

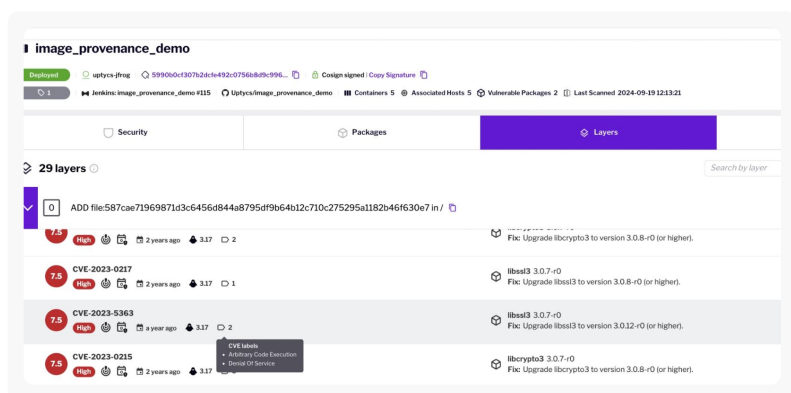
# Comprehensive Software Supply Chain Security with Uptycs

## What We Do

### Secure Hybrid Cloud Workloads At Scale

Uptycs integrates CI/CD scanning, runtime monitoring, and compliance enforcement to secure hybrid cloud workloads.

- **Comprehensive Scanning and Detection:** Identifies vulnerabilities throughout CI/CD workflows and runtime, safeguarding software pipelines.
- **Threat Analysis:** Detects and traces malicious code, conducting risk-based analysis.
- **Automated Compliance:** Enforces policies to secure the software supply chain, ensuring compliance with industry standards.



## How We Do It

### Scalable Guardrails Across the Software Lifecycle

Uptycs provides end-to-end lifecycle security, proactively defending developer code and the software supply chain.

Uptycs offers robust security across the entire software supply chain, providing real-time visibility, advanced threat detection, and automated security measures from code development through runtime. By protecting each stage, Uptycs ensures vulnerabilities and threats are mitigated without disrupting development workflows. This comprehensive approach includes contextual risk management, CI/CD integration, and runtime monitoring, empowering teams to address risks swiftly while maintaining compliance and efficient operations.

## Enforce Secure Development Processes

- **Shift-Left Image Scanning:** Integrate vulnerability scanning into build pipelines, enabling developers to scan images as they create software.
- **Policy-Driven Image Hardening:** Block images with malware, secrets, or vulnerabilities using CI/CD integrations with Jenkins, GitHub, AWS CodeBuild, and others.
- **Image Integrity and Trust:** Use Uptycs Kubernetes Admission Controls to block untrusted or unsigned images from deployment.

## Trace Runtime Threats to Code Commits

- **Runtime Detection:** Leverages eBPF technology to identify and block critical threats, such as ransomware and cryptominers, linking detected issues directly to source code commits for swift remediation.
- **Image Provenance:** Links runtime threats to specific code lines for root cause analysis.
- **Commit Traceability:** Integrates with GitHub Advanced Security for comprehensive scanning.

## Identify Key Risks and Misconfigurations

- **Supply Chain Posture Management:** Scans repositories and CI/CD postures for vulnerabilities.
- **Software Catalog & SBOM:** Maps open-source and third-party components, identifying risks.
- **Risk Prioritization:** Correlates findings with active processes for better prioritization.

## Secure Your Software Supply Chain

Uptycs provides end-to-end security for the entire software supply chain, from initial code commits to runtime environments. This comprehensive approach enables proactive threat detection and defense, minimizing risks that arise throughout the software development lifecycle. By safeguarding every phase, Uptycs strengthens an organization's ability to detect, respond to, and prevent modern security challenges with confidence.

## Success Stories

"Uptycs was deployed on a large scale as a key component of our Security posture."

**Comcast**  
Vice President IT Security

"I would not want to do security anywhere without this level of visibility"

**Steve Shedlock**  
Incident Response Team Lead SEI

Uptycs is the leading cloud security platform for large hybrid cloud environments. We extend security visibility from development to runtime, ensuring consistent protection and compliance across the application infrastructure. That's why enterprises like PayPal, Comcast, and Nutanix rely on Uptycs to secure the development ecosystems they use to build their applications and run their workloads.



Secure Everything from Dev to Runtime

[See Uptycs in action](#)