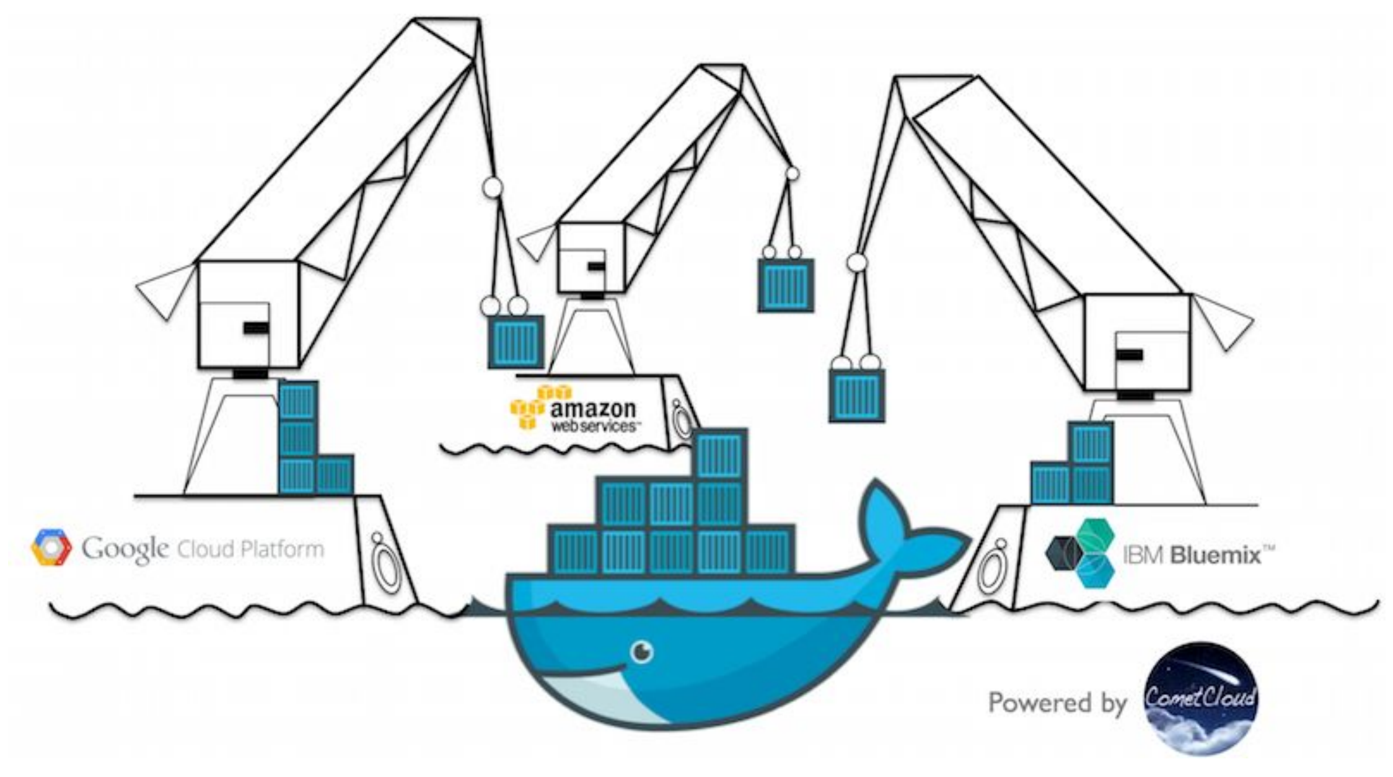
CIMCOR | Ensuring Information Security in a Containerized World

CIMCOR

1 The Rise of Containerization



Containers were born out of issues that arose when software developers started moving applications from one computing environment to another. Virtualization was a tremendous asset, but every time an application was shared via virtualization, the entire OS had to go along with it. **Containers allow developers to build their application and combine it with all of that application's dependencies** - libraries, binaries, configuration files, etc - to create one large package that can be run effectively on Linux and Windows. Because containers run on a minimal OS, they can be multiple orders of magnitude smaller than Virtual Machines, which leads to faster startup times and improved flexibility.

2 Shortage of Security Awareness

according to the National Cyber Security Alliance **more than**

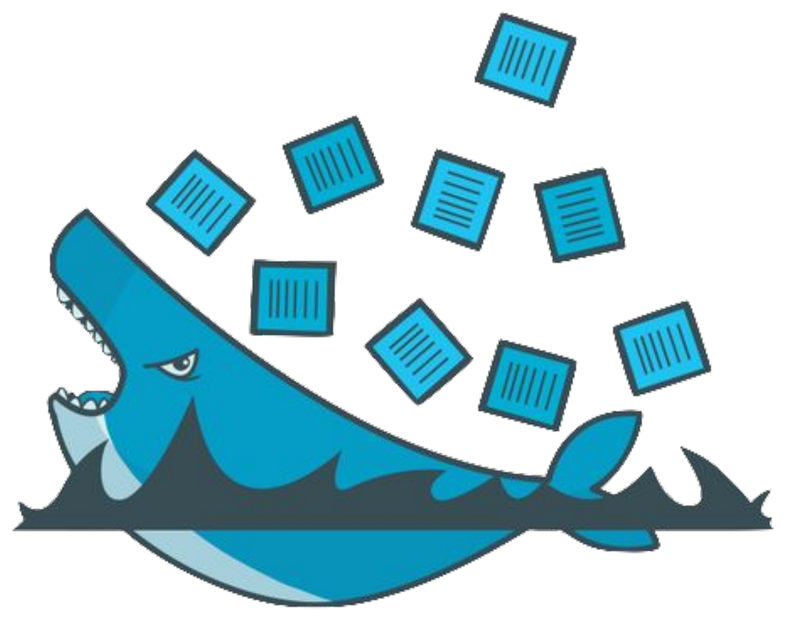
75%

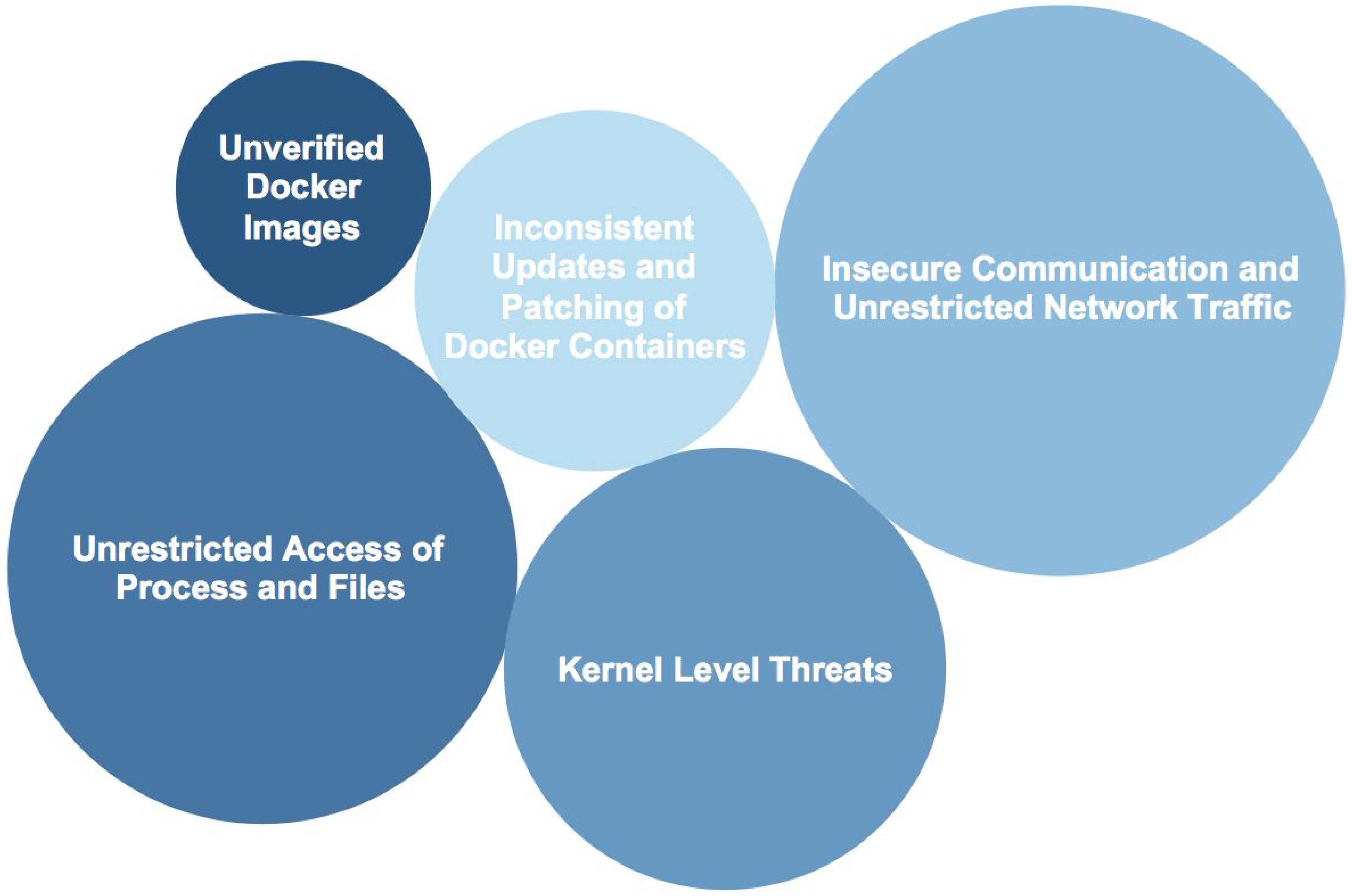
of small business employees leave their computers unsecured

3 Docker Vulnerability Analysis

CVE's	CVSS	Description
CVE-2014-9357	10.0	This vulnerability was identified in Docker Version 1.3.2 which allowed the execution of arbitrary code with root privilege. During the decompression of LZMA (.xz) archives, there was a privilege escalation vulnerability. This vulnerability was patched by version 1.3.3.
CVE-2014-6407	7.5	This vulnerability was identified in Docker Version 1.3.1 which allowed privilege escalation through symlink and hard link traversals found in the Docker's image extraction. This vulnerability was patched by version 1.3.2.
CVE-2015-3630	7.2	This vulnerability was identified in Docker Version 1.6.0 and allowed attackers to bypass security due to weak permissions on the /proc paths. Attackers could access sensitive information and perform unauthorized actions due to the security bypass. This vulnerability was patched by version 1.6.1.
CVE-2014-3499	7.2	This vulnerability was identified in Docker 1.0.0 which indicated that Docker was using "world-readable" and "world-writable" permissions on the management socket. This vulnerability allowed local users to gain root privileges to the local machine. This vulnerability was patched by version 1.0.1.
CVE-2015-3627	7.2	This vulnerability was identified in Docker 1.6 and the Libcontainer version 1.6.0 that allowed a "mount namespace breakout" when a container was respawned. This function created an exploit to allow codes to escape the container. Through this exploit, attackers can create a privilege escalation. This vulnerability was patched in Docker 1.6.1.

4 Top 5 Container Deployment Risks





Unverified Docker Images

Inconsistent Updates and Patching of Docker Containers

Insecure Communication and Unrestricted Network Traffic

Unrestricted Access of Process and Files

Kernel Level Threats

5 The Future of Containerization

Efficiency

Evolution Iteration

Open Source

Sharing Flexibility Secure

Reference:
Docker » Docker : Vulnerability Statistics. (n.d.). Retrieved May 9, 2017, from http://www.cvedetails.com/product/28125/Docker-Docker.html?vendor_id=13534
What is a Container. (2017, May 04). Retrieved May 10, 2017, from https://www.docker.com/what-container#/package_software
OCI Moves into 2017. (n.d.). Retrieved May 05, 2017, from https://www.opencontainers.org/blog/2017/01/23/oci-moves-into-2017

Andy Herman
Full-Time MSIM

Colin Andrade
Full-Time MSIM

Chang (Jay) Liu
Full-Time MSIM

Information School
UNIVERSITY of WASHINGTON