INTEL® CLEAR CONTAINERS

Amy Leeland
Program Manager
Clear Linux, Clear Containers
And Ciao

Containers are…

Speedy

Fast create, update and uninstall cycle.

Request and provision in (milli)seconds

Manageable

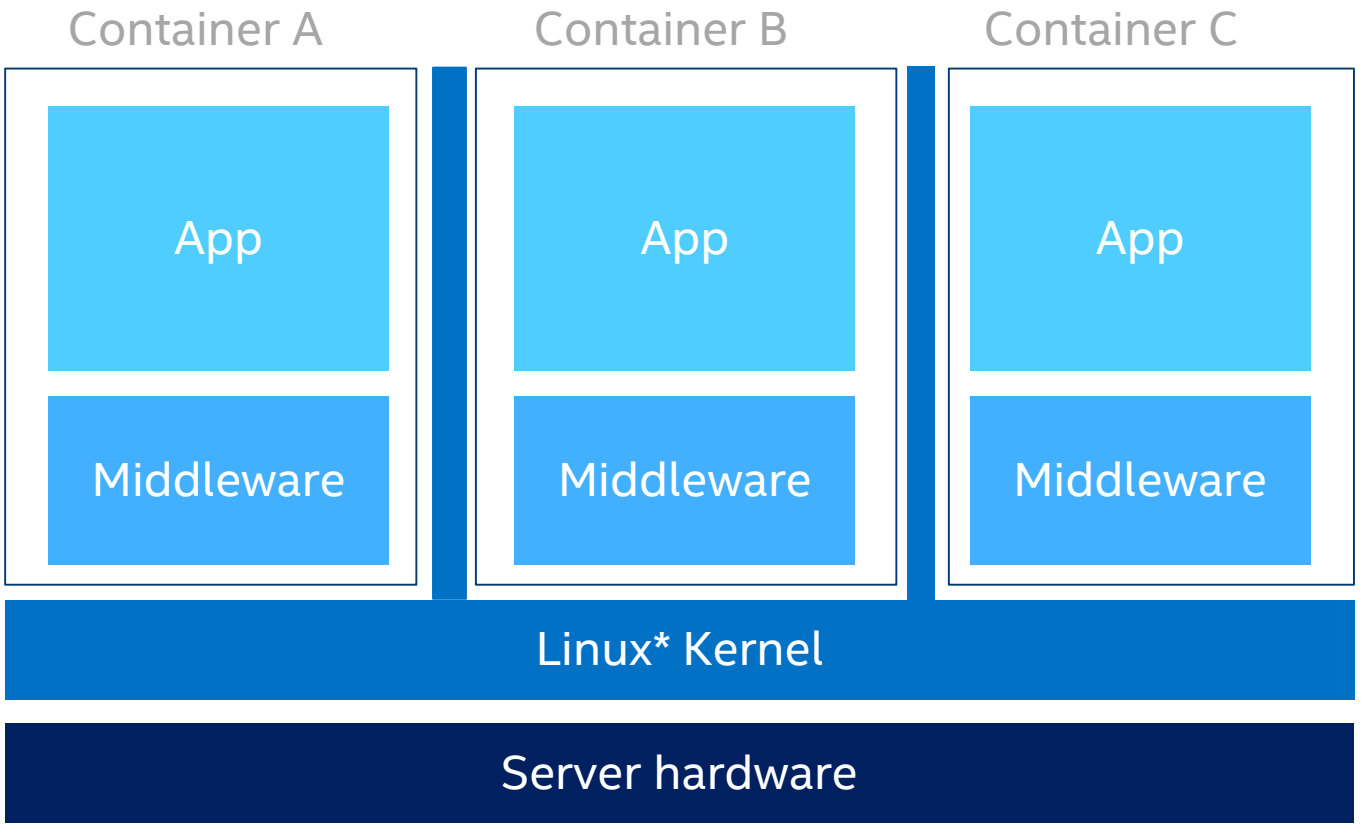
Containers take the complexity out of bundling, distributing and installing applications

Easy

Simple and easy to use and maintain

Secure?

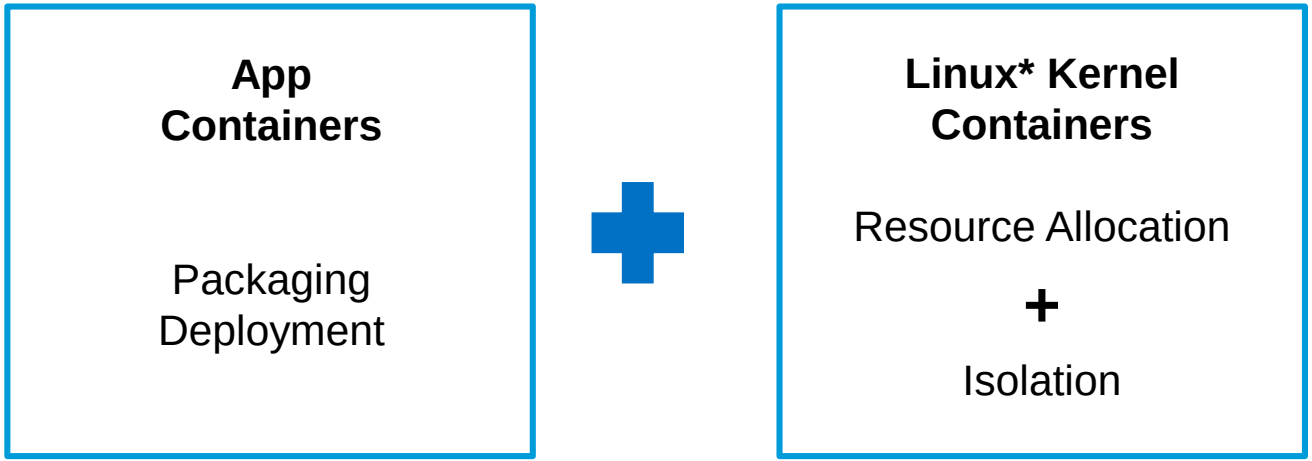
What about security and isolation? Can a container include hardware isolation like a Virtual Machine?



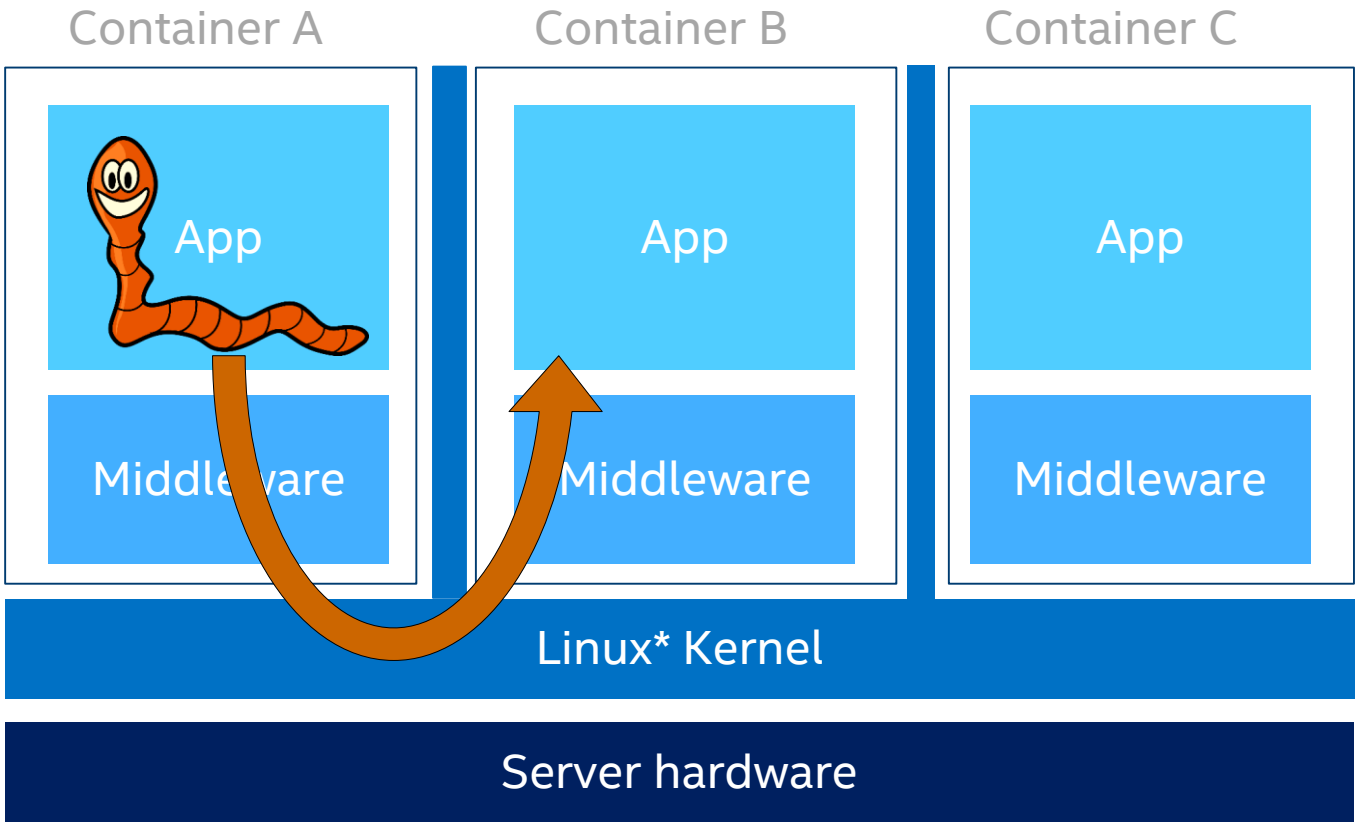
*Other names and brands may be claimed as the property of others.

The word “Container” is used for different things

Containers =



*Other names and brands may be claimed as the property of others.



*Other names and brands may be claimed as the property of others.

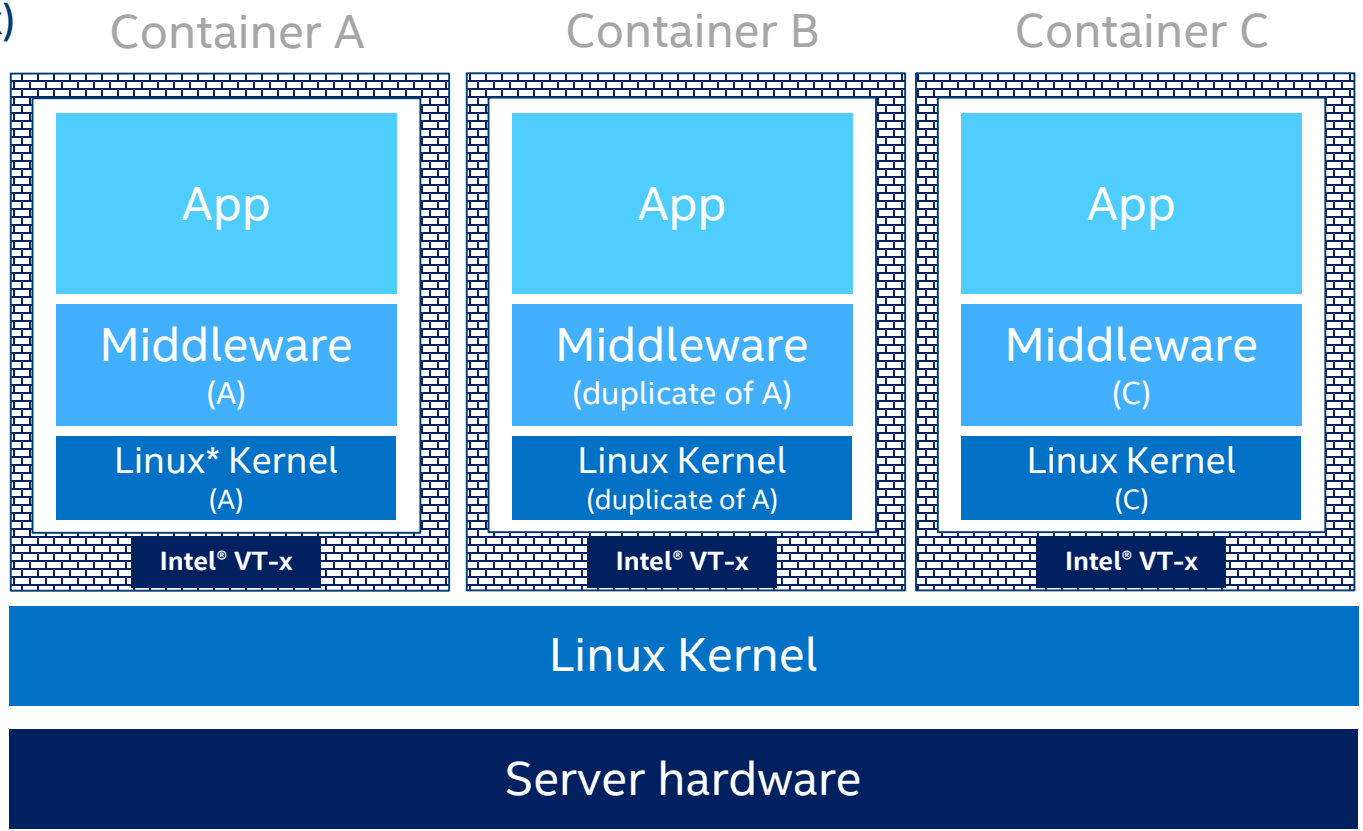
*Other names and brands may be claimed as the property of others.

intel Software

INTEL® CLEAR CONTAINERS

http://www.clearlinux.org

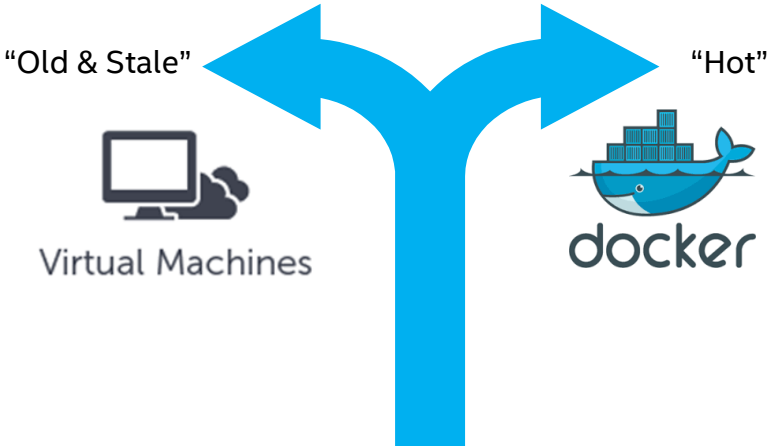
Intel® Clear Containers and Intel® Virtualization Technology (Intel® VT-x)



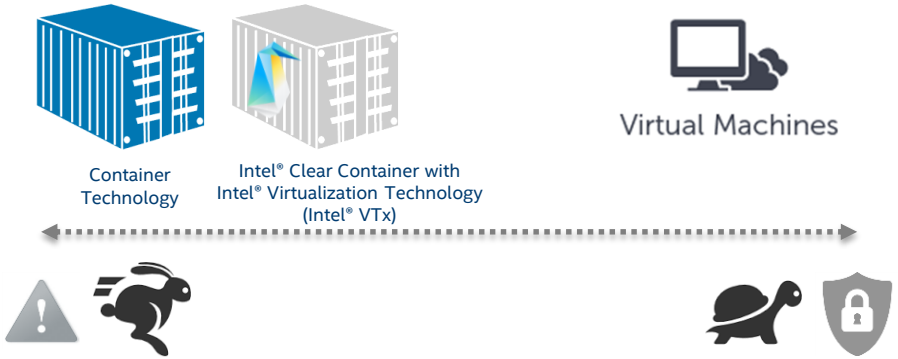
*Other names and brands may be claimed as the property of others.

With Clear Containers, there is now a continuum between containers and virtual machines

Before Intel® Clear Containers
Q1'15



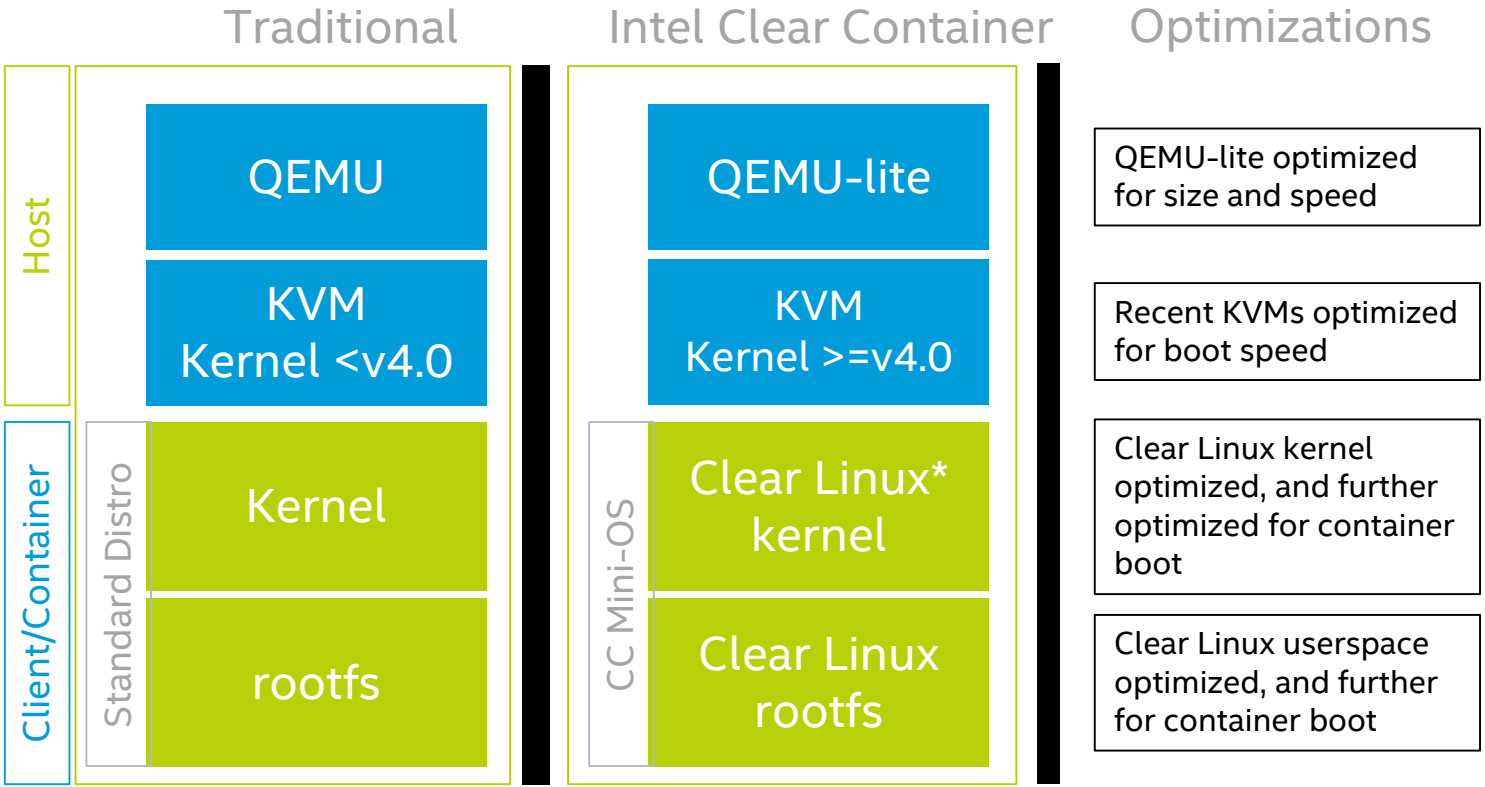
After Intel Clear Containers
Q4'15



*Other names and brands may be claimed as the property of others. The nominative use of third party logos serves only the purposes of description and identification.

Intel® Clear Containers vs traditional VMs

How we made them smaller and faster



*Other names and brands may be claimed as the property of others.

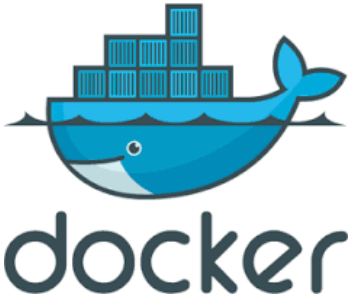
Intel® Clear Containers with Docker*!

2.0

Intel® Clear Containers 2.0 Available on GitHub* and clearlinux.org

OCI

Intel® Clear Containers are OCI spec compatible



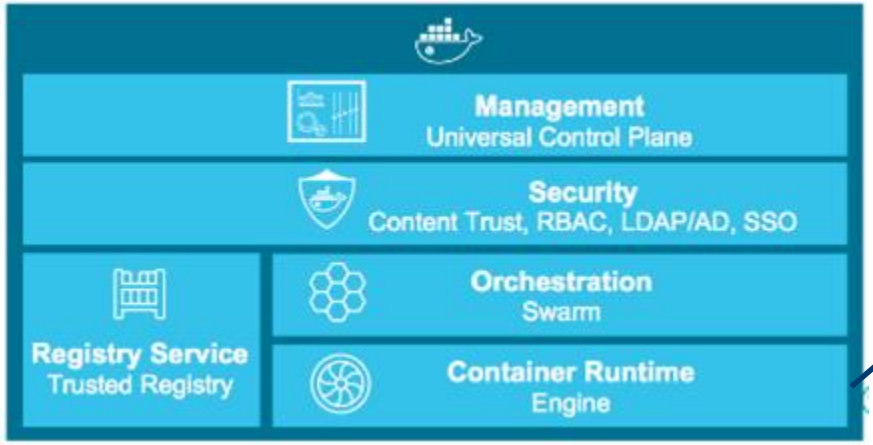
1.12

Switchable runtime in Docker 1.12

*Other names and brands may be claimed as the property of others.

intel Software

Intel® Clear Containers adds a new runtime for Docker*



Intel Clear Containers provide a plugin replacement of runc with cor, our OCI runtime.

*Other names and brands may be claimed as the property of others. The nominative use of third party logos serves only the purposes of description and identification.

Industry engagement: CoreOS

Security-minded capabilities

rkt is built from the ground up to be ready for security-focused environments. Many of these principles weren't invented at CoreOS — instead, we applied common, everyday best practices that have been largely overlooked in the container industry so far.

Architected for best practices

rkt strives to embody the Unix "tools" philosophy and learn from decades of best practices in architecture and security. This includes image signature validation by default, and privilege separation between different tasks, like image discovery and retrieval — unprivileged operations in rkt — versus container execution, requiring root access. rkt's daemonless model means it can integrate easily with standard init systems, such as systemd and upstart, or with cluster orchestration systems, like Nomad and Kubernetes.

Pluggable isolation, including KVM-based "Clear Containers"

Modular isolation means that rkt supports a variety of techniques for running containers. While software-isolated Linux `cgroup`s containers are the default, advanced solutions like Intel's KVM-based "Clear Containers" or host-level rkt `fly` provide selectable degrees of container confinement.

Intel Clear Containers

With Intel's Clear Containers-based stage1, rkt is able to execute standard ACIs with CPU-enforced isolation. This balances the best of both worlds: application-focused packaging and deployment efficiencies, with the explicit hardware-guaranteed isolation of a virtual machine.

rkt fly

With the `fly` stage1 isolation environment, rkt executes a standard container image with full access to the host environment. This means you can run specially-privileged software, such as system management agents that need full host access, while maintaining image signature and deployment policies. Using rkt with `fly` retains the packaging and distribution benefits of app containers for even the lowest-level system programs.

- CoreOS announces use of Clear Containers technology in rkt 1.0
- We provide lightweight Tier 1 OSV support

Legal notices and disclaimers

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at intel.com, or from the OEM or retailer.

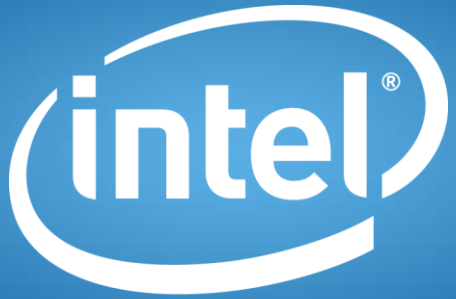
No computer system can be absolutely secure.

Tests document performance of components on a particular test, in specific systems. Differences in hardware, software, or configuration will affect actual performance. Consult other sources of information to evaluate performance as you consider your purchase. For more complete information about performance and benchmark results, visit http://www.intel.com/performance.

Intel, the Intel logo and others are trademarks of Intel Corporation in the U.S. and/or other countries.

The nominative use of third party logos serves only the purposes of description and identification. *Other names and brands may be claimed as the property of others.

© 2016 Intel Corporation.



Software