



From a trusted supply chain to the agents that build on it, secure by default with Docker.

Attackers have stopped treating the software supply chain and AI as separate targets. Docker helps you secure both at once on one platform, with a hardened foundation under everything your team builds and a governed boundary around the agents that build it.

YOUR CURRENT NEEDS

SECURE-BY-DEFAULT ARCHITECTURE

DOCKER DELIVERS

Verifiable control

what agents can reach,
and who allowed it

Isolated execution

where agents run

Trusted content

what you build with



EVIDENCE

The policy over every agent, and the record that proves it.

One policy across the organization, an MCP Gateway that denies unvetted servers by default, and an audit log of every decision to your SIEM.

The boundary around the agents that build your software.

A microVM per agent session with its own kernel, rules set before the agent starts, and no path back to the host.

The foundation for everything your team builds.

Images, Helm charts, MCP servers and system packages built from source and signed, with near-zero CVEs and support past end of life.

SIGNED

SBOM • VEX • PROVENANCE • AUDIT LOGS



Implement a secure foundation and a single boundary for a trusted software supply chain.

Docker Hardened Images

Start from a foundation of minimal, signed images built from source.



Give your team evidence for every compliance review and a secure foundation with near-zero CVEs, without a migration project.	Up to 95% smaller attack surface with near-zero CVEs	Signed evidence on every image SBOM, VEX and SLSA Build Level 3 provenance	One line to adopt on the Alpine and Debian images your teams already run
---	--	--	--

Docker Sandboxes

Put every agent session in a dedicated microVM with kernel-level isolation and no path back to the host.



Run your agents in YOLO mode inside a boundary you own.	Delete and restart in seconds disposable sandboxes with no state to clean up	No credentials inside the sandbox real secrets injected by a proxy at runtime	No path back to the host a dedicated microVM with its own kernel for every agent session
---	---	--	---

Docker AI Governance

Set one policy for all your teams and enforce it on every developer's machine.



Govern every agent in your organization, and show auditors what each agent did and who allowed it.	Every decision on the record agent identity, user and resource, logged locally or to your SIEM	No data leaves your environment on the developer's machine or in your own cloud tenant	One policy for all your teams across filesystem, network and MCP
--	---	---	---

WHAT'S INCLUDED

Docker Hardened Images

- 7-day SLA on critical and high CVEs
- FIPS and STIG variants
- Extended Lifecycle Support up to 5 years past end of life
- Hardened Helm charts, MCP servers and system packages
- Customizations rebuilt with every guarantee intact
- Full CVE visibility, nothing suppressed

Docker Sandboxes

- Full Docker inside, including builds from Docker Hardened Images
- Infrastructure-enforced boundary, not a system prompt
- File, network and secret rules set before the agent runs
- Works with Claude Code, Codex, GitHub Copilot, Gemini CLI, Kiro and Docker Agent
- Fast cold starts
- Runs natively on macOS, Windows and Linux

Docker AI Governance

- Team policies with RBAC via SAML and SCIM
- MCP Gateway and managed catalog, default-deny on unvetted servers
- Sandbox and MCP governed in one console, one policy model
- Vendor-neutral across any model, agent and tool
- Organization and team policies developers cannot override
- Integrates with your EDR, SIEM, identity and secrets tooling

WHAT CUSTOMERS SAY

“For the first time, I don’t have to worry about what’s hiding in our base images. That mental overhead is gone, and we can finally focus on the security challenges that are unique to Attentive.”

Jacob Rickerd, Principal Security Engineer, Attentive

“Docker Sandboxes let agents have the autonomy to do long-running tasks without compromising safety. We’re excited to integrate Sandboxes into Warp so that developers can run agents freely with a consistent environment, regardless of whether agents are running locally or in the cloud.”

Ben Navetta, Engineering Lead, Warp

Docker’s approach

We aim to provide a single platform that gives your developers and their agents a secure foundation and a trusted ecosystem in the workflows they already use, so that secure by default is the only way software gets built in the agentic era.

