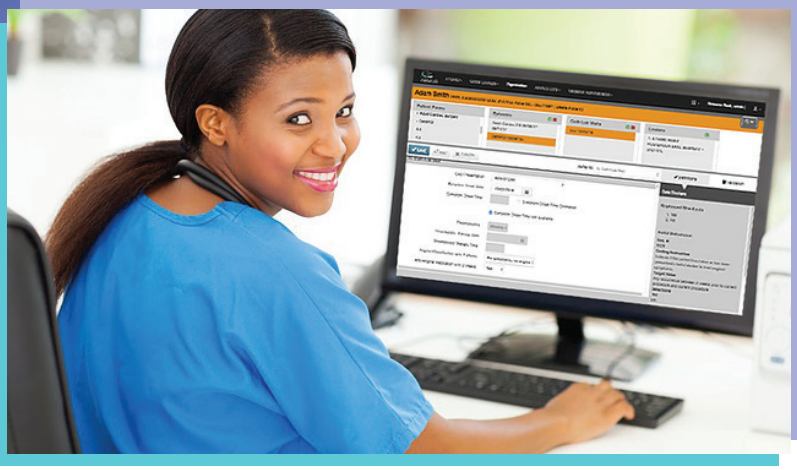
StackRox

ARMUS
Case Study



ARMUS is a leading global clinical registry software and service provider that gives outcomes improvement powers to hospitals, physicians, and clinical quality coordinators by delivering impactful data analytics and reporting tools. The company's goal is to use real-time actionable clinical, financial, and patient-reported information to sustain better outcomes, reduce post procedure complications, lower costs, and improve patients' lives.

With each transaction, the company's technology is making data-driven classifications, forecasts, and risk assessments based on statistical analysis of multiple, large data sources. Given the sensitive nature of protected health information and the HIPAA standards for sensitive patient data protection, robust and reliable data security is vital to ARMUS.

Meeting the need for always-on data

As it grew to become an industry leader, ARMUS recognized a need to dynamically scale resources up and down so it could drive faster updates than previously established processes. Supporting hospitals and large medical facilities that are operating 24/7 renders maintenance windows impossible. The company transitioned to containers and Kubernetes to deliver software updates without making data unavailable.

With its transition to the cloud-native application development stack, ARMUS immediately realized it needed a new approach to security. "The old tools are not equipped for this environment, and we have to

ARMUS

ARMUS provides cloud-based clinical registry services to its healthcare clients, to collect, measure, analyze, and improve clinical outcomes and patients' lives.

Headquarters:
Foster City, CA

Founded: 1992

Environment:
Google Cloud Platform, Google Kubernetes Engine

www.armus.com

find our most important vulnerabilities and remediate them as soon as possible," says Cyrus Makalinaw, security and privacy officer for ARMUS.

"Seeing what needs to be fixed right away, right there in the dashboard, is a huge value to us."

– Cyrus Makalinaw, security and privacy officer

Leveraging StackRox to secure patient data

Makalinaw heads up a small team that has to run as efficiently as possible, and they work very closely with the operations team. The team relies on the StackRox Kubernetes Security Platform – its automation, tie in with CI/CD, and on-going compliance checks has helped the team operationalize container security.

"Seeing what needs to be fixed right away, right there in the dashboard, is a huge value to us," says Makalinaw. "The StackRox software also showed us where our Kubernetes network connections weren't right – we had servers that could reach each other that shouldn't." The fact that StackRox automatically generates the correct Kubernetes network segmentation policies helps streamline operations. "Anything that helps to automate processes is invaluable," says Makalinaw.

ARMUS relies on StackRox to secure its Kubernetes and container environments across the full application development life cycle. In particular, ARMUS leverages StackRox for:

- **Compliance** – StackRox provides the automated and on-demand controls that ARMUS needs to support and demonstrate compliance with industry standards including SOC 2 and HIPAA.
- **Risk-based prioritization** – StackRox provides a dynamic, multi-factor risk assessment that enables ARMUS to immediately triage the highest-risk deployments in the environment at all times.
- **Threat detection** – StackRox automatically detects container attacks in seconds, using rules, whitelists, and behavioral modeling for runtime detection and response. ARMUS is able to spin up a new server while doing forensics on any targeted data without impact to its clients.
- **Vulnerability management** - StackRox enforces ARMUS' policies across the entire life cycle based on vulnerability information – at build time with CI/CD pipeline integration, at deploy time using dynamic admission control, and at runtime with its Kubernetes-native enforcement.

StackRox

StackRox helps enterprises secure their containers and Kubernetes environments at scale. The StackRox Kubernetes Security Platform enables security and DevOps teams to enforce their compliance and security policies across the entire container life cycle, from build to deploy to runtime. StackRox integrates with existing DevOps and security tools, enabling teams to quickly operationalize container and Kubernetes security. StackRox customers span cloud-native start- ups Global 2000 enterprises, and government agencies.

LET'S GET STARTED

Request a demo today!
info@stackrox.com
+1 (650) 489-6769
www.stackrox.com