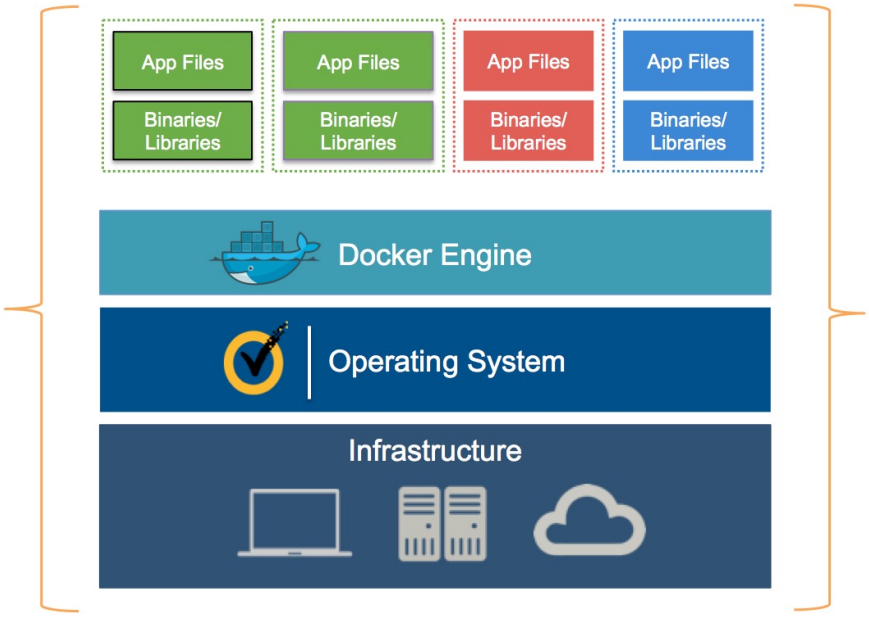
Symantec™ Data Center Security: Server Advanced

Agentless protection for Docker containers

Data Sheet: Security Management

Solution Overview

Docker containers make it easy to develop, deploy, and deliver applications where containers can be deployed and brought down in a matter of seconds. This flexibility makes it very useful for DevOps to automate deployment of containers. Symantec Data Center Security: Server Advanced provides agentless Docker container protection that allows you to achieve the performance benefits of Docker without sacrificing security. Full application control enables administrator privilege de-escalation, patch mitigation, and protection against zero day threat in today's heterogeneous data centers.



Security Challenges for Docker Deployments

Docker containers expose new threat surfaces. The host operating system, Docker daemon and containers are open to vulnerabilities that can be breached. Some of the recently known Docker vulnerabilities and exploits are:

- Docker daemon currently requires root privileges and Docker recommends that only trusted users should be allowed access to Docker daemon.
- Docker can be started with incorrect parameters for host network, which can shut down the host.
- The shocker code exploit exposed a Docker vulnerability for container breakout.
- Recent CVE reports show that vulnerabilities being introduced with deployments.
- Docker Hub has become the go-to destination for pre-built containers, as it hosts over 100,000 free apps. However, these pre-built containers have no security requirements and can contain vulnerabilities that could be used as attack vectors.

Security Questions for Your Docker Deployment

1. How can I monitor users that are added to the Docker host?
2. How do I ensure that only Docker daemon is running, and how do I restrict access of other applications?
3. Can I ensure the right set of network parameters are applied for running Docker?

Symantec

4. How do I ensure that any existing vulnerabilities on Docker of the daemon host are safe from exploit?

Symantec Data Center Security: Server Advanced for Docker

Symantec Data Center Security: Server Advanced is designed to ensure the right protection for your Docker containers by providing Visibility, Compliance, Hardening, and Management.

Visibility

Symantec Data Center Security: Server Advanced provides a single view to the entire container deployment with their metadata and power status.

Compliance

- With Symantec Data Center Security: Server Advanced, security teams can apply Unix real-time security and compliance monitoring policy to the Docker host. The host as well as the containers will be monitored. This will include Real time file monitoring of the Docker host and the containers.
- Helps ensure that security teams can ensure files and services specified in the CIS Docker benchmark are being monitored.
- Helps monitor all containers that are downloaded and deployed from Docker Hub thus providing an audit trail.
- Helps track users that are created on Docker hosts, giving you the ability to enforce user rights compliance.

Hardening

- Provides agentless security to each container by providing isolation of the containers from each other, from Docker daemon and Docker hosts. This prevents from any exploits that may result in container breakout.
- Helps to deliver host protection by hardening policy without impacting Docker daemon and Docker hosts.
- Applies a host based firewall policy to restrict network access.

Management

- Symantec Data Center Security: Server Advanced policies and events can be accessed with RESTful API's. This makes it easy to integrate Symantec Data Center Security: Server Advanced with existing DevOps workflow of automation and orchestration. Thus security is delivered at run time and built-in to the containers during provisioning.

Learn more about Symantec Data Center Security at Symantec.com

Additional Symantec Data Center Security Offerings

Symantec Data Center Security: Server delivers agentless anti-malware, agentless network IPS, in-guest file quarantine, file reputation services for VMware hosts and virtual guests. It integrates with VMware vCenter, VMware NSX, Palo Alto Networks Next Generation Firewall and Rapid 7 Nexpose to automate and orchestrate application-level security throughout the lifecycle of the workload.

Symantec Data Center Security: Server Advanced protects both physical and virtual servers in on-prem, hybrid, and cloud-based data centers by delivering (1) application and protected whitelisting, (2) fine-grained intrusion detection and prevention, (3) file, system and admin lockdown, (4) and file integrity and configuration monitoring. Data Center Security: Server Advanced helps minimize time and effort and reduce operational costs by using out of the box monitoring and hardening for most common data center applications. Help protect your OpenStack based data centers using file integrity monitoring of all OpenStack modules and with full hardening of the Keystone identity service module.

Symantec Control Compliance Suite enables asset and network auto discovery, automates security assessments and calculates and aggregates the CVSS/CIS risk scores. Customers use Control Compliance Suite to enable basic

security hygiene, and gain visibility into their security, compliance, and risk postures. Customers use this intelligence to prioritize remediation and optimize security resource allocation.

Symantec Protection Engine delivers content scanning, antimalware, outbreak detection, anti-spam, insight and reputation services, and granular content filtering technologies for various types of data stores such as cloud storage, NAS, email, and AWS. Out-of-the-box support is available for NetApp NAS, Microsoft Exchange, and SharePoint Data Stores, and a robust SDK enables custom integration for other data stores.

More Information

Visit our website

http://enterprise.symantec.com

To speak with a Product Specialist in the U.S.

Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec Corporation (NASDAQ: SYMC) is the global leader in cybersecurity. Operating one of the world's largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives.

Symantec World Headquarters

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

21367559 08/16