deepwatch

CUSTOMER SUCCESS STORY

Deepwatch Secures Code in AWS environment for Insurance SaaS Provider

Deepwatch AWS Level 1 MSSP with Modern Compute Security Specialty

CUSTOMER

One of the largest and most trusted SaaS providers to the insurance industry, this company delivers solutions that improve processing, enhance customer experiences and empower the use of data for insurers.

CHALLENGE

As a SaaS provider, this company hosts proprietary code, code that if corrupted could inflict significant financial cost and loss of reputation. Their hybrid cloud model includes AWS development in a siloed division. A migration to container deployment by th AWS-focused team required more resources than expected including new compute and storage fees. As budgets got tighter, the volume of alerts only increased. The company's top 3 threats included ransomware, source code corruption and availability of business systems.

SOLUTION

Deepwatch, an AWS Level 1 MSSP with the Modern Compute Security specialty, offers a comprehensive security solution including monitoring of AWS container environments by integrating with and leveraging data from AWS Guard Duty. This gave the team a dedicated squad of resources with AWS container security knowledge, allowing them to accelerate adoption of a containerized approach.

Deepwatch was able to continuously monitor cluster activity to identify malicious or suspicious behavior that represents potential threats to container workloads. Threats detected included clusters accessed by known malicious actors or Tor nodes, API operations performed by anonymous users, and privilege-escalation techniques such as launch of a container with root-level access on the Amazon Elastic Kubernetes Service (Amazon EKS) clusters This ensured that any compromise of the the source code deployed is detected fast and remediated.

Deepwatch was able to bring additional AWS-focused resources to the organization without increasing headcount, faster and for less money than building capabilities in-house while ensuring availability of the business systems.

ENTERPRISE DETAILS

Headquarters: Hartford, CT

Industry: Saas Platform Provider

Employees: 400

Customer Since: January 2020

Security Team: 5

Deepwatch was able to bring additional AWS-focused resources to the organization without increasing headcount

OUTCOME

Availability of business systems through 24x7x365 monitoring, threat detection and remediation capabilities for the entire IT environment from on-prem to AWS containers. Deepwatch squad served as a true extension of the security team to deliver complete protection for AWS container services including Amazon Elastic Container Service (Amazon ECS) and Amazon Elastic Kubernetes Service (Amazon EKS).

Significant cost avoidance or ROI realization is made possible when partnering with Deepwatch. As teams mature into more complex solutions such as containers, the speed of development must face the velocity of oncoming threats. When combined with AWS Marketplace incentives such as EDP, outsourced security services can be more cost effective than building more capacity in house.

Ransomware protection. Using Deepwatch threat analytics, the company now correlates telemetry data from multiple security tools to detect any unauthorized access or code in the environment.Mitigating the impact of such threats can deliver better ransomware protection.

deepwatch™

ABOUT DEEPWATCH

Deepwatch delivers data-driven managed security services while extending customers' cybersecurity teams and proactively advancing their SecOps maturity. Powered by our innovative cloud-native platform, Deepwatch is trusted by leading global organizations to provide 24/7/365 managed security services.

CONTACT US

GET STARTED

4030 W Boy Scout Blvd. Suite 550
Tampa, FL 33607

www.deepwatch.com