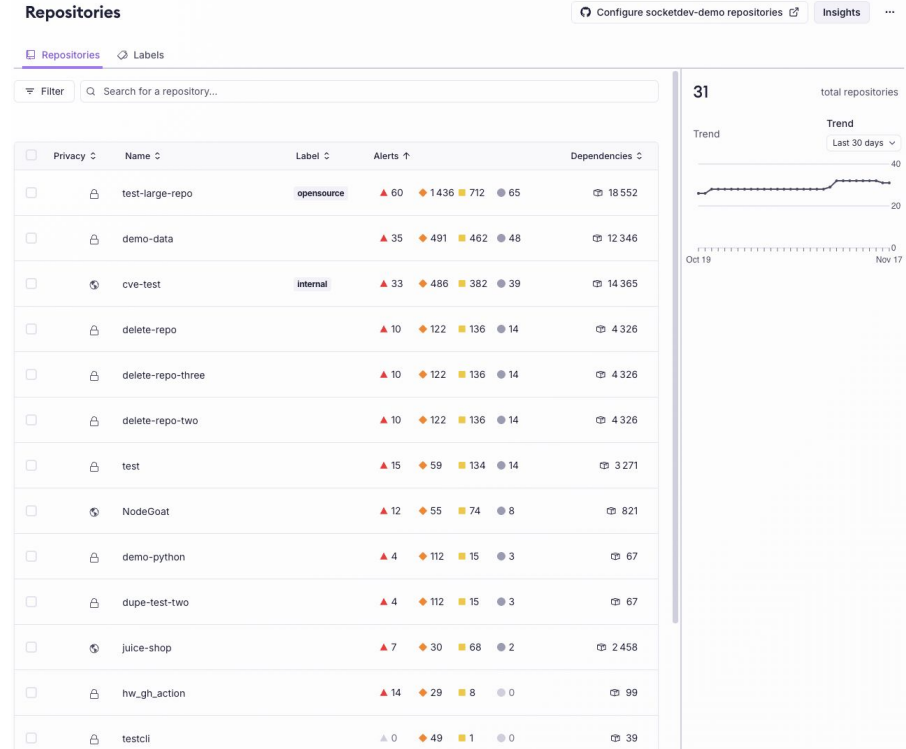
# Alerts

- Populated by the latest scan on the default branch
- It creates snapshots of scan results to provide trend information over time
- By default these snapshots are done once every 24 hours
- View of all alerts across all repositories
- Common starting point for many customers



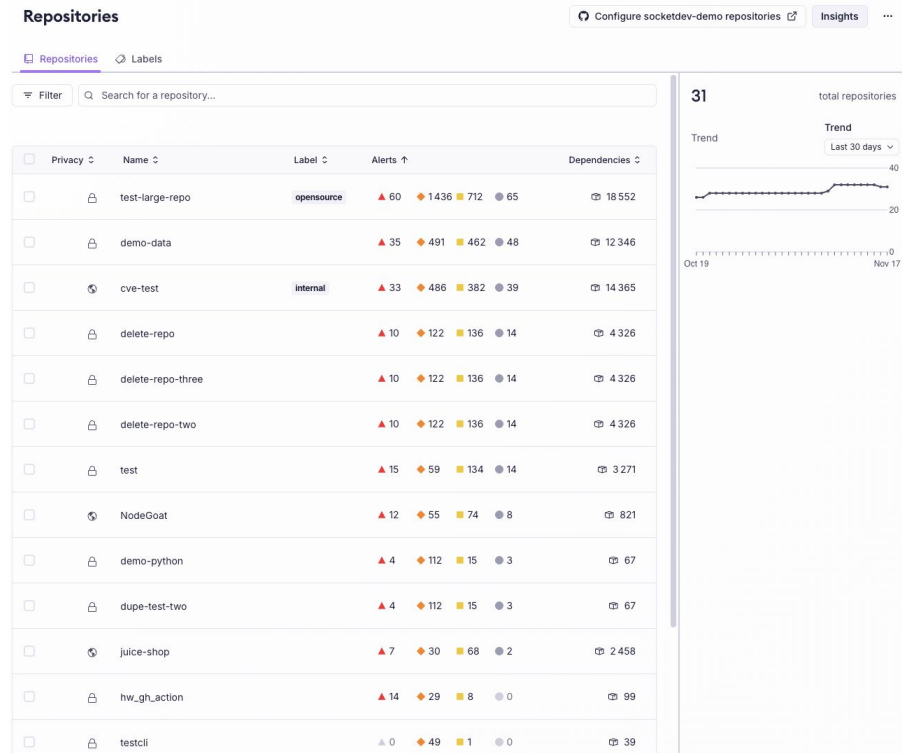
# Repositories

- High level summary of alerts based on the default branch
- Can manage and assign Repository labels
  - Labels provide Filtering
  - Customized Security policy
  - Customized Legal Policy
- Can drill in to see repository specific information



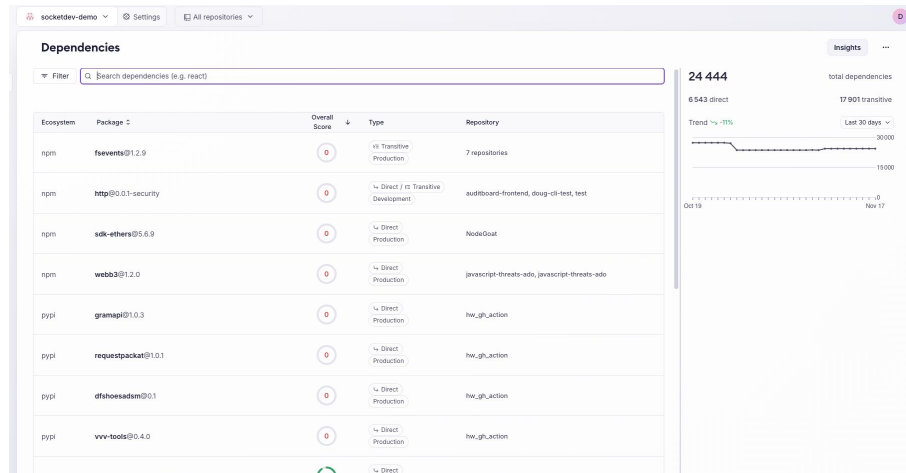
# Repositories

- High level summary of alerts based on the default branch
- Can manage and assign Repository labels
  - Labels provide Filtering
  - Customized Security policy
  - Customized Legal Policy
- Can drill in to see repository specific information



# Dependencies

- All detected dependencies in the default branch
- Will show which repositories has that dependency
- Can be filtered by the top level repositories filter
- Quick view of the overall quality of your dependencies



# Scans

- All scans created on any branch
- These will be a live view of the alerts for the detected dependencies
  - It might take a few moments for the alerts to be resolved
- Dependencies are a point in time resolution
- Ability to see the associated manifest files with the scans

Scans ⓘ

All PRs

Filter Search by ID, branch, or repository

| <input type="checkbox"/> Ran at         | Repository                | Branch                              | PR  | Commit                                                                   |
|-----------------------------------------|---------------------------|-------------------------------------|-----|--------------------------------------------------------------------------|
| <input type="checkbox"/> 17 minutes ago | socket-python-cli         | doug/add-new-reach-and-fix-docker-i |     | Doug/add reach params and fix unverified flag (#130) (c3d4a77)           |
| <input type="checkbox"/> 2 days ago     | socket-python-cli         | doug/add-reach-arams-and-fix-unver1 |     | Remove typo (b6ab69c)                                                    |
| <input type="checkbox"/> 2 days ago     | juice-shop                | master                              |     | Merge pull request #2816 from aaradhychinche-alt/patch-1 (f15283c)       |
| <input type="checkbox"/> 2 days ago     | NodeGoat                  | master                              |     | Merge pull request #290 from za/add-blank-space (c5cb68a)                |
| <input type="checkbox"/> 2 days ago     | socket-python-cli         | doug/add-reach-arams-and-fix-unver1 |     | Fix comment issues with regression introduced in 2.2.15 (#129) (55ebf3d) |
| <input type="checkbox"/> 2 days ago     | socket-python-cli         | doug/add-reach-arams-and-fix-unver1 |     | Fix comment issues with regression introduced in 2.2.15 (#129) (55ebf3d) |
| <input type="checkbox"/> 2 days ago     | socket-python-cli         | doug/add-reach-arams-and-fix-unver1 |     | Fix comment issues with regression introduced in 2.2.15 (#129) (55ebf3d) |
| <input type="checkbox"/> 2 days ago     | socket-python-cli         | doug/add-reach-arams-and-fix-unver1 |     | Fix comment issues with regression introduced in 2.2.15 (#129) (55ebf3d) |
| <input type="checkbox"/> 6 days ago     | javascript-threats-gitlab | douglas2251848-main-patch-51258     | #45 | Update .gitlab-ci.yml file (c2a2d2f)                                     |
| <input type="checkbox"/> 6 days ago     | javascript-threats-gitlab | douglas2251848-main-patch-51258     |     | Update .gitlab-ci.yml file (c2a2d2f)                                     |
| <input type="checkbox"/> 6 days ago     | javascript-threats-gitlab | douglas2251848-main-patch-51258     | #45 | Edit package.json (b9dd551)                                              |
| <input type="checkbox"/> 6 days ago     | javascript-threats-gitlab | douglas2251848-main-patch-51258     |     | Edit package.json (b9dd551)                                              |

# Firewall Telemetry

- All requests that have gone through Socket Firewall
- What the action was (block/warn/ignore)
- What **purl** was requested
- In the future being able to triage from here

## Telemetry

Search by PURL (e.g. pkg:npm/lodash@1.0.0)

| Time                       | Event ID                             | PURL                                                   | Action |
|----------------------------|--------------------------------------|--------------------------------------------------------|--------|
| > 2025-11-14T14:40:31.254Z | 8a4dc2aa-0fa5-4dac-a20d-062e4da48b51 |                                                        | -      |
| > 2025-11-14T14:40:19.204Z | e4f89953-fafd-4a80-8a69-8db9847c84fc |                                                        | -      |
| > 2025-11-14T14:40:04.767Z | 218423f7-4374-45e8-8163-6a919bdfc396 |                                                        | -      |
| > 2025-11-14T14:39:20.013Z | c423d644-a8e6-44d0-a1b8-1ebca7539b54 |                                                        | -      |
| > 2025-11-13T20:08:35.627Z | 14664fd1-02b0-4707-a5fc-31f3ce273835 |                                                        | -      |
| > 2025-11-13T20:08:35.757Z | 9fa157dd-b981-407d-99e0-6eb31cafd40e | <a href="#">pkg:npm/node-abi@3.83.0</a>                | 🔍      |
| > 2025-11-13T20:08:35.883Z | 2c5612a0-b78e-4c09-89e8-2505fd98c6c8 | <a href="#">pkg:npm/@opengis/fastify-table@2.0.76</a>  | 🔍      |
| > 2025-11-13T20:08:23.637Z | aedb6302-8bd8-468d-b303-525b6ca86ba6 |                                                        | -      |
| > 2025-11-13T17:49:48.119Z | ad279d63-ce63-4399-b747-7908403d1bb4 | <a href="#">pkg:npm/@opengis/fastify-table@2.0.76</a>  | 🔍      |
| > 2025-11-13T17:49:47.879Z | e202d2a5-2417-4606-9825-e9af57caef6a |                                                        | -      |
| > 2025-11-13T17:49:48.000Z | ef0af51f-bf03-404c-b696-c38634ec71f8 | <a href="#">pkg:npm/node-abi@3.81.0</a>                | 🔍      |
| > 2025-11-13T17:49:35.354Z | 4e607648-a9dc-4fe1-9350-6cb106dc123e |                                                        | -      |
| > 2025-11-13T15:45:22.250Z | e8d61307-f58c-490f-bad0-3397032a5e4a | <a href="#">pkg:npm/@smithy/middleware-serde@4.2.5</a> | 🔍      |
| > 2025-11-13T15:45:20.315Z | 0d92f6e6-93f4-4423-abab-e9533826e7fd | <a href="#">pkg:npm/set-cookie-parser@2.7.2</a>        | 🔍      |
| > 2025-11-13T15:45:20.117Z | 0e900043-6e2d-440d-9936-e9c086e24be0 | <a href="#">pkg:npm/pg@8.11.6</a>                      | 🔍      |

# Socket Threat Feed

Threat Feed ⓘ

Last month  
Packages with threats  
**37964**

Total  
Packages with threats  
**213478**

▼ Filter    🔍 Search packages...    Sort by: Published ▼

| Status | Ecosystem | Name                                              | Version                                  | Artifact                 | Threat Type | Published    | Last threat detected |
|--------|-----------|---------------------------------------------------|------------------------------------------|--------------------------|-------------|--------------|----------------------|
| 🔴 Low  | npm       | @chacab/claude-code                               | 2.0.42                                   | —                        | 🔒           | 2 hours ago  | 2 hours ago          |
| 🔴 Low  | npm       | jonreap                                           | 3.1.8                                    | —                        | 🔒           | 3 hours ago  | 3 hours ago          |
| 🔴 Low  | npm       | @eculia/tortend                                   | 15.0                                     | —                        | 🔒           | 4 hours ago  | 3 hours ago          |
| 🔴 Low  | chrome    | CoTik                                             | 1.0.125                                  | —                        | 🔒           | 5 hours ago  | 5 hours ago          |
| 🔴 Low  | chrome    | RevCare Extension Chrome                          | 1.72                                     | —                        | 🔒           | 6 hours ago  | 6 hours ago          |
| 🔴 Low  | npm       | ci-site                                           | 1.0.1488                                 | —                        | 🔒           | 6 hours ago  | 6 hours ago          |
| 🔴 Low  | npm       | @coinbase/legentik                                | 0.0.0-nightly-2023116210417              | —                        | 🔒           | 8 hours ago  | 8 hours ago          |
| 🔴 Low  | npm       | com.mispanet.unlity                               | 5.5.3                                    | —                        | 🔒           | 9 hours ago  | 7 hours ago          |
| 🔴 Low  | github    | fabassod/wilo-voice-call-action                   | 6eeed3aff770a70190e46d760c1d2d9f6d17b76c | —                        | 🔒           | 9 hours ago  | 9 hours ago          |
| 🔴 Low  | pypi      | py3-protectore                                    | 5.0.0                                    | py3-none-any.whl         | 🔒           | 10 hours ago | 10 hours ago         |
| 🔴 Low  | maven     | org.finos.legend.engine/legend-engine-regl-client | 4.52.1                                   | classifier-shadedext.jar | 🔒           | 10 hours ago | 10 hours ago         |
| 🔴 Low  | npm       | nodemetaback                                      | 25.6.7                                   | —                        | 🔒           | 11 hours ago | 11 hours ago         |
| 🔴 Low  | npm       | @segment/action-destinations                      | 3.444.3-staging-ee8b6488f0               | —                        | 🔒           | 12 hours ago | 12 hours ago         |

- View into our live **confirmed** findings
- Can filter by ecosystem
- These are all of our detections and not specific to your organization
- Can search by package and version

# Settings

# Settings

- Security Policy
- Legal
- Scans
- API Tokens
- WebHooks
- Socket Basics
- Members
- SSO
- Audit Log

# Security Policy

- Default policies that can be selected to control the amount of noise
- Four modes
  - **Block:** Alerts in this section will fail the integrations and return an error
  - **Warn:** Alerts in this section will trigger a comment but won't fail the integrations
  - **Monitor:** Alerts in this section will show up in reports but not to developers
  - **Ignore:** These will be hidden by default

**Security Policy**

**Low Noise**  
Traditional SCA

- Block malicious dependencies
- Warn about critical CVEs
- Monitor all CVE severities

**Default**  
Ideal for most customers

- Defend against supply chain risks
- Block malicious dependencies
- Warn about critical CVEs, typosquats, protestware

**Higher Noise**  
For more engaged teams

- Block vulnerable or malicious dependencies
- Show more warning alerts to developers
- Great for active security involvement

Customize alert actions for your organization below. You can choose to block, monitor, warn, or ignore on each alert type, or alternatively set the action back to inherit from the default policy. Custom settings will override the default policy setting and stay in effect until you change them or remove all custom settings via the button to the right. [Learn more](#)

Search alerts... **Group by** ▾ Remove Custom Settings

**Block 2**

| Alert                                                    | Category          | Severity | Action                                                            |
|----------------------------------------------------------|-------------------|----------|-------------------------------------------------------------------|
| <input type="checkbox"/> Deprecated <a href="#">🔗</a>    | Maintenance       | Medium   | <input checked="" type="radio"/> Block<br>Custom setting          |
| <input type="checkbox"/> Known malware <a href="#">🔗</a> | Supply chain risk | Critical | <input type="radio"/> Block (inherited)<br>Default policy setting |

**Warn 5**

| Alert                                                                | Category          | Severity | Action                                                           |
|----------------------------------------------------------------------|-------------------|----------|------------------------------------------------------------------|
| <input type="checkbox"/> Critical CVE <a href="#">🔗</a>              | Vulnerability     | Critical | <input type="radio"/> Warn (inherited)<br>Default policy setting |
| <input type="checkbox"/> Possible typosquat attack <a href="#">🔗</a> | Supply chain risk | Critical | <input type="radio"/> Warn (inherited)<br>Default policy setting |
| <input type="checkbox"/> Git dependency <a href="#">🔗</a>            | Supply chain risk | High     | <input type="radio"/> Warn (inherited)<br>Default policy setting |
| <input type="checkbox"/> GitHub dependency <a href="#">🔗</a>         | Supply chain risk | High     | <input type="radio"/> Warn (inherited)<br>Default policy setting |
| <input type="checkbox"/> HTTP dependency <a href="#">🔗</a>           | Supply chain risk | High     | <input type="radio"/> Warn (inherited)<br>Default policy setting |

# Legal Policy

**Legal** beta

[License Policy](#) [License Overlays](#)

Manage which licenses are allowed, denied, or otherwise in projects across your organization.

[By preset](#) [By class](#) [By license](#) [By package](#) [By string](#) [Options](#)

Customize the license policy with alert settings (allow, monitor, warn, deny) for specific licenses in the table below.

Filter

Search licenses

Sort by: Name (ascending)

| License ID                   | License Name                                    | Setting | OSI Approved | FSF Libre | License Classes     | More Info                       |
|------------------------------|-------------------------------------------------|---------|--------------|-----------|---------------------|---------------------------------|
| LicenseRef-RAIL-A            | Responsible AI END USER LICENSE AGREEMENT       | Deny    | -            | -         |                     | <a href="#">License Details</a> |
| LicenseRef-SIL-AI-RAIL-M-1.0 | SIL RAIL-M License v1.0                         | Deny    | -            | -         |                     | <a href="#">License Details</a> |
| Abstyles                     | Abstyles License                                | Deny    | -            | -         |                     | <a href="#">License Details</a> |
| AFL-1.1                      | Academic Free License v1.1                      | Allow   | ✓            | ✓         | permissive (bronze) | <a href="#">License Details</a> |
| AFL-1.2                      | Academic Free License v1.2                      | Allow   | ✓            | ✓         | permissive (bronze) | <a href="#">License Details</a> |
| AFL-2.0                      | Academic Free License v2.0                      | Allow   | ✓            | ✓         | permissive (bronze) | <a href="#">License Details</a> |
| AFL-2.1                      | Academic Free License v2.1                      | Allow   | ✓            | ✓         | permissive (bronze) | <a href="#">License Details</a> |
| AFL-3.0                      | Academic Free License v3.0                      | Allow   | ✓            | ✓         | permissive (bronze) | <a href="#">License Details</a> |
| AMPAS                        | Academy of Motion Picture Arts and Sciences BSD | Allow   | -            | -         | permissive (bronze) | <a href="#">License Details</a> |
| AdaCore-doc                  | AdaCore Doc License                             | Deny    | -            | -         |                     | <a href="#">License Details</a> |

- Enabled the detection of License Policy Violations
- Three tabs of configuration
  - By preset: This is a coarse setting where it sets the by license for you
  - By class: This is a little bit more granular than by preset
  - By license: Allows you to set the license action per individual license
- By Package and By String allow manual overrides
- Options can change how the license detection works

# Scans

- Settings which impact how Socket Scans are ran and evaluated
- Reachability
  - Precomputed Reachability: by default is on but can be turned off
  - Tier 3: by default is off but can be enabled
  - Monitor Unreachable Alerts: if enabled CVEs that are unreachable will be monitor instead of block/warn
- Ecosystems: Enable/disable ecosystem support

## Scans

### Reachability

#### Full Application Reachability ⓘ

Use Tier 1 (full application) reachability analysis to detect how your application code is using its dependencies. For details, read the [Reachability Analysis docs](#).

[Read docs](#)

#### Precomputed Reachability ⓘ

Enable Tier 2 (precomputed) reachability analysis to detect which parts of transitive dependencies are actually used by your direct dependencies' code. For details, read the [Reachability Analysis docs](#).



#### Dependency Reachability ⓘ

Enable Tier 3 (dependency) reachability analysis to detect which transitive dependencies are actually used in your dependencies' code. For details, read the [Reachability Analysis docs](#).



#### Monitor Unreachable Alerts

If enabled, unreachable CVEs (as determined by Tier 1/2 reachability) will alert with the "monitor" action rather than "block" or "warn." This takes precedence over security policies but not manual triage.



### Ecosystems

Configure which ecosystems to scan for alerts.

 Cargo



 Chrome Web Store



 GitHub Actions



 Go



 Hugging Face



 Maven



 npm



 NuGet



# API Tokens

API Tokens ⓘ [+ Create API token](#)

| NAME                              | TOKEN             | MAX QUOTA  | LAST USED AT | CREATED AT   |     |
|-----------------------------------|-------------------|------------|--------------|--------------|-----|
| main-token                        | sktsec_b1q-g***** | 10,000,000 | Nov 17, 2025 | Sep 24, 2023 | ... |
| limited-permissions               | sktsec_22Vv3***** | 10,000,000 | Oct 25, 2023 | Oct 25, 2023 | ... |
| gltlab_token                      | sktsec_t7UIl***** | 10,000,000 | Aug 04, 2024 | Nov 22, 2023 | ... |
| bitbucket integration             | sktsec_zq7ua***** | 10,000,000 | Sep 23, 2024 | Nov 30, 2023 | ... |
| dependency-test                   | sktsec_s-paY***** | 1,000,000  | Jun 05, 2024 | Jun 05, 2024 | ... |
| siem-test                         | sktsec_Yiurt***** | 1,000,000  | Jul 03, 2024 | Jul 03, 2024 | ... |
| Test Key                          | sktsec_uY87I***** | 1,000,000  | Aug 24, 2024 | Aug 24, 2024 | ... |
| Sales Threat Feed Token           | sktsec_kHtd7***** | 1,000,000  | Nov 04, 2025 | Aug 29, 2024 | ... |
| brets-token                       | sktsec_hrM0E***** | 1,000,000  | Mar 19, 2025 | Jan 24, 2025 | ... |
| brets-token                       | sktsec_0wHjX***** | 1,000,000  | Apr 29, 2025 | Apr 29, 2025 | ... |
| export_test                       | sktsec_9q86m***** | 1,000,000  | May 24, 2025 | May 21, 2025 | ... |
| socket-mcp-test-token-dont-delete | sktsec__2q5c***** | 1,000,000  | Nov 16, 2025 | Jul 01, 2025 | ... |

- Area to manage the org level API Tokens
- All API Tokens can different scopes
- If a user uses a token on an endpoint without the right scope they will be denied access
- API Tokens can be rotated

# WebHooks

- Support for Generic WebHooks
- Alert
  - These event types are for alerts from the Org Alerts
  - When there is a change to the alert a push notification can be sent
- Pull request
  - Currently only available for Github PRs

## Create webhook

Name:

Description: (Optional)

URL:

Signing Key:

Generate



Events:

☐ alert

Alert events

☐ pull-request

Pull request

Filters:

Select repositories

ADVANCED SETTINGS

Cancel

Confirm

# Socket Basics

## Socket Basics ⓘ

SAST Languages ▾

SAST Rules Configuration ▾

Secret Scanning ▾

Container & Dockerfile Scanning ▾

External CVE Scanning ▾

Socket Tier 1 ▾

S3 Upload ▾

Integrations ▾

Console Logging ▾

Additional Parameters

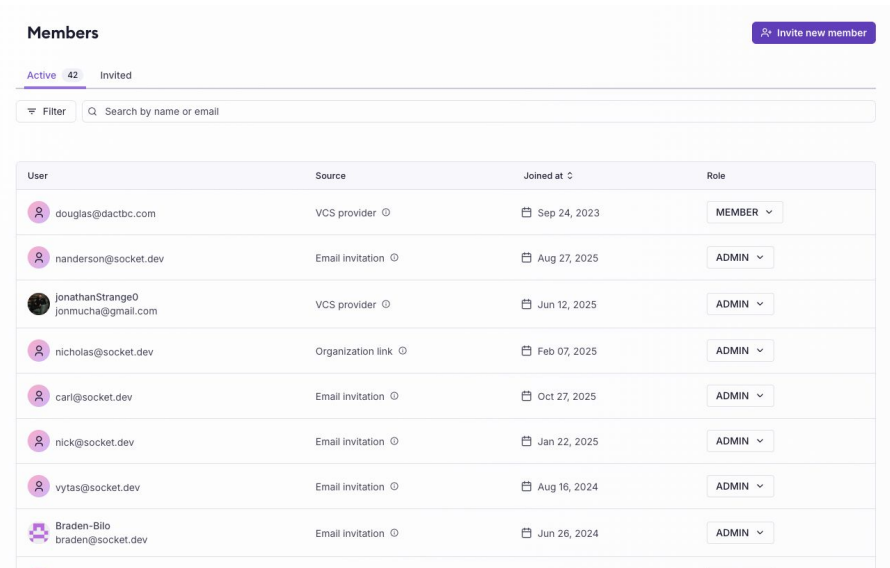
Additional parameters for Socket SCA scanning

- Configuration for the Socket Basics tool
- Granular controls for integrations and customizations
- Currently only at the Org Level
- Can be overridden with local configurations when running

# Members

- Area to manage who has access to the Socket Dashboard
- Four level of roles
  - Owner: Owner can't be deleted and is an Admin
  - Admin: Has full control over everything except changing owner
  - Member: Can see most things but can't change settings
  - Contributor: Can't make any changes

<https://docs.socket.dev/docs/users#/>



The screenshot shows the 'Members' management page in the Socket dashboard. At the top right is a purple button labeled 'Invite new member'. Below the title, there are tabs for 'Active' (42) and 'Invited'. A search bar with a 'Filter' dropdown and a search icon is present. The main content is a table with columns: User, Source, Joined at, and Role. The table lists eight members with their email addresses, source of invitation, join dates, and roles (MEMBER or ADMIN). Each row has a dropdown arrow next to the role.

| User                                                                                                                        | Source              | Joined at    | Role     |
|-----------------------------------------------------------------------------------------------------------------------------|---------------------|--------------|----------|
|  douglas@dactbc.com                      | VCS provider ⓘ      | Sep 24, 2023 | MEMBER ▾ |
|  nanderson@socket.dev                    | Email invitation ⓘ  | Aug 27, 2025 | ADMIN ▾  |
|  jonathanStrange0<br>jonmuchas@gmail.com | VCS provider ⓘ      | Jun 12, 2025 | ADMIN ▾  |
|  nicholas@socket.dev                     | Organization link ⓘ | Feb 07, 2025 | ADMIN ▾  |
|  carl@socket.dev                         | Email invitation ⓘ  | Oct 27, 2025 | ADMIN ▾  |
|  nick@socket.dev                         | Email invitation ⓘ  | Jan 22, 2025 | ADMIN ▾  |
|  vyas@socket.dev                         | Email invitation ⓘ  | Aug 16, 2024 | ADMIN ▾  |
|  Braden-Bilo<br>braden@socket.dev        | Email invitation ⓘ  | Jun 26, 2024 | ADMIN ▾  |

# SSO

## Single Sign-On

Organization slug

This is your organization's slug within Socket. Use this name to log in with SSO.

socketdev-demo 



● Inactive

Allow organization members to log in using an Identity Provider.

Configure

Do you need to share this configuration link with your team? [Generate link](#)

☐ **Require SSO on login**

Require organization members to login with SAML to access the organization. Note: admins and owners will always be able to login with email.

### Default member role

New members signing in via SSO will join with this role

Member 



# Audit Log

- View for any changes in the Socket Dashboard
- Can filter by different event types
- Can export to CSV or JSON

## Audit Log

Select event type

Export JSON

Export CSV

D

douglas@socket.dev - Created webhook

✓

createWebhook - 11/17/2025, 11:37:29 AM

```
{ "url": "https://localhost/test", "name": "Demo", "events": [ { "pull-request:scan" }, { "userid": "5e72a772-b67a-4285-a979-ab12a9e2ac1e", "webhookid": "19", "organizationid": "63327" }
```

D

douglas@socket.dev - Updated organization setting

✓

updateOrganizationSetting - 11/15/2025, 7:18:43 AM

```
{ "userid": "5e72a772-b67a-4285-a979-ab12a9e2ac1e", "settingKey": "issueRules", "settingValue": { "deprecated": { "action": "error" } }, "organizationid": "63327" }
```

D

douglas@socket.dev - Updated organization setting

✓

updateOrganizationSetting - 11/15/2025, 7:17:23 AM

```
{ "userid": "5e72a772-b67a-4285-a979-ab12a9e2ac1e", "settingKey": "licensePolicy", "settingValue": { "warn": { "strings": [] }, "allow": { "strings": [ "0BSD", "AAL", "ADSL", "AFL-1.1", "AFL-1.2", "AFL-2.0", "AFL-2.1", "AFL-3.0", "AMDPLPA", "AML", "AMPAS", "ANTLR-PD", "ANTLR-PD-fallback", "APAFML", "Adobe-2006", "Afmparse", "Apache-1.0", "Apache-1.1", "Apache-2.0", "Artistic-1.0", "Artistic-1.0-Perl", "Artistic-1.0-cil", "Artistic-2.0", "BSD-1-Clause", "BSD-2-Clause", "BSD-2-Clause-FreeBSD", "BSD-2-Clause-NetBSD", "BSD-2-Clause-Patent", "BSD-2-Clause-Views", "BSD-3-Clause", "BSD-3-Clause-Attribution", "BSD-3-Clause-Clear", "BSD-3-Clause-HP", "BSD-3-Clause-LBNL", "BSD-3-Clause-Modification", "BSD-3-Clause-No-Nuclear-License-2014", "BSD-3-Clause-No-Nuclear-Warranty", "BSD-3-Clause-Open-MPPL", "BSD-4-Clause", "BSD-4-Clause-Shortened", "BSD-4-Clause-UC", "BSD-Source-Code", "BSL-1.0", "Bahyph", "Barr", "Beerware", "Bitstream-Charter", "Bitstream-Verano", "BlueOak-1.0.0", "Borceux", "CC-BY-1.0", "CC-BY-2.0", "CC-BY-2.5", "CC-BY-2.5-AU", "CC-BY-3.0", "CC-BY-3.0-AT", "CC-BY-3.0-AU", "CC-BY-3.0-DE", "CC-BY-3.0-IGO", "CC-BY-3.0-NL", "CC-BY-3.0-US", "CC-PDDC", "CCO-1.0", "CECILL-B", "CNRI-Jython", "CNRI-Python", "CNRI-Python-GPL-Compatible", "CIATistic", "Condor-1.1", "Crossword", "CrystalStacker", "Cube", "DOC", "DSDP", "ECL-1.0", "ECL-2.0", "EFL-1.0", "EFL-2.0", "Entessa", "FSFUL", "FSFULLR", "FTL", "Fair", "Giftware", "HPND", "HTMLTIDY", "IBM-pibs", "ICU", "JG", "ISC", "ImageMagick", "Info-ZIP", "Intel", "JasPer-2.0", "LPL-1.0", "LPL-1.02", "LPL-1.3c", "Leptonica", "Libpng", "License :: Eiffel Forum License (EFL)", "License :: OSI Approved :: Academic Free License (AFL)", "License :: OSI Approved :: Apache Software License", "License :: OSI Approved :: Attribution Assurance License", "License :: OSI Approved :: BSD License", "License :: OSI Approved :: Eiffel Forum License", "License :: OSI Approved :: Zope Public License", "LicenseRef-anti-grain-2005", "LicenseRef-matplotlib-CLA", "Linux-OpenIB", "MIT-0", "MIT-CMU", "MIT-Festival", "MIT-Khronos-old", "MIT-Modern-Variant", "MIT-Wu", "MIT-advertising", "MIT-enna", "MIT-feh", "MIT-open-group", "MIT-testrege", "MITNFA", "MS-PL", "MTL", "Miros", "MulanPSL-1.0", "MulanPSL-2.0", "Multics", "Mup", "NASA-1.3", "NBPL-1.0", "NCBI-PD", "NCSA", "NIST-PD", "NIST-PD-fallback", "NLPL", "NRL", "NTP", "Naumen", "Net-SNMP", "NetCDF", "Newslet", "OGTSL", "OLDAP-1.1", "OLDAP-1.2", "OLDAP-1.3", "OLDAP-1.4", "OLDAP-2.0", "OLDAP-2.0.1", "OLDAP-2.1", "OLDAP-2.2", "OLDAP-2.2.1", "OLDAP-2.2.2", "OLDAP-2.3", "OLDAP-2.4", "OLDAP-2.5", "OLDAP-2.6", "OLDAP-2.7", "OLDAP-2.8", "OML", "OpenSSL", "PDDL-1.0", "PHP-3.0", "PHP-3.0.1", "PSF-2.0", "Plexus", "PostgreSQL", "Python-2.0", "Python-2.0.1", "Qhull", "RSA-MD", "Rdisc", "Ruby", "SAX-PD", "SAX-PD-2.0", "SGI-B-2.0", "SMLNJ", "SWL", "Saxpath", "Spencer-86", "Spencer-94", "Spencer-99", "TCL", "TCP-wrappers", "TU-Berlin-1.0", "TU-Berlin-2.0", "UPL-1.0", "Unicode-3.0", "Unicode-DFS-2015", "Unicode-DFS-2016", "Unicode", "VSL-1.0", "Vim", "W3C", "W3C-19980720", "W3C-20150513", "WTFPL", "Wsuipa", "X11", "XFree86-1.1", "Xerox", "Xinet", "ZPL-1.1", "ZPL-2.0", "ZPL-2.1", "Zed", "Zend-2.0", "Zlib", "blessing", "bzlib-2.0.5", "bzlib-2.0.6", "curl", "diffmark", "eGenix", "libpng-2.0", "libsealinux-1.0", "libtiff", "mpich2", "ms-cla", "ms-limited-public", "ms-sspl", "ms-ws-routing-spec", "msj-sample-code", "psutils", "xinetd", "xpp", "zlib-acknowledgement", "Minpack", "X11-distribute-modifications-variant", "X11-swapped", "HP-1989", "JG-short", "JSON", "CC-BY-4.0", "MIT", "SunPro", "CDDL-1.0", "CDDL-1.1", "CPL-1.0", "EPL-2.0", "ErlPL-1.1", "IPL-1.0", "LGPL-2.0", "LGPL-2.0+", "LGPL-2.0-only", "LGPL-2.0-or-later", "LGPL-2.1", "LGPL-2.1+", "LGPL-2.1-only", "LGPL-2.1-or-later", "LGPL-3.0", "LGPL-3.0+", "LGPL-3.0-only", "LGPL-3.0-or-later", "License :: OSI Approved :: Common Public
```

# Customer Use Cases

# Customer Use Cases

## Salesforce

- Socket is on the 'paved road' for development
- Socket has replaced Snyk as core SCA tool
- CLI tool workflows with Socket worked at scale
- Socket's reachability outperformed both Snyk and Endor in comparisons
- Want protection against non-CVE threats as part of SCA

## Netflix

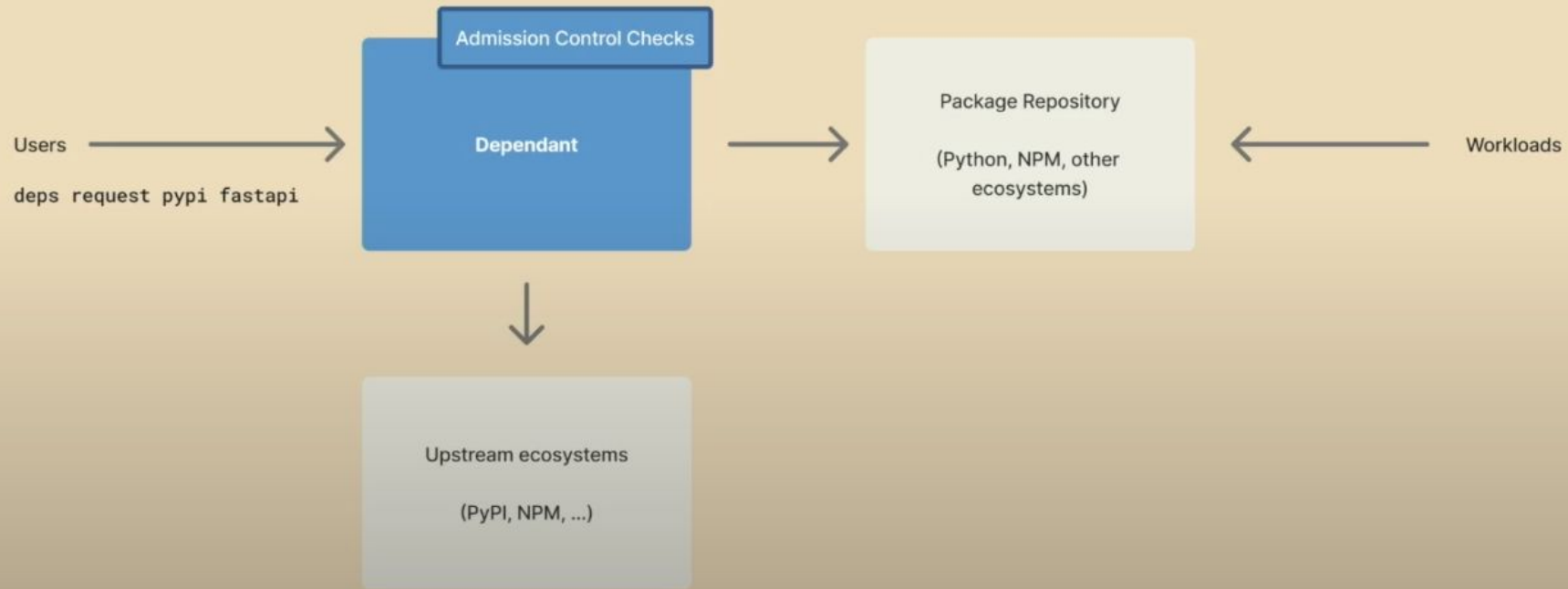
- Also using 'paved road' model
- Socket replaced Snyk as well as increased scope significantly
- Netflix didn't see value in CVE-based paid SCA tooling
- See value in reachability and deeper scanning
- Netflix reviewed building vs buying
- Rollout is deliberate, going group-by-group

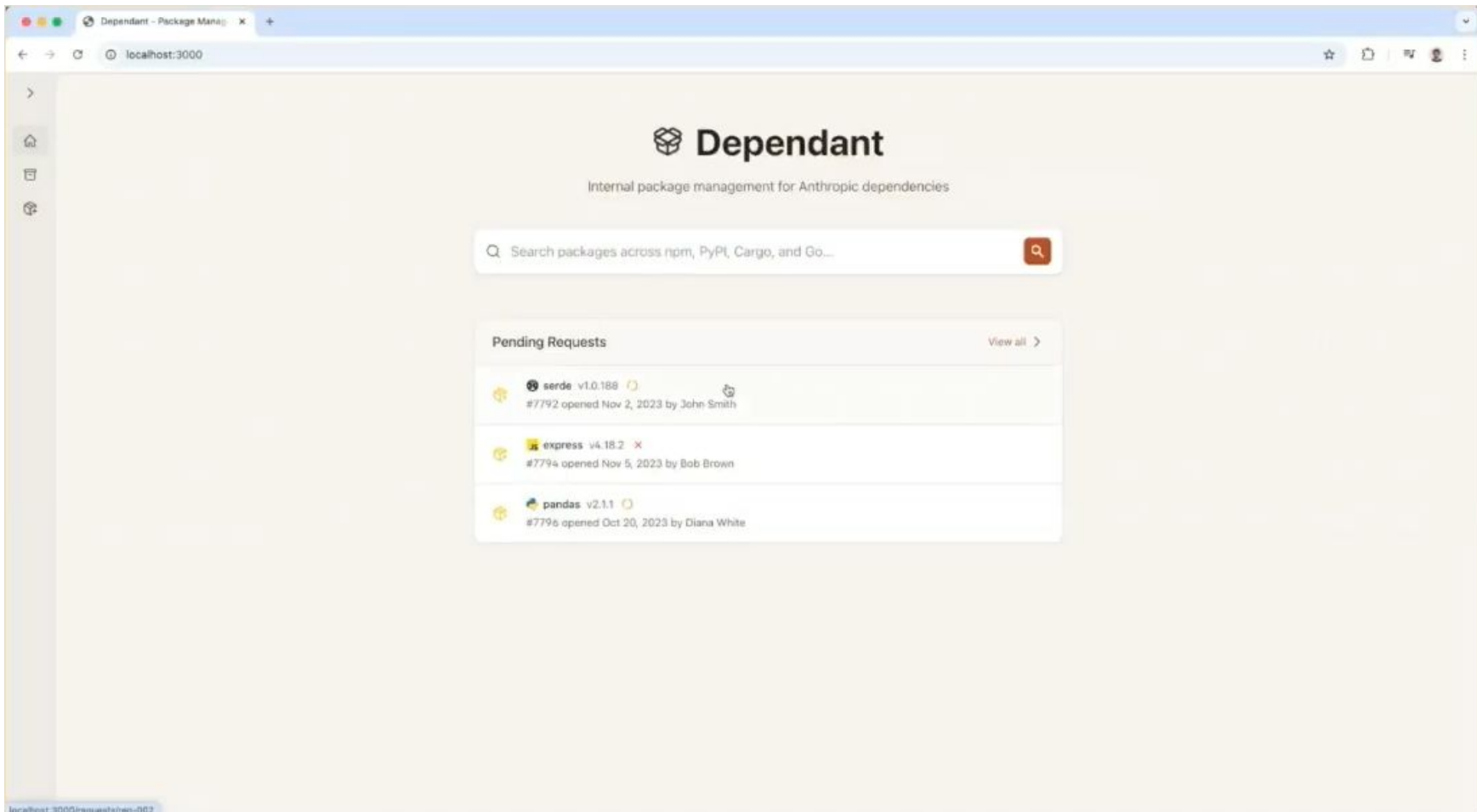
# Similar customer deployments

## Anthropic\*

- Anthropic is heavily reliant on Socket data on open source packages
- Built “Dependant” - storage for deps
- Devs can request new packages
- Anything under “X” Socket supply chain score requires admin approval

*\*Link to Anthropic's B-Sides talk: [YouTube](#) + Socket Case study: [Link to Case Study](#)*





Socket

# Roadmap

## Recently Shipped

- Socket Basics
- Socket Firewall Enterprise
- Hugging Face models
- Extension Guard
  - Chrome Extensions
  - OpenVSX
- General Webhook Support
- Socket Fix 2.0

## This quarter

- Self hosted Gitlab Integration
- Native Jira Integration
- Socket CLI Binary
- Proactive Malware Campaign Notifications
- Support Portal in Socket Dashboard

## Next quarter

- Granular RBAC
- Repo level permissions
- 2 Way Jira Integration
- Socket Firewall: Registry mode