attentive® | docker

Building Faster, Securing Smarter: How Attentive Eliminated 90% of CVEs with Docker Hardened Images

Executive Summary

- **Open-source CVE churn and AI-accelerated dependency sprawl** create an impossible dilemma: patch faster than adversaries exploit vulnerabilities, or accept an expanding attack surface and mounting compliance risk. Reactive patching cannot scale to meet this challenge.
- **Docker Hardened Images (DHI)** shift the paradigm from reactive remediation to proactive prevention. These minimal, continuously-maintained base images deliver near-zero CVEs, automated SBOM generation, signed attestations, and enterprise SLAs. This eliminates the operational burden of maintaining custom hardened images while also improving build times, one of the drivers for Attentive's push on Hardened Images.
- **Attentive's implementation validates the business case.** Their fast POC demonstrated 90% CVE reduction, 36% smaller images, and 2.5 hours of daily build time savings, translating to 650 hours recovered annually. Zero production incidents during rollout proved that security improvements accelerate rather than impede development.
- **This playbook documents Attentive's progression from POC to organizational standard**, covering:
  - ✓ 'Build vs. buy framework' for evaluating total cost of ownership
  - ✓ POC execution strategy with measurable success metrics across security, performance, developer experience, and compliance
  - ✓ Production rollout patterns including CI/CD integration, policy enforcement, and phased deployment strategies
  - ✓ Quantifiable business impact demonstrating ROI to leadership through cost reduction, risk mitigation, and competitive advantage

Organizations following this blueprint transform hardened images from one-time migrations into sustainable operational standards, building security into engineering culture rather than bolting it on after development.

This article was contributed by Stephen Commiso, Anna Chernyshova, and Daniel Stelzer.

Content

Section 1: Securing the Container Supply Chain

Why Secure Foundations Matter Now

Supply chain attacks have become the primary vector for enterprise compromise. Malicious packages increase 156% year-over-year, with 91% of organizations experiencing a software supply chain incident and 86% of production workloads containing high risk vulnerabilities. The 2024 XZ Utils backdoor demonstrated how adversaries exploit foundational components embedded in countless distributions.

Supply Chain Security Trends

156%
YoY growth of malicious packages (Sonatype, 2024)

91%
of organizations experienced a supply chain security incident in previous 12 months (ESG, 2024)

2.8 million
malicious repositories planted on Docker Hub over 5 years (JFrog, 2024)

Understanding exactly what is being built and shipped, and whether it originates from verified sources, has become foundational to secure software delivery. Without inventory, organizations cannot answer basic questions: What packages exist in our base images? Are they signed? Do they contain known vulnerabilities? Are those vulnerabilities exploitable in our context?

AI-assisted coding accelerates the problem by propagating outdated libraries and vulnerable patterns at unprecedented velocity. In the last two quarters of 2025, we've seen software supply chain attacks using AI reach unprecedented scales. Attacks like Shai Hulud further illustrate the scale of the challenge. Regulatory frameworks now mandate patch response timelines (CISA requires critical vulnerabilities patched within 15 days), but engineering teams can't patch their way out of this problem fast enough.

That's where verified, minimal, continuously-maintained base images that prevent vulnerabilities from entering the supply chain come in.

Attentive's Hardening Image Initiative

attentive®

About Attentive

Attentive provides an AI-powered SMS, email, and push marketing platform that enables personalized mobile messaging at scale. Founded in New York City in 2016, the company has 1,000 employees and serves 8,000+ leading retail and e-commerce brands.

Attentive's hardening image initiative started when their platform team identified that one of their base images powering dozens of production services would reach end-of-life (EOL) in May 2025. The security team recommended image hardening as part of the upgrade path, **but implementing custom hardened images across every service exceeded their bandwidth**.

Meanwhile, Attentive's build infrastructure had accumulated technical debt over the years. Services lacked multi-stage builds, used minimal layer caching, and each team maintained its own base image variations.

> **"Having the table-stakes problem of base image security solved for us by Docker Hardened Images allowed me to focus my time on other time and cost-saving actions, such as multi-stage and multi-arch builds."**
>
> Stephen Commiso, Principal Engineer

This pattern is not uncommon: operational triggers spark urgency, but security teams lack the capacity to implement solutions. Everyone agrees that ad-hoc base-image management creates needless toil. So they need to make a choice: develop internal hardening capabilities or adopt vendor-maintained hardened images.

Rather than treating the EOL deadline as a simple patching problem, the platform engineering team at Attentive recognized it as an opportunity to fix foundational issues.

The Build vs. Buy Decision

The decision framework to build internally or adopt a vendor-maintained catalog centers on total cost of ownership versus delivered value. This is why it's crucial to inspect the true cost of DIY hardening, beyond the "visible" effort:

DIY Requirement	"Visible" Effort	Hidden Costs
Base Distribution Curation	Selecting minimal packages, testing functionality across services	Expertise in multiple distros, managing breaking changes across versions
Security Advisory Monitoring	Daily CVE tracking, patch evaluation, relevance assessment	24/7 operational burden, alert fatigue
Rebuild & Testing Pipeline	Automated builds, compatibility testing, regression prevention	Infrastructure costs, CI/CD complexity
SBOM Generation	Tooling, validation, format standards (SPDX, CycloneDX)	Only 24% of orgs have complete SBOMs (Linux Foundation)
Provenance & Signatures	SLSA compliance, signing infrastructure, key management	Specialized expertise required, cryptographic key rotation
SLA Documentation & Staffing	Commit to patch windows, staff on-call rotations	Competes with feature development priorities
Multi-Distribution Support	Alpine, Debian, Ubuntu, RHEL variants	Multiplies all above costs by N distributions
Multi-Architecture Builds	ARM64, AMD64 compatibility and testing	Additional infrastructure and cross-platform tooling

These hidden costs often cause organizations to realize that the ongoing operational burden soon exceeds initial estimates.

Attentive's Build vs. Buy Reality Check

“Our central security team supports hundreds of developers. They could write reports and make recommendations about hardened images, but actually implementing custom hardening across every service? That's beyond their bandwidth.”

Stephen Commiso, Principal Engineer

There are certain cases when building in-house makes sense:

- **Large, dedicated security teams** with explicit image maintenance mission
- **Highly specialized tech stacks** that rely on uncommon distros or proprietary dependencies
- **Air-gapped environments** where external dependencies are limited
- **Non-standard compliance requirements** that extend beyond FedRAMP, SOC 2

The Docker Hardened Images catalog provides FIPs and STIG-compliant images to support federal security baselines without slowing down delivery.

But for most organizations, adopting a catalog of secure, minimal, and verified baseline images outweighs the total cost of ownership of building in-house, both in immediate value and in measurable mid-to-long-term outcomes.

What Docker Hardened Images Deliver

Docker Hardened Images shift the burden to specialized teams maintaining images as their core competency. The value extends beyond avoiding DIY costs:

Capability	Immediate Value	Measurable Outcome
Minimal, Secure Baseline	Near-zero CVEs	Up to 95% CVE reduction
Continuous Patching	Updates outside your sprint cycles	Meet CISA mandates (≤15 days critical, ≤30 days high)
Built-in Attestations	SBOM + provenance + signatures ready for audits	Streamlined audit cycles
Enterprise SLAs	Documented patch windows (typically ≤7 days critical)	Predictable remediation, reduced firefighting
Multi-Arch Support	ARM64 + AMD64 maintained in parallel	Infrastructure cost savings
VEX Data	Exploitability context for reported CVEs	Focus remediation on genuine threats, eliminate false positive noise
Professional Support	Technical assistance during implementation	Attentive cited responsive support as key success factor

Attentive's evaluation validated this value proposition. After comparing Docker with competitors' offering, they selected the former based on three factors:

Security and performance: near-zero CVEs, continuously patched images, reduced final image sizes that would increase CI/CD pipeline speed.

Implementation ease: minimal engineering lift that would allow to quickly validate a POC and then migrate more services thanks to the large catalog of available images.

Integrated offerings: Docker Hardened Images was a natural fit to consolidate into the Docker ecosystem along with Docker Business and Testcontainers Cloud.

Thanks to Docker's deep commitment to collaborating with their customers, Attentive **was able to complete their first POC in two days**, demonstrating significant security and performance gains. The following KPI framework helped them define success.

Defining Success: The KPI Framework

Because hardened images represent a platform initiative affecting the entire engineering organization, success requires measurable objectives aligned with stakeholder priorities:

	Key Metrics	Target Outcomes
Developer Experience (DevEx)	• Build time reduction • Image start time • Deployment lead time	• 30-60 second build time savings • Faster container startup
Application Security (AppSec)	• Critical/high CVEs in base • Time-to-remediate • VEX-validated exploitable CVEs	• Up to 95% CVE reduction • Meet CISA mandates (15-day critical, 30-day high) • Focus remediation on genuine threats
Governance, Risk, Compliance (GRC)	• % workloads with SBOM +provenance +signature • Audit cycle time • Evidence collection effort	• 100% workload coverage • 40% faster audit cycles • 50% reduction in manual compliance tasks
Finance/Cloud Operations	• Image size deltas • Egress cost reduction • Storage footprint • ARM adoption rate	• 30-60% smaller images • Measurable egress savings • Reduced storage costs • Infrastructure cost reduction through ARM

This KPI framework serves multiple purposes:

Builds the business case by quantifying value during the concept phase.

Identifies services where migration delivers maximum impact during rollout.

Justifies continued investment and demonstrates ROI to leadership.

Align Metrics with Initiative Drivers

Select 3-5 metrics aligned with your primary initiative drivers. These can be:

- Risk reduction and compliance metrics for GRC;
- Build times and deployment frequency for developer productivity;
- Infrastructure savings from smaller images and ARM adoption for cost optimization;

With the business case established, it's now time to validate that DHI delivers measurable improvements with minimal engineering lift through a focused proof of concept that de-risks compatibility and builds internal confidence.

Section 2: From POC to Production

Running Your Proof of Concept

POC timelines depend on organizational context. Larger organizations validating across more services, distributions, or architectural patterns may require more time. Smaller teams with simpler stacks can move faster. Attentive completed their POC in two phases spanning only a few days:

Phase 1 - Minimum viable DHI image setup (1 day):

1. Configure build environment **feature flags** for gradual DHI images opt-in
2. Establish **authentication** to the DHI repository
3. Update **Dockerfiles** with DHI base image (drop-in replacement)
4. Address **dependency changes** from Ubuntu to Debian base distribution
5. **Cache DHI base image** in internal ECR registry

Phase 2 - Rollout and testing (couple of days):

1. **Compare** baseline vs. DHI-based images (size, CVE counts)
2. **Integrate with CI/CD** pipeline and validate scanning results
3. **Security team review** of compliance artifacts (SBOMs, attestations)

Result: Zero production incidents, a 90% immediate reduction in CVE count, and a 30-second build time improvement per service.

Attentive's teams quickly validated compatibility by stacking existing installations on DHI and iterating through trial-and-error before moving on to optimizations.

This approach works best for teams with robust rollback mechanisms and high operational maturity, which made the rapid validation possible in this case. Although it may not suit every organization, the key point is that timeline is secondary to the measurement framework. A successful proof of concept delivers measurable gains while requiring a reasonable engineering effort, hence the importance of choosing the best entry point from the start.

More impact for security teams

"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 at Attentive

Start Small, Measure Thoroughly

To get started, we recommend to choose 2-3 representative services that reflect your production reality:

- **API service:** High-traffic, frequently deployed, security-sensitive
- **Batch job:** Long-running, resource-intensive, fewer dependencies
- **Web service:** Customer-facing, mixed dependencies, caching layers

These services will be helpful to de-risk the full rollout by exposing compatibility issues before committing.

Choosing Your Distro Base (without Overthinking)

Although Docker Hardened Images are distroless, Docker offers compatibility with both Debian and Alpine Linux distributions. In Attentive's case, both image variants were tested, which contributed to a smoother rollout.

POC Essentials

Regardless of timeline, every POC requires these foundational steps:

Authentication Setup	• Configure Docker Hub credentials • Set up CI/CD access • Verify registry permissions
Image Caching	• Cache DHI in internal registry • Measure pull performance
Dockerfile Migration	• Replace FROM statements • Validate builds
Initial Deployment	• Deploy to test/staging environment • Validate service functionality • Verify image compatibility
Metrics Collection	• Set up security monitoring • Track performance metrics • Measure DevEx improvements • Document compliance gains

If the infrastructure supports traffic splitting, you can optionally include a **canary deployment** step in the POC:

Feature Flag Configuration	• Set up canary deployment controls • Configure rollback procedures
Canary Deployment	• Deploy to subset of production traffic (e.g., 10%) • Monitor behavior and metrics • Gradually increase traffic percentage

What to Measure: Building Your Business Case

Track metrics across stakeholder perspectives. For this, establish baseline measurements before POC, then demonstrate improvement after DHI migration.

Attentive's POC focused on developer security, as well as productivity and build performance. Their metrics captured:

650 hours build time saved yearly (31 seconds per build across 287 daily builds times 260 business days per year)

36% image size reduction overall

90% CVE elimination

0 incidents during rollout

Security Posture Improvements

	What to Track	Attentive Results
CVE Reduction	Compare critical/high CVEs before vs. after	**90% elimination**
SBOM Coverage	% services with verifiable SBOM	0% → 100% (auto-generated)
Signed Provenance	% images with verifiable attestations	0% → 100%
VEX Data Availability	Exploitability context for reported CVEs	Reduces false positive noise 60-80%

Security Outcome Benchmark

Target **up to 95% CVE reduction** in base images compared to standard public images. Organizations consistently achieve near-zero critical/high vulnerabilities after DHI migration.

Why SBOMs Matters

According to Gartner, "by 2025, 60% of organizations building or procuring critical infrastructure software will mandate and standardize SBOMs in their software engineering practice, up from less than 20% in 2022". DHI closes this gap immediately with signed, auto-generated software composition data.

Performance and Efficiency Gains

	What to Track	Attentive Results	Industry Benchmark
Image Size	Compare compressed sizes	**36% reduction**	30-60% typical
Build Time	Seconds saved × daily frequency	**31 sec × 287 builds = 2.5 hrs/day**	20-60 seconds/build
Pull Time	Time from pull to container ready	Proportional to size	10-30% faster
Container Start	Startup time improvement	Faster from minimal footprint	15-25% improvement

Why Performance Matters

Faster builds enable higher deployment frequency. Smaller images reduce egress costs, storage footprint, and auto-scaling response time. You can calculate your build time savings with a simple formula:

(seconds saved per build) × (daily build count) × (days per year) = **annual time savings**

Example: 30 seconds × 200 builds/day × 260 days = **1,560 hours/year** recovered for feature development

Developer Experience Metrics

	What to Track	Success Criteria
Dockerfile Complexity	Lines changed per service	10-15 lines (drop-in replacement)
Build Break Rate	% builds failing post-migration	<5% with quick resolution
CI Pipeline Duration	Total pipeline time change	Neutral or improved
Engineering Effort	Person-hours for POC	<40 hours

Why DevEx Matters

Developer productivity currently suffers from security overhead. JFrog estimates $28,000/developer/year spent on security tasks, 19% of time lost to CVE management. DHI reduces this burden through drop-in replacements requiring minimal retooling.

Compliance and Audit Readiness

	What to Track	Success Criteria
SBOM Generation	Automatic, signed, SPDX/CycloneDX	Eliminates manual generation effort
VEX Data	Exploitability context	Focus remediation on genuine threats
Provenance	SLSA-aligned attestations	Faster third-party risk reviews
Evidence Packages	Pre-packaged compliance artifacts	40-50% faster audit cycles

Why Provenance Matters

Docker provides signed attestation like SBOMs and SLSA 3 level provenance. Leveraging these during the build process will help your teams save time, for example, by reducing the number of scans needed to safely assess vulnerabilities.

From POC to Production Rollout

Successful POCs create momentum and enthusiasm, but sustainable adoption requires discipline. Organizations that succeed treat them as an engineering standard: embedding hardening into CI/CD pipelines, rollout processes, and team workflows.

Evaluating POC Results

Attentive entered their POC with developer security as well as productivity as the success metrics, and the results exceeded expectations. The team projected a **2.5-hour daily reduction** in build times across their pilot services, translating to **12.5 hours saved per week**. Engineers immediately noticed faster feedback loops during local development and CI runs, and the team experienced zero build breaks during rollout.

200+ Services, Zero Drama

"The rollout was completely transparent to product teams. We had zero issues across over 200 services, which was particularly impressive since we were simultaneously switching Linux distributions from Ubuntu to Debian. All the heavy lifting happened during POC."

Stephen Commisso, Principal Engineer

From POC to Production in 6 weeks: How Attentive executed the migration

Following their POC, Attentive migrated their entire service fleet using a 2-phase approach:

Phase 1: Pilot Validation

- Selected canary services across diverse categories (mix of service types and workload patterns);
- Services opted in via environment variable in makefiles;
- Validated production behavior with representative workloads.

Phase 2: Organization-Wide Default

- Flipped feature flag to make DHI the default for all services;
- Minimal code changes required (10-15 lines in the base Dockerfile, with any overrides to the default being a couple of lines);
- The platform team optimized Dockerfile patterns, creating templates that reduced migration time and enabled self-service adoption, accelerating Phase 2 rollout.

Key technical enablers:

- Feature flags built during POC phase;
- Environment variables for granular service control;
- Canary validation de-risked full rollout.

With build performance gains validated and no developer friction introduced, Attentive had clear evidence that DHI delivered on its core promise: security improvements that accelerate rather than impede development velocity.

Technical Integration: Embedding DHI into Your Pipeline

Strengthening the security posture starts with embedding hardened images across your infrastructure while avoiding the "snowflake" effect, where each team maintains custom image variants that multiply maintenance burden.

1. Baseline Image Strategy

Standardize on one DHI base image per major runtime and distribution to minimize maintenance overhead. Platform engineering should maintain a small set of blessed base images (e.g., node:20-alpine-dhi, python:3.11-debian-dhi) that service teams consume directly.

When additional tooling or dependencies are required across multiple services, use **Docker's customization capabilities** rather than forking DHI images or maintaining bespoke Dockerfiles.

Anti-pattern: Each service team customizes DHI differently, recreating the maintenance problem hardened images were meant to eliminate.

Recommended pattern: Platform engineering maintains 3-5 standard base images (e.g., node:20-alpine-dhi, python:3.11-debian-dhi) with customizations applied through Docker's UI when teams need shared dependencies.

Customization Advantages

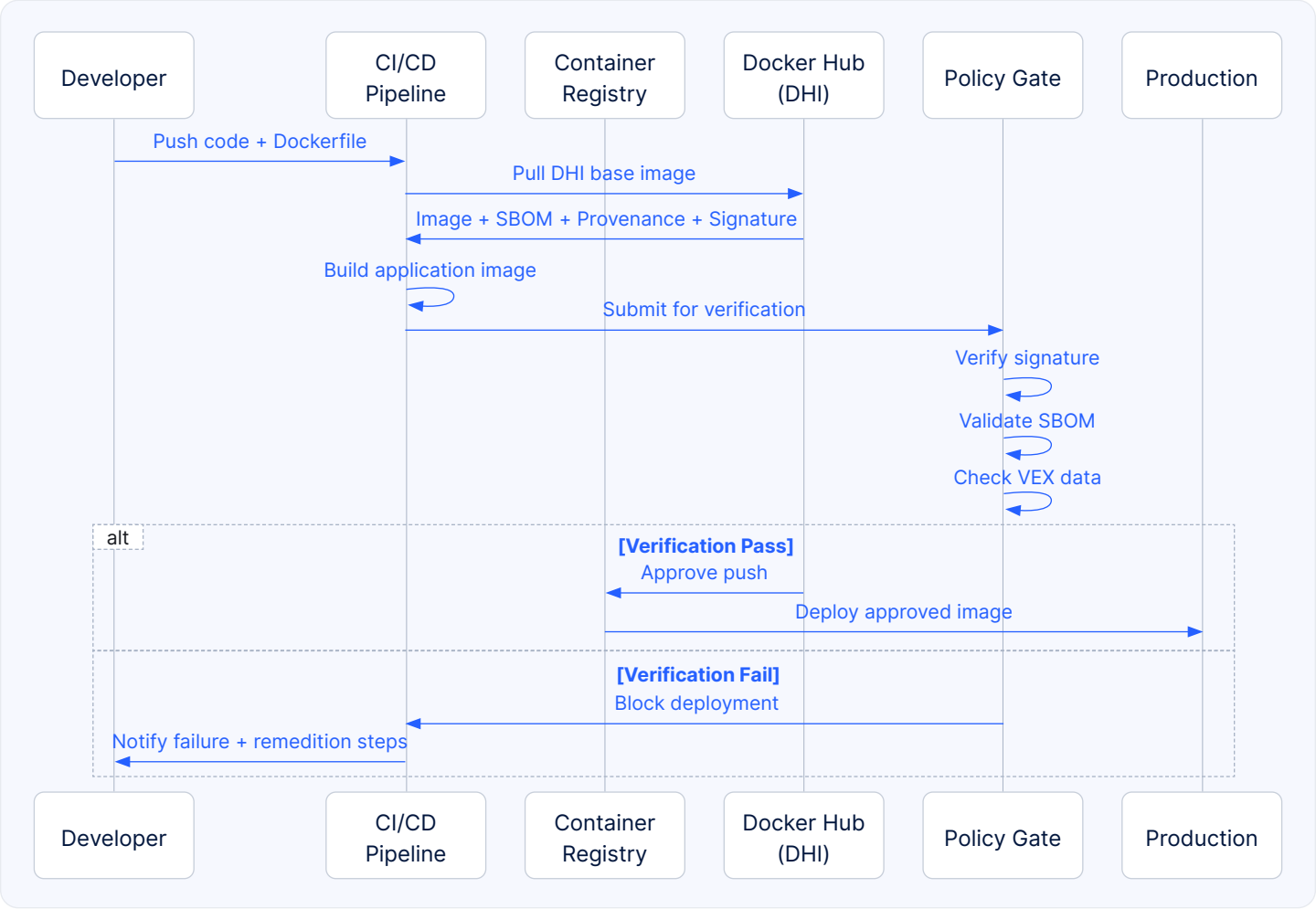
Docker Hardened Images customization feature runs your modified images through the same build and security pipeline as base DHI images. Customized images receive:

- ✓ The same **signed SBOMs** and **attestations** as base images;
- ✓ **Automatic rebuilds** when CVEs are discovered in DHI base layers;
- ✓ Docker's published **SLA coverage** for patching and updates.

This means customizations don't sacrifice the security guarantees that justified adopting DHI in the first place.

2. CI/CD Pipeline Integration

Adopting DHI at the image level solves the base layer security problem, but real organizational impact requires integration into CI/CD workflows. Without enforcement mechanisms, teams will drift back to unhardened images over time. Progressive security gates transform DHI into an enforced standard, validating attestations at build time and blocking deployments that fall outside policy. This creates a feedback loop where security becomes a natural checkpoint rather than a post-deployment audit.



Implementation checklist:

Integration Point	Action	Purpose
Image Pinning	Pin to immutable digests (not tags)	Prevent tag mutation attacks
Signature Verification	Verify Docker signatures in pipeline	Confirm image authenticity
Attestation Validation	Check SBOM + provenance presence	Ensure supply chain metadata exists
Policy Enforcement	Block non-DHI images in protected branches	Prevent drift from standard
Alerting	Wire alerts for new base availability	Enable proactive updates
Lag Detection	Flag workloads >N days behind latest	Identify update bottlenecks

3. Attestation Infrastructure

Treat attestations as first-class artifacts alongside container images. Store SBOMs and provenance data in your artifact repository (Artifactory, Nexus, or cloud storage) with indexing that makes them searchable by service name, image digest, and timestamp.

Set retention policies to match compliance requirements (typically 1-3 years) and configure access controls so CI/CD can write attestations while audit and security teams can query them programmatically.

✓ Docker SBOM attestation docs ✓ Docker SLSA provenance docs

VEX data consumption

Docker provides VEX (Vulnerability Exploitability eXchange) data indicating which reported CVEs are actually exploitable in DHI context. Configure scanners to consume VEX data, filtering false positives so teams focus remediation on genuine threats.

4. Drift Prevention Controls

Long-term drift prevention relies on two complementary mechanisms: automated policy controls and periodic audits.

Policy admission controllers (OPA/Gatekeeper/Kyverno) enforce DHI standards at deployment time by validating registry sources, signature presence, image freshness, and digest pinning.

Periodic audits catch drift in running workloads through weekly scans that identify outdated base images, generate automated tickets for teams exceeding update SLAs, and surface organizational compliance metrics on dashboards.

Section 3: Measuring Momentum

Platform initiatives that cannot quantify their impact struggle to justify continued investment when competing with feature development and operational firefighting.

This section **translates technical wins into business outcomes** across three dimensions: quantifiable results, stakeholder-specific value, and operational maturity.

The Numbers That Drive Decisions

Organizations need concrete data demonstrating return on investment. Industry benchmarks provide context, but stakeholders require organization-specific metrics proving value in their environment.

Attack Surface and Risk Reduction

Metric	Typical Improvement	Attentive Results	Business Impact
CVE Reduction	Up to 95% decrease in base image vulnerabilities	90% reduction	Reduced attack surface, faster audit cycles
Time to Remediation	Close 50-day gap vs. industry avg (65 days)	Meet CISA mandates (15-day critical, 30-day high)	Regulatory compliance, reduced exposure window
SBOM Coverage	0% → 100% across workloads	100% auto-generated, signed	Closes gap affecting 76% of organizations
Exploitable Vulnerabilities	60-80% reduction in false positives via VEX	Focus security team on genuine threats	Efficient remediation resource allocation

Near-zero CVEs in base images shift security team focus from reactive patching to proactive architecture improvements. Organizations meeting CISA vulnerability response mandates avoid potential penalties and reputational damage. Complete SBOM coverage addresses the compliance gap, accelerating vendor assessments and third-party risk reviews.

Performance and Efficiency Gains

Metric	Typical Improvement	Attentive Results	Annual Impact (Example)
Image Size	30-60% reduction	36% decrease	Lower egress costs, faster deployments
Build Time	20-60 seconds/build	31 seconds × 287 builds/day = 2.5 hrs/day	650 hours/year recovered
Pull Time	10-30% faster	Proportional to size reduction	Faster auto-scaling, improved incident response
Container Start	15-25% improvement	Faster from minimal footprint	Higher deployment velocity

Build time savings compound across daily operations. Attentive's 2.5 hours saved daily translates to 650 hours annually, the equivalent of nearly 4 months of engineer productivity recovered for feature development. Faster containers improve auto-scaling responsiveness during traffic spikes, reducing the risk of degraded customer experience during demand surges.

Calculating Your Savings

Build Time ROI: (seconds saved per build) × (builds/day) × (260 workdays) = annual hours recovered

Infrastructure Savings: (image size reduction %) × (storage costs + egress costs) = monthly savings

Example: 40% size reduction across 1,000 images pulling 10 times daily = significant egress cost reduction in cloud environments with per-GB transfer pricing.

Multi-Arch as Cost Optimization Enabler

DHI's multi-arch capability wasn't part of Attentive's original hardened images initiative, but it became a bonus enabler for cost optimization.

DHI's ARM64 + AMD64 images (maintained in parallel) allowed Attentive's teams to switch architectures without rebuilding base images.

They migrated **40% of production workload to AWS Graviton** (ARM64) processors with zero compatibility issues, delivering **12-15% production cost reduction**.

This demonstrates how platform investments create compound value: DHI's multi-arch capability became an enabler for cost optimization initiatives beyond its primary focus.

Developer Productivity Recovery

Developer time represents the largest cost in most engineering organizations. DHI deployment recovers time currently lost to security overhead.

Industry Data	DHI Impact	Recovered Capacity
$28,000/developer/year on security tasks	Minimal retooling, drop-in replacement	Reduce overhead 30-50%
19% developer time on security-related work	Automated SBOM, continuous patching	Recover 5-10% time to features
3.5 hours/week reviewing false positives	VEX data filters noise	Eliminate 60-80% false positive review

Source: JFrog/IDC Survey, 2024

Faster builds, smarter security

"We wanted to prove that better security could actually make engineers faster, not slow them down. The hardened image rollout was our chance to demonstrate that."

Jacob Rickerd, Principal Security Engineer at Attentive

Compliance and Audit Acceleration

Organizations facing SOC 2, ISO 27001, or industry-specific compliance requirements (PCI DSS, HIPAA, FedRAMP) benefit from pre-packaged evidence that auditors can verify programmatically rather than through manual documentation review.

	Before DHI	After DHI	Time Savings
SBOM Generation	Manual per service, inconsistent formats	Automated, signed, standardized	50+ hours/audit eliminated
Vulnerability Documentation	Manual tracking, spreadsheet management	Pre-packaged evidence with VEX context	40% faster audit cycle
Provenance Verification	Ad-hoc processes, missing for many services	SLSA-aligned attestations for all images	50% reduction in evidence collection effort
Third-Party Risk Reviews	Months to document dependencies	Queryable SBOMs accelerate reviews	60% faster vendor assessments

Mapping Value to Every Framework That Matters

DHI adoption addresses requirements across multiple compliance frameworks simultaneously, creating leverage for organizations maintaining several certifications.

Evidence generated for one framework often satisfies overlapping controls in others, **turning a single hardened image investment into compliance efficiency across all domains**.

FedRAMP / FIPS

Federal Mandate	DHI Alignment
NIST SSDF (OMB M-22-18)	SLSA-aligned supply chain security
Continuous Monitoring	Automated vulnerability tracking
Evidence Collection	Pre-packaged attestation bundles
Supply Chain Transparency	Complete provenance documentation

SOC 2 / ISO 27001

Control Domain	DHI Alignment
Change Management	Immutable image digests, signed provenance
Vulnerability Management	Continuous patching with documented SLAs
Software Composition	Complete SBOM coverage with VEX data
Access Control	Signature verification in pipeline gates

PCI DSS / HIPAA

Requirement	DHI Alignment
Baseline Hardening	Minimal attack surface, near-zero CVEs
Software Inventory	Automated SBOM generation
Third-Party Risk	Signed provenance from trusted vendor
Patch Management	7-day SLA for critical vulnerabilities

What Leadership Actually Cares About

Technical teams celebrate CVE reductions and build time improvements. Leadership evaluates initiatives through business impact lenses: cost, risk, and competitive advantage.

	DHI Contribution	Quantifiable Outcome
TCO Reduction	Eliminate internal hardening costs + developer productivity gains	Per developer/year savings + audit efficiency
Risk Mitigation	Close 50-day remediation gap, meet regulatory mandates	Avoid compliance penalties, reduce breach probability
Competitive Advantage	Faster releases, stronger security posture in sales cycles	Win security-conscious customers, shorten sales cycles
Operational Efficiency	Automated patching reduces firefighting	Platform team capacity freed for strategic work

Four Pillars of Operational Maturity

Organizations that sustain DHI long-term build discipline around four pillars:

- **Policy**: concise, 3-sentence policies (base images, update cadence, exceptions), enforced gradually (from visibility, to warnings and finally blocking).
- **Procedure**: automated compliance workflows. As an example, the publication of a new image version can trigger an automated PR with test results, with auto-merge enabled for low-risk patches.
- **Governance & Enforcement**: hard gates combined with break-glass procedures. CI/CD pipelines and cluster admission controllers prevent non-compliant configurations from reaching production. When enforcement blocks a deployment, actionable error messages guide teams toward migration resources or exception workflows.

Making the Case for Broader Adoption

Following POC validation, expanding adoption requires navigating competing priorities.

Some organizations set hard migration deadlines with executive backing, providing tooling and support to meet 90-day windows. This mandate-plus-support approach works when compliance creates urgency and leadership enforces accountability.

Others use internal champions to showcase wins, remove friction, and let success drive organic adoption. This fits engineering-driven cultures where bottom-up adoption beats mandates.

Large organizations often combine both: mandate DHI for new services while supporting existing migrations and granting time-bound exceptions with business justification. This takes longer but offers flexibility.

Key accelerators that speed adoption:

- **Internal champions**: Recruit early adopters to demonstrate success
- **Self-service tooling**: Build one-command migration scripts that reduce effort from hours to minutes
- **Success stories**: Share real metrics (build time savings, CVE reductions, faster deployments) to build confidence
- **Friction removal**: Provide templates and clear documentation that make the secure path easier than building from scratch

Conclusion

Attentive's migration to Docker Hardened Images proves the technology works when implementation follows disciplined principles. Their POC proved technical feasibility with minimal changes and zero production incidents.

With 2.5 hours of daily build time savings translating directly into faster feature delivery, Attentive successfully demonstrated that better security can actually make engineering orgs faster, rather than slowing them down.

The path from POC to standard was clear: focused pilot, measurement against priorities, systematic rollout with automated enforcement. Attentive didn't treat DHI as a one-time security upgrade but transformed it into a higher engineering standard.

Organizations should follow this playbook: start with measurable POC objectives, build momentum through early wins, and scale through operational discipline. The images solve base layer security. Sustained success requires treating them as an ongoing standard, not a project.

Next Steps:

- ✓ Run your POC with measurable objectives
- ✓ Track security metrics, performance, and developer experience
- ✓ Build your business case with audience-specific value frameworks

The choice isn't security versus velocity. It's reactive patching versus secure foundations. Start with minimal, secure production-ready images maintained by experts, and build the discipline that turns a successful POC into sustained practice.