CASE STUDY

HealthVerity Cures Critical Alerts with Clear Diagnosis

HealthVerity provides the nation's largest healthcare and consumer data ecosystem, where healthcare providers, payers, and programs can discover, license, and link healthcare data.

HealthVerity was founded in 2014 because healthcare organizations needed a reliable HIPAA-compliant platform where they could analyze disparate datasets to reveal insights and answers. But, quickly, the vision of HealthVerity grew from providing data interoperability to establishing a comprehensive data platform. Today, the HealthVerity platform helps organizations manage, match, and track healthcare and consumer data in one place to understand patient journeys and uncover new insights.

The HealthVerity platform includes HealthVerity Census, which de-identifies patient data by replacing personally identifiable information (PII) with a HealthVerity ID. This ID then becomes the key to securely linking a patient's journey across disparate and fragmented datasets. With this layer of identity security in place, HealthVerity can allow its clients to use Java applications or APIs to analyze more than 150 billion healthcare and consumer transactions covering 330 million U.S. patients.

HealthVerity now partners with leading pharmaceutical manufacturers, hospitals, payers, and government agencies. The HealthVerity platform has become the standard for rapidly storing, exchanging, managing, and analyzing healthcare and consumer data to achieve deeper insights in compliance with strict privacy regulations.

Challenges

Every business wants to target a critical customer need. HealthVerity found one and built a platform around it.

The need was so great, in fact, that the company's platform quickly grew from a simple infrastructure with five cloud accounts to a microservices model with hundreds of cloud accounts. The move to cloud-based microservices allowed developers to build quickly and scale up fast. However, Jim Shank, VP of engineering security at HealthVerity, needed to make sure that these new builds were keeping customer data protected.

As a cybersecurity veteran, Jim knew that healthcare data is a constant target for cyberattacks. And he knew that, in healthcare, client trust is hard to win but easy to lose. "For us, security is a daily exercise," Shank says. "It's a continual journey, and it's an effort to secure and maintain the confidence of our customers."

Using cloud service provider (CSP) security tools, HealthVerity ran NIST 853 reports that indicated its systems were compliant, but Shank's team wanted deeper insight. The team began to manually inspect accounts that were being created and saw that there were hidden issues. But, as the number of accounts continued to grow,

"As the company scales and grows, we can put our attention into using the Lacework FortiCNAPP platform for new products or services. We don't have to give much attention to existing services. We're just using the platform to monitor and manage those to make sure that they don't go in the wrong direction."

Jim Shank
VP of Engineering Security, HealthVerity

Details

Customer: HealthVerity

Industry: Healthcare

Location: Philadelphia, PA

Business Impacts

- Enabled security and development to scale together during rapid growth
- Reduced hundreds of critical alerts in the first month to 22 per week, then to 0
- Empowered developers to write secure infrastructure code by shifting security left

the team knew these manual efforts weren't scalable, and that these "hidden issues" were being exacerbated. They needed a way to quickly, consistently, and proactively find and fix both new and existing cloud security issues.

For Shank's team, the need moved beyond simple compliance. He knew that the company shifted to microservices to accelerate development and innovation. And he knew that security could not be perceived as a roadblock to those goals. The security team wanted to monitor the system against Center for Internet Security (CIS) benchmarks, find and prioritize issues in real-time, efficiently ticket their resolutions, and identify actions to prevent similar issues in the future. The team also needed automation to help scale its responses as the company continued to grow.

Solution

Back to the basics

Shank knew that compliance is table stakes for any company but especially for those in regulated industries like healthcare. The Health Insurance Portability and Accountability Act (HIPAA) is the law of the land, and any company looking to survive in the industry has to follow that law to the tee.

However, Shank also knew that CSP security tools alone weren't going to do the job for his growing company. "We wanted to get some more automation behind understanding when our cloud services were not properly configured. And we were really interested in prioritizing those issues."

Business Impacts (cont.)

- Gained continuous visibility into security posture, with

Solution

- Lacework FortiCNAPP

"We wanted to get some more automation behind understanding when our cloud services were not properly configured. And we were really interested in prioritizing those issues."

Jim Shank
VP of Engineering Security, HealthVerity

While surveying a crowded vendor landscape, HealthVerity quickly identified Lacework FortiCNAPP as the solution that could help them maintain compliance excellence at limitless scale.

"We saw that Lacework FortiCNAPP is very well adapted and configured to support our mission of identifying non-compliant cloud resources," Shank says. "That makes it very easy for you to gain insights into what resources are misconfigured and what actions need to be taken to remediate those issues—that was the primary motivator for getting the product, initially."

From a compliance perspective, Shank knew that the Lacework FortiCNAPP platform would allow Shank's team to continuously and automatically assess its environment against a large number of pre-set regulatory guidelines like HIPAA and industry standards like CIS. The security team could also easily create custom policies unique to HealthVerity.

After onboarding the platform, Shank's team realized that identification was only half the battle. To ensure that HealthVerity developers were using their time as efficiently as possible, the security team needed a way to prioritize their highest-priority issues.

Issue identification, done. Now, they needed to know where to look first.

First things first

Shank needed a way to discern which vulnerabilities and misconfigurations were most pressing. He needed a way to seamlessly communicate these needs to developers. And ultimately, he needed dev teams within HealthVerity to know that his security team was doing everything possible to ensure developers weren't wasting their precious time on meaningless issues.

Lacework FortiCNAPP offered a way to prioritize alerts, manage the alert lifecycle, and seamlessly collaborate on alerts across teams and tools. This empowered his team to turn the rush of emergencies into clear, targeted diagnoses for developers.

The platform offered Shank's team a number of features to help with alert prioritization. For example, its custom risk score highlights your most critical issues by scoring vulnerability risk in the context of your own environment—like determining whether the issue is actively running in production. Shank's team could also benefit from the platform's identity management capabilities, which, like the custom risk scoring, highlight overly permissive identities based on the context of their unique cloud environment.

"The Lacework FortiCNAPP platform identifies issues by severity," Shank says. "It was very easy for us to make sure we were working with the right teams to remediate the findings it identified. When you look at the scale and the numbers we handled, you're giving back a lot of time to the analysts and engineers by having that automation configured and enabled."

Once they identified its biggest issues, HealthVerity took advantage of the platform's bi-directional integration with Atlassian Jira. With one click, Shank's team could ship security alerts directly into existing developer workflows. These Jira tickets automatically included details about the issues and identified the development teams that needed to address them. Any communications or updates made within the Jira ticket were reflected in the Lacework FortiCNAPP platform and vice-versa.

"For each of those environments, we loaded information from the tool into our ticketing system, and that combined the powers of those tools and what they can do to track issues to remediation," Shank says. With Lacework FortiCNAPP data flowing into the ticketing system, the company used the systems in tandem to drive down misconfiguration events and issues over time.

Treat the sickness

As HealthVerity identified misconfigured accounts, it used the combination of Lacework FortiCNAPP and Jira ticketing to find and resolve root issues in their Infrastructure-as-Code (IaC) templates. Some services were configured and deployed incorrectly from the start, which caused exponentially more issues as the environment scaled.

The Lacework FortiCNAPP platform quickly identified these issues and provided rich context on what made them important. Each security alert explains, in detail, what it is, when it was triggered, why it matters, and how to fix it. Developers can then use this context to quickly find a resolution.

"Lacework FortiCNAPP helps us provide detailed information on account configurations as we walk through the path to triage and resolution," notes Sixtus Ajab, security analyst for HealthVerity. "If we find a vulnerability that was a result of account misconfiguration, we can fix the root issue. That means we will not see that vulnerability anymore as new resources are added to the environment."

When it comes to its cloud vulnerabilities—as the adage goes—HealthVerity was able to treat the sickness rather than just the symptoms. And because it did, their its overall alerts decreased over time.

Respect the dev experience

HealthVerity had moved to microservices to speed up its code development. A traditional security gate before each release would have worked against company goals, so the security team needed ways to integrate within existing developer workflows and toolchains.

Shank's team went to work. They used the Lacework FortiCNAPP platform to make intersections with the development team more efficient. As new alerts came in, Shank's team of security analysts began confirming each ticket's platform-assigned priority. Then, without leaving the platform, the security team would seamlessly connect each validated alert to a Jira ticket, along with notes from the investigation, findings, and recommendations.

HealthVerity developers also began taking advantage of the platform's IaC security capability. This way, developers could learn of errors in their infrastructure code while writing it without slowing down or leaving their workflows. Since many of HealthVerity's misconfigurations were rooted in insecure IaC templates, this process change substantially reduced the number of alerts coming into their environments.

"Now, we don't spend as much time remediating or resolving issues," Shank says. "Today, for all of the production, staging, and even most of the dev accounts, our cloud security posture and hygiene are well-managed. The platform has helped us be more efficient and more diligent about deploying security services, shifting left to build in cybersecurity earlier. That's been very good for our organization."

Results

A cure for alerts

The team saw hundreds of critical and high-severity alerts in the first month that HealthVerity onboarded Lacework FortiCNAPP. It was a state of emergency. The security team worked with the development team, using data and analysis from the platform to diagnose and resolve the top issues.

The alerts tapered off, but the platform still identified a sizable number of critical, high, and medium severity alerts per week

over the first four months. HealthVerity realized many of these issues were tied to errors within IaC templates. As the security team prioritized these fixes, the weekly average dropped by 60% and included zero critical alerts.

The reduction in alerts has reinforced Shank's confidence in his company's cloud security posture. "One mistake, and we could lose a lot of customers," Shank says. "We rely on the Lacework FortiCNAPP platform to give us the feedback that we need to ensure that we're doing the right things to maintain each customer's confidence and the security posture they expect us to have."

Fast and secure

Speed drove Shank to search around for a new cloud security solution. His team needed to keep pace with HealthVerity's development teams, and their incumbent tool wasn't doing the job. Now, with the Lacework FortiCNAPP platform, speed is a benefit that both development and security teams within HealthVerity can enjoy.

According to Ajab, the biggest advantage of the Lacework FortiCNAPP platform for the security team is its speed. "From my perspective, the most important benefit is providing me with real-time information as events occur. As we are speaking, if there is any anomalous activity in our security environment, especially with a cloud account, the platform will notify me with a ticket. Then, I can be more proactive in taking action sooner."

On the other side, HealthVerity developer teams can build infrastructure quickly, knowing that their code is secure from the beginning. "We got the platform team to change their behaviors," Shank says. "They know to check the platform before they even deploy. Now, they're using the tool that allows them to shift left to make sure their accounts are secure."

A single source of truth

The Lacework FortiCNAPP platform allows HealthVerity's team to measure overall security health over time as their cloud footprint grows. The team can also seamlessly report these findings to interested parties, such as executives or their board of directors.

"From a management perspective, what I need out of the tool is near-real-time feedback on our security posture," Shank says. "Is it getting better? Is it getting worse? How is it changing, if it is changing? To me, the near-real-time feedback on the security posture of the accounts and systems that you load in is the number-one benefit of all."

The Lacework FortiCNAPP platform helped the HealthVerity security team get a handle on their immediate compliance needs within their AWS environment. But the platform has also prepared HealthVerity for its future compliance needs. As a company grows, it typically expands beyond a single cloud provider. Lacework FortiCNAPP enables HealthVerity to assess its compliance across multiple clouds from a single location.

Vision for the future

Jim Shank's security team within HealthVerity has become an operationally efficient powerhouse, thanks in part to the Lacework FortiCNAPP platform. It continuously monitors the company's overall security posture, has significantly reduced overall alerts, secured the company's cloud infrastructure, and effectively turned developers into security team members.

"As the company scales and grows, we can put our attention into leveraging the Lacework FortiCNAPP platform for new products or services," Shank says. "We don't have to spend as much time supporting existing services. The platform is monitoring and managing those to make sure that they don't go in the wrong direction."

When the security team can spend its time on more advanced work, that means better security for HealthVerity and a better foundation for the company's growing vision.

Schedule a demo today

September 26, 2024 10:52 PM / 2893720-0-0-EN