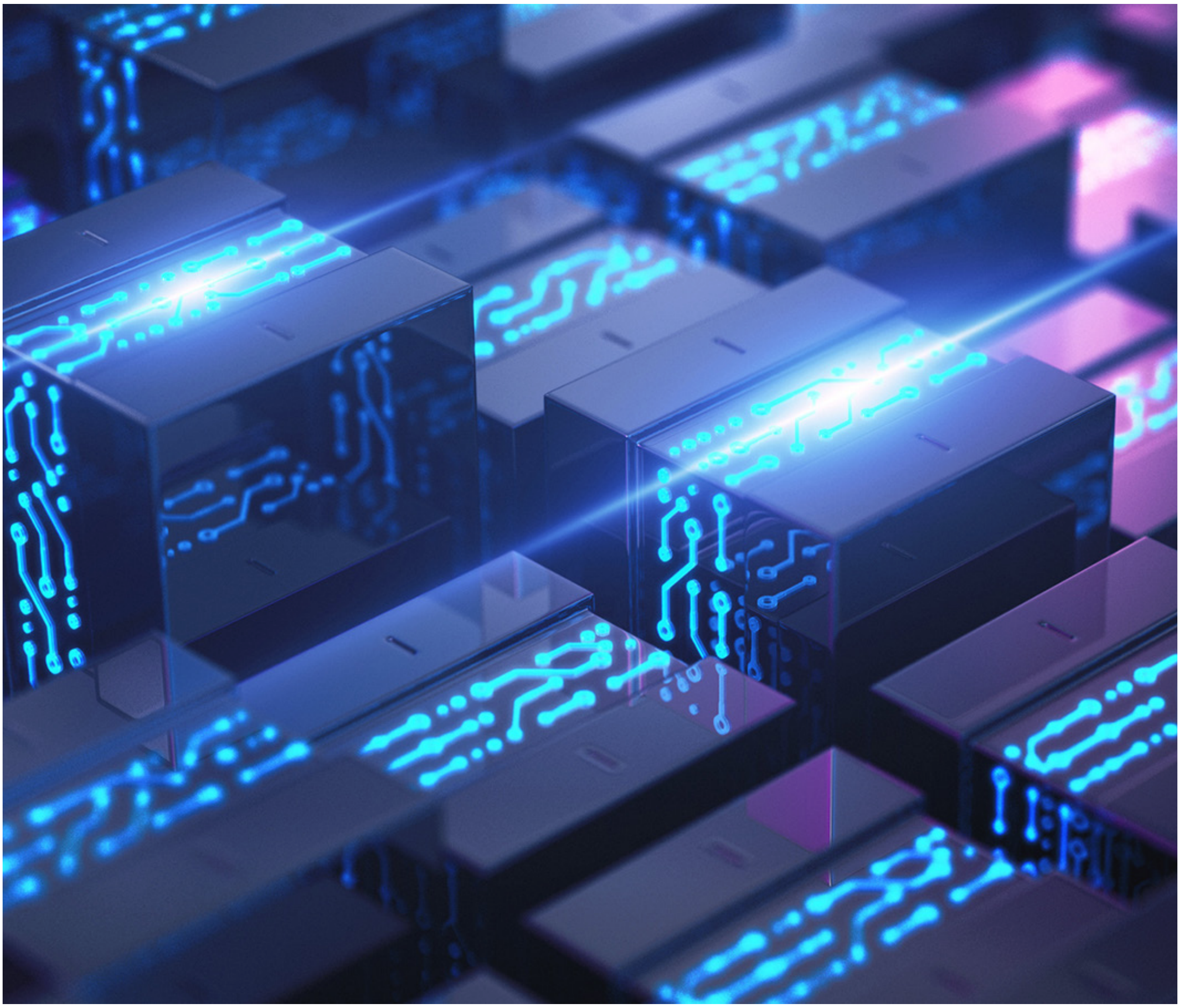
CIO FROM IDG | Red Hat | snyk

Snyk locks down security for Red Hat® OpenShift® development lifecycles



For businesses moving to the cloud to pursue complex modernization and digital transformation initiatives, DevOps methodologies and open source, containers, and cloud native technologies are increasingly common and important. The ability to build and deploy applications in smaller component units gives development teams power, flexibility and choice. The end result? The ability to scale rapidly, experiment and swiftly deliver new customer features and services.

But there's no such thing as a free lunch; the agility and resilience benefits resulting from containers and open source come at a cost. Alongside their widespread adoption, there has been a surge in container vulnerabilities. According to Snyk's "The State of Open Source Security Report 2020", most container images have 50 or more vulnerabilities, and only 39% of organizations have container vulnerability testing in their automated delivery pipelines. The resulting IT stack is exposed to significant vulnerabilities in open source dependencies, and has the potential to create licensing and compliance violations as well.

When container security is built into the development process, developers can ship faster and handle ongoing monitoring with ease

Containing new workloads

We know that the need for efficiency and speed in developing applications is driving increasing adoption of open source and containers. However, in attempting to expedite development by leveraging open source, code reuse and third-party scripts, enterprises face greater potential for risk.

Furthermore, as containers are often defined and built by developers and DevOps teams, the maintenance of operating system components and packages, previously managed by dedicated system administrators and virtual machine managers, has shifted to those same developer and DevOps teams. This shift in responsibility, combined with the fact that containers can be updated and deployed in a matter of seconds, requires a new approach to security methodology as a whole.

With this shift in ownership and the popularity of container-based workloads, developers and DevOps teams face a pressing need to map out software risk in a clear and actionable way. When container security is built into the development process, developers can ship faster and handle ongoing monitoring with ease.

The Snyk security platform allows developers to proactively find and fix vulnerabilities and software license violations in containers, infrastructure as code, and open source dependencies.

Snyk's developer-first security tools support and integrate into the technologies that OpenShift users prefer, prioritizing the developer experience and overall business efficiency.

By more easily embedding security features into continuous development processes and tools, developers are able to continue to move fast while supporting their security team's goals for workloads running on Red Hat® OpenShift®, the company's open source container application platform.

This shift to developer-led security enables developers to leverage the power of Snyk right inside their workflow so that vulnerabilities in open source code dependencies, containers, and Kubernetes configurations can be flagged and acted upon prior to code even hitting the CI/CD pipeline.

Developers largely outnumber security professionals in most IT departments, but when they work in unison with their security counterparts, the result is improved vulnerability management, compliance, and policy enforcement. As a result, security engineers are able to enhance security without becoming a roadblock for developers.

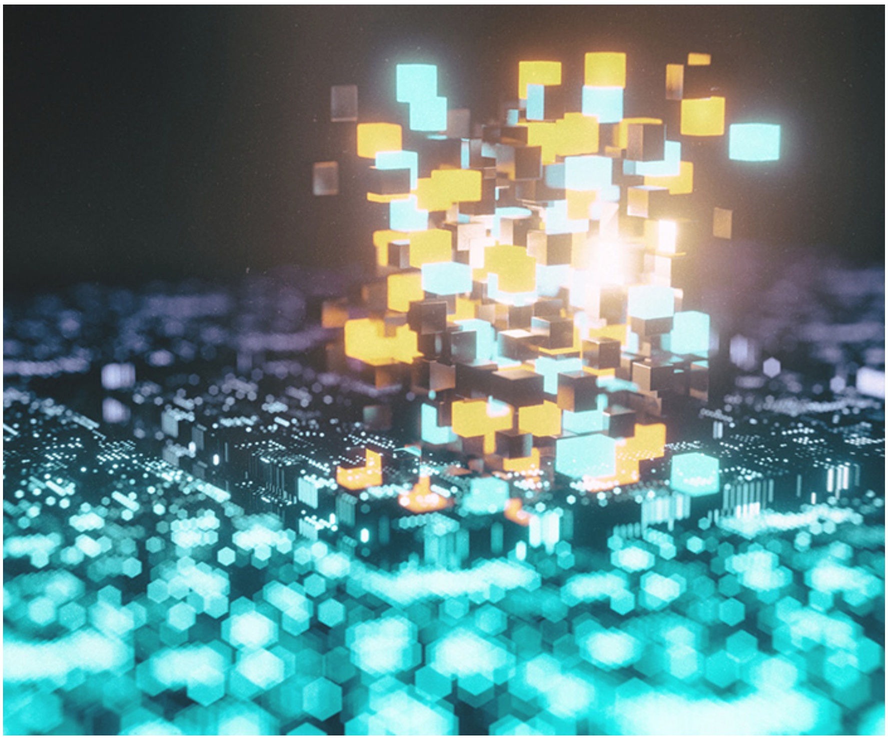
With Snyk Intel, its proprietary vulnerability database, Snyk also powers insights for Red Hat CodeReady Dependency Analytics, a plug-in into IDEs (Integrated Development Environment) such as CodeReady Workspaces, VS Code and JetBrains IntelliJ to automatically analyse the code being built and provide recommendations to address security risks and licensing problems.

When developers and security professionals work in unison, the result is improved vulnerability management, compliance, and policy enforcement

Shifting left for OpenShift

Snyk's new OpenShift integration, delivered as a certified Red Hat® OpenShift® Operator, allows for the detection and scanning of workloads on OpenShift clusters. Snyk scans the underlying containers in Kubernetes workloads and also provides pod configuration details that help identify areas of increased risk.

By providing developers with actionable insights early on, Snyk's work with Red Hat makes the process of building containerised deployments more secure and automated. It allows Red Hat OpenShift administrators to free up valuable time to work on new service innovations, instead of being a bottleneck for deployments. OpenShift operators can now drive the integrity and security of clusters from a workload perspective and automate security features into the development and delivery processes, enabling efficiency while limiting tradeoffs.



As workloads are deployed or changed within OpenShift clusters, Snyk detects and tests the underlying container images for vulnerabilities, plus it also provides information on the running pod configuration issues that might make those workloads less secure. Snyk delivers ongoing protection after workloads are scanned, to provide up-to-date vulnerability details on production applications. What's more, the pod configuration details help to prioritize where you should focus your fix efforts. Snyk Container's integration with OpenShift clusters makes these reports clear, as shown in the example below.

Additionally, by resolving vulnerabilities as early as possible, application development proceeds fast and without interruptions later once applications are running in production. The integration enables software engineers to configure applications and bring in custom code where needed knowing that vulnerability and compliance issues will be flagged immediately and fixed, long before deployment.

Although this integration and partnership is new in 2020, the technology itself can be retro-fitted to existing projects to lock down their vulnerability risk.

Snyk can simplify the risk/reward tradeoff of any change and help developers prioritize fixes for issues posing the greatest risk

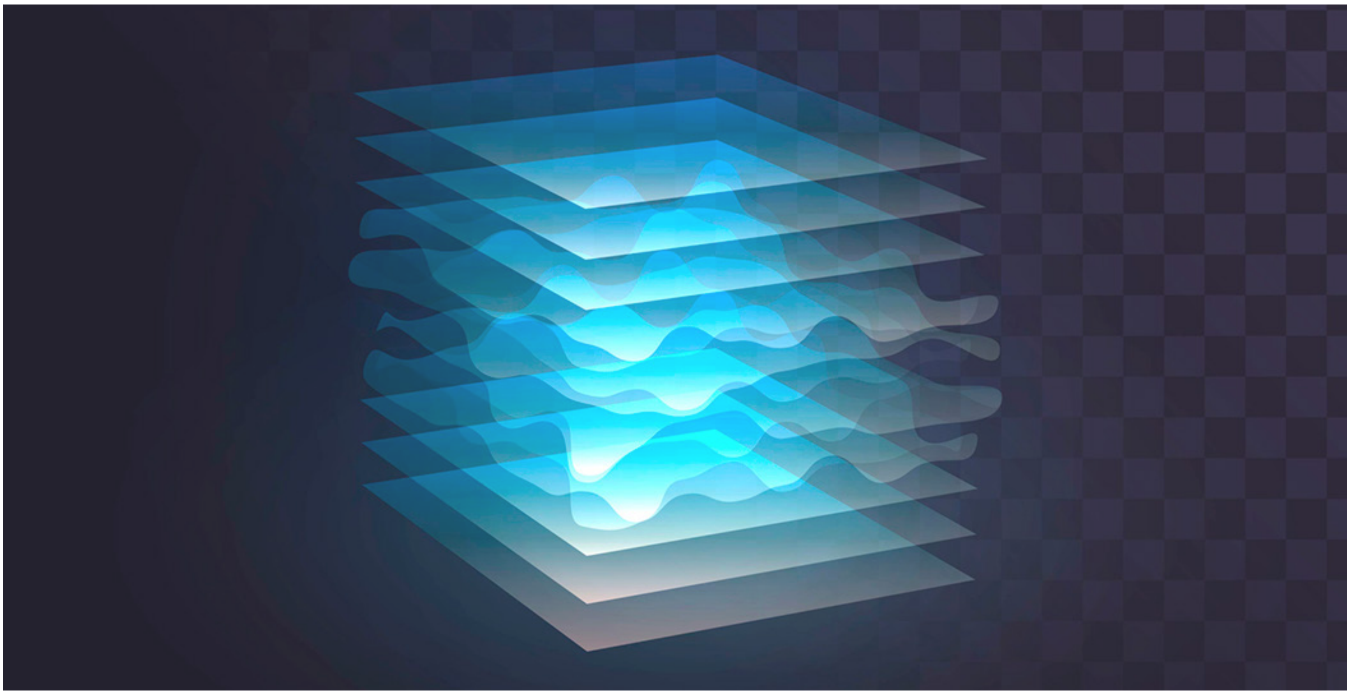
Snyk secures the entire OpenShift software development lifecycle

For developers who want to address security as early as possible in the software development lifecycle, Red Hat CodeReady Dependency Analytics, a hosted service on OpenShift, integrates the Snyk Intel Vulnerability Database. This provides vulnerability and compliance analysis for applications, directly from the IDE. CodeReady Dependency Analytics includes access to the Snyk Intel Vulnerability Database, which is a curated database of both unique and known open source software security advisories.

Snyk Intel goes beyond Common Vulnerabilities & Exposures (CVE) vulnerabilities and includes many additional non-CVE vulnerabilities that are derived from several sources.

The Synk Intel database also includes automated machine learning with expert analysis maintained by a dedicated Snyk research team, so the information it presents to the developer is a compound analysis that represents the most holistic view possible of the risks in the open source code.

Snyk will recommend the smallest version change needed to resolve a vulnerability, ensuring that security is improved while minimising the impact of the change. With numerous public and private data sources used to quantify and advise on the known risk of a given change, Snyk can simplify the risk/reward tradeoff of any change and help developers prioritize fixes for issues posing the greatest risk.



Snyk at work

Integrating Snyk with Red Hat allows developers to continuously test and monitor for newly disclosed vulnerabilities. Mapping out the full application dependency tree, Snyk can be utilised at the Command Line Interface (CLI), used to monitor and fix vulnerabilities in projects via code management systems, or employed via Application Programming Interfaces (APIs).

In terms of use, Snyk allows developers to execute a single-click fix from a User Interface (UI) or CLI wizard. It then automatically calculates the minimal direct dependency version upgrade needed. When a direct replacement or upgrade is not available, Snyk offers precision patches to remediate issues in live code. Snyk Container integrates across the developer workflow to allow coders to build and use containers in a secure way, providing advice to address vulnerabilities, while also monitoring workloads in Kubernetes clusters for new vulnerabilities.

Working throughout the breadth of the full application lifecycle from code development to deployed applications, Snyk's integration with Red Hat® OpenShift® allows programmers to integrate with GitHub, Bitbucket or GitLab to continuously scan code, testing every commit.

The DevSecOps dream

It is critical for developers to streamline security into their existing workflows and processes to prevent convoluted and complex vulnerabilities from slowing them down in their pursuit of rapid application development and effective software builds.

With Snyk helping to secure the entire OpenShift software development life cycle, the DevSecOps dream becomes a reality. Living this dream paves the way to greater developer engagement, greater application security and greater use of more automated Red Hat OpenShift workloads.

CIO FROM IDG | Red Hat snyk