GUAC Case Study

Guidewire

How Guidewire Cloud Platform is using and collaborating with open source GUAC

Guidewire Software creates the platform that property and casualty insurers trust to engage, innovate, and grow efficiently.

Securing the software supply chain is paramount for the Guidewire Cloud Platform (GWCP). More than 540 insurers in 40 countries use GWCP and other Guidewire solutions to run insurance suite applications.

Guidewire's customers trust the platform to engage, innovate, and grow efficiently. GWCP combines digital, core, analytics, and machine learning and runs more than 10,000 workloads.

GWCP is a platform-as-a-service (PaaS) offering built on Kubernetes that enables Guidewire enterprise customers to enter the market faster with a competitive level of scalability and elasticity with the added benefit of traceability and compliance for software supply chain security.

ABOUT

- Insurance | Cloud Platform
- HQ: San Mateo, California
- GWRE (NYSE)
- Guidewire Cloud Platform runs 10K+ workloads
- www.guidewire.com

KEY CHALLENGES

- Trace and trust running applications
- Robust security evidence for compliance and auditing
- Enforce deployment-gating security policies
- Protect against attacks and threats through out the software supply chain
- View trends and analytics across projects

VALUED OUTCOMES

- Flexible architecture that integrates with Guidewire's platform and other software
- Trace every step of a running application – from build to production
- Meet security/compliance requirements for internal teams and pass along that advantage to customers

Staying safe with open source GUC

Innovative supply chain security for Guidewire Cloud Platform

www.guac.sh | August 2024

Scale and protect

Anoop Gopalakrishnan, Guidewire's VP of Engineering, vividly recalls the Log4Shell incident in 2021. Although the Guidewire engineering team handled the crisis with speed and ingenuity, this is not a scenario anyone wants to relive. The team spent countless hours and sleepless nights to address each customer's unique setup as quickly as possible in order to locate and fix the problem.

> ***"The challenge was identifying where the issue was for each customer and their unique system.***
>
> ***Plus, finding out who was moving towards a patch was very difficult to coordinate."***

As Guidewire increased in market share and onboarded more customers to the platform, Anoop and the engineering team began to build a more robust mechanism to provide evidence of security to their own compliance and auditing teams, which was in turn immensely valuable for their customers.

When searching for a solution, Guidewire initially set out to build its own. Anoop was inspired by the various secure software supply chain papers and research done in the area. And yet, he knew the open source community could hold a solution that his team could get started with immediately and build upon, tailoring it to their needs.

Guidewire's questions:

- ***How can we trace a running application down to all the steps that led up to its deployment in production?***
- ***How do we demonstrate the contents of a platform's running component, including the commits and third-party libraries it uses?***
- ***How can we trust the trace graph?***
- ***How can we empower our teams to enforce policies that can act as a gate to deny deployments to the platform based on specific libraries or their versions?***
- ***How can we visualize the various trends across projects/teams and provide an analytic center to encourage better practices?***
- ***How can we keep ourselves and our customers safe from man-in-the-middle attacks, supply chain poisoning, and software counterfeiting?***

Turning to open source

To prepare for the future, Anoop looked to the open source software (OSS) community. From his experience contributing to and using Spring Boot and other tech, he knew it was resourceful, quick, and brilliant at addressing nuanced, modern software problems. And he was right.

"*Going back to the Log4Shell example, GUAC would have helped us identify where the vulnerability was, trace the fix process, and share that information with customers much more efficiently and effectively."*

"When I found Parth Patel, a GUAC maintainer, and the GUAC community, I reached out to see how development was going. Were they active? Were theyinterested in working with an external group to tailor this solution to our particular needs? These questions would provide critical feedback to me and allow me to consider whether it would be the right choice for us," says Anoop.

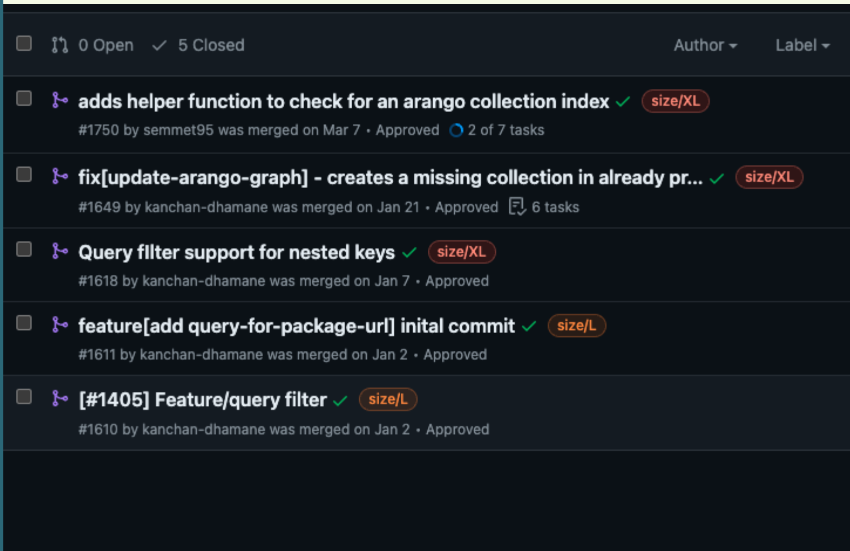
Parth and Anoop hit it off, sharing each team's goals, needs, and roadmap. The two teams meet monthly to discuss progress, needs, open PRs, and feedback. This allows GUAC and Guidewire to participate in a symbiotic relationship, proving what open source software can offer.

Guidewire also aims to create a policy engine on top of GUAC for their internal team as well as their enterprise customers in the cloud. This will enable everyone to go from ideation to production as fast and securely as possible.

"The advantage we see with GUAC is its flexibility and plugin architecture, which helps users achieve SLSA compliance at different levels," says Anoop.

"Being a platform as a service, we are generating a lot of secure, immutable artifacts like SBOMs, attestations, and provenance from different parts of the platform. We extend GUAC to our custom solution, which helps us to ingest, collate, and present the information in a consumable format for our internal teams as customers."

"To us, the biggest value is GUAC's open nature and the community behind it. We are pleased to be aligned with a tool backed by Google, Kusari, and other engineers with many years of experience and expertise in this industry."



□ adds helper function to check for an arango collection index ✓ size/XL
#1750 by semmet95 was merged on Mar 7 • Approved 2 of 7 tasks

□ fix[update-arango-graph] - creates a missing collection in already pr... ✓ size/XL
#1649 by kanchan-dhamane was merged on Jan 21 • Approved 6 tasks

□ Query filter support for nested keys ✓ size/XL
#1618 by kanchan-dhamane was merged on Jan 7 • Approved

□ feature[add query-for-package-url] inital commit ✓ size/L
#1611 by kanchan-dhamane was merged on Jan 2 • Approved

□ [#1405] Feature/query filter ✓ size/L
#1610 by kanchan-dhamane was merged on Jan 2 • Approved

GUAC

Stay ahead of threats

Sitting at the forefront of the software supply chain industry by way of maintaining a cloud platform, Anoop predicts supply chain threats will become more complex as the industry progresses.

In addition, Anoop expects there will be greater focus on the following in terms of secure software development:

- Using AI/ML to detect, mitigate, and evolve to target new threats, thereby freeing up precious resources to focus on more strategic threats

- Bringing transparency to the entire software supply chain and a greater emphasis on bills of materials of various kinds, like Hardware BOMs, Environment BOMs, etc., while Software BOMs still take up the majority of the mindshare

- Internal collaboration with a focus on efficient data and transparency of the security process, which will result in a greater tendency for shift-left practices

- Software lifecycle-oriented approaches for detecting privacy concerns in code using static analysis

- Awareness and demand for provenance and attest-ations from vendors of software across the board

Anoop hopes to collaborate with like-minded institutions to build open source frameworks and tools with the same goal.

The Guidewire engineering team is in the development phase with GUAC. They look forward to maturing into the production phase, bringing GWCP the added compliance and dependency management capabilities while mitigating risks like another Log4Shell incident.

According to Anoop, "Our approach is to be pragmatic and at the same time involve ourselves with standards that can benefit many companies in these areas. This is what brought us to become more involved in the GUAC community."

> ***"We continue researching these areas with our teams to bring value to our customers and the Guidewire community at large."***

Learn more about GUAC

Graph for Understanding Artifact Composition, or GUAC, ingests and leverages metadata like Software Bill of Materials (SBOMs), SLSA attestations, and more to map out relationships between software components, enabling users to fully understand their software security position, and take appropriate, accurate action.

See the latest releases, documentation and videos on GUAC's architecture and how it works.
www.guac.sh

GUAC