ABOUT THE COMPANY
This enterprise eSports and mobile gaming platform is trusted by 75 million users in India and Indonesia and 90 million users worldwide. It offers multiple Android and iOS applications across categories such as casual games, card games, fantasy gaming, and esports.

The company employs over 1,000 employees across offices in Bengaluru, Pune, New Delhi, Jakarta, Singapore, and New York.

CHALLENGES THEY FACE
Reputation is make-or-break in mobile gaming and eSports, where players are wagering real money from their digital wallets and demand safeguards against cheating and fraud. The DevOps team must perform frequent updates of the 100 backend services that support its platform of over 70 games to ensure that compliance is up-to-date with all ISO 27001, PCI DSS, and other regulatory requirements. These standards also mandate strict security monitoring for vulnerabilities and rapid remediation.

The company wanted to enable software updates with a security-first approach that would make the platform safe for customers against common attacks in the esports industry, like account takeover, phishing, and doxing. They also required that their 350 developers and staff be able to be productive during times of heavy load or system upgrades and scale cost-effectively for multiple global sites.

INDUSTRY
- Mobile Gaming and eSports

PROBLEM
- Development insufficiently focused on security
- Unable to scale cost-effectively

RESULTS
- Centralized artifact management
- Strong and consistent security posture across all development
- Shift left security to developers
- Block vulnerabilities from mission-critical backend services
- Compliance with ISO 27001 and PCI DSS standards and audits
- Rapid remediation of zero-day issues
- Zero downtime for upgrades
- Scalable for multi-region and multi-cloud
- Deployments at least twice a day

SOLUTIONS
- JFrog Artifactory
- JFrog Xray
RESULTS

To enable a consistent security posture for all development, the “SSC tools that are used within the developer ecosystem must support different technologies.” JFrog Artifactory’s universal repository management brings all of the company’s artifacts together. It builds them into one place where they can be tracked and scanned by JFrog Xray to identify and block vulnerable components.

Using JFrog IDE extensions and Xray local file scanning, the company also shifts security left to enable developers to identify vulnerable packages early.

A high availability infrastructure self-managed in an AWS cluster fulfills disaster recovery requirements for compliance audits. It allows company admins to update their mission-critical JFrog Platform with zero downtime, even during prime working hours.

Upon data transfer to Artifactory, the company completed the changeover in a week. The company now deploys highly secure builds at least twice daily, updating 70% of its backend services each month, and is beginning to scale for multiple regions and cloud service providers.

“We were able to onboard JFrog in a jiffy; It was pretty smooth, and I have all the support that I need.”

---

“This is a simpler approach that will definitely secure our environment. I would recommend JFrog to anybody who’s looking for an artifact management solution that secures their software supply chain, and I don’t think they will find anything better than JFrog.”

Senior Engineering Manager