Symantec.

Application Containers Need Security Too

Five Challenges You Can't Overlook

1 • 2 • 3 • 4 • 5

Like most agile organizations, you are probably adopting containers to deliver applications. However, you may not necessarily understand the security implications and the unintended consequences they bring. This doesn't mean that containers can't be trusted–as with deployment of any new technology, security gaps just need to be accurately identified and addressed. The five major security challenges for containers are:

1 Lack of Visibility

Containers appear as servers to security analysts, leaving no security events trail to follow when conducting forensics.

2 Open-Source Software Vulnerabilities

Most containers use open source libraries, requiring vulnerability assessment before deployment.

3 Compliance

With container technology being new, traditional security tools don't support enforcement of security configuration standards.

4 Unrestricted Access

A single application bug can expose the entire container ecosystem, including the host and adjacent containers, to attackers.

5 Kernel-Level Threats

Attackers who gain access to containers can also access the management framework or host to cause further damage.

What are you using to secure containers?

Migrating applications, data, and operations to containers doesn't mean you'll increase risk. Using appropriate protections with containers promotes operations that are just as secure—and often more secure—than before.

Symantec Cloud Workload Protection offers the same functionality for securing your hosts as it does for securing containers without increasing complexity.

Learn More: go.symantec.com/cwp

Symantec.