Benefits:

The container doesn't interact with the hardware the way an OS or other typical applications do, so there's a degree of separation, and thus safety, in how far a breach in a container can go affecting the host.

Limits:

The container still runs at the same layer as other applications, so if a container became infected, it could possibly still grant access to other applications it's interfacing with and cause them to be infected as well.