HCL



Industry: Information Technology Products: HCL AppScan Region: North America/US

Business Challenges

Our customer was faced with the following business challenges:

- Improving the security protection of their products without disrupting the current SDLC process.
- Reducing the probability of a security issue that could delay shipping of new versions.

We were surprised by the deployment process. We were expecting something more complicated than deploying a WAR file to our Tomcat!

Technical Manager DevOps team

Solution

Integrate IAST into the customer's existing QA process and leverage automatic, manual and sanity tests to extend Application Security Testing (AST) coverage and transform DevOps to DevSecOps.

Results

Improved AST coverage and remediation processes, due to informative records of security issues such as full call stacks and exploit examples that are reported by the IAST agent.



Business Case for IAST

The company was already utilizing DAST as part of their SDLC, mostly in the late stages. This common practice provided good results, but had several downsides to it:

- When a significant security vulnerability was discovered, it caused a delay in the release, since DAST was introduced as one of the last steps before a new version was shipped. Remediation efforts for security vulnerabilities were high due to the DAST scanner's less detailed information.
- There was a significant time gap between writing the code and discovering vulnerabilities.

Integrating IAST

The company has an extensive Quality Assurance (QA) process due to its codebase's size and complexity. The QA process includes automated and manual testing that ranged from simple sanity scenarios to complicated edge cases. Every new version also added more functionality, so further tests was introduced into the QA process.

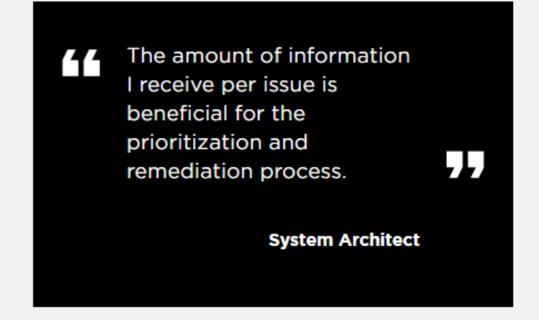
The QA infrastructure is Docker-based and orchestrated using Jenkins. Since the team didn't want to change their existing containers, they decided to integrate IAST by using a simple script that utilizes AppScan's APIs to download and deploy the agent to the web server, after applications are successfully built and published.

Effects

A significant benefit that developers instantly reported was the amount of information the security vulnerabilities contained. Having the line of code that originated the issue, along with an example of an exploit that triggered it, reduced remediation efforts significantly. Since the QA process is adjacent to the development process, the code changes that resulted in new security vulnerabilities are fresh in developers minds when approaching to resolve security issues.

Another benefit that the security team reported was reducing issues detected in DAST scanning, since the QA process now helped to resolve issues earlier in the SDLC.

From a maintenance perspective, the Security and DevOps teams were impressed since integrating the IAST agent only requires a single straightforward script, and the agent itself is evergreen (meaning that it updates automatically). Another great thing is that the QA team can keep adding new tests for every new functionality it develops, keeping AST coverage up to date with every new version. The process keeps improving as a byproduct of the SDLC itself.



About the company

Due to the cybersecurity domain's sensitive nature, the company requested to stay anonymous in this particular case study. The company is a software company in the IT e market that provides services to SMBs and large enterprises.

The technology stack used in this case study is:

Java

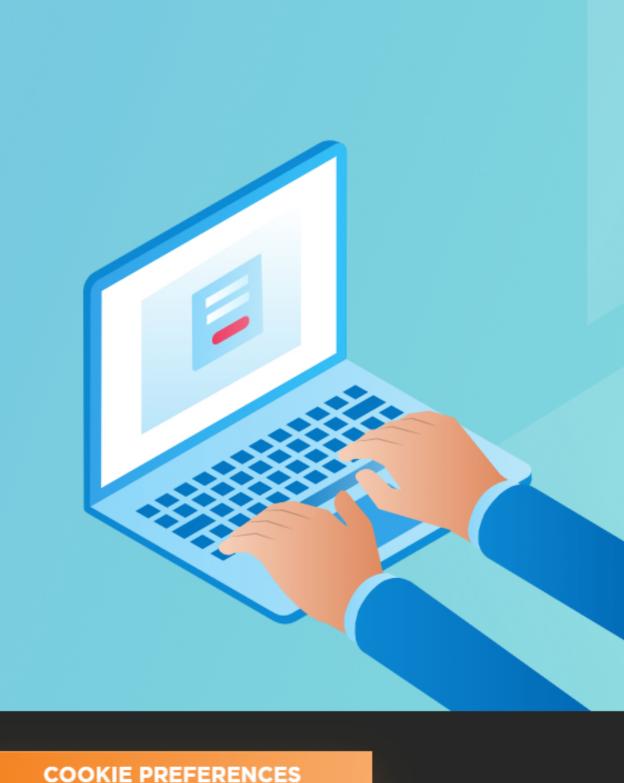
Tomcat Docker

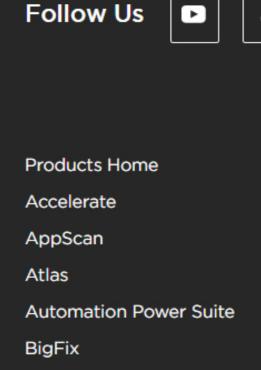
Jenkins

DOWNLOAD STORY

To learn more about how IAST can benefit your organization, please read and share our informative white paper

WHITE PAPER





Clara

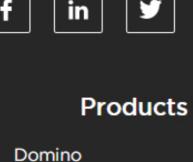
Commerce

Compass

DevOps

Connections

Digital Experience



Link

Hero

Leap

Notes

OneDB

OneTest

RTist

SafeLinx

Sametime

OneTest Embedded





SoFy Unica Verse Version Vault Volt MX Workload Automation Mainframe Solutions Z Asset Optimizer

Z Data Tools

View All

Z Abend Investigator

Z and I Emulator

Resources Home Key Facts

Resources

Client Advocacy **Success Stories** Analyst Reports Video Gallery Partner Connect Product Lifecycle

Demo Portal

Submit Idea

Open Source

Ecommerce

About HCL Software **About Us**

HCL Ambassadors Events & Webinars Acquisition FAQ Government - US Federal News Welcome Contact Us

Legal Disclaimer Privacy Accessibility Compliance Software Disclaimer **Future Products** Cookie Statement