GuardiCore

SOLUTION BRIEF

# Securing Containerized Applications and Workloads with GuardiCore Centra™

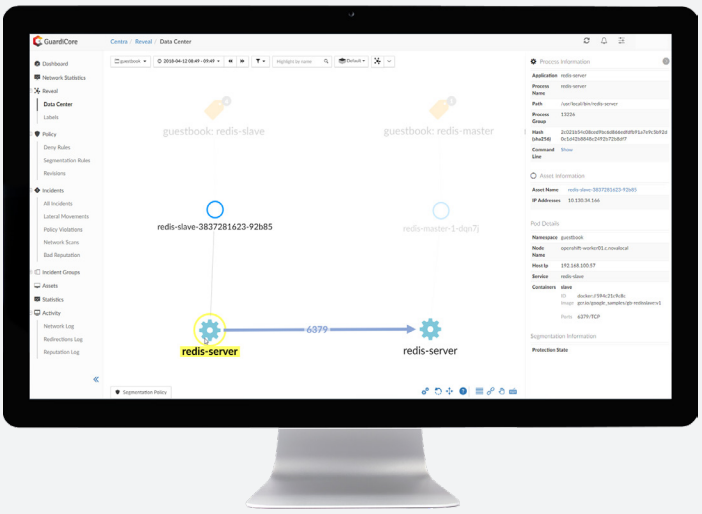
## All the Agility of Containers Without Sacrificing Security

Just like other abstraction technologies such as virtualization, containers present several significant challenges for security teams. First, containers limit visibility into the network topology and communication flows of the processes running on individual containers. Second, the ease of scaling containers creates a need for security teams to continuously incorporate container orchestration metadata into asset labels and topology maps so they can create logical security controls. Third, unless micro-segmentation policy engines are "container aware," policies cannot be pushed down to control process-level communications within individual containers. And finally, containers increase the attack surface area and provide a new vector for attacks and malicious actors to go undetected. With the GuardiCore Centra™ Security Platform you can reduce compliance risks and enforce security policies within containerized applications throughout the build, deploy and runtime environments in any hybrid infrastructure.

## Regain Visibility

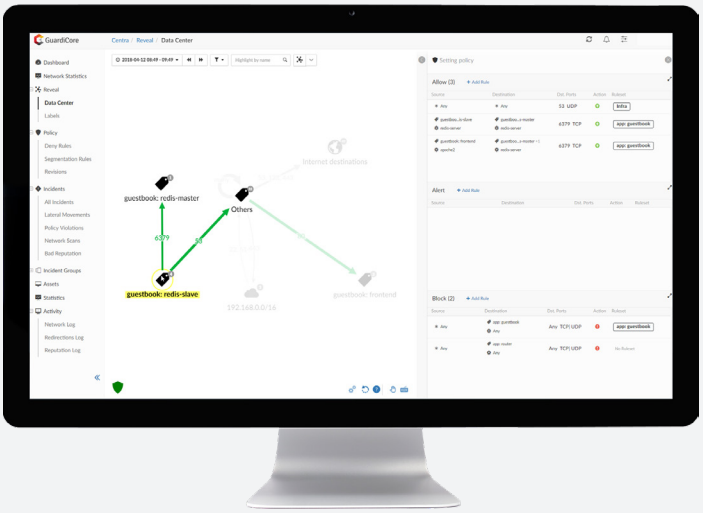
### See every container, pod and communication flow with detailed orchestration data

GuardiCore Centra enables you to see the entire container cluster from the application perspective including control planes, load balancers and routers. Using best-in-class visibility, DevSecOps teams can visualize pod-to-pod and pod-to-vm communication flows down to the process level, develop strong security policies and troubleshoot configuration issues.



## Scale Security with Applications and Workloads

### Incorporate native pod labels so security controls scale and migrate with containers

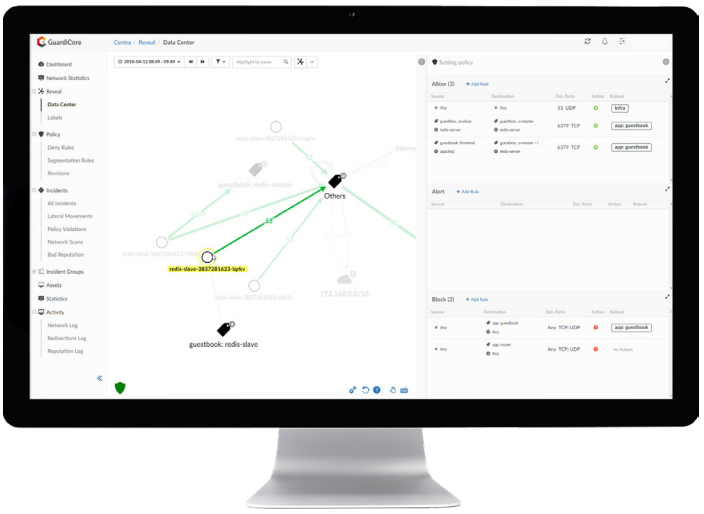



A true Cloud Workload Protection Platform, Centra integrates with several container orchestration platforms enabling security teams to incorporate native labels into asset descriptions and micro-segmentation policies and ensure security controls scale with the cluster while also providing constant protection. In addition, native label integration simplifies investigations of policy violations and accelerates remediation.

## Solve Compliance Challenges

### Deploy containers in PCI-sensitive workloads and demonstrate compliance

GuardiCore helps to solve compliance challenges by enabling the production of real-time or historical flow diagrams and enforcement of segmentation policies within containers that support PCI-DSS 3.2 requirements for tracking and monitoring of all access to network resources and restricting connections between untrusted networks and system components in the cardholder data environment.




## About GuardiCore

GuardiCore is an innovator in data center and cloud security focused on delivering more accurate and effective ways to protect critical applications from compromise through unmatched visibility, microsegmentation and real-time breach detection and response. Developed by the top cyber security experts in their field, GuardiCore is changing the way organizations are fighting cyber attacks in their data centers.