▸ EVERY BUILD UNDER YOUR CONTROL_

Untrusted Code, Governed.

> Scanners list what your build declares.
> Provenance attests to where it came from.
> **Endura controls what it does.**

Runtime Sensor observes what every pipeline actually does, turns that behavior into least-privilege policy, and enforces it in the Linux kernel.

```
/opt/endura/sensor

$ sudo systemctl enable --now endura-sensor
$ endura sensor status
active (online)

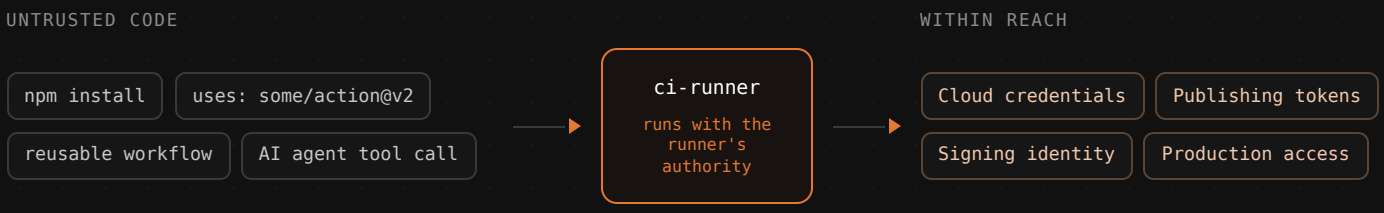
$ sudo endura job start --mode enforce \
    --workspace ./ci_job
3f9a1c7e5b2d8046

$ sudo endura sensor logs -f
> DENY path.open ~/.npmrc
> DENY ip.connect 45.9.148.0/24:443
```

▸ THE BUILD IS THE BREACH_

Your Pipeline Holds Every Key You Own

Every build runs code nobody fully reviewed, and it executes the moment it is pulled in. Before tests, before scans, before review, it already runs with the authority of the runner.



619M+	2,236	100%	267
monthly downloads of packages hijacked in a single August 2026 attack	malicious package versions published on August 4, 2026	of 2026's three largest npm attacks carried valid provenance	days on average to identify and contain a supply chain compromise

▸ THREAT COVERAGE_ 40+ techniques

Pipeline Threats, Stopped At Execution

- File Access
- Memory Attacks
- Container Breakouts
- Process Injection
- Credential Theft
- Network Exploitation
- Privilege Escalation
- Kernel Exploitation
- Reverse Shells
- Malicious Persistence

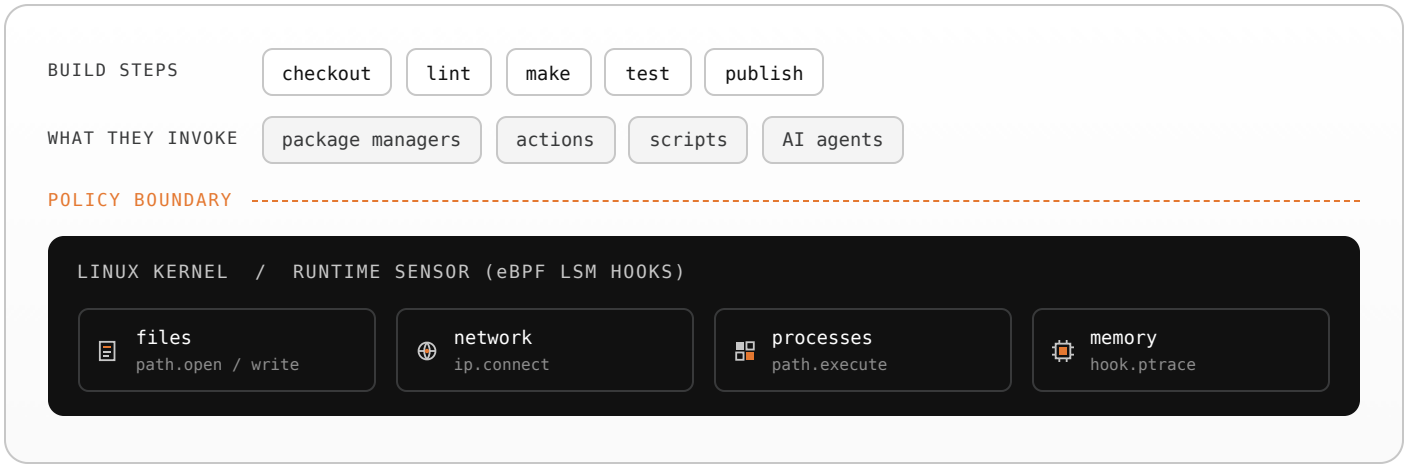
Behavior-based, not signature-based. Endura denies actions outside your policy, including techniques that have no name yet. Because it governs behavior rather than manifests, coverage does not change with the package ecosystem.

▸ ENGINEERED FOR ENFORCEMENT_

eBPF LSM hooks

In The Kernel, Where Code Can't Hide

Runtime Sensor runs as eBPF below the build and everything it invokes. File, network, process, and memory operations all pass through the kernel to happen at all, so that is where policy is enforced. Where eBPF LSM is unavailable, the Sensor monitors and terminates the offending process after detection, a weaker guarantee than inline denial.



50+	40+	<5%	22
kernel-level security hooks	threat techniques prevented	typical build overhead	validated Linux release targets

▸ FOUR STAGES_

Team Server + Runtime Sensor

From Observation To Enforcement In Four Stages

01 DISCOVER_

Every Pipeline, Monitored

See every pipeline across providers and environments in one place.

02 DERIVE_

Every Behavior, Captured

Runtime Sensor records what a build touches, from the kernel.

03 ENFORCE_

Every Action, Governed

Deny-by-default policy, enforced with eBPF LSM hooks while the build runs.

04 RESPOND_

Every Violation, Actionable

Violations arrive with the rule and the process chain, routed to Slack, Teams, or email.

▸ POLICY AS CODE_

Assigned per pipeline

Versioned JSON, Reviewed Like Any Other Code

Endura derives a baseline from what your builds actually do, you refine it into an intentional boundary, and observe mode validates it before anything is denied.

.endura/policy.json

```
{
  "mode": "enforce",
  "ip": {
    "connect": [
      "/usr/bin/curl|api.example.com|{80,443}",
      "all|140.82.112.0/20|443"
    ]
  }
}
```

POLICY PRIMITIVES

`path.open`	File opens, such as `~/.ssh`, `~/.aws`, or `~/.npmrc`
`path.create` / `path.write`	File creation and modification
`path.execute`	Execution chain: grandparent, parent, target
`ip.connect`	Outbound connections by program, host or CIDR, and port
`hook.ptrace`	Tracing of, or memory access to, another process

Rules take 1 to 3 operation-specific fields, with the **`all`** wildcard, **`{a,b}`** expansion, and **`%workspace%`** variables. Covered operations not listed are denied.

▸ DEPLOYMENT AND OPERATION_

SaaS or 100% self-hosted

Ships As A Package, Runs As A Service

DEPLOYMENT

Runs under systemd, Docker, Podman, or as a Kubernetes DaemonSet. Team Server as SaaS or self-hosted.

HOST REQUIREMENTS

Linux kernel 5.11+ with BPF LSM, BTF at `/sys/kernel/btf/vmlinux`, root, 1 GiB memory, outbound HTTP(S).

ACCESS AND ALERTING

OIDC sign-in with role, resource, and policy controls. Alerts to Slack, Teams, and email.

FAILURE BEHAVIOR

Sensor shutdown or loss of Team Server does not stop running jobs. A denial stops the offending process, which can fail that step.

▸ ENDURA APPLIED_

Self-replicating credential harvester

Case Study: The Shai-Hulud npm Worm

01 THE ATTACK

Install Hook Runs First

A preinstall script executes during `npm install`, before tests, scans, or review.

THE POLICY THAT STOPS IT

`path.execute` limited to the interpreters the build actually needs. The bundled scanner never reaches its first stage.

02 THE ATTACK

Credentials Swept From The Runner

A bundled secret scanner sweeps the filesystem and environment for npm, GitHub, AWS, and Vault credentials.

THE POLICY THAT STOPS IT

`path.open` limited to the files the build needs. Credential files such as `~/.npmrc`, `~/.aws`, and `~/.ssh` stay out of reach.

03 THE ATTACK

Secrets Leave, Worm Republishes

Stolen tokens are pushed to an attacker-controlled repository, then used to publish poisoned versions of more packages.

THE POLICY THAT STOPS IT

`ip.connect` limited to the hosts and ports the build publishes to. The exfiltration socket never opens.

Outcomes depend on the policy in force. Endura governs what a payload may do on your runner. It does not stop the upstream account compromise that published the package.

▸ COMPATIBILITY_

x86_64 today, ARM64 on the roadmap

Runs Where Your Builds Already Run

OPERATING SYSTEMS	22 PROFILES
AlmaLinux	9, 10
Alpine Linux	3
Amazon Linux	2023
Arch Linux	Rolling
CentOS Stream	10
Debian	12, 13
Fedora	44
Gentoo Linux	Rolling
openSUSE Leap	15.6, 16.0
Oracle Linux	8 UEK, 9, 10
Red Hat Enterprise Linux	9, 10
Rocky Linux	9, 10
Ubuntu	24, 25, 26

CI/CD PROVIDERS	12
GitHub	■
GitLab	■
Jenkins	■
Bamboo	■
TeamCity	■
AWS CodeBuild	◪
Azure Pipelines	◪
CircleCI	◪
Argo Workflows	◪
Travis CI	◪
CloudBees	◪
Koji	□

AUTH PROVIDERS	OIDC
CyberArk	
Google Identity	
Microsoft Identity	
Oracle Identity Cloud	

NOTIFICATIONS	ALERTS
Slack	
Microsoft Teams	
Email	

ACCESS CONTROL	RBAC
Viewer	
Operator	
Administrator	
Personal access tokens	
Resource scoping	

■ Discovery + adapter ◪ Adapter: CI context, no auto-discovery □ Discovery only

22 validated release targets across 13 distribution families. Where no provider tier applies, a build is still enforced as a generic workload. One Sensor per host or node protects up to 24 concurrent registered jobs.



▸ READY WHEN YOU ARE_

See What Your Builds Are Doing

Deploy Runtime Sensor on one pipeline, run it in **derive** mode to record every file, connection, and process your build touches, then refine, observe, and enforce.

REQUEST A DEMO

endurasecurity.com

© 2026 Infrared Security, LLC. d/b/a Endura Security · 18376 Southampton Drive, Lewes, DE 19958.