VERACODE

Keap Finds and Fixes Security Flaws Faster to Assure Regulatory Compliance

CRM developer improves code quality while saving time and money in the DevSecOps life cycle with Veracode Continuous Software Security Platform.

keap

Customer
Keap

Industry
Software & Technology

Location
Mesa, Arizona, United States

Veracode Products
Static Analysis
Dynamic Analysis

"Since Veracode integrates with Jira, we no longer need someone to enter and assign security tickets to developers. We are able to use that resource for more productive tasks."

Joseph Mask
Staff Site Reliability Engineer
Keap

Keap is a SaaS-based software leader that provides an all-in-one CRM, powering sales and marketing automation for small businesses. Keap products are designed to help businesses increase profit and build their book of business by automating follow-ups, tracking leads, and closing sales. On average, Keap enables its 125,000-plus users to add more than 4 million contacts, send more than 24 billion emails, and process over $2.5 billion in invoices annually.

Challenge

Because customers entrust Keap with their most sensitive data, any breach would cost the company both financially and in reputation loss. Therefore, Keap needed an application security solution that would help its developers find and fix flaws quickly and efficiently. Moreover, because Keap also processes payments, it needed to ensure compliance with Payment Card Industry (PCI) requirements and state regulations.

Solution

- Implement Veracode Static Analysis and Dynamic Analysis early in the software development life cycle.
- Integrate Veracode solutions with Jira, enabling developers to receive scan results instantaneously instead of waiting weeks.
- Take advantage of Veracode remediation guidance and technical support to empower developers to find and fix security flaws quickly.
- Leverage Veracode to assess applications across multiple standards to achieve and demonstrate compliance with both government regulations and customer requirements.

Results

- Improved developer adoption of application security best practices.
- Enabled developers to find flaws earlier in the SDLC, resulting in significant time and cost savings.
- Assured PCI and state regulatory compliance, allowing more frequent but shorter audits.
- Accelerated release of new software and application enhancement with confidence that the code is secure.

Learn More