sysdig | APREE HEALTH

CUSTOMER STORY

# Apree Health Partners with Sysdig to Gain Container Visibility and Meet Compliance

Everyone deserves to live their healthiest life, but many people aren't given the opportunity to do so.

Apree Health seeks to change that. By combining advanced primary care with best-in-class digital engagement, they strive to tear down the health industry's data silos. To that end, they've developed a suite of platforms and solutions to reduce benefits complexity; support deeper personalization; and help patients achieve better, more affordable outcomes.

Accessible via both web and mobile, Apree Health's software is also compatible with wearable devices. Focused as much on prevention as treatment, the company has incorporated gamification into its software to encourage people to seek care.

apree health

**INDUSTRY**

Software Technology

**CHALLENGES**

- Meet SOC 2 and HITRUST compliance and provide clear evidence to auditors
- Lack of visibility into containerized environments
- Inefficient, ineffective, and unintuitive existing tooling

**OUTCOMES**

- Ability to achieve, maintain, and prove compliance without sacrificing agility
- 80% reduced time to remediation
- >10 hours per month saved on security and compliance

CHALLENGES

## Kubernetes, Compliance, and Data Security

Built atop custom, self-managed Kubernetes deployment, Apree Health's platform consists of roughly 150 nodes across 10 environments. The company provisioned and configured its heavily customized infrastructure through a combination of Chef and Terraform, leveraging Google Chronicle for security information and event management (SIEM).

Originally hosted across multiple data centers, this complex system required considerable time and effort to manage and monitor. When the company migrated to Google Cloud before an impending Health Information Trust Alliance (HITRUST) audit, Apree Health Senior Manager of Information Security David Quisenberry saw a chance for improvement.

"There's nothing like compliance to help write a check for things you've wanted for a while," said Quisenberry. "This was the perfect opportunity to get the tools we needed to do our jobs better."

The HITRUST Common Security Framework certification encapsulates the high standards of security and data integrity to which health care vendors must adhere. Apree Health has been HITRUST-compliant for nearly five years. They also adhere to Service Organization Control (SOC) Type 2, a voluntary framework focused on the secure management of customer data.

"We go through a full HITRUST audit every other year," Quisenberry said. "In the off year, HITRUST chooses a random selection of controls to drill into. Our most recent full audit was last year, scheduled to occur shortly after undergoing a number of changes in our environment."

Because many of Apree Health's controls and systems were either server- or virtual machine-driven, they identified a number of potential compliance issues related to file integrity monitoring, system baselines, and configuration scanning.

"We needed a more efficient and effective way to not only meet our compliance requirements, but also gather and present evidence to auditors," Quisenberry said. "We also knew as a security team that we had a lot of gaps in incident response and container monitoring. Because we didn't have a lot of time or engineering bandwidth, it wasn't feasible to build our own solution – we needed everything available out of the box."

> "Sysdig is very good at container and cloud security using runtime insights. Their platform does everything we need it to do, and their support team is phenomenal. It's a big differentiator."
>
> **David Quisenberry**
> Senior Manager of Information Security
> at Apree Health

SOLUTIONS

## Conquering a Time Crunch and Cost

With the impending audit, Apree Health was operating on an incredibly tight timeline. Although they briefly evaluated other solutions, they ultimately chose to do a proof of value with **Sysdig** making the decision to deploy the platform shortly thereafter. With help from Sysdig Customer Success, the two companies working together completed the entire rollout – including a compliance review – in under two months.

"We didn't have a large budget, nor did we have a great deal of time," Quisenberry said. "After assessing the Sysdig platform, we concluded that it did everything we needed. We also had confidence that with Sysdig's support, we could get it implemented and operational in time, and they proved us right."

Through powerful runtime insights, Sysdig empowered Apree Health to identify, visualize, and eliminate Kubernetes vulnerabilities, threats, and misconfigurations in real time. Automated evidence gathering and reporting, coupled with out-of-the-box policies for both SOC 2 and HITRUST, ensured that Apree Health was ready for its audit shortly after deployment.

> "Sysdig's continuous scanning and automated evidence gathering save our security operations team a ton of time. It also gives us a cleaner way of collecting and conveying evidence to auditors."
>
> **David Quisenberry**
> Senior Manager of Information Security at Apree Health

## Seamless Integration with Google

Core functionality aside, one of Sysdig's primary selling points for Apree Health was its seamless integration with Google Chronicle. All the company had to do was provide API key information. Out-of-the-box rules for file integrity monitoring also proved immensely beneficial.

"We're primarily a Google shop," Quisenberry said. "One of the things we really liked was how quick we were able to tie Sysdig into Chronicle. The integration was very clean and painless."

## Unprecedented Visibility, Efficiency, and Control

Sysdig provides Apree Health with deep visibility into its Kubernetes deployment through a single, unified view. This, along with its vulnerability and misconfiguration scanning, has been invaluable to the company's compliance efforts. It's also made things significantly easier for Apree Health's security operations team when it comes to risk, threat, and vulnerability management.

"Sysdig has helped automate what would otherwise be a mountain of manual work," Quisenberry said. "We can now not only see our entire Kubernetes environment, but also take more immediate action to address problems or threats. The ability to automatically create Jira tickets based on CIS [Center for Internet Security] benchmarks has been particularly helpful in managing and documenting risk."

SOLUTIONS

## Easier Audits, Streamlined Security

"In preparation for our audit, we knew that we wanted to capture all audit records in our SIEM and build more robust incident response capabilities," Quisenberry said. "Sysdig's continuous scanning and automated evidence gathering saves us a ton of time where that's concerned. It also gives us a cleaner way of collecting and conveying evidence to auditors."

This ultimately translates to considerably simpler audits with fewer mandatory reviews. Sysdig's intuitive visualization and reporting tools makes third-party security and compliance assessments far simpler.

"Transparency in the industry is a good thing – we shouldn't be afraid to show people where the food's made," Quisenberry said. "We should be the equivalent of a high-end restaurant where you can go back in the kitchen and everything is spotless. With Sysdig, we can show evidence that we're doing things properly."

## Exceptional One-on-One Support

"Sysdig's support team has been excellent – responsive, helpful, and knowledgeable, especially over Slack," said Quisenberry. "The fact that we've had the same support representative since the beginning really makes it feel like we're getting white glove service."

Although there were some hiccups over the complexity of Apree Health's Kubernetes deployment, Quisenberry and his team were more than satisfied with how Sysdig addressed these challenges.

"Sysdig has consistently taken immediate action to help address any issues we encounter," said Donovan Ellison, Cloud Security Engineer at Apree Health. "Since the completion of deployment, their solution has worked out of the box."

> "Sysdig's support team has been excellent — responsive, helpful, and knowledgeable, especially over Slack. The fact that we always have the same support representative really makes it feel like we're getting white glove service."
>
> **David Quisenberry**
> Senior Manager of Information Security
> at Apree Health

## Planning for the Future

Looking towards the future, Apree Health's security operations team seeks to fulfill three primary initiatives.

The first is to continue building out and optimizing their security stack for more robust threat management and incident response. Second, they want to invest in the training and growth of their employees. Finally, they want to leverage Google BeyondCorp to transition to a zero-trust security framework.

Sysdig is helping them pursue all three.

"When evaluating products, you really want to distill down to what the vendor is good at," Quisenberry said. "Sysdig is very good at container and cloud security using runtime insights. Their platform does everything we need it to do, and their support team is phenomenal – it's been great working with them."

To learn more about Apree Health, visit **apreehealth.com**.

apree health

**INDUSTRY**

Health Care/Software Technology

**INFRASTRUCTURE**

Google Cloud

**ORCHESTRATION**

Kubernetes (Self-Managed)

**SOLUTION**

Sysdig Secure

## About Sysdig

In the cloud, every second counts. Attacks move at warp speed, and security teams must protect the business without slowing it down. Sysdig stops cloud attacks in real time, instantly detecting changes in risk with runtime insights and open source Falco. We correlate signals across cloud workloads, identities, and services to uncover hidden attack paths and prioritize real risk. From prevention to defense, Sysdig helps enterprises focus on what matters: innovation.

Sysdig. Secure Every Second.

To learn more about Sysdig, visit **sysdig.com.**

REQUEST DEMO →