Cadent Modernizes Their Kubernetes Application Security with Deepfactor

Truly connecting with viewers across households, devices, and screens is no small challenge in today's fragmented TV landscape. Cadent is the largest independent platform for advanced TV advertising and monetization—where the best of data-driven linear and connected TV is at their customers' fingertips. Whether customers are trying to target specific viewers or reach new audiences, Cadent's solutions let them take on TV's toughest challenges to meet their greatest goals.

CADENT

CUSTOMER:
David Huang, VP Global Tech Operations

INDUSTRY:
TV Advertising

VIDEO:
https://www.youtube.com/watch?v=JGA5QEtsSlQ

// The Story behind Cadent's Digital Transformation

In order to maintain Cadent's reputation as an industry leader, David Huang, VP of Global Tech Operations, recognized an opportunity for application modernization to further improve the velocity and security of their releases.

> Reimagining applications in a cloud-native, microservices architecture would enable Cadent to address growing customer demand more quickly.

David also saw an opportunity to establish a proper DevSecOps pipeline to automate the integration of security at every phase of the software development lifecycle (SDLC), from initial design through integration, testing, staging, deployment, and delivery.

While leadership was supportive of the application modernization initiative, David wanted the team to really understand and appreciate the challenges facing the organization's definition of success—particularly the requirements around creating a next-generation DevSecOps pipeline.

"Our team is responsible for the entire SDLC, which means we need to analyze our code; review open-source compliance; check on third-party vulnerabilities, and ensure the service is both secure and performant," explained David. "And as we reviewed our current collection of security tools in the modernized setting, we realized we needed observability for our containerized workloads running in Kubernetes."

For more detail, the following table highlights some of the drivers and criteria behind Cadent's evaluation of their existing application security process:

Challenge	Requirement
Existing approach to AppSec was reactive, meaning many issues and risks were either missed or discovered late in the development process causing untimely delays.	With the move to cloud-native development and Kubernetes, Cadent required a DevSecOps pipeline that was proactive, Kubernetes-aware, and would enable developers to ship releases fast and secure.
Using their current tooling, developers were struggling to extract value from long—yet incomprehensive and disjointed—SAST reports which lacked visibility into application runtime. This blind spot extended to SCA and container image scans, where vulnerabilities weren't grouped and prioritized by applications.	Cadent required meaningful, end-to-end insights captured in runtime, with alerts that were prioritized and easy to triage on a per-application level. Cadent needed a tool that could be fully integrated into the CI/CD pipeline.
Without visibility into application behavior, AppSec was unable to define "Rules" and be informed of policy violations.	Cadent wanted to provide AppSec teams with high-level insights into the changes going into each release and the subsequent impact to the (expanding) attack surface.

// Why Cadent Chose DeepFactor

When evaluating available options for streamlining their DevSecOps pipeline, Cadent wanted a modern developer security platform that was ready to address the significant increase in supply chain, security, privacy, and compliance risks posed with the adoption of cloud-native development. More importantly, this product needed to be capable of providing developer security information for containerized workloads.

> "What makes Deepfactor interesting is its ability to observe our components early on in the development and build process—even before we perform the full regression scan going into production."
>
> —**DAVID HUANG**
> VP OF GLOBAL TECH OPERATIONS, CADENT

"We believe observing applications in runtime to analyze security risks is important for both containerized and monolith applications. And because we're in the process of modernizing, we're able to take advantage of the rich insights provided through Deepfactor's analysis of applications running in Kubernetes." David continued, "For example, many of our existing tools, such as our DAST scanners, are going to have issues looking into containers sitting behind the Kubernetes load balancer."

"What makes Deepfactor interesting is its ability to observe our components early on in development and build process—even before we perform the full regression scan going into production," shared David. "By integrating Deepfactor directly into our Jenkins Pipeline, we're hoping to identify changes to supply chain and security risks as early as possible. And with our AppSec tooling now running directly alongside the application in the container, Deepfactor should help our engineers prioritize vulnerabilities and issues in real-time."

// Cadent's Success with Deepfactor

During the Proof of Value—in which DeepFactor was successfully deployed and integrated into Cadent's Jenkins Pipeline—the DeepFactor team ensured that Cadent was able to quickly introduce developer security information into the software development lifecycle with a simple, easy-to-understand Kubernetes integration.

Once implemented, Deepfactor provided Cadent with instant and valuable information not available with their existing security tools: "Almost immediately, Deepfactor was able to show processes in our application running as root, which was obviously a behavior violation," recalled David. "We were able to remediate that problem before going into production. And since Deepfactor is observing individual services at runtime, our developers are given a much more refined view into the application's security posture. This refinement extends to both the SBOM and SCA reports."

Given the immediate impact Deepfactor is having on Cadent's application security strategy, David and his team are excited to see the engagement between the companies continue: "This entire process has been great. Whether over Zoom or Slack, Deepfactor engineering is always active, doing their best to answer questions as they come up. In terms of the product, [Deepfactor] engineering has been quick to push out updates, and we feel the product is rapidly maturing into something truly unique."

For those interested in Deepfactor after learning about Cadent's success story, consider getting started with the following resources:

- **Deepfactor Demo:** **Request a demo** so you can see how the Deepfactor developer security platform can help you team ensure secure code.

- **Deepfactor Brochure:** Review our **Brochure** for the latest information on the industry's first continuously observability platform for AppSec.

- **Deepfactor Webinar:** Consider attending a **Webinar**, where you can learn more about the product directly from our product and engineering teams!

{deepfactor}

Deepfactor is a developer security platform that enables engineering teams to quickly discover and resolve security vulnerabilities, supply chain risks, and compliance violations early in development and testing. For more information, follow Deepfactor on **Twitter** or **LinkedIn** or **contact us**.