VERACODE

DATASHEET

Veracode Container and IaC Security

Secure Containers, Ship Faster: Build and deploy cloud-native apps with confidence.

Containers and Infrastructure-as-Code (IaC) accelerate cloud-native development, but vulnerabilities, misconfigurations, and hardcoded secrets expose organizations to breaches. Vulnerabilities in containers pose a major obstacle to secure and widespread container adoption. Late-stage scanning delays remediation, disrupts CI/CD pipelines, and increases costs, especially in regulated industries like BFSI, government, and healthcare.

Veracode Container and IaC Security empowers developers to build secure containers and IaC files early in the SDLC. Integrated into CI/CD pipelines and accessible via an intuitive CLI, it scans for vulnerabilities, misconfigurations, and secrets, delivering actionable insights to fix issues fast. This ensures secure deployments, compliance with standards like CIS Benchmarks, and reduced risk without sacrificing speed.

Faster Remediation: Veracode's CLI and actionable insights cut remediation time by up to 50%.

Veracode TEI Report

50%

KEY USE CASES & BENEFITS

Scan Containers Early in CI/CD Pipelines: Identify vulnerabilities during development with a CLI integrated into tools like GitHub Actions, cutting remediation time by 50% without slowing builds.

Prioritize Critical Issues with Policy-Driven Insights: Use contextual findings to focus on high-severity flaws and misconfigurations, reducing audit preparation time by 30% for compliance with standards like CIS Benchmarks.

Detect Secrets and Vulnerabilities in IaC and Containers: Secure the software supply chain by addressing 75% of container vulnerabilities and secrets like AWS keys, ensuring compliance with various frameworks.

Scale Security Across Large-Scale Container Deployments: Support 10,000+ containers with sub-minute scans in AWS, Azure, or on-premises setups, enabling secure growth without performance bottlenecks.

Align Teams with a Unified Security Platform: Bridge development and security with a developer-first CLI and integrated platform, delivering secure software faster than fragmented tools.

Why Veracode Container Security?

- **Seamless Developer Integration:** Our intuitive CLI embeds security directly into existing workflows, enabling developers to scan and fix issues without disrupting their environment.
- **Comprehensive Security Coverage:** Offers broad detection of vulnerabilities, infrastructure-as-code misconfigurations, and secrets.
- **Early Detection in the SDLC:** Proactively scans during development, preventing insecure containers from reaching production.
- **Precise and Reliable Results:** Delivers accurate findings by combining trusted open-source tools with the power of the Veracode Platform.
- **Unified Security Platform:** Integrates seamlessly with Veracode's broader Application Security Testing suite, streamlining security tooling.

Accelerate cloud-native development
without compromising security.

KEY FEATURES

- ✓ **Comprehensive Scanning:** Scans container images, IaC files (Terraform, CloudFormation, Kubernetes manifests, Dockerfiles, Helm charts), and repositories for vulnerabilities, misconfigurations, and hardcoded secrets.
- ✓ **CI/CD Integration:** Embeds security into pipelines (e.g., GitHub Actions, Jenkins) with fast CLI-based scans, supporting multiple targets (images, directories, archives).
- ✓ **Software Bill of Materials (SBOM):** Generates SBOMs in JSON, CycloneDX, and SPDX formats for compliance and supply chain transparency.
- ✓ **Policy Enforcement:** Prioritizes critical issues with pre-built policies, highlighting severe vulnerabilities for rapid remediation.
- ✓ **Trusted Open-Source Technology:** Leverages Syft, Grype, and Trivy for accurate, reliable results across major base OS (Alpine, Ubuntu, Debian, RHEL, Amazon Linux).
- ✓ **Contextual Remediation:** Provides file-and layer-specific findings with actionable fix recommendations, reducing developer workload.

TECHNICAL SPECIFICATIONS

Supported Base Operating Systems: Alpine Linux, Amazon Linux, CentOS, Debian, Ubuntu, Red Hat Enterprise Linux, Oracle Linux, Busybox, Distroless.

Supported IaC Formats: Terraform, AWS CloudFormation, Azure ARM Templates, Kubernetes manifests, Dockerfiles, Helm charts.

Scan Targets: Container images, container image archives, file system directories, Git repositories.

Security Findings:

- **Known Vulnerabilities:** Publicly reported flaws, including insecure deserialization and OS/package vulnerabilities.
- **IaC Misconfigurations:** Access control issues, network traffic exposures, non-compliance with CIS Benchmarks.
- **Hardcoded Secrets:** Cloud keys (AWS, GCP), platform tokens (GitHub, GitLab, Slack), DevOps keys (NewRelic, Databricks), eCommerce tokens (Stripe, Shopify), cryptographic keys (RSA).

Integration Points:

- **CI/CD pipelines:** GitHub Actions, Jenkins, CircleCI, GitLab CI, and 30+ other tools.
- **Command Line Interface (CLI):** Runs on Linux-compatible or Mac desktops with Docker installed.
- **APIs:** REST APIs for automation and integration with tools like Jira.
- **Output Formats:** Text, JSON, SBOM (CycloneDX, SPDX, SWID).

Performance:

- **Scan Speed:** Sub-minute scans for typical container images; handles 10,000+ containers in high-velocity environments.
- **Scalability:** Supports large-scale deployments with no performance degradation.

Technologies Used: Open-source projects (Syft, Grype, Trivy) and Veracode Platform for unified management and analytics.

Deployment Options: Cloud-based SaaS (access via tools.veracode.com) or on-premises for regulated environments. Requires Internet access, Docker, and Veracode API credentials.

Compliance Support: Aligns with NIST 800-53, OWASP Container Security Verification Standard, and CIS Benchmarks; generates SBOMs and audit-ready reports.

Access Management: Integrated with Veracode Platform's role-based access controls.

Contact Us

Contact us today to learn more about how Veracode Container Security can help you reduce risk and secure your application security. Visit www.veracode.com to schedule a demo or request additional information.

VERACODE