

Secure Your Open Source

Presented by
Alan Seiden





Modernization, APIs, Open Source on IBM i

- ◆ **Seiden PHP+ Server for IBM i**
- ◆ **Develop** RPG, PHP, Node.js, Python...
- ◆ **Support** Node, PHP, open source
- ◆ **Developer Support and Mentoring**

www.seidengroup.com

Topics for this session

- ◆ Web server permissions and mistakes to avoid
- ◆ Safe open source installation and upgrade
- ◆ Supply chain poisoning issues and solutions
- ◆ Other web and API protection, including from AI bots

Avoid these mistakes
with web
permissions and settings

Mistakes people make

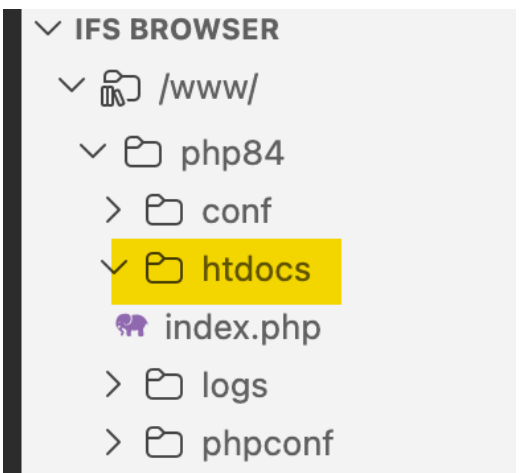
- ◆ Mistake #1: Putting sensitive files in the document root
- ◆ Mistake #2: Allowing uploads into the document root
- ◆ Mistake #3: Allowing applications to write to the document root

- ◆ Why always the document root? It is meant to be accessible from browsers and API callers. Only put there what you want potentially accessible.
- ◆ Details coming up

Typical web server directories

Defined in a web server config file or without a web server

- ◆ **/www/myserver/htdocs** (or htdocs/public)
 - ◆ "Public folder" (document root)
 - ◆ Contents can include code and static files (.js., .css, images, fonts)
- ◆ **/www/myserver/src/application** and so on.
 - ◆ Code that is not meant to be served directly, but pulled in by code in the document root
- ◆ **/www/myserver/config** or env etc.
 - ◆ Configuration files



Mistake 1: Sensitive files in doc root

- ◆ Example: .env file
- ◆ .env files can contain passwords and other secrets
- ◆ They should not be put in the document root. (I've seen it happen)
- ◆ For extra protection against this mistake, use web server rules

Protect from leaking .env and other files

- ◆ .env, .htaccess, .gitignore, and "hidden" files
- ◆ Use Apache directives :

```
<LocationMatch "/\.(?!well-known/)">  
Require all denied  
</LocationMatch>
```
- ◆ Test that access is blocked by running:
 - ◆ `curl https://mysite.com/.htaccess`
 - ◆ Curl command should return "HTTP/1.1 403 Forbidden"

Mistake 2: Uploads into doc root

- ◆ Example: allowing the user to upload images or spreadsheets and placing the files into document root
- ◆ Risk: User could upload a file containing code, then execute it using a browser, curl, etc. The code file could then, potentially, make other code changes, exfiltrate data, etc.
 - ◆ See Mistake 3 for an additional protective step
- ◆ Protection:
 - ◆ Your application should save uploaded files to a temporary work directory, NOT directly into document root.
 - ◆ A separate process should check the file for correct extension, contents, etc.
 - ◆ Only then move it to document root, if appropriate, or better still, launch it as a temporary file in the browser.

Mistake 3: When apps can write to doc root

- ◆ The document root should be read-only, except by authorized people or processes that are supposed to add or change code
- ◆ QTMHHTTP should never have *W privilege on directories or files in the document root or its subdirectories
- ◆ The setup below looks all right if ALAN is a special user

```
Work with Authority

Object . . . . . : /www/seidenphp/htdocs
Type . . . . . : DIR
Owner . . . . . : ALAN
Primary group . . . . . : *NONE
Authorization list . . . . . : *NONE

Type options, press Enter.
  1=Add user   2=Change user authority   4=Remove user

Opt  User          Data Authority  --Object Authorities--
      Authority    Exist  Mgt  Alter  Ref
--
*PUBLIC *EXCLUDE
ALAN    *RWX      X    X    X    X
QTMHHTTP *RX        X    X    X    X
```

Open source safety

Benefits of Open Source Software

- ◆ Rapid innovation
- ◆ Protection from vendor business decisions
- ◆ Community and sharing
- ◆ Common tools across platforms
- ◆ Solve problems yourself if needed

Examples

- ◆ VS Code, Code for i, and community extensions
- ◆ IBM's MCP Server (for AI)
- ◆ IBM's Mapepire database connector
- ◆ PHP and Python languages
- ◆ Node and javascript frameworks

New to Open Source on IBM i?

- ◆ How to set up your open source environment
<https://www.seidengroup.com/open-source-documentation/>

OPEN SOURCE DOCUMENTATION

We've written documentation to cover common scenarios when installing and configuring PHP and other open source environments. The following are links to our growing library of public documentation.



In addition, forward-thinking businesses engage Seiden Group for [SmartSupport](#) and [Install & Learn setup](#) to learn and to help ensure snappy, continuous service to users. Let us know if we can help!



Seiden Group Documentation Library

Open Source Environment

- ▶ [How to Set Up the IBM i Open Source Environment](#)
- ▶ [How to Configure and Use SSH on IBM i](#)
- ▶ [Overcome 'Permission Denied' for Long User Profiles in](#)

Language-specific tips

Stay current

- ◆ Open source, dynamic languages change more quickly than traditional languages such as RPG
- ◆ Each has its own lifecycle that you should get familiar with
 - ◆ Example: PHP releases a new version yearly with smaller monthly updates
- ◆ Check **<https://endoflife.date>**

Release	Released	Active Support	Security Support	Latest
8.5	5 months ago (20 Nov 2025)	Ends in 1 year and 8 months (31 Dec 2027)	Ends in 3 years and 8 months (31 Dec 2029)	8.5.5 (09 Apr 2026)
8.4	1 year and 5 months ago (21 Nov 2024)	Ends in 8 months (31 Dec 2026)	Ends in 2 years and 8 months (31 Dec 2028)	8.4.20 (09 Apr 2026)
8.3	2 years and 5 months ago (23 Nov 2023)	Ended 4 months ago (31 Dec 2025)	Ends in 1 year and 8 months (31 Dec 2027)	8.3.30 (15 Jan 2026)
8.2	3 years ago	Ended 1 year and 4 months ago	Ends in 8 months	8.2.30

Current versions of languages

◆ PHP

- ◆ PHP 8.5: newest stable release
- ◆ PHP 8.4, 8.3, 8.2: still maintained
- ◆ PHP 8.1 and below: EOL
- ◆ Check: `php -v`



◆ Node.js

- ◆ Node.js 22: newest on IBM i
- ◆ Node.js 20: EOL April 2026
- ◆ Node.js 18: EOL April 2025
- ◆ Check: `node -v`



◆ Python

- ◆ Python 3.13: newest on IBM i
- ◆ Python 3.9: EOL 2025
- ◆ Python 3.6: EOL 2021
- ◆ Check: `python --version`



Have a plan for regular upgrades

- ◆ Applications in production should have an upgrade plan
- ◆ Set up a development area you can test new versions in
 - ◆ If no dev partition, use a “chroot” container
- ◆ Consider a minor update at least quarterly
- ◆ Set aside time to upgrade and test

PHP

- ◆ Basic extensions are compiled in already
 - ◆ Not as important to download extra packages as with other languages
- ◆ Database connectors and toolkit are most mature
- ◆ Includes most of what's needed for web/API, so does not need many extra packages
- ◆ Official Support
 - ◆ Options here:
 - ◆ <https://www.ibm.com/support/pages/php-ibm-i>
 - ◆ (Seiden Group and Zend/Perforce)

Package security tip for PHP

- ◆ Prevent insecure package updates
- ◆ Install **Roave/security-advisories** in Composer.json
 - ◆ `composer require --dev roave/security-advisories:dev-latest`
- ◆ Then, whenever you run Composer `require` or `update`, throws error if any known security issues

```
./composer.json has been updated

Running composer update roave/security-advisories
Loading composer repositories with package information
Updating dependencies
Your requirements could not be resolved to an installable set of packages.

Problem 1
- laravel/framework is locked to version v8.22.1 and an update of this p
- roave/security-advisories dev-latest conflicts with illuminate/databas
- Root composer.json requires roave/security-advisories dev-latest -> sa

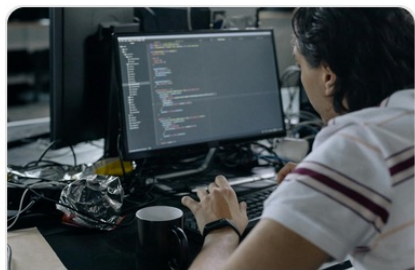
Installation failed, reverting ./composer.json and ./composer.lock to their
```

<https://github.com/Roave/SecurityAdvisories>

Python

- ◆ I was about to say I had not heard about any hacking of the Python ecosystem (more later about supply chain attacks). This one was caught/stopped quickly.

📰 News for python supply chain hack



Three separate supply-chain attacks hit npm, PyPI, and Docker Hub within...

1 day ago

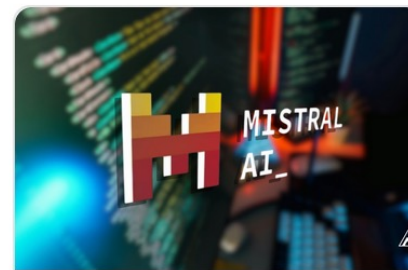
 msn.com



GitHub Confirms Hack Impacting 3,800 Internal Repositories

2 hours ago

 securityweek.com



Microsoft Flagged Mistral AI Hack in PyPI Malware Supply Attack

5 days ago

 memeburn.com



M > Wor TanS Guar

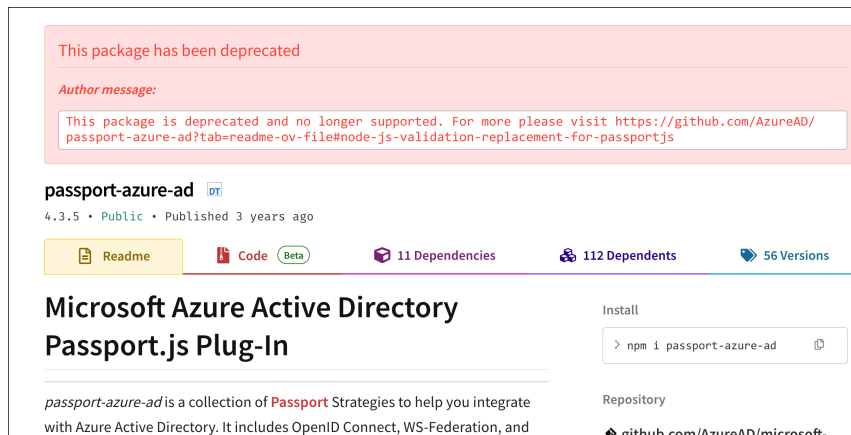
8 day

 the



Node


- ◆ Designed to use downloadable modules for needed functionality
- ◆ There are millions of modules that rely on each other
- ◆ Install modules via "npm" command
- ◆ Modules evolve, change. Need to keep an eye out



This package has been deprecated

Author message:

This package is deprecated and no longer supported. For more please visit <https://github.com/AzureAD/passport-azure-ad?tab=readme-ov-file#node-js-validation-replacement-for-passportjs>

passport-azure-ad 

4.3.5 • Public • Published 3 years ago

[Readme](#) [Code](#) Beta [11 Dependencies](#) [112 Dependents](#) [56 Versions](#)

Microsoft Azure Active Directory Passport.js Plug-In

Install

```
> npm i passport-azure-ad
```

Repository

github.com/AzureAD/microsoft-

passport-azure-ad is a collection of **Passport** Strategies to help you integrate with Azure Active Directory. It includes OpenID Connect, WS-Federation, and

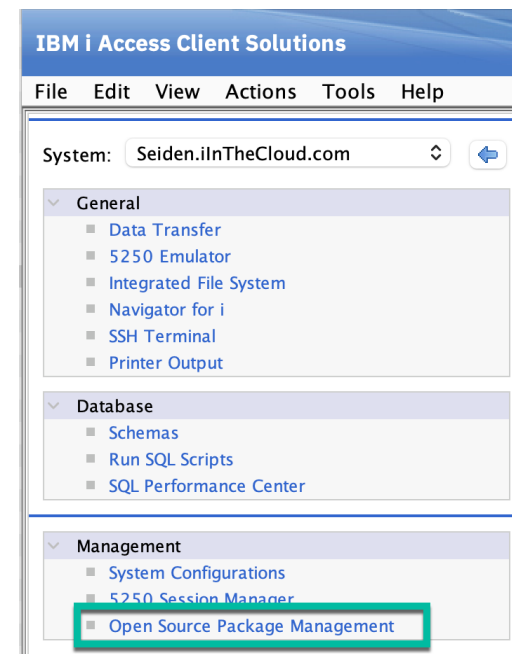
Installing open source (safely)

General safety principles

- ◆ Use versions you have tested and that have no known security vulnerabilities
- ◆ Do not install packages from public repositories directly into production
- ◆ Test in a test area, and once the packages are proven, move those proven versions to production

Set Up Open Source Environment

- ◆ <https://www.seidengroup.com/php-documentation/how-to-set-up-the-ibm-i-open-source-environment/>
- ◆ IBM i SSH server service must be running (port 22 by default)
 - ◆ STRTCPSVR *SSHD to start SSH
- ◆ Install environment using Access Client Solutions (ACS) Open Source Package Management



Get a "good known working repository"

- ◆ Clone a repository that you can install again, as needed, in production or other servers.

Clone Repo for Offline Use

Source Repository

- IBM default `https://public.dhe.ibm.com/software/ibmi/products/pase/rpms/repo-base-7.3`
- Specify a location:

Destination (IFS)

`/QOpenSys/QIBM/UserData/rpm_repos/ibm`

- Clear repository before download (recommended)

Additional Operations

- Configure package manager to use this cloned repository
- Allow package manager to skip repositories that may require Internet access
- Create nginx configuration files for serving this cloned repository to other IBM i systems [?](#)

Clone Repository

File | Progress

Why do you need a "good working" repo?

- ◆ If you find a bug in a package
- ◆ Example: ODBC driver 1.1.0.28 had several bugs
- ◆ Can't we use **yum downgrade** to bring us back to 1.1.0.27? In this case, yes, but not always, because IBM deletes older versions from their live repository.
- ◆ One of our PHP support customers needed ODBC 1.1.0.23 in production to match what they had in development, but since IBM no longer hosted 1.1.0.23, the company had to manually copy files from /QOpenSys and missed some, causing weeks of extra work and confusion

Why else?

- ◆ To have a version that will have **no unexpected security issues**.
- ◆ For more on the risks of security issues that can pop up, we will cover supply chain poisoning.

Repotrack for quicker cloning

- ◆ The ACS clone/mirror approach will copy ALL files in a repository, even the ones you do not need, and all old versions.
- ◆ If you only want **specific components and their dependencies**, the **repotrack** command is quicker.
- ◆ Example of downloading only the needed rpm files for PHP and related components:

```
cd /mydir  
repotrack "php-*" siteadd ibm-iaccess ibmichroot  
yum install *
```

Supply Chain Issues

Npm hack in September 2025

- ◆ <https://www.seidengroup.com/2025/10/17/what-the-shai-hulud-npm-worm-means-for-node-js-developers/>
- ◆ Situation: Node.js applications can use hundreds of npm modules. In the last year, these have been hacked more than once



The Node.js ecosystem has been disrupted by self-replicating malware called **Shai-Hulud**.

In September 2025, researchers found that Shai-Hulud **had infected more than 500 npm packages**, including some from trusted maintainers. The worm did not just publish a few bad versions. It spread automatically, using stolen credentials to infect other packages owned by the same developer.

Steps of the attack

- ◆ Began with phishing of an npm maintainer
- ◆ People who installed the compromised npm were affected, as the worm searched for secrets such as npm tokens, GitHub access tokens, and cloud credentials
- ◆ It also added hidden GitHub Actions workflows that sent data to attacker-controlled servers
- ◆ ... and more...

Mitigation instructions at the time

- ◆ Suspend non-critical npm deployments until dependencies are reviewed against the [Qualys list of affected packages](#).
- ◆ Rotate credentials: npm tokens, GitHub tokens, deploy keys, and any cloud credentials used in pipelines.
- ◆ Audit CI/CD pipelines and GitHub workflows for unauthorized changes, especially new or altered workflow files.
- ◆ Investigate unusual outbound activity during builds, such as suspicious HTTP(s) requests or unexpected modifications to package.json.
- ◆ Do not rely solely on npm audit. It may not yet flag all affected versions. Use the Qualys list and targeted scripts.

Node npm community reacted

- ◆ Removal of over 500 compromised packages
- ◆ Blocking upload of packages related to the worm
- ◆ Mandatory two factor authentication (2FA) in future
- ◆ Use of OpenID Connect authentication to replace long-lived tokens
- ◆ Adoption of gradual rollouts, rather than immediate publishing that can cause rapid infection of many packages

Our customers have noticed

Last week, a customer emailed me:

Hi Alan,

We are reaching out regarding the recently identified pattern of software supply chain compromises, affecting major open-source software repositories like Node Package Manager, Composer, Nuget, Pypi, and associated GitHub repositories, which introduces significant risk to ALL software development and CI/CD environments.

As part of our third-party risk management program, we are requesting confirmation of your organization's assessment and response to this issue. Please provide the following information:

Whether your environment uses any affected packages (see below links of recent packages affected)

Actions taken to identify potential exposure (e.g., inventory review, SBOM analysis)

Mitigation steps implemented (e.g., suspension of updates, hash pinning, repository proxies)

...

Beware automatic installation scripts

- ◆ <https://it.slashdot.org/story/26/06/01/1624228/red-hat-npm-packages-compromised-to-spread-a-credential-stealing-worm>
- ◆ RedHat npm packages affected by this one
- ◆ "Each compromised package **declares a preinstall script** in its package.json that executes node index.js automatically on every npm install, before any application code runs and before the developer has any indication something is wrong. The index.js file is 4.2 MB payload hidden behind multiple layers of obfuscation."
- ◆ The script finds AWS access keys, Github Actions secrets, Azure credentials, HashiCorp Vault tokens...

NEW: npm update to control scripts

- ◆ <https://github.blog/changelog/2026-06-09-upcoming-breaking-changes-for-npm-v12/>
- ◆ npm 11.16.0 will **warn** about unapproved scripts
- ◆ npm 12 will **block** unapproved scripts
- ◆ Example of approving scripts for odbc module:

```
npm approve-scripts odbc  
Approved odbc:  
  added odbc@2.4.7
```
- ◆ We must approve odbc npm scripts because the installation runs node-gyp (needed to compile the odbc driver).
- ◆ I ran `npm install npm@latest -g`

General rule: minimize dependencies

- ◆ Always minimize the number of third party components you use, even frameworks
- ◆ For Node.js, specifically, minimize the number of npm modules
 - ◆ An npm often uses many others underneath, multiplying your exposure
- ◆ Example: [Axios npm supply chain compromise](#) (March 2026)
 - ◆ Axios provides HTTP request support from Javascript
 - ◆ Browser "AJAX" calls
 - ◆ HTTP calls from Node.js on the server
 - ◆ Commonly used module
 - ◆ Native alternative: Fetch API (modern browsers and Node 21/22)

For Github Actions, pin to a version

- ◆ You can guarantee using a [specific version of a Github action](#) via commit SHA hash
- ◆ `actions/checkout@692973e3d937129bcbf40652eb9f2f61becf3332`
- ◆ Real example from our work with a customer's Github Actions

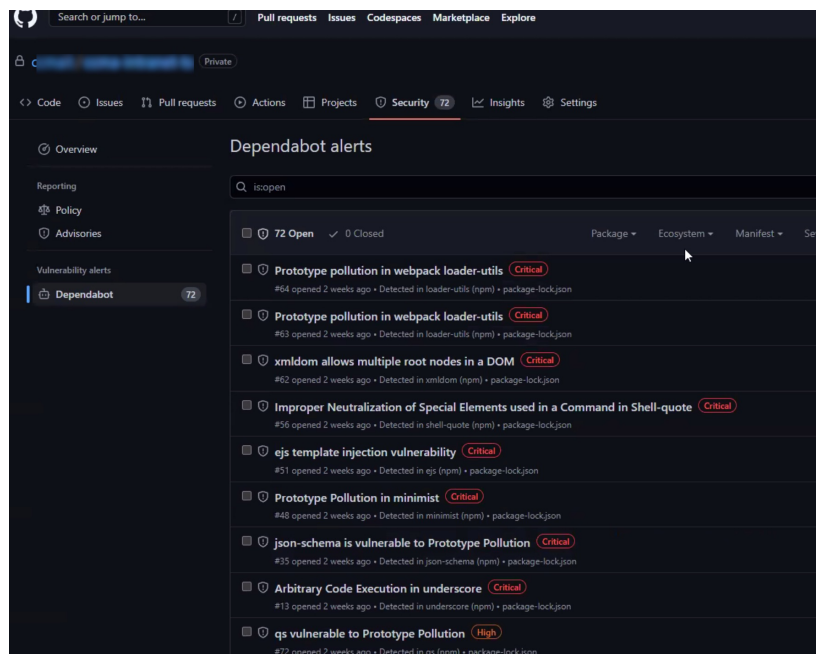
```
jobs:
  build:
    runs-on: ubuntu-latest

    permissions:
      contents: read
      packages: write

    steps:
      - uses: actions/checkout@34e114876b0b11c390a56381ad16ebd1391 |d5| # v4.3.1
      - uses: docker/setup-buildx-action@8d2750c68a42422c14e847fe6c8c |403b4cbd6f # v3.12.0
      - uses: docker/login-action@c94ce9fb468520275223c153574b0c |6fe4bcc9 # v3.7.0
      with:
```

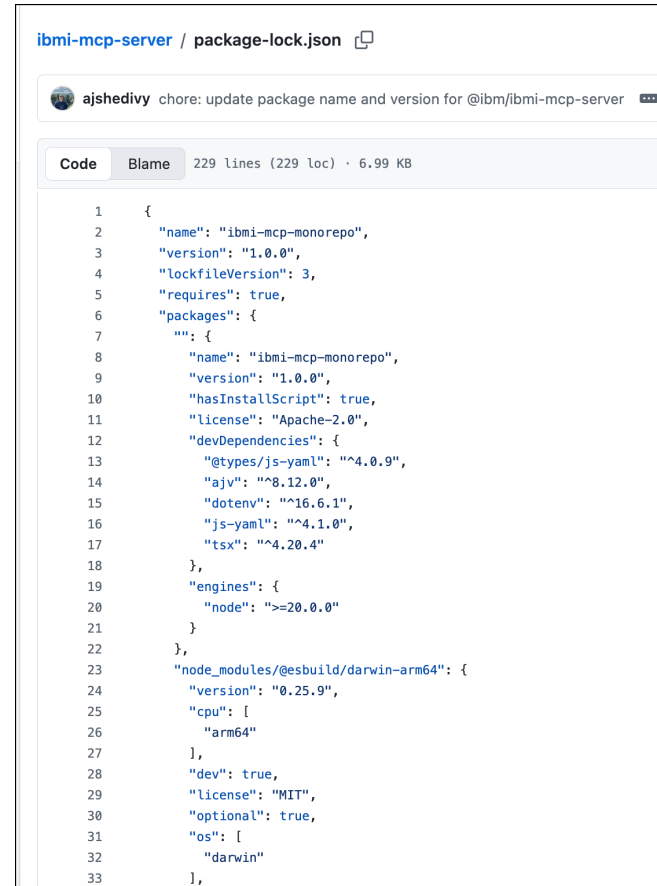
Security: GitHub Dependabot

- ◆ Dependabot looks for security updates on packages
- ◆ You can set it up to scan your private Git repository for updates for packages that your project uses



"npm ci"

- ◆ I asked IBM at the time, "What about applications such as MCP server, built in Node and using npm modules? Are they safe?" (<https://github.com/IBM/ibmi-mcp-server>)
- ◆ IBM answered: Don't just "npm install" it. Do `npm ci` ("clean install") using a known `package-lock.json` with known good versions

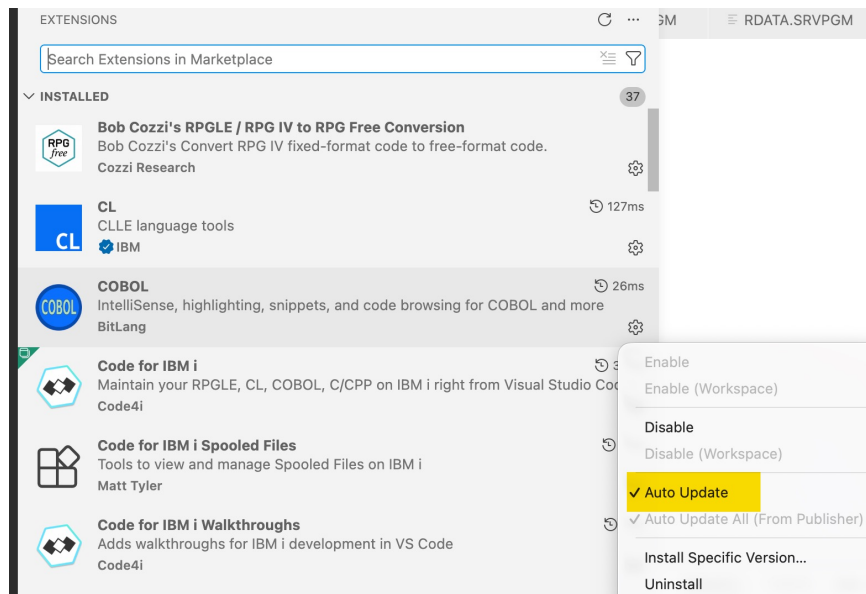


```
ibmi-mcp-server / package-lock.json
ajshedivy chore: update package name and version for @ibm/ibmi-mcp-server
Code Blame 229 Lines (229 loc) · 6.99 KB
1 {
2   "name": "ibmi-mcp-monorepo",
3   "version": "1.0.0",
4   "lockfileVersion": 3,
5   "requires": true,
6   "packages": {
7     "": {
8       "name": "ibmi-mcp-monorepo",
9       "version": "1.0.0",
10      "hasInstallScript": true,
11      "license": "Apache-2.0",
12      "devDependencies": {
13        "@types/js-yaml": "^4.0.9",
14        "ajv": "^8.12.0",
15        "dotenv": "^16.6.1",
16        "js-yaml": "^4.1.0",
17        "tsx": "^4.20.4"
18      },
19      "engines": {
20        "node": ">=20.0.0"
21      }
22    },
23    "node_modules/@esbuild/darwin-arm64": {
24      "version": "0.25.9",
25      "cpu": [
26        "arm64"
27      ],
28      "dev": true,
29      "license": "MIT",
30      "optional": true,
31      "os": [
32        "darwin"
33      ],

```

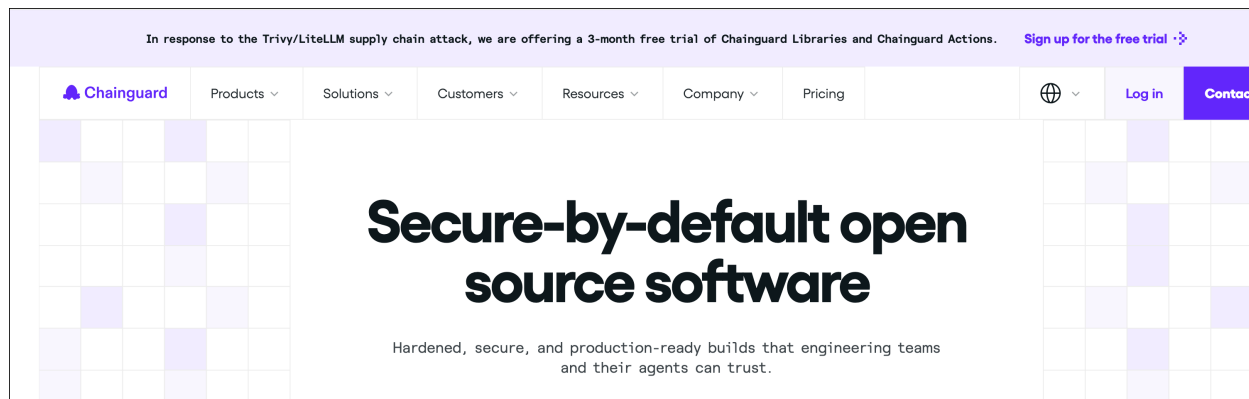
What about VS Code?

- ◆ VS Code extensions have been hit (GlassWorm recently)
- ◆ Suggestion: use Auto Update only for your most trusted extensions
- ◆ Consider OWASP IDE-VulScanner (has its own dependencies)



One more trend in supply chain

- ◆ Commercial repositories of tested components
- ◆ More like how IBM curates its own open source
- ◆ One company I spoke to at the Linux Foundation MCP Dev conference in New York in April:
 - ◆ <https://www.chainguard.dev/>



Industry email yesterday

- ◆ Email from Chainguard that I received 15 June 2026:

Hi, Alan, a couple of weeks ago I wrote about [the hardest fork](#): the choice between letting open source security fragment into a dozen rival patch sets nobody can reconcile, or doing the hard, coordinated thing instead. I said it would only work if we built it together, and admitted I had no idea if we actually would.

Here's the update: the industry showed up. It's called [Athena](#), and it's live.

Athena is a coalition for the orchestrated defense of open source with more than two dozen members including BNY, Chainguard, Cisco, Cloudflare, Corridor, Depthfirst, Docker, J.P. Morgan, Kyndryl, LTM, and PWC.

What about RPG?

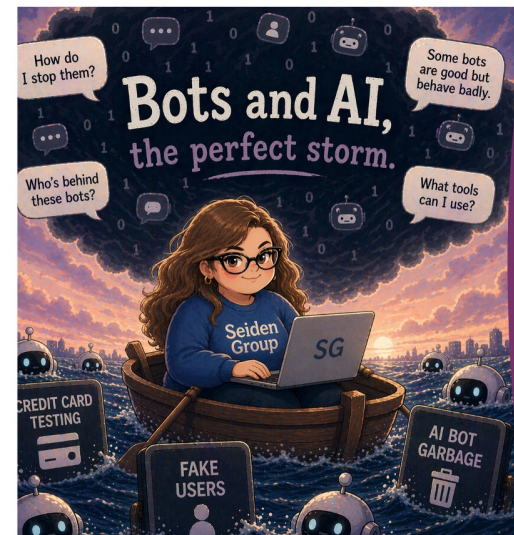
RPG Benefits for APIs

- ◆ **Easy deployment – no dependencies to manage**
- ◆ **No "yearly/quarterly upgrade cycle"**
- ◆ **Direct, native integration with Db2**
 - ◆ No need to "make a connection"
 - ◆ No extra database jobs to manage (e.g. QZDASOINIT jobs)
- ◆ **A solid API back-end**

Protect from Bots

A few tips about bot protection

- ◆ For an expanded presentation by Holly Lacher from the Seiden team, go to <https://www.seidengroup.com/2026/06/15/access-modern-security-for-ibm-i-and-connected-web-environments/>
- ◆ Holly presented more about bots for the OCEAN group
- ◆ Includes details on defeating credit card number testing



'bots can keep your site busy

- ◆ Bots can tie up your site if use many connections/threads
- ◆ Review web server logs for repeated access by bots
 - ◆ Now AI training bots

The screenshot shows a log file with columns: ID, REQUEST_URL, STATUS, BYTES, RESPONSE, REQUEST_TS, and CHANGE_TS. The log contains numerous entries with a status of 200 and a response of 144, indicating successful requests. The REQUEST_TS column shows a high frequency of requests, suggesting a bot is accessing the site.

- ◆ You can restrict by IP using firewall
- ◆ We are also seeing success with commercial reverse proxy services, such as Cloudflare, to reduce denial of service attacks by bots

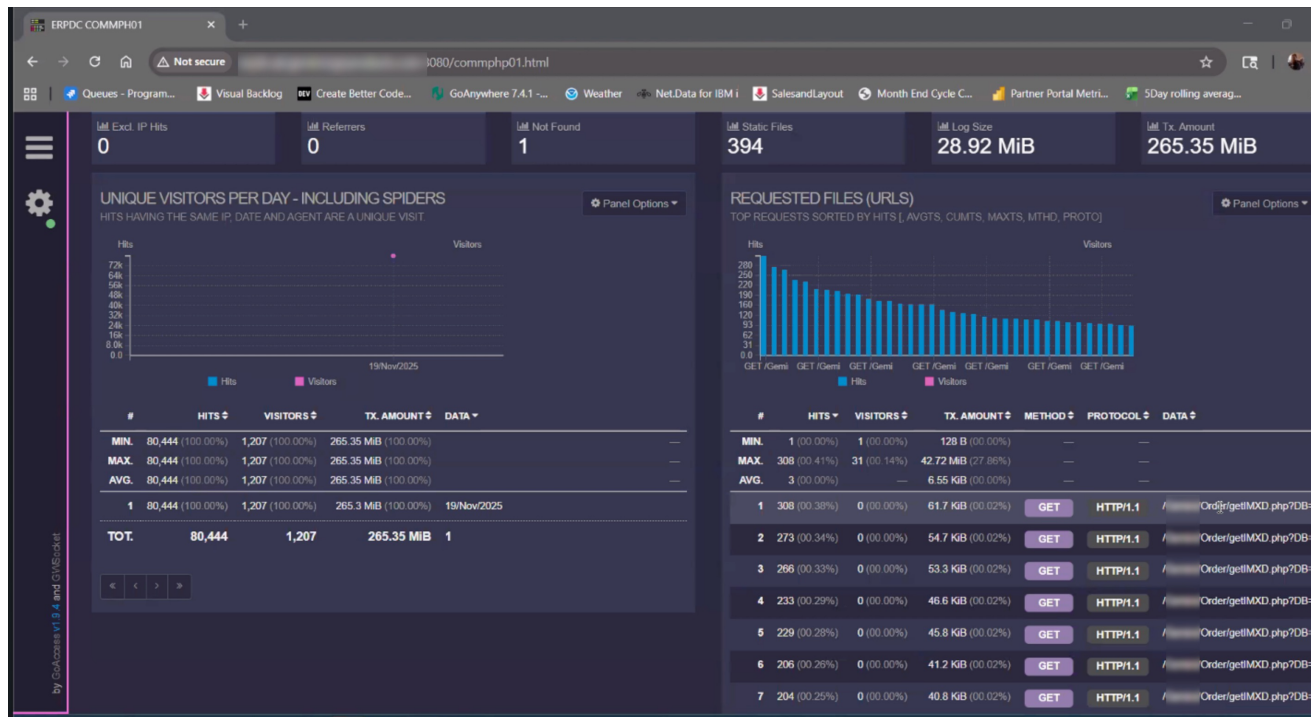


Cloudflare I was there

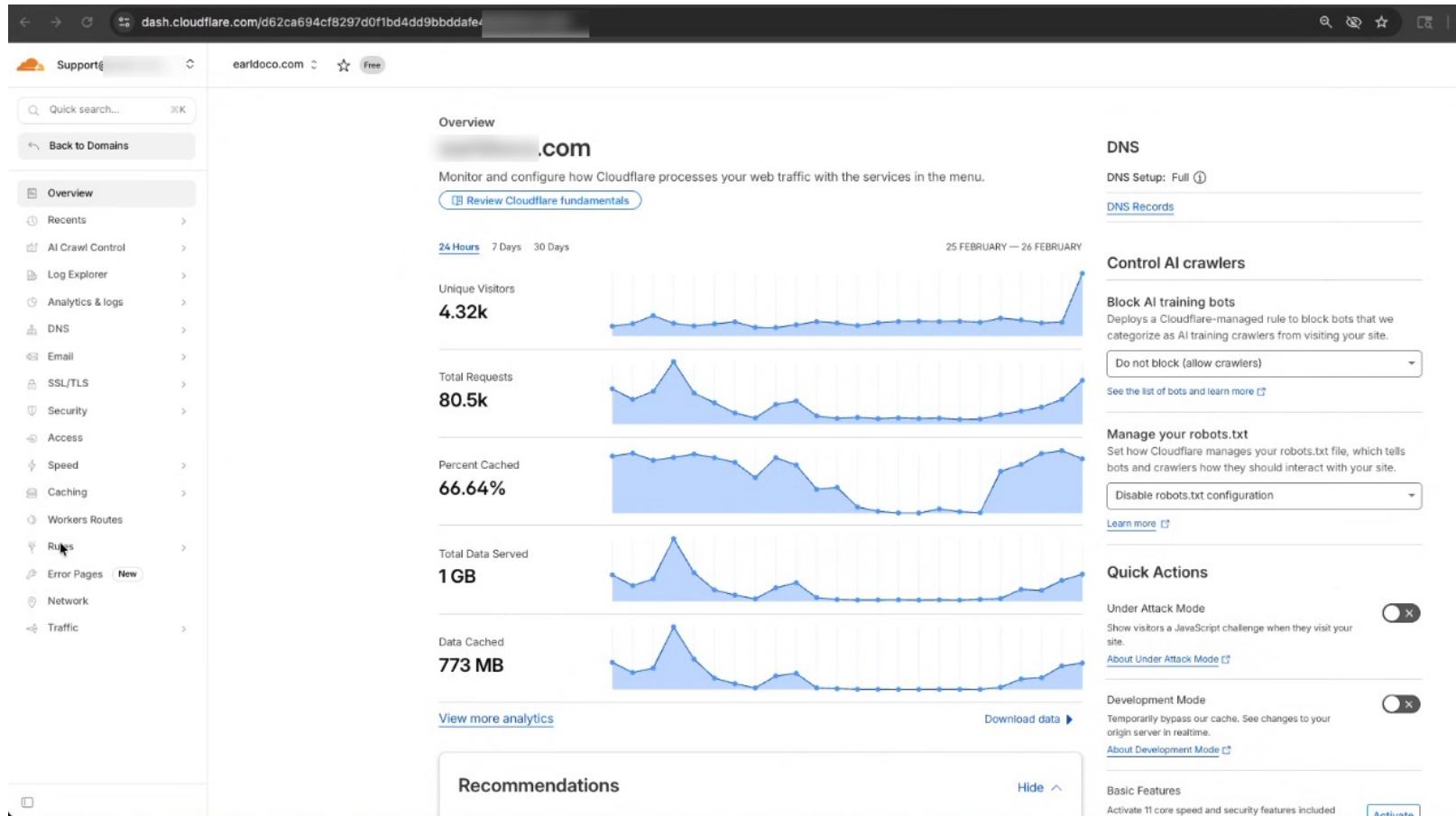


Try GoAccess

- ◆ See what bots and spiders are coming in
- ◆ <https://goaccess.io/> and IBM i version from Seiden Group



Cloudflare management (free version)



AI Crawl Control







AI Crawl Control Documentation

Analyze and control how AI Crawlers access your content.

Crawlers

Select crawler Select operator + Add filter Last 24 hours (CST)

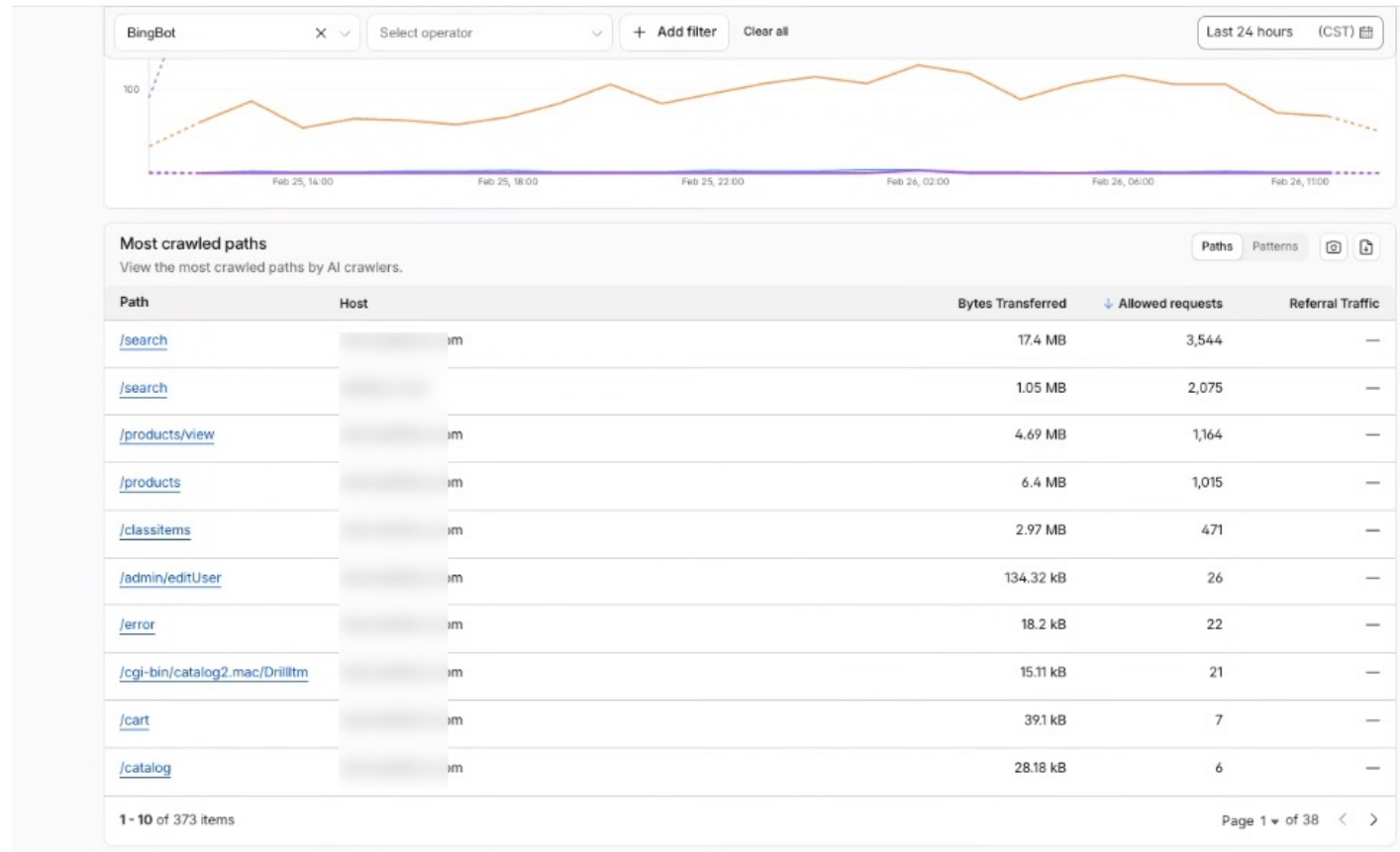
Show inactive crawlers

<input type="checkbox"/> Crawler	Category	Bytes Transferred	Requests	Action
<input type="checkbox"/> BingBot Microsoft	Search Engine Crawler	49.63 MB	 Allowed: 8.78k Unsuccessful: 42	Allow Block
<input type="checkbox"/> Googlebot Google	Search Engine Crawler	5.52 MB	 Allowed: 1.06k Unsuccessful: 36	Allow Block
<input type="checkbox"/> PetalBot Huawei	AI Crawler	92.34 kB	 Allowed: 90 Unsuccessful: 104	Allow Block
<input type="checkbox"/> Applebot Apple	AI Search	141.87 kB	 Allowed: 31 Unsuccessful: 27	Allow Block
<input type="checkbox"/> Bytespider ByteDance	AI Crawler	994 B	 Allowed: 1 Unsuccessful: 2	Allow Block
<input type="checkbox"/> ChatGPT-User OpenAI	AI Assistant	0 B	 Allowed: 0 Unsuccessful: 3	Allow Block
<input type="checkbox"/> Novellum AI Crawl Novellum	AI Crawler	0 B	Allowed: 0 Unsuccessful: 0	Allow Block
<input type="checkbox"/> Anchor Browser Anchor	AI Crawler	0 B	Allowed: 0 Unsuccessful: 0	Allow Block
<input type="checkbox"/> Amazonbot Amazon	AI Crawler	0 B	Allowed: 0 Unsuccessful: 0	Allow Block
<input type="checkbox"/> archive.org_bot Internet Archive	Archiver	0 B	Allowed: 0 Unsuccessful: 0	Allow Block
<input type="checkbox"/> CCBot Common Crawl	AI Crawler	0 B	Allowed: 0 Unsuccessful: 0	Allow Block
<input type="checkbox"/> ClaudeBot	AI Crawler	0 B	Allowed: 0	Allow Block

<https://blog.cloudflare.com/introducing-ai-crawl-control>

AI Crawl Control (detail)

Free AI Crawl Control



AI bots misbehaving

Free AI Crawl Control

BingBot X Select operator + Add filter Clear all Last 24 hours (CST)

www www.com/robots.txt		Successful: 7 Unsuccessful: 0	200 OK	Not set
_domainconnect _domainconnect.earldoco.com/robots.txt		Successful: 0 Unsuccessful: 0	530 Origin DNS Error	Not set
autodiscover autodiscover.earldoco.com/robots.txt		Successful: 0 Unsuccessful: 0	521 Web Server Is Down	Not set
email email.com/robots.txt		Successful: 0 Unsuccessful: 0	403 Forbidden	Not set
e e.com/robots.txt		Successful: 0 Unsuccessful: 0	403 Forbidden	Not set

1 - 5 of 17 items Page 1 of 4

Violations

Identify AI crawlers requesting paths currently disallowed by your robots.txt. This list only shows violations on highest-traffic paths. Filter by Crawler, Operator, or Hostname to view detailed activity.

Crawler	URL	Directive	Requests
BingBot Microsoft	search	Disallow: /	3544 Violations
BingBot Microsoft	ch	Disallow: /	2075 Violations
BingBot Microsoft	products/view	Disallow: /	1164 Violations
BingBot Microsoft	products	Disallow: /	1015 Violations
BingBot Microsoft	classitems	Disallow: /	471 Violations

Honeypot traps (paid version)

Pro plan

Web application exploits DDoS attacks **Bot traffic** API abuse Client side abuse Domain settings

Assets and endpoints Rule templates Detection tools Dashboard version Clear all

AI Labyrinth Beta 📄 🔴

AI Labyrinth modifies your web pages by adding nofollow links that contain AI-generated content to disrupt bots ignoring crawling standards. The nofollow links added do not alter the contents of your web pages and are only visible to bots.

General Bot traffic

Block AI bots 📄

Deploys a Cloudflare-managed rule to block bots that we categorize as AI training crawlers from visiting your site. [See the list of bots and learn more](#)

Configurations

Blocks AI Bots scope: Do not block (off) ✎

General Bot traffic DDoS attacks

Instruct AI bot traffic with robots.txt Beta 📄 🔴

Creates or updates your robots.txt file to signal that your content should not be used for AI training.

Chat

Documentation ✕

[Go to full documentation](#)

Cloudflare Docs 🔍 ☰

On this page > Overview

The AI Labyrinth adds invisible links on your webpage with specific `Nofollow` tags to block AI crawlers that do not adhere to the recommended guidelines and crawl without permission. AI crawlers that scrape your website content without permission will be stuck in a maze of never-ending links, and their details are recorded and used by all Cloudflare customers who choose to block [AI bots](#).

These links do not impact your search engine optimization (SEO) or your website's appearance, and are only seen by bots. AI bots that respect no-crawl instructions will safely ignore this honeypot.

To enable [AI Labyrinth](#):

Old dashboard 🔗 **New dashboard**

- 1 Log in to the [Cloudflare dashboard](#), and select your account and domain.
- 2 Go to **Security > Bots**.
- 3 Select **Configure Bot Fight Mode**.
- 4 Enable **AI Labyrinth**.

LLM filters (Personal info and more)

New filter

PII in LLM prompt

equals

No

Cancel Apply

LLM PII Categories

Has PII in LLM prompt

LLM unsafe Topics

Has unsafe topics in LLM

Sep 9, 2025

60:100e:b243:abd2:5984:...

www. com

Custom rules by country and more

Security

Security rules




Secure your domain with security actions that run on incoming requests. Configure both Cloudflare's managed rules and your own custom security rules. You can build custom security rules from scratch or use templates to help you get started.

[Security rules documentation](#) [Traffic sequence](#)

Security rules DDoS protection

Custom rules Status

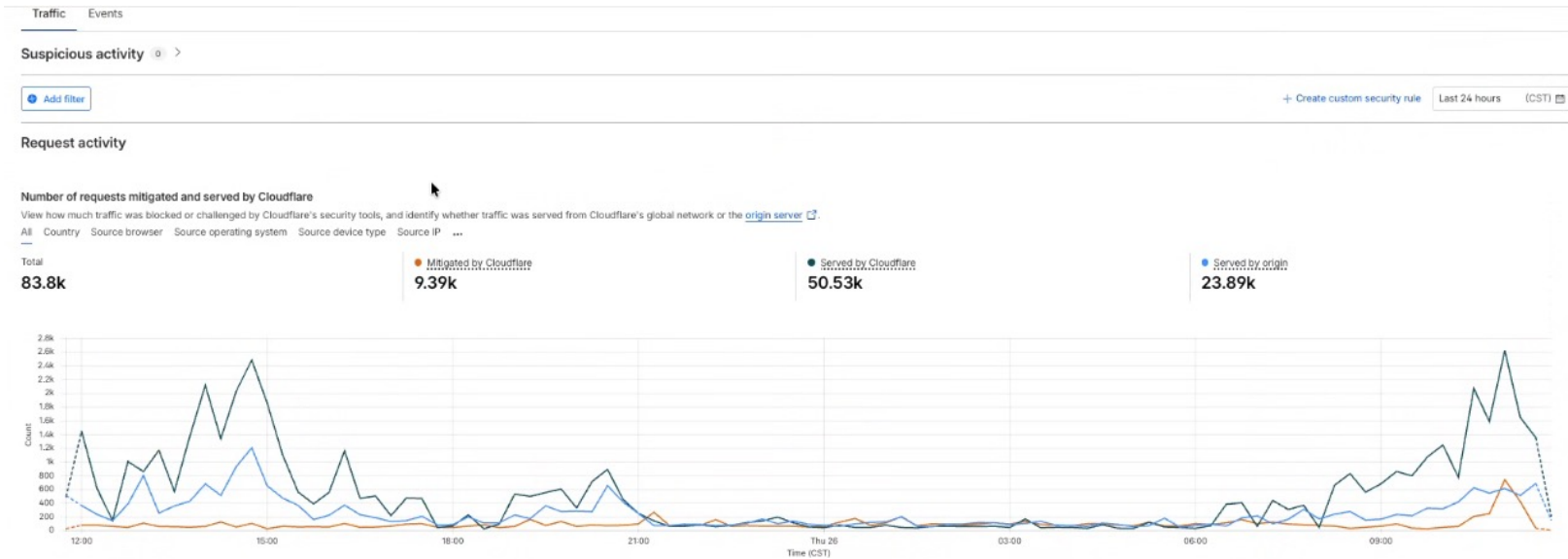
Custom rules 3/5 used [Create rule](#) [Summarize with Cloudy](#) [Go to detection settings](#)

Order	Name	Match against	Action	CSR ⓘ	Events last 24h	
1	Block bad actor countries	Country is in AF, BY, CN, CG, CD, CU, HT, IR, IQ, KP, LR, LY, MM, RU, RW, SO, SD, SY, VN, BR	Block	-	 1.47k	Active ⋮
2	Outside US	Country does not equal US	Managed Challenge	0%	 7.71k	Active ⋮
3	AI Crawl Control - Block AI bots by User Agent	URI Path does not equal /robots.txt, User Agent contains Amazonbot, User Agent contains Anchor Browser, User Agent contains Applebot,...	Block	-	 31	Active ⋮

[Show all rule types](#)

- ◆ See who tried to solve managed challenge ("are you a human?")
- ◆ "WAF Score" shows threat risk

Overview of benefit to the server



- ◆ Stopped 50,000 unneeded requests (even in the free version)

Key Take-Aways

- ◆ What did you learn that you will use?
- ◆ Anything important you hoped to see?

Free Resources from Seiden Group

- ◆ Code for i Fridays
 - ◆ <https://www.seidengroup.com/vs-code-for-i-fridays/>
 - ◆ Next: June 19 at 2:30pm ET
- ◆ IBM i Strategy and Tips (monthly)
 - ◆ <https://www.seidengroup.com/tips/>
- ◆ PHP Free Upgrade Assessment
 - ◆ <https://www.seidengroup.com/free-php-upgrade-assessment/>

Node.js v20 and Other Updated Packages Require New IBM i Repositories
by Alan Seiden

IBM i The latest IBM i open source packages, such as Node.js v20, require new IBM i repositories. We've heard from several perplexed clients wondering why Yum tells them "No package nodejs20 available" during their node upgrade.

This article shows you how to install the latest IBM i repositories to enable your open source updates well into the future . . .

[Read More](#)

What IBM i Users Should Check when Learning of an Open Source Security Vulnerability
by Alan Seiden

 <https://>
API & Web Security

Security continues to be a top concern in IT, especially among upper management.

This article shows how to check IBM i open source components to ensure they are at a patched level if a vulnerability is reported . . .

[Read More](#)

Contact | Stay in Touch

Alan Seiden

Seiden Group

Ho-Ho-Kus, NJ

alan@seidengroup.com

201-447-2437



Monthly Tips:

seidengroup.com/tips

Open Source Support and Seiden PHP+ Server

<https://www.seidengroup.com/seiden-php-for-ibm-i/>

