SOLUTION BRIEF

Securing Containers: Think Your Containers are Secure? Think Again.

Symantec

Introduction

It's true that applications running in containers have some security advantages over classic applications running on servers, but that doesn't mean they don't need to be secured. For example, containerized apps may have a smaller attack surface, thanks to the Docker daemon being smaller than a virtualized operating system, but it would be a mistake to assume this means they need less security.

To the contrary, the use of containers can introduce a number of security risks that must be addressed before they can be trusted to safely run critical applications. One of those risks is posed by the lack of visibility in the container environment. It's very difficult to understand what's going on within and among all your containers, particularly when used in Infrastructure-as-a-Service (IaaS) environments. And it's difficult to perform forensic analysis or regulatory audits when incident activity isn't available for your security analysts.

To overcome the negatives, you need visibility into container activities across all environments to identify changes that expose your applications to vulnerabilities and malicious files. Symantec gives you the visibility and security you need for containers, hosts, and storage across your public cloud and private clouds, and on-premises data center environments.

We also give you the ability to scan private Docker registry images stored in cloud services like S3 to ensure that neither end users nor other applications can upload malicious software to your container storage back end.

Container Security Done Right

Symantec Cloud Workload Protection gives you a homogenous approach to securing your heterogeneous environments. With Cloud Workload Protection, you'll quickly and easily mitigate container security risks, while retaining the business agility and operational efficiencies they offer. Cloud Workload Protection delivers container and storage protection via a single console, giving you:

- **Visibility** – Gain insight into all container activities to stay informed of container security postures and status across all environments.
- **Vulnerability Identification and Compliance Validation** – Continually scan your environment to identify vulnerabilities and determine their impact on your risk and compliance objectives.
- **Threat Detection** – Detect attacks and malware targeting your container infrastructure, even at the kernel level, and block them before they propagate and threaten the integrity and privacy of your operational environment and data.
- **Control** – Enforce policies that mitigate vulnerabilities within your applications and threats to your data. Automate the response to new vulnerabilities and attacks with network and application-level controls and isolation.
- **Simplicity** – Use a single cloud-based console to automate your workload, storage, and container security.

Try Cloud Workload Protection Suite for Free

Successful organizations modernizing their IT infrastructure are looking to adopt containers while keeping their business and IT risks in check. With Cloud Workload Protection and CWP for Storage, you can secure containers and related storage from a single console to improve your operational efficiency, while enabling your DevOps teams to build security into their CI/CD workflows.

Discover for yourself the difference Symantec makes. **Sign up for a free trial of our Cloud Workload Protection suite now**.

Symantec Cloud Workload Protection

Discovery and visibility of containers across public cloud and on premises

- Discovery and visibility of workloads deployed via containers across AWS, Azure, Google Cloud Platform, private clouds and on premises.
- Identification of workload security postures.

Robust workload protection across public clouds and on-premises environments

- Single console for policy enforcement and anti-malware, anomaly detection, and hardening protection for workloads across public cloud, private cloud, and traditional on-premises data center environments.
- Protection and monitoring for Docker containers, including support for leading container orchestration tools such as Kubernetes, Chef, Puppet, and Ansible.

Elastic, cloud-native protection

- Cloud-native integration enables DevOps to build security for workloads and storage directly into continuous integration and deployment (CI/CD) workflows.
- Security that scales elastically and automatically with dynamic cloud infrastructure.

Symantec Cloud Workload Protection for Storage

Vulnerability and threat detection

- Automatic and scheduled scans of Amazon S3 buckets supports discovery and mitigation of malware threats before they impact containerized applications, related services, and users.
- Scale the threat scanning infrastructure elastically with load-for-cost optimization.

Protection of cloud applications, services, and users

- Receive administrative alerts to prevent data breaches when Amazon S3 buckets are misconfigured or exposed to the public internet.
- Automatically identify and block the latest threats using Symantec's suite of anti-malware technologies, including reputation analysis and advanced machine learning.

DevOps alignment

- Securely adopt containers and serverless technologies, such as AWS Lambda, to support CI/CD initiatives.
- Automatically protect S3 buckets to minimize DevOps and administrative workloads.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec™

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

Copyright © 2018 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

19A174278_SB_CWP-SECURING-CONTAINERS_EN