CAPSULE8

SOLUTION BRIEF

How Capsule8 Protects Containerized Environments

Why Runtime Container Security Matters

Containers are often thought of as creating a light isolation boundary at the application-level; an issue in one container won't disturb the others containers. However, containers co-exist on the same host, sharing the same underlying OS and hardware resources.

The reality is that isolation cannot be treated as a security property of containers. Because containers share hosts, any compromise of the host—such as via kernel exploitation—removes the assumed isolation boundary. As a result, access to one container allows access to all other resources on the host.

Even if the application-level boundary holds, unwanted activity in running containers can still lead to major incidents. A cryptominer hogging resources, a developer debugging in production, or an attacker reading sensitive data in a single container can easily jeopardize security and operational performance.

Unwanted activity in containers can jeopardize the security and performance of hosts, too.

Capsule8 detects activity inside containers, unlike traditional tools relying on kernel modules.

Capsule8 was built for the unique threat models of cloud and microservices environments.

The Right Solution

To protect containers as they operate in production, you need modern enterprise infrastructure protection. Capsule8 provides detection and resilience for Linux systems in any environment, including cloud-native systems—from cloud computing, orchestrators, to container runtimes such as Docker, containerd, and CRI-O.

Capsule8 finds and stops unwanted activity on Linux systems that jeopardizes your containerized environments. Our detection is crafted with the threat models of cloud-native systems in mind and pinpoints workloads, not just hosts.

Capsule8's team includes some of the most active researchers in container escapology. To continually test our product's container protection, we actively develop new container escape exploits for Linux kernel vulnerabilities.

What we detect

Capsule8 is built to protect your containerized systems from runtime threats to security and performance, including:

- Container escapes via kernel exploitation or RunC
- Repeated program crashes
- Disabling of native security mechanisms (like SELinux)
- New files executed in containers
- Developers debugging containers running in production
- Starting shells in running containers
- Unauthorized remote interactive shells
- Userland container escapes

Capsule8 also allows you to create custom policies leveraging container metadata, so you can extend Capsule8's protection to meet the concerns of your unique environments. For instance, you can restrict the ability for specific containers to write new files, run new programs after startup, read cloud metadata, have multiple users running, make outbound network connections, or spawn shells.

How it works

Capsule8's agent relies on stable Linux features, namely kprobes and perf, that work on any relatively modern kernel. This approach also means Capsule8's agent can collect activity from inside containers, leaving no coverage gaps in microservices environments, in contrast to traditional tools which rely on kernel modules.

Unlike existing Linux auditing solutions, which use a monolithic, global configuration, Capsule8 operates at the cgroup level. This allows you to bind different detections and policies to different control groups, and means Capsule8 lets you detect unwanted activity on a per-container basis.

Capsule8 collects and exposes container metadata so you can pinpoint exactly which workload is involved in an event out of potentially hundreds running on a host. This helps minimize your time to recovery by accelerating triage and incident response.

Many organizations are already using Capsule8 across their unique infrastructure deployments and environments. We can protect your mix of cloud-native Linux systems, including:

aws · cri-o · Amazon EKS · podman · docker · redhat · kubernetes · Azure · containerd

CAPSULE8

Try **Capsule8 Protect** now

Request a demo: info.capsule8.com/request-a-demo

For more information: info@Capsule8.com
Capsule8.com
@Capsule8