



CUSTOMER SUCCESS STORY

ACCELERATING FOR “WHAT’S NEXT” AT THE CUTTING EDGE OF MOBILITY

COMPANY

Yunex Traffic is a global leader in intelligent traffic solutions, developing novel mobility solutions for hundreds of cities, highway authorities, and mobility providers all over the world. Founded and matured under the Siemens technical umbrella, Yunex Traffic’s 3100 employees help transform cities into places where people can live, work and move more freely with better quality of life, fewer accidents, and cleaner air, while contributing to solving our climate crisis.

CHALLENGES

The need to modernize development at Yunex Traffic was acute: A legacy of monolithic on-premises applications conflicted with growing customer demands to operate Yunex Traffic’s solutions in their chosen cloud environments. A once-a-year release cadence was incompatible with rapid remediation, updates, and changing mandates in this highly regulated industry. Classified as critical infrastructure, traffic control is subject to rule-making bodies like the European Programme for Critical Infrastructure Protection (EPCIP). Compliance failures can result in financial penalties for customer cities, as well as public safety risk from cyberattack.

Yunex Traffic sought to accelerate a transition to DevOps and cloud-native development, designing around container-based microservices using Docker, Helm, and Kubernetes. Vulnerabilities were also top-of-mind: “Security has always been important to us and as our solutions are now reachable from the internet, it gained even more importance.”



INDUSTRY

- Infrastructure Engineering Design and Consultancy Services



PROBLEM

- Infrequent (annual) release cadence for legacy applications
- Customers demand cloud native
- Strict regulatory compliance requirements
- As critical infrastructure, requires strong security
- Open-source license clearing processes too complex



RESULTS

- Conversion to cloud native development with Docker and K8s
- Cloud-hosted development infrastructure
- Releases and updates any (or every) day
- Security integrated into DevOps
- Detect and block vulnerable 1st and 3rd party code
- Fast, streamlined OSS license clearing
- Rapid remediation of zero day issues
- Access to advanced security research



SOLUTIONS

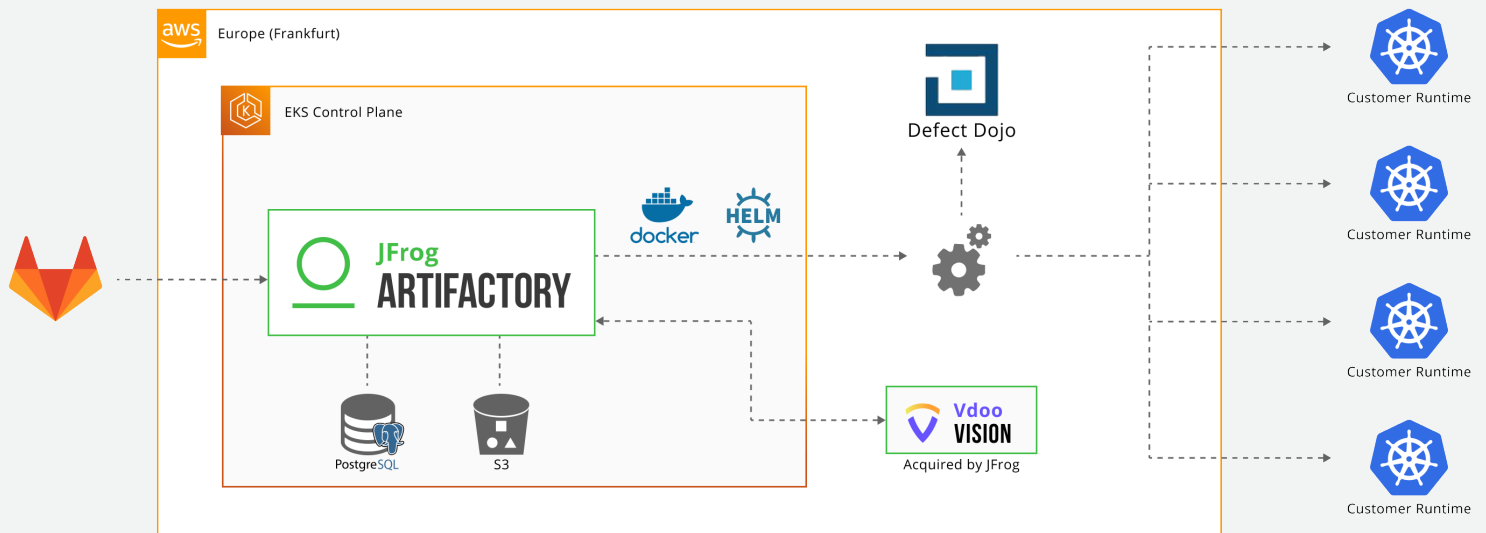
- JFrog Artifactory
- JFrog Xray

RESULTS

Yunex Traffic moved development to the cloud, self-managing Artifactory in an AWS cluster. Instead of ad-hoc repositories in shared drives as before, Artifactory local repositories for Maven, Gradle, NuGet, Docker, and Helm, as well as remote repositories to proxy DockerHub and other sites provide “the single place to collect artifacts wherever they come from, to have one place for control of what we’re doing.”

Centralized binary management enables deep integration of cloud native development, security, and license clearing efforts, scanning for vulnerabilities and reducing Yunex Traffic’s legal exposure. With risks more visible and minimized, Yunex Traffic’s automation can continuously deliver updates to every customer’s cloud and/or on-premises environments from production Docker and Helm registries in Artifactory.

JFrog helped prepare Yunex Traffic for “What’s Next,” enabling them to rapidly respond to new regulatory requirements and zero-day bugs with high-quality microservice updates on-demand. “When we had that issue with log4j, it was announced on Friday afternoon and [using JFrog] by Monday at noon we had all cities rolled out with the patch.”



We typically had one big delivery to customers per year- We are currently able to more or less continuously roll out now.”

Hanno Walischewski, Chief System Architect at Yunex Traffic



www.jfrog.com



www.facebook.com/artifrog/



www.twitter.com/jfrog



www.linkedin.com/company/jfrog-ltd

