Geisinger

Geisinger Expands CrowdStrike Usage to Protect AWS Cloud Workloads

Since 2017, Geisinger Health System has used CrowdStrike to protect its on-premises electronic health record (EHR) software.

As one of America's most innovative health systems, Geisinger decided in 2021 to migrate its EHR to Amazon Web Services (AWS). It expects this migration to the cloud will enable life-saving technologies while saving millions of dollars each year.

But this is no small feat. Some 400 applications and numerous workflows need to be migrated to AWS. Critically, those applications need to be protected, as does the sensitive data contained within them.

Geisinger was familiar with the shared responsibility model: while AWS was responsible for security of the cloud, Geisinger was responsible for security in the cloud. That's when Geisinger turned again to CrowdStrike.

Protection from PCs to Pods

CrowdStrike provides Geisinger with a cybersecurity platform that protects endpoints to cloud workloads, and everything in between.

Core to the solution is CrowdStrike Falcon® Cloud Security, which includes cloud workload protection and cloud security posture management.

"All the benefits of migrating our EHR to the cloud means nothing if it's not protected," said Geisinger CISO Zack Gable. "CrowdStrike helps protect us from PCs to pods."

The Geisinger security team's emphasis on cloud security reflects the changing IT landscape. While the cloud brings numerous benefits around cost, scale and flexibility, it also introduces new security risks. A breach can disrupt the entire health system's daily operations.

Geisinger chose the CrowdStrike Falcon® platform to protect its on-premises infrastructure, and CrowdStrike Falcon® Complete Cloud Security to do the same for its cloud systems.

Falcon Complete Cloud Security is CrowdStrike's fully managed detection and response service for cloud workloads. The managed service is backed by CrowdStrike's industry-leading Breach Prevention Warranty, which covers costs should a breach occur within the protected environment. (No customer has ever made a claim against the warranty.)

INDUSTRY

Healthcare

LOCATION/HQ

Pennsylvania, USA

CHALLENGES

- Geisinger needed cloud workload protection to secure its AWS workloads
- It wanted everything to be simple, streamlined and comprehensive
- And to complement its existing on-premises infrastructure protections

SOLUTION

With CrowdStrike, Geisinger gets an end-to-end security platform — along with human expertise — to protect its endpoints, cloud workloads and everything in between.

> "CrowdStrike gave us the flexibility to quickly move from protecting our PCs to AWS pods at the click of a button, and with the same platform we know and trust."
>
> –Zack Gable, Geisinger CISO

The Obvious Choice for Cloud Workload Protection

Cloud migrations of this scale are fraught with complexity. Geisinger wanted a simple solution for cloud protection and it got that with CrowdStrike.

Because the health system was already using the Falcon platform for endpoint protection, adding the sensor for cloud workload protection was as simple as licensing the module. Deployment was streamlined compared to most implementations. Cost and complexity were lower as well.

"A lot of companies offer a cloud-based sensor product, but because we were already a CrowdStrike customer, adding cloud workload protection was streamlined," said Gable.

This unified approach to security made sense to Gable. Because of CrowdStrike's single-agent architecture, Geisinger can deploy cloud workload protection and continue using the same management console to monitor everything, from PCs to servers to Kubernetes pods. No managing multiple systems — just one platform to secure its entire infrastructure.

"CrowdStrike gave us the flexibility to quickly move from protecting our PCs to AWS pods at the click of a button, and with the same platform we know and trust," said Gable.

Keeping the Focus on the Patient

The CrowdStrike and AWS partnership gives joint customers like Geisinger a streamlined approach to cloud workload protection.

As an AWS Security Competency Partner and AWS Global Public Sector Partner of the Year, CrowdStrike offers more than 12 integrations with AWS core services, including Guard Duty, Security Hub and Control Tower, to ensure the most hardened cloud environment possible.

CrowdStrike is trusted by more than 100 healthcare organizations worldwide for endpoint and cloud protection.

"CrowdStrike has enabled us to continue driving our secure cloud journey so we can focus on providing the best patient care possible," concluded Gable.

RESULTS

One security platform for protecting its entire infrastructure

Cloud security deployed in minutes, not weeks

Zero training costs or security gaps

CROWDSTRIKE OFFERINGS

- Falcon® Complete Falcon Security
- Falcon® Cloud Security with Containers
- Falcon® Prevent next-generation antivirus
- Falcon® Insight endpoint detection and response
- Falcon OverWatch™ managed threat hunting
- Falcon® Discover IT hygiene
- Falcon® Intelligence

ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data. Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

CrowdStrike: **We stop breaches.**

Follow us: **Blog** | **Twitter** | **LinkedIn** | **Facebook** | **Instagram**

Start Free Trial

Learn more **www.crowdstrike.com**