



Pivvot Secures Dynamic DevOps Environment

Company Name

Pivvot

Website

www.pivvot.com

Region

United States

Industry

IT, Engineering, Oil and Gas

Employees

26

Partner

AWS Partner Network (APN)

Competitor Displaced

N/A

Products

- Deep Security Smart Check

IT Environment

- AWS
- ECS
- Docker



“We’re able to protect a container pre-runtime by understanding what’s going on in the environment from a security perspective before it even hits production.”

Jason Cradit

Sr. Director, Information & Technology, Pivvot

CUSTOMER

Pivvot is a software company that delivers cloud-based intelligent asset management systems to infrastructure organizations in industries such as oil and gas, power, and transport. It needed to ensure security while continuing to empower ongoing and rapid innovation. To be agile and maintain constant release cycles, Pivvot relies on a cloud-based microservices architecture. It has moved to Docker® and Amazon Elastic Container Service™ (ECS) in Amazon Web Services™ (AWS) for scalability and high-performance container orchestration.

CHALLENGES

Pivvot manages highly sensitive customer data assets and delivers solutions to a diverse customer base in the public cloud. Working with clients in industries where security is paramount, Pivvot maintains a highly secure application development pipeline. This requires build scanning, image registry scanning at pre-runtime, securing the host, and providing Docker® and Kubernetes® protection at runtime. The constant changes in the threat environment create an ongoing challenge. Pivvot must go from build to deploy quickly and with confidence that solutions are secure when released to production.

Business Benefits

- Sensitive data secured within a dynamic DevOps environment
- Accelerated application program interface (API) operationalization
- Enhanced integration between the DevOps and Security teams

With software in DevOps environments delivered continuously, security must be automated and built in from the start. Pivvot needed a flexible, scalable, and integrated security solution that could:

- Ensure data assets remain secure throughout the product development life cycle and life of the product
- Enable fast and simple development processes that include security
- Provide flexibility and scalability to meet customer and business requirements
- Keep up with the rapidly changing development environment on AWS

SOLUTIONS

With Trend Micro™ Deep Security™ Smart Check, security is embedded into Pivvot's development process, allowing them to:

- Develop new applications that meet compliance requirements and customer demands from the start—at first build and in each subsequent build
- Operationalize new products and be able to scale more quickly and easily by taking advantage of Deep Security's automation capabilities
- Support the migration of its APIs to a container architecture on Amazon ECS by using Smart Check for continuous container image scanning
- Detect vulnerabilities pre-runtime with Smart Check's dashboard visibility
- Build with confidence, knowing that Trend Micro is able to keep pace with Amazon's development environment and services

Every one of Pivvot's customers is unique in their needs. By applying smart security controls that meet security, compliance, and customer requirements, Smart Check helps Pivvot build securely so it can focus on customer enablement and business growth.

MORE INFORMATION

For more information, please go to www.trendmicro.com



Securing Your Connected World

©2018 by Trend Micro Incorporated. All rights reserved. Trend Micro, and the Trend Micro t-ball logo, OfficeScan and Trend Micro Control Manager are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. [CS01_Pivvot_DevOps_Case_Study_181214US]