Layered Insight™

Company Overview

Container Native Application Protection

Business Innovation and Digital Transformation are changing the pace and scale at which applications are being developed. To stay agile, application development is employing new processes, such as DevOps, and new technologies, such as containers. With these rapid changes, how do you balance speed and agility of Devops with security and compliance of SecOps?

DevSecOps: unify DevOps and SecOps

With the adoption of containers, what are the challenges of DevOps? How do developers understand the composition of container images, monitor communication of microservices based architectures, or enforce business requirements of containerized applications?

What about SecOps? How do security personnel understand security and configuration of containerized applications, monitor containerized applications in production, or protect containerized applications in production?

Organizations need to unify DevOps and SecOps by providing complete visibility and control of containerized applications through the entire lifecycle. Using the industry's first embedded security approach, Layered Insight's Container Native Application Protection solutions provide value for both DevOps and SecOps, including:

Accurate insight into container images

Adaptive analysis of running containers

Automated enforcement of container behavior

Accurate insight into container images

By statically scanning container images after the build process, Layered Assessment and Layered Compliance solve the challenges of accurate insight. Layered Assessment identifies the contents, including system binaries, software libraries, and other dependencies, and vulnerabilities within the container images. Layered Compliance enforces specific rules and business policies based on the assessment to determine if the container image can be run in production.

Key features:

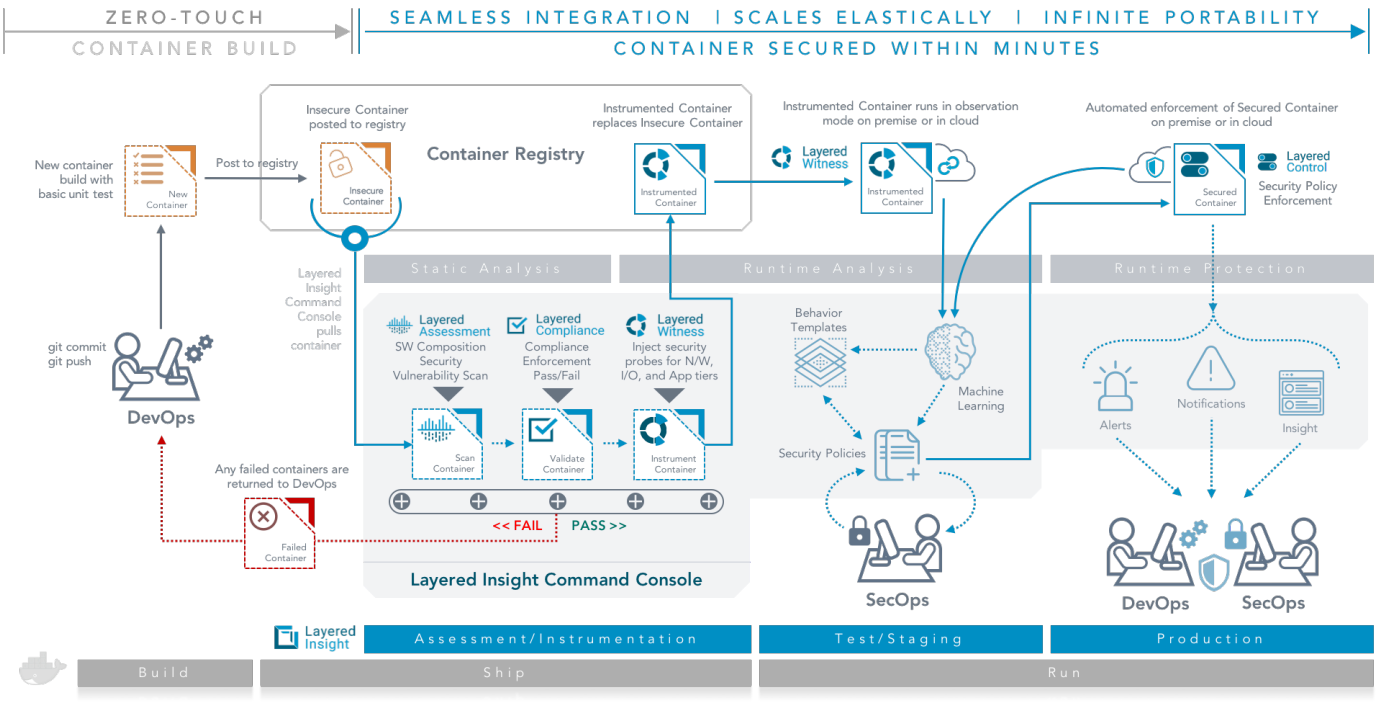
- **Software composition** – Complete and continuous visibility into container images.
- **Vulnerability assessment** – Continuous monitoring of vulnerabilities and impact analysis.
- **Compliance validation** – Enforcement of vulnerability, package, and open source license rules.

Adaptive analysis of running containers

By injecting security probes in every layer of the container image to monitor all network, storage, and application activities, Layered Witness solves the challenges of adaptive analysis of running containers.

Key features:

- **Runtime activity** — Deep, runtime analysis into all container activities, including network, storage and application layers.
- **Container communication** — Automatic creation of intra- and inter- container communication and connectivity.
- **Behavior profiles** — Automatic, and continuous, creation of activity and behavior profiles for each container.



Automated enforcement of container behavior

Layered Control solves the automated enforcement of the normal container behavior by leveraging the analysis (automatically created behavior baselines) from Layered Witness and blocking abnormal or malicious behavior. Layered Control provides automated enforcement of the following areas:

1. **Network** — Intra- and inter- application container communication, at service, process, IP or port level, and blocking processes from performing DNS benchmarking.
2. **Process** — Processes running only whitelisted binaries, limiting runaway forking of other processes, and restricting access to all system calls not included in the activity and behavior policies.
3. **Storage** — Read-only and read-write paths and allowed mount points.
4. **Application** — Application execution paths from higher level languages all the way through system calls.

Key features:

- **Behavior policies** — Enforcement of pre-defined or automatically created activity and behavior policies for each container.
- **Anomaly detection** — Deep Learning-based behavior anomaly detection across all activities, including network, storage and application layers.
- **Runtime protection** — Comprehensive, continuous activity and behavior enforcement, across the network, storage and application layers.

Overall benefits

By leveraging Layered Insight's solutions, organizations can reap the benefits of adopting containerized applications for both DevOps and SecOps, including:

- Security and compliance at the speed of business Innovation
- Zero touch for developers and seamless Integration with DevOps
- Portability, performance and scalability across all container orchestrations, stacks and lifecycles

Layered Insight™

Learn more at **www.layeredinsight.com**

Email us at **info@layeredinsight.com**

Layered Insight, the pioneer and global leader in Container Native Application Protection, enables organizations to unify DevOps and SecOps by providing complete visibility and control of containerized applications. Using the industry's first embedded security approach, Layered Insight solves the challenges of container performance and protection by providing accurate insight into container images, adaptive analysis of running containers, and automated enforcement of container behavior. Balance the speed and agility of DevOps with the security and compliance of SecOps by visiting **www.layeredinsight.com**.