MDfit increases security visibility for its serverless infrastructure using Stealthwatch Cloud on Amazon Web Services

The customer summary

Customer name
MDfit

Industry
Healthcare

Location
Pittsburgh, Pennsylvania

About MDfit

MDfit is a software platform that enhances healthcare provider communication and delivers accurate data to find the right provider at the right time. The platform supports data provider management, secure communications, referrals, and scheduling functionality presented according to providers' preferred contact methods, clinical expertise, and locations.

By connecting the right resources to the right patient in a secure environment, MDfit helps healthcare organizations strengthen the patient-clinician connection, promoting greater patient satisfaction, loyalty, and quality of care.

Adopting the serverless model to accelerate customer outcomes

MDfit platform infrastructure, both production as well as development, is deployed entirely on Amazon Web Services (AWS) and all the operations and security are managed by a small team. The platform has typically utilized a traditional web-app-database infrastructure model. Over the last 18 months, however the MDfit platform has been enhanced to utilize the serverless framework, making use of AWS services including AWS Lambda, Amazon DynamoDB and Amazon API Gateway. As the platform transitioned from a more traditional server-based infrastructure to a serverless framework, the MDfit team was able to increase the speed of development through faster code reviews and deployment. In fact, they broke some of the code into more discrete chunks and eliminated the need to write code from scratch for various capabilities that are now delivered by the AWS serverless platform. In addition to the increase in speed, the adoption of these new technologies provides significant scale and security advantages. However, it can be a challenge to monitor the environment via traditional, mostly agent based, security solutions.

Addressing security concerns around dynamic environments and sensitive healthcare data

Under the HIPAA regulations, cloud services providers (CSPs) such as AWS are considered business associates. The Business Associate Addendum (BAA) is an AWS contract required under HIPAA regulations to ensure that AWS appropriately safeguards protected health information (PHI). With MDfit serving customers in the healthcare industry and handling a large amount of sensitive data, being able to prove that their platform is meeting the security and compliance requirements is the baseline for every new technology and feature.

From an architecture standpoint MDfit decided to utilize technologies configured in accordance with the guidance in the "Architecting for HIPAA Security and Compliance on Amazon Web Services" whitepaper. This guidance includes prescriptions for ensuring that data is encrypted in transit and at rest, that adequate audit logging is being performed, and that backup and disaster recovery plans are in place. This AWS guidance represents security best practices regardless of the regulated status. By adopting it across the platform MDfit ensures that all data, including ePHI, is adequately protected.

> "If we treat everything as sensitive, we know we aren't going to make any mistakes."
>
> **Sean O'Brien**
> Chief Operating Officer, MDFit

Detecting anomalies through continuous monitoring

Since the healthcare sector continues to be a significant target for malicious actors; the security of the MDfit platform is critical to developing and maintaining customers' trust. It is extremely important to be able to continuously monitor for anomalous activity which could indicate a security threat.

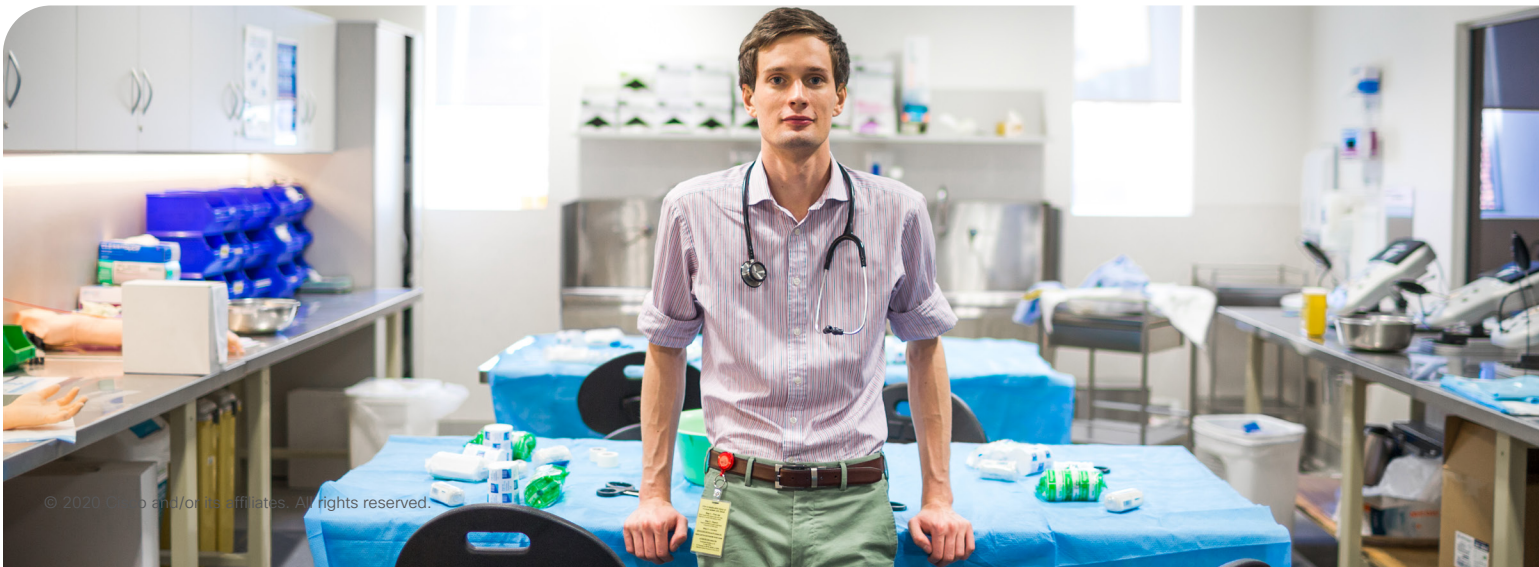
Thus, MDfit needed to enhance the ability of a small team to monitor the significant security log volumes generated by the AWS services in the platform. Stealthwatch Cloud, an agentless security solution, helped them address their current and prospective customers' concerns about data protection in a heavily regulated industry.

Achieving business outcomes and providing customer value

MDfit evaluated several security solutions and chose Cisco Stealthwatch Cloud, a SaaS-delivered behavioral threat detection tool. Using Stealthwatch Cloud, MDfit is able to get complete visibility into their AWS environment by ingesting Amazon VPC Flow Logs and CloudTrail logs. Additionally, this solution is agentless and doesn't require deploying any agents or sensors.

"By changing our security provider we saved approximately 50% in our monitoring costs and we get better visibility. We are basically paying less and getting more"

Sean O'Brien
Chief Operating Officer, MDFit



These benefits ultimately allowed MDfit to achieve the following business outcomes:

Speed of innovation:

- MDfit continuously adds new services and features to their platform to enhance customer value. Implementing Stealthwatch Cloud gave them additional ability to monitor Amazon VPC flow logs and to see functions spinning up and talking to the databases and elastic search clusters, thus maintaining a high level of assurance for existing and new services.

Reduced operational costs

- Since the change in security provider MDfit has saved approximately 50% in monitoring costs while getting better visibility and more flexibility when using AWS native tools.

Time savings

- Stealthwatch Cloud was installed in just two hours and now requires approximately 50% less maintenance, allowing the small IT team to focus time and resources on serving customer needs.

Employee productivity

- The implementation of Stealthwatch Cloud provided MDfit with high-fidelity actionable alerts that ultimately increase employee productivity by saving several hours per week of staff time.

Risk mitigation and assurance

- With Stealthwatch Cloud near real time visibility into traffic flows, as well as with Amazon API Gateway calls (AWS CloudTrail) MDfit can quickly identify changes in activity and traffic patterns when infrastructure or code changes are made.

Next Steps

To learn more about Stealthwatch Cloud on AWS, visit our webpage, on-demand webinar, and get started with a 60-day free trial from AWS Marketplace.

"The ability to continuously monitor native Amazon logging as well as the VPC flow logs was one of the capabilities that was really compelling and unique of Stealthwatch Cloud"

Sean O'Brien
Chief Operating Officer, MDFit

2076534 04/20