ARMOR

WHITEPAPER

RISK CONTAINED.
DEVELOPMENT
UNRESTRAINED.

WHAT ARE CONTAINERS AND CONTAINERIZED ARCHITECTURE?

CLOUD ARCHITECTURES CONTINUE TO EVOLVE

As organizations more heavily adopt the public cloud through infrastructure-as-a-service (IaaS) vendors, they must also deal with evolving and complex architectures. It started with the virtualization of servers and shared compute resources and has evolved to platform-as-a-service (PaaS), serverless, and container architectures. IT and cybersecurity teams must evaluate and be prepared to embrace these architectures.

Ultimately, the challenge IT and cybersecurity teams face is to secure these new architectures while unifying visibility. And that visibility extends across servers, endpoints, containers, and PaaS services, where traditional security models don't apply.

Because containers allow portability and consistency across the spectrum of public, private, and virtualized environments, they are becoming a go-to technology in the industry. This paper will discuss how containers have become a must-have technology in today's cloud era and can serve as a primer for IT and IT security teams to understand containers' appeal to developer and DevOps teams within their organizations.

WHAT ARE CONTAINERS?

Containers are as they sound—they hold something. In this context, a container is a logical storage box that houses an application and its related components. The concept of containers is not new, though their usage has accelerated with the increased adoption of the cloud. Docker, a computer program that "virtualizes" (i.e., containerizes) operating systems (OS), refers to containers as simply, "a standardized unit of software." Forrester offers a more specific description: "Containers bundle applications with the software libraries that they depend on, allowing developers to create 'build once, run anywhere' code making applications very portable."
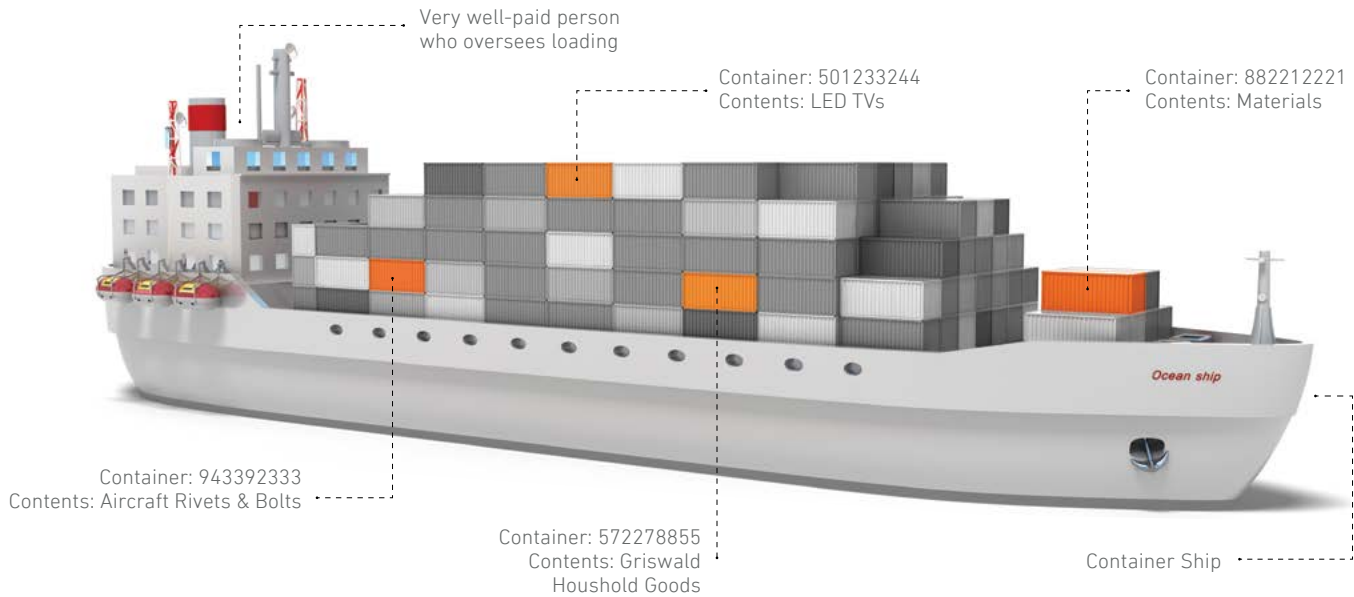
> A container is a standardized unit of software.
>
> — Docker

APP 1	BIN/LIBS
APP 2	BIN/LIBS
APP 3	BIN/LIBS
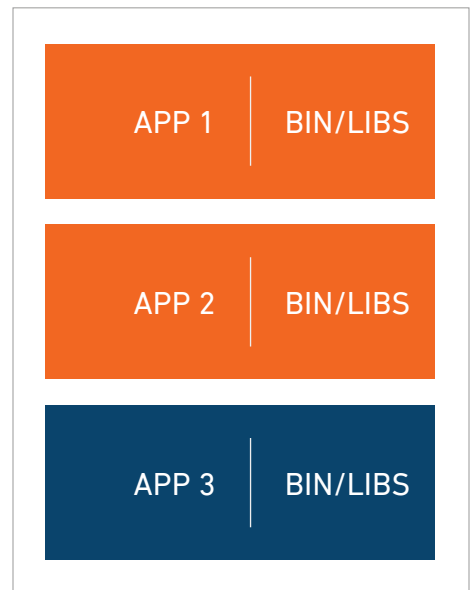
CONTAINERS—LOGICAL & PHYSICAL

Logical containers have often been compared to the physical ones in the cargo shipping industry. Large 40-foot containers are a standardized way to store and move cargo of all different types, sizes, weights, and measures. That container can then be shipped by truck and train to a port, loaded on a container ship, and transported to any destination in the world.

Very well-paid person who oversees loading

Container: 501233244
Contents: LED TVs

Container: 882212221
Contents: Materials

Container: 943392333
Contents: Aircraft Rivets & Bolts

Container: 572278855
Contents: Griswald Houshold Goods

Ocean ship

Container Ship

Containers serve a similar purpose in the logical world, as shown in the table below.

LOGICAL CONTAINERS VS. SHIPPING CONTAINERS		
Logical container	=	Physical container
Applications, binaries, and libraries	=	Physical goods being shipped
Container management/orchestration tools	=	Container/shipping management systems
Container repositories	=	Distributed physical container storage locations
Container OS	=	Ports and port authorities, trucking companies, railway networks, train operators, and ship transport companies
Host operating system	=	City, state, federal, and international government; business, legal, regulatory, international, and other frameworks; and resource allocation schemes
Cloud or on-premise infrastructure	=	Electrical grid, critical infrastructure, navigable waterways, roadways

CONTAINERS DETAILED

While both virtual machines (VM) and containers enable application portability, containers are significantly lighter and more portable. The main reason is that, unlike VMs, containers do not include an OS and its associated kernel (i.e., the part of the OS that loads first upon boot-up and eventually runs memory, disk, process, and task management). In containerization, a single kernel resides in the host OS and is shared among containers. All that's housed in a container is the application code and related binaries and libraries.

THE ABSENCE OF A KERNEL BENEFITS CONTAINERS IN SEVERAL WAYS

1

CONTAINER SIZE

Container sizes can be as small as 10MB, whereas VMs can easily exceed 10GB (a Windows Server 2016 VM, for instance, could be about 32GB).

2

LOWER MEMORY REQUIREMENTS

The memory requirements of containers are significantly lower than those of VMs. It's not just about the memory VMs consume, which must be larger to accommodate a kernel, it's about the stage in their lifecycle when VMs consume those memory resources. VMs grab all the memory that's been allocated to them upon boot-up—regardless of whether they need it or not.

3

FASTER BOOT TIMES

A typical VM requires a few minutes to boot because of its kernel—some containers require less than a second.
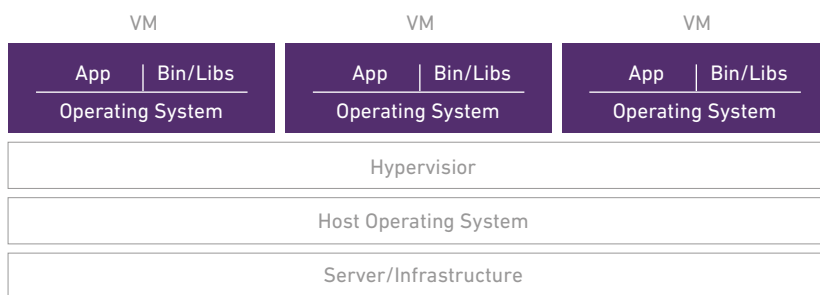
While containerized architecture yields clear performance and efficiency advantages, containers are also computationally less expensive than an application running on a dedicated OS.

Conversely, this approach drives better OS utilization as it allows more applications to run on the underlying host OS.
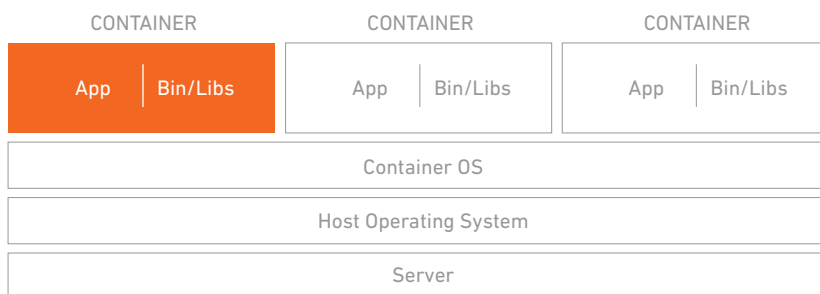
VIRTUALIZATION VS. CONTAINERS

The container OS is the technology that makes containers possible. Though there are a growing number of container platforms available, Docker and Kubernetes are the most popular today.
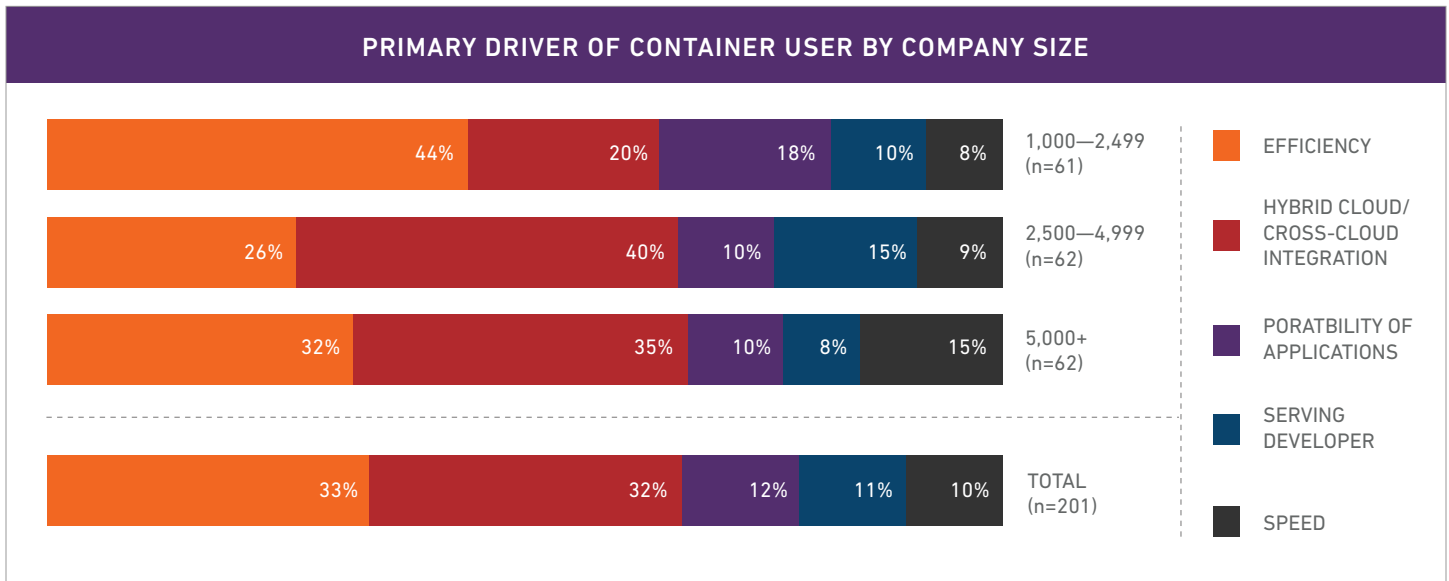
VIRTUALIZED STACK

VM	VM	VM
App | Bin/Libs	App | Bin/Libs	App | Bin/Libs
Operating System	Operating System	Operating System

Hypervisior

Host Operating System

Server/Infrastructure

VS

CONTAINER STACK

CONTAINER	CONTAINER	CONTAINER
App | Bin/Libs	App | Bin/Libs	App | Bin/Libs

Container OS

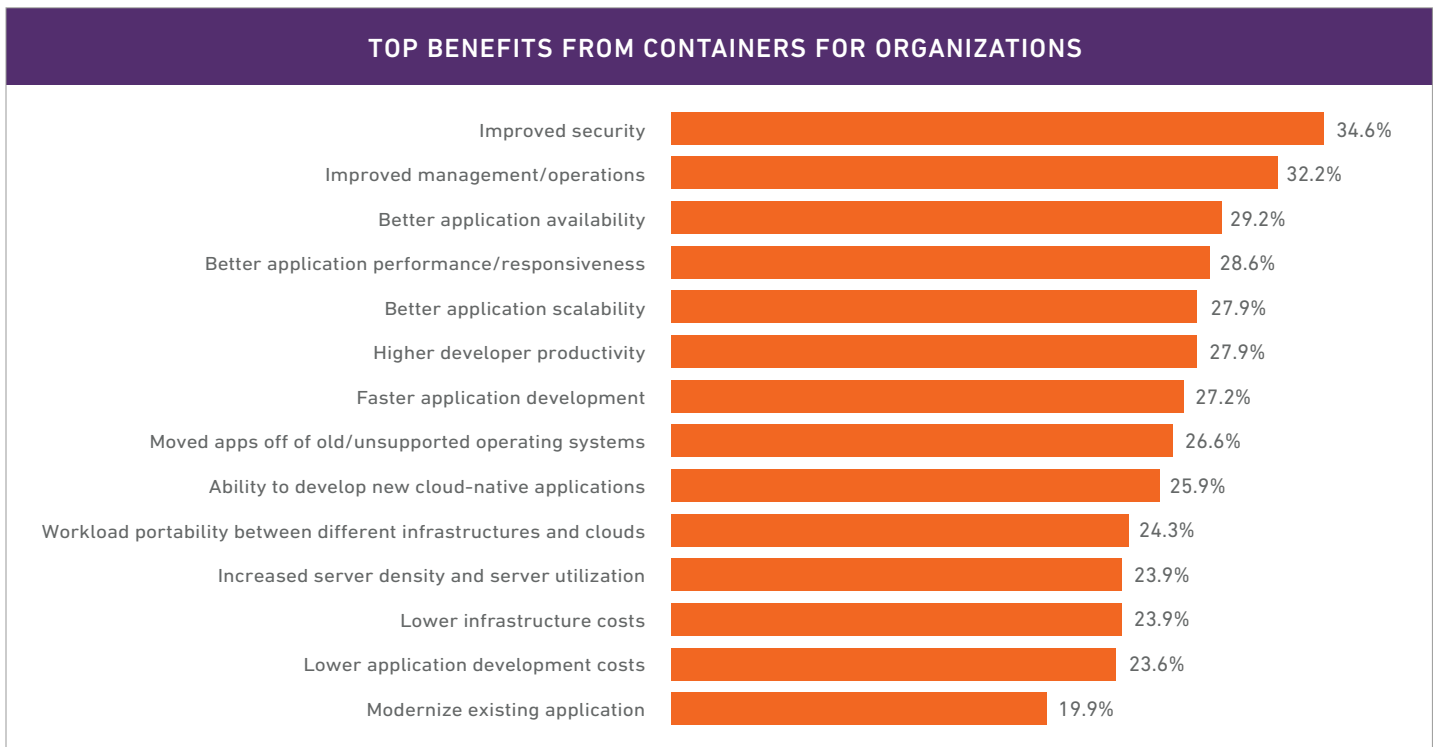| Host Operating System |
|---|

Server

Containers provide the following benefits to developers and DevOps teams:

■ **SPEED**
Container architecture allows nearly instantaneous creation and deletion of containers from existing images.

■ **SCALABILITY**
Containers can be created and operational in seconds to provide additional application processing and capacity.

■ **PORTABILITY**
Like their counterparts in the physical world, the idea behind containers is that they can be easily recreated in other cloud and IT environments. Additionally, they help avoid vendor lock-in.

■ **EFFICIENCY**
Containers leverage, in most cases, the underlying host and host OS, which means the container and the application within aren't burdened by running their own OS, making applications faster and easier to deploy and improving application performance.

PRIMARY DRIVER OF CONTAINER USER BY COMPANY SIZE

44%	20%	18%	10%	8%	1,000—2,499 (n=61)
26%	40%	10%	15%	9%	2,500—4,999 (n=62)
32%	35%	10%	8%	15%	5,000+ (n=62)
33%	32%	12%	11%	10%	TOTAL (n=201)

Legend:
- EFFICIENCY
- HYBRID CLOUD/ CROSS-CLOUD INTEGRATION
- PORATBILITY OF APPLICATIONS
- SERVING DEVELOPER
- SPEED

Source: 451Research, "Hybrid cloud drives growing container production use and disruption," May 2017

IDC did similar analysis on the benefits of containers driving increased adoption (see below). The results show security as the No. 1 benefit of containers. Though we see clear security benefits from using containers, it's apparent that the other benefits— speed and efficiency for developers and DevOps—are integral parts of the overall value proposition. It's not often a technology comes along with so many compelling benefits vs. tradeoffs.

TOP BENEFITS FROM CONTAINERS FOR ORGANIZATIONS

Benefit	Percentage
Improved security	34.6%
Improved management/operations	32.2%
Better application availability	29.2%
Better application performance/responsiveness	28.6%
Better application scalability	27.9%
Higher developer productivity	27.9%
Faster application development	27.2%
Moved apps off of old/unsupported operating systems	26.6%
Ability to develop new cloud-native applications	25.9%
Workload portability between different infrastructures and clouds	24.3%
Increased server density and server utilization	23.9%
Lower infrastructure costs	23.9%
Lower application development costs	23.6%
Modernize existing application	19.9%

Source: IDC

COMMON CONTAINER USE CASES

DevOps and development teams are the primary force driving the adoption of containers. Because of the accelerated time-to-market for deployment of testing and production environments for new applications. Meanwhile, IT may be pushing the use of containers to move legacy applications into the cloud with the intent to refactor them for the cloud in the future.

Though security teams may see the advantages inherent in the use of containers, it's unlikely they would push container usage unilaterally—especially without clear security solutions in place to protect containers—but development and DevOps already see the value of containers and leverage them. Smart security teams would likely want to exploit their full security value in the future.

■ **PRODUCTION DEPLOYMENTS**
According to 451 Research, 52% of enterprises are either in the initial stages or have broadly deployed production applications in containers.

■ **MICROSERVICES DEPLOYMENT**
Containers are particularly ideal for microservices deployments, which break down traditionally monolithic or large-scale application architectures into specialized micro applications.

■ **DEPLOYMENT OF DEV APPLICATIONS FOR TESTING**
Containers allow for rapid deployment of applications under development and testing, eliminating the complications associated with configuring and managing the underlying host OS. The ability to spin containers up and down quickly and easily aligns with the needs of DevOps and developer teams.

■ **"LIFT AND SHIFT" OF LEGACY APPLICATIONS**
Whether refactored or not, deploying legacy applications in containers can accelerate the shift to the cloud, while freeing up costly on-premise resources and footprint.

■ **RUNNING OF TRIALS AND PILOT PROJECTS**
Containers also provide an efficient mechanism to run trials and pilot projects without the additional overhead associated with managing the OS or infrastructure.

CONTAINERS EN MASSE

CONTAINER PLATFORMS

The increase in the adoption of container technology and resulting proliferation of containers means organizations will need the ability to manage it all.

This is where the real value of container platforms comes into the picture. Container platforms provide full lifecycle management of creating, imaging, deploying, and destroying containers. Currently, the top container platforms are Docker, Amazon Elastic Container Service (ECS) for Kubernetes, Kubernetes, Azure Container Service, and Google Container Engine, in order of greatest adoption in 2018 (Source: IDC).

CONTAINER ORCHESTRATION

For organizations pursuing a microservices application architecture, container orchestration tools or orchestrators are critical. Orchestrators automate the underlying container infrastructure to manage and make sense of the scale of containers across your environment. Orchestrators also provide load balancing of the services the containerized applications perform. Organizations select the most appropriate orchestration tool based on the scale and complexity of the containers in their environments, the technical expertise on staff, and other factors. Typical tools include Docker Swarm, Kubernetes, Mesosphere DC/OS, and many others.
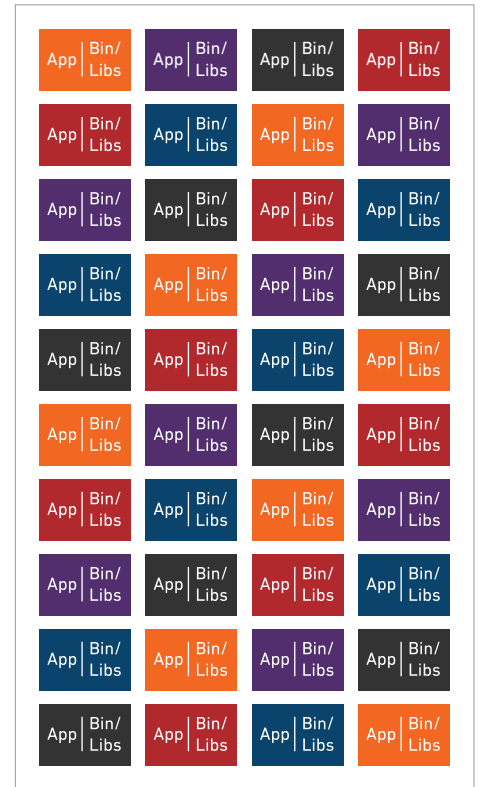
CONCLUSION

Containers represent a clear and compelling value proposition for use by developers, DevOps teams, and even IT. They are a logical evolution of cloud architecture and a go-to technology for a variety of use cases with clear benefits to organizations.

However, containers do represent an expanded attack surface for IT and security teams to secure, working closely with their business colleagues in development and DevOps teams. Though security is trailing the use of containers to date, the good news is that security solutions are quickly evolving to provide coverage for this growing trend.

ABOUT ARMOR

Armor is a cloud security company that takes the complexity out of protecting your data, whether it resides in a private, public, or hybrid cloud—or in an on-premise IT environment. We provide managed security solutions that give you a clear picture of threats facing your organization. This allows us to provide you with the people and security resources to stop attacks before they happen and react quickly and effectively when they do, keeping your data safe and compliant. Wherever you are on your cloud journey, Armor can help. We make cybersecurity simple.

ARMOR