nexus container

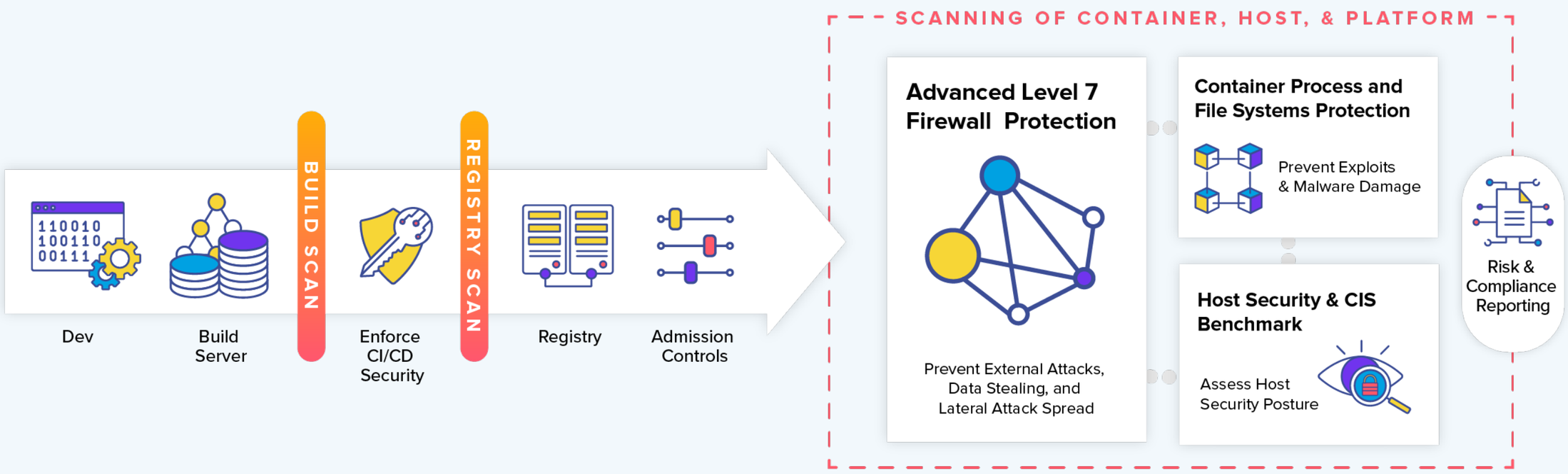
Protect containers from build to production.

The increasing popularity of containers — Docker image pulls were estimated at *~90 billion* in 2020 — also means an increasing susceptibility to container attacks. But securing a container's infrastructure requires more than just a quick vulnerability scan. End-to-end container security means taking a layered security approach — enforcing security and compliance requirements AND protecting networks, containers, and hosts in real time.

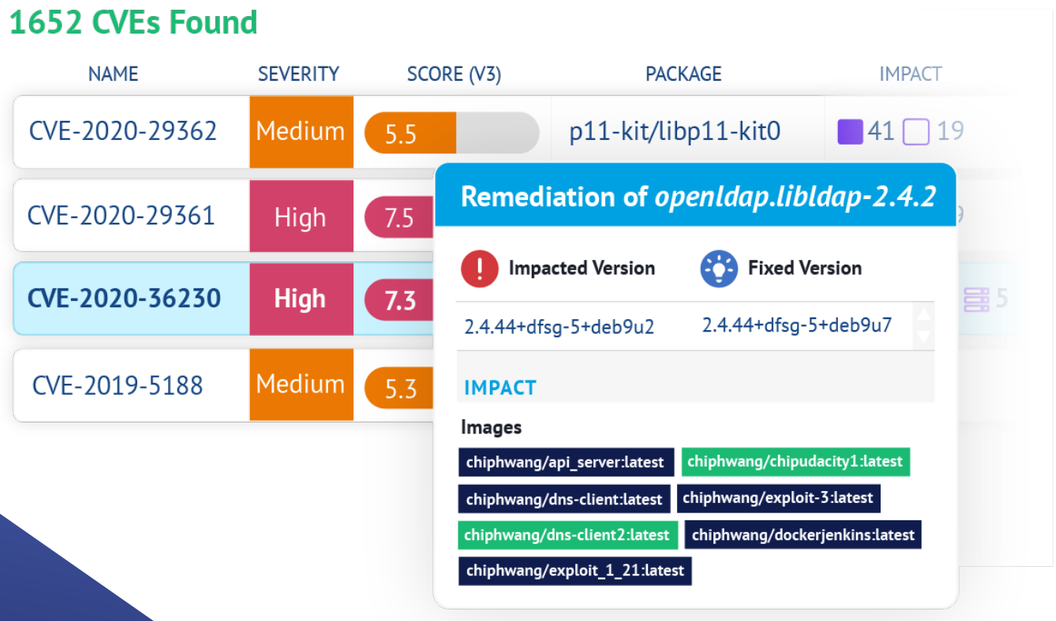
Nexus Container does it all — providing full life cycle security for Kubernetes-native containers, from build to ship to run.

We find — and stop — your vulnerable container images from deploying, and we are the only solution with behavioral inspection that can identify all network traffic at Layer 7 and every container process to automatically create behavior-based security policies, enforce Data Loss Protection, and prevent zero-day malware and network attacks, tunnel, and breaches.

Container Security With Nexus Container



Pipeline Security | *Run-Time Security*

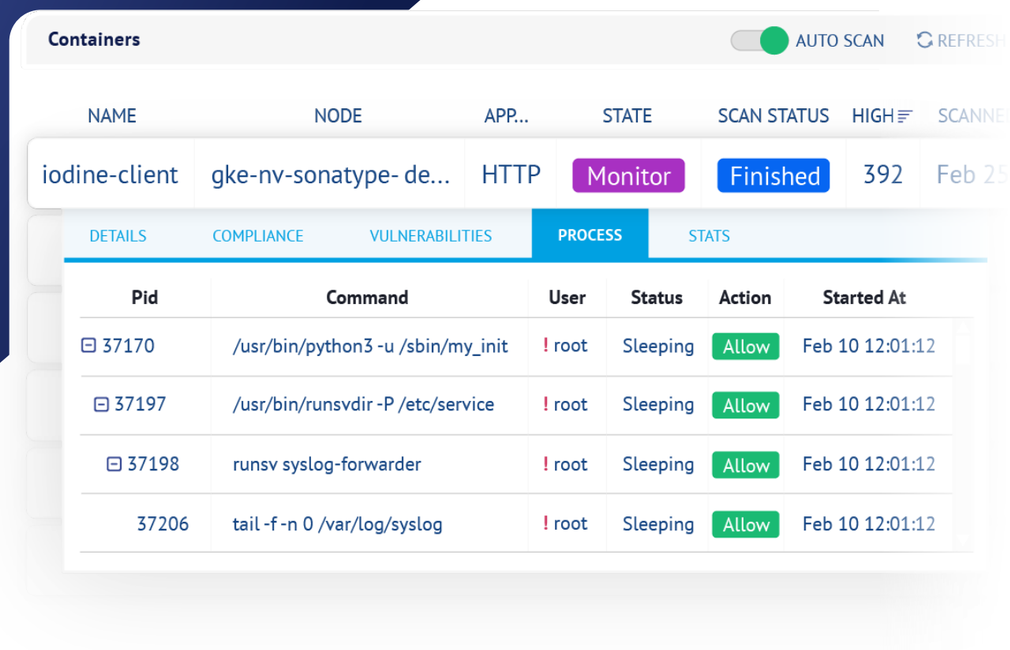


End-to-End Vulnerability Management, Compliance, and Auditing

Full life cycle vulnerability (CVE) & compliance scanning — during build, registry scans, and run-time. Manage container and application-level risk with admission controls to stop vulnerabilities from entering your SDLC, policy management to guide and enforce actions, and detailed remediation guidance.

[1] Sonatype's 2020 State of the Software Supply Chain report

www.sonatype.com

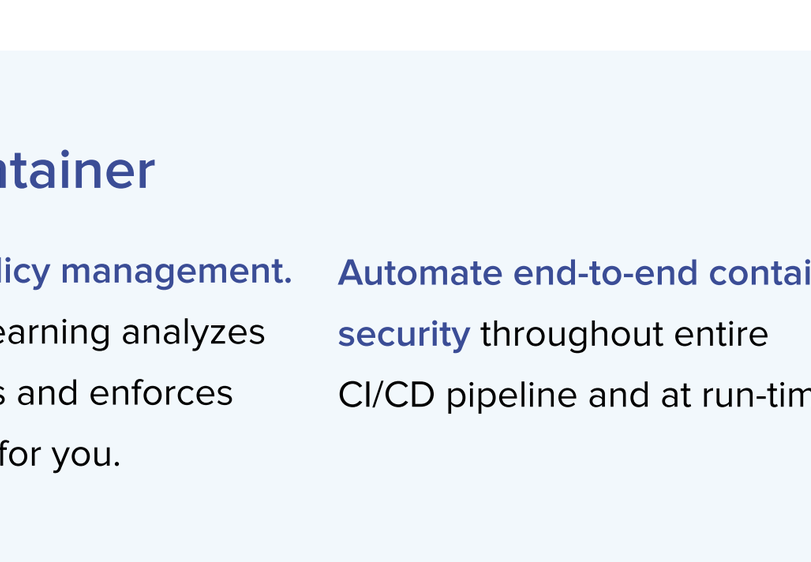


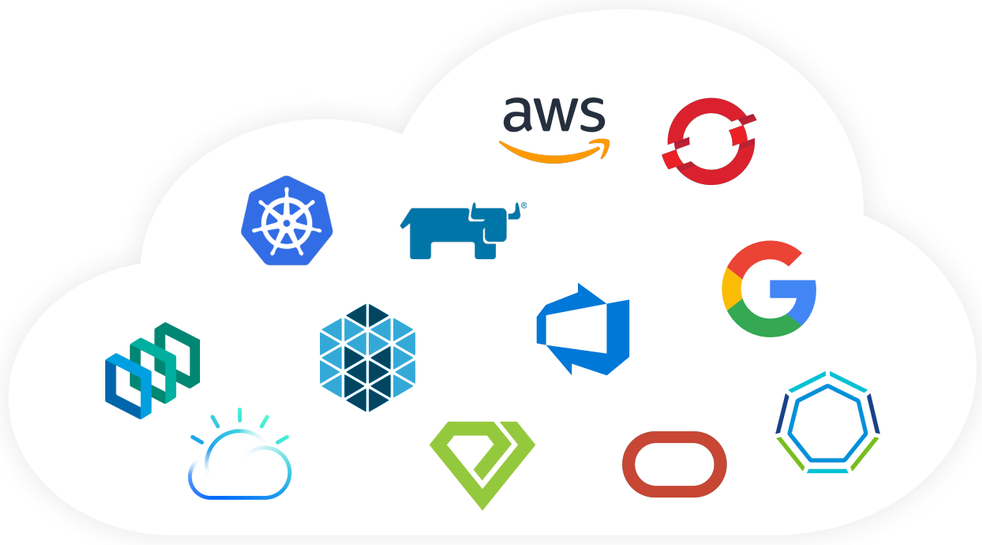
Host and Container Attack Prevention

Real-time vulnerability scanning during run-time for hosts and orchestration platforms, such as Kubernetes. Monitor live containers for suspicious process and file system activity and privilege escalation detection, with host process blocking.

Layer 7 Network Traffic Inspection for Data Loss Protection and Zero-Day Attacks Prevention

Continuously monitor running containers to prevent insider attacks which bypass network L3/L4 protections and safeguard sensitive data, PII, credit cards etc., with the only container DLP engine.





Cloud-Native Automation and Integration

Integrated with orchestration and management platforms: Kubernetes, Red Hat OpenShift (certified container & operator), Rancher (catalog listed), AWS ECS/EKS, Mesos etc., Google GCP/GKE, Azure/AKS, IBM Cloud, OKE, PKS, Diamanti, VMWare Tanzu, PKS.

Key Benefits of Nexus Container

Identify vulnerabilities and compliance issues before containers deploy.

Prevent cyber attacks with real-time visibility into network activity.

Save time on policy management. Our behavioral learning analyzes traffic then builds and enforces security policies for you.

Automate end-to-end container security throughout entire CI/CD pipeline and at run-time.

sonatype

Sonatype is the leader in developer-friendly, full-spectrum software supply chain management providing organizations total control of their cloud-native development life cycles, including third-party open source code, first-party source code, infrastructure as code, and containerized code. The company supports 70% of the Fortune 100 and its commercial and open source tools are trusted by 15 million developers around the world. With a vision to transform the way the world innovates, Sonatype helps organizations of all sizes build higher quality software that's more aligned with business needs, more maintainable, and more secure.

Sonatype has been recognized by Fast Company as one of the Best Workplaces for Innovators in the world, two years in a row and has been named to the Deloitte Technology Fast 500 and Inc. 5000 list for the past five years. For more information, please visit Sonatype.com, or connect with us on Facebook, Twitter, or LinkedIn.