Data Center Security: Server Advanced

Agentless Protection for Docker Containers

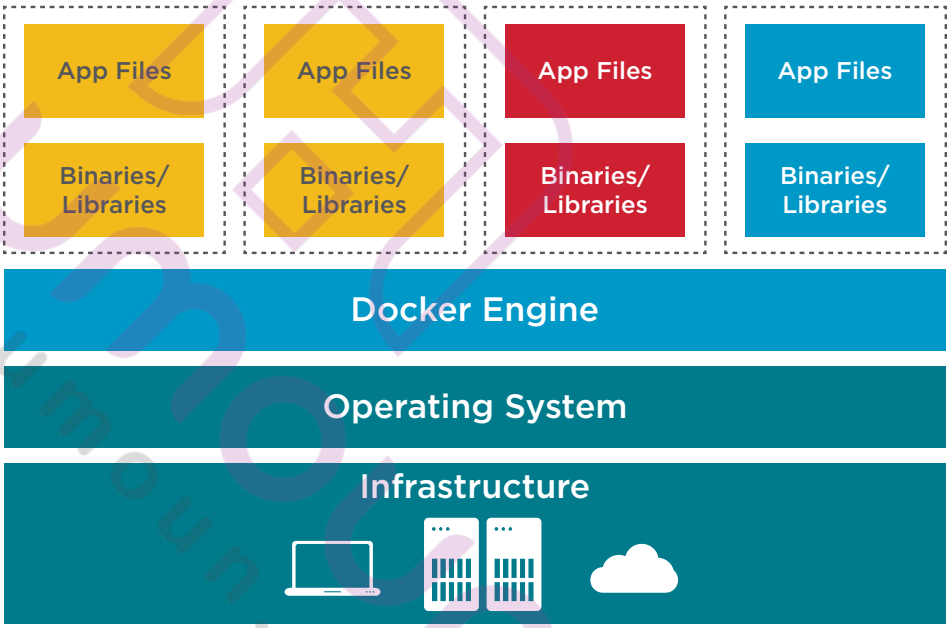
Security Challenges for Docker Deployments

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 as follows:

- 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 the 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 are 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.

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 threats in today's heterogeneous data centers.



Security Questions for Docker Deployment

- How can I monitor users that are added to the Docker host?
- How do I ensure that only Docker daemon is running, and how do I restrict the access of other applications?
- Can I ensure the right set of network parameters are applied for running Docker?
- 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 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 are monitored. This includes 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, enabling 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 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 APIs. 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.

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 virtual guests.

Symantec Cloud Workload Protection (CWP) allows enterprises to secure their critical workloads wherever they are—public clouds, private clouds, and physical on-premises data centers—all from a single centralized console. CWP is a native cloud SaaS offering that automates workload security, providing discovery, visibility, and protection against advanced malware and threats across multiple cloud service providers (AWS, Azure, GCP, OCI). Automatic identification of workload security posture and software services, including visibility into infrastructure changes and flow logs, enables automatic policy recommendations and deployment. CWP provides multi-layered protection for cloud compute instances including anti-malware scanning, application control, and isolation to help block exploits targeting known and unknown vulnerabilities, OS hardening that helps to stop zero-day threats, and real-time file integrity monitoring (RT-FIM) that helps prevent unauthorized system changes.

Docker containers and Orchestration applications are also supported. Cloud-native integration with public cloud platform APIs allows CWP to both share and consume information in real-time, along with any changes to cloud infrastructure and security settings. Public cloud API integration also enables DevOps practitioners to build security directly into service deployment workflows, ensuring that workloads are protected, and that security scales automatically with dynamic cloud infrastructure. The CWP cloud console can also be used to manage Symantec Data Center Security (DCS) agents on virtualized and physical on-premises servers.