

# Lemonade's Sweet Strategy for Runtime Application Protection



[lemonade.com](https://lemonade.com) ↗

Company size  
**1,001-5,000 employees**

Vertical  
**Insurance**

Environments (cloud)



Key need  
**Enhance cloud vulnerability management with accurate alerts**

Cloud Security unlocked  
**0.04% false positive rate**

## About Lemonade

Lemonade offers renters' insurance, homeowners' insurance, car insurance, pet insurance, and term life insurance in the United States and Europe. It has harnessed advanced AI technology to revolutionize the insurance experience.

From AI-driven chatbots that streamline policy issuance to a fully digital, cloud-native platform, Lemonade offers customers a delightful interface that traditional insurers struggle to match. Lemonade's proactive stance on cybersecurity enhances its reputation as a trusted insurer in the digital age.

## The Challenge - Understanding Active Vulnerabilities

Lemonade, a full-stack insurance carrier built to provide the best, most delightful, and most transparent insurance experience in the world, has integrated Sweet's cloud application security solution to bolster its runtime security defenses. Since 2020, [Jonathan Jaffe](#), Chief Information Security Officer at Lemonade, has implemented advanced security strategies at Lemonade, and has been pivotal in ensuring Lemonade's cloud-native technology stack remains protected and secured.

Prior to Sweet, Lemonade's security team faced a burdensome challenge as it worked through large numbers of security alerts in its expansive cloud environment. Amidst the noise, Lemonade spent more effort than it wanted to separating exploitable vulnerabilities from theoretical ones. Once the exploitable vulnerabilities were panned, the security team still had to identify which had fixes. All of this had to be done to allow Lemonade to prioritize which vulnerabilities to fix. The effort involved in this process was significant.

Despite the importance, Lemonade had trouble identifying an effective runtime solution to streamline this process. The security team did not want to add multiple additional tools to its security stack, but rather include an encompassing cloud solution that could identify multiple runtime gaps at once.

## From Managing Vulnerabilities to Managing Risks

Upon integrating with Sweet, Lemonade further improved its ability to manage vulnerabilities by focusing on exploitable runtime risks. Jaffe emphasizes **“Sweet provides awareness of package vulnerabilities that are exploitable in a much more useful way than a lot of other products do. It narrows down exploits to what can actually be exploitable.”**

Identifying and prioritizing exploitable—and fixable—vulnerabilities helps Lemonade avoid bombardment by irrelevant alerts. This precision enhances security effectiveness, and strengthens collaboration with the development team, by presenting actionable insights rather than overwhelming team members with non-critical issues.



**Prioritize vulnerabilities**



**Reduce white noise**

## 100% Visibility into Lemonade’s Cloud Applications

In addition to leveraging runtime insights to manage vulnerabilities, Sweet addressed gaps in Kubernetes security, offering important capabilities in detection and response generally not available in standard Kubernetes deployments. Jonathan Jaffe notes **“Sweet fills typical Kubernetes security gaps. Few, if any products out there, provide reliable Kubernetes detection and response.”**

Sweet extends its functionality beyond detection and response to include other areas such as non-human identities management and providing a comprehensive graphical views of Lemonade's environment topology. This visibility is helpful to Lemonade's DevOps team, offering insights into resource relationships and aiding in task prioritization. **“It’s the first time we’ve been able to point to graphs that show where resources are in relation to other resources. That helps us understand the context of a problem and how to prioritize what to work on.”**



**Detection & response for kubernetes**



**Non-human identities management**



**Topology view of entire environment**

## Real-time Detection and Response of Sophisticated Attacks

With Sweet, Lemonade is able to maintain robust protection against advanced threats that could circumvent other defensive layers. **“Having something at runtime is yet another layer of defense above other standard defenses such as network defenses and protocol defense.”**

An example of an advanced threat is code injection. This occurs when malicious code is inserted into a dependency or a component of the application. Despite best efforts in securing coding and vulnerability management, dependencies can be compromised or inadvertently introduce vulnerabilities. Sweet Security monitors the execution of code at runtime and can detect whether there's an attempt to inject malicious code into the application's codebase.

## The Future of Lemonade is Sweet

As with most companies, security is a priority at Lemonade. Sweet Security helps Lemonade remain at the forefront of digital innovation in the insurance industry.