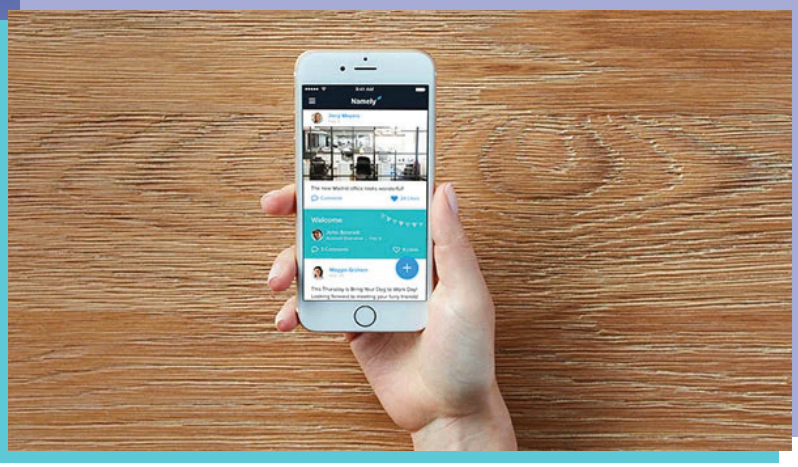
StackRox

# Namely

## Case Study



Namely provides cloud-based software that brings human capital management (HCM), benefits, insights, and payroll into a single-view platform to help modern HR teams analyze the workforce with data-driven analysis. The Namely platform integrates with applicant tracking, identity management, ERP, compliance, E-Verify solutions, and more.

Namely bridges the gap between HR and IT to ensure that employee data is encrypted and secure. Beyond basic hiring and benefits advocacy, HR policies dictate the manner in which employees can access work systems from home or from other locations, putting HR professionals directly in the critical path for employees to access data and the rules for viewing such information.

**Leveraging Amazon EKS in human resources and corporate security**

The company turned to containers and Kubernetes to accelerate innovation on its SaaS-based platform, running entirely on Amazon EKS. "With hundreds of services constantly being released and updated, Kubernetes allows us to scale and shape our environment to meet evolving customer demands," says Dan Certner, SVP and head of engineering at Namely.

Given the sensitive nature of the data on the Namely platform, security is a top priority for the company. Security requirements include:

- detecting and preventing non-compliant workloads
- tracking configuration baselines and drift
- monitoring compliance across all clusters, nodes, and containers
- detecting and preventing unauthorized access, privilege escalation, data exfiltration, lateral movement, and other runtime behavior anomalies

Namely

Namely is a cloud-based human resources, payroll, and benefits platform that helps modern HR teams make data-driven decisions about people and understand what's really going on in the workforce.

Headquarters: New York

Founded: 2012

Environment:
Kubernetes, Amazon EKS

www.namely.com

Namely

"After a little research, we discovered that only StackRox provides Kubernetes-native security, with enforcement directly in Kubernetes and insights we could get only by having the security tool pull in declarative data from Kubernetes."

– Dan Certner, SVP and head of engineering

"With this wide spectrum of security demands, I realized that how security ran in our infrastructure was crucial to our success," says Certner. "I started looking for tools that could deliver policy enforcement without adding third-party in-line proxying or blocking that might be more intrusive or oblique. We needed a model where controls reside in the infrastructure so we could keep moving toward security as code."

### Enter StackRox

"After a little research, we discovered that only StackRox provides Kubernetes-native security, with enforcement directly in Amazon EKS and insights we could get only by having the security tool pull in declarative data from Kubernetes," reports Certner. Namely is relying on StackRox to scan thousands of deployments to surface risky configuration details, detect which CVEs impact its images, and alert on any unapproved image details Namely has deemed unfit for production. "StackRox has provided advancements in visibility that let us make more informed decisions, keep up with our growing scale, and respond quickly to risky changes."

### Leveraging StackRox Capabilities

- **Vulnerability management** – StackRox scans and assesses vulnerabilities across Namely's images, containers, and running deployments.
- **Threat detection** – StackRox monitors, collects, and evaluates system-level events within each container in Namely's Kubernetes environment, quickly targeting suspicious activity.
- **Incident response** – Namely leverages StackRox to pinpoint suspicious runtime behavior and to continuously improve security.
- **Configuration management** – StackRox identifies misconfigurations across images, containers, and clusters, preventing accidental exposures.
- **Risk profiling** – StackRox uses Kubernetes deployment details to assess risk across the entire environment, enabling Namely to focus remediation efforts on its riskiest assets.
- **Real-time compliance management** – StackRox provides standard-specific checks across CIS Benchmarks, NIST, PCI, and HIPAA, with more than 300 controls and continuous compliance assessments.

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) 385-8329**
**www.stackrox.com**

©2020 StackRox, Inc. All rights reserved.