GENERAL DYNAMICS MISSION SYSTEMS

CONFIDENCE in your digital world

Cyber and Electronic Warfare Systems

Protecting Data in A Modern Enterprise
Solution Overview

July 2018

GENERAL DYNAMICS
Mission Systems

Focus of this Session

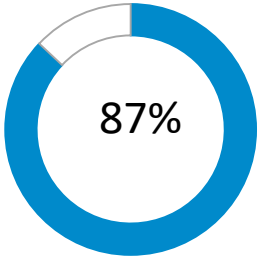
- Red Hat® OpenShift® is powering the move to containers and microservices
- GDMS' PitBull® secure OS enhances solutions like OpenShift® by enabling the processing of information at multiple security levels on a single infrastructure
- The combination of these technologies enables:
  - Easy development and delivery of system components by everyone
  - Flexible scaling of systems through container management
  - More effective use of hardware resources by eliminating parallel hardware strings required for non-MLS security architectures
  - Users to operate in a single, integrated data environment with strong security controls

We are using technology to address the simple problems, letting the humans focus their attention and energy on the operational problems.

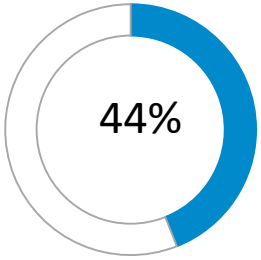
Topics

- Cloud Trends
- Transformation to Containers and Microservices
- Securing Containers with Red Hat® OpenShift®
- Enabling MLS systems with PitBull®
- Secure Cloud Computing
- Multilevel Security (MLS) and Cloud Computing
- Enabling MLS Containers with Red Hat® OpenShift® and PitBull®

IT Leaders: *"Change is Coming"*



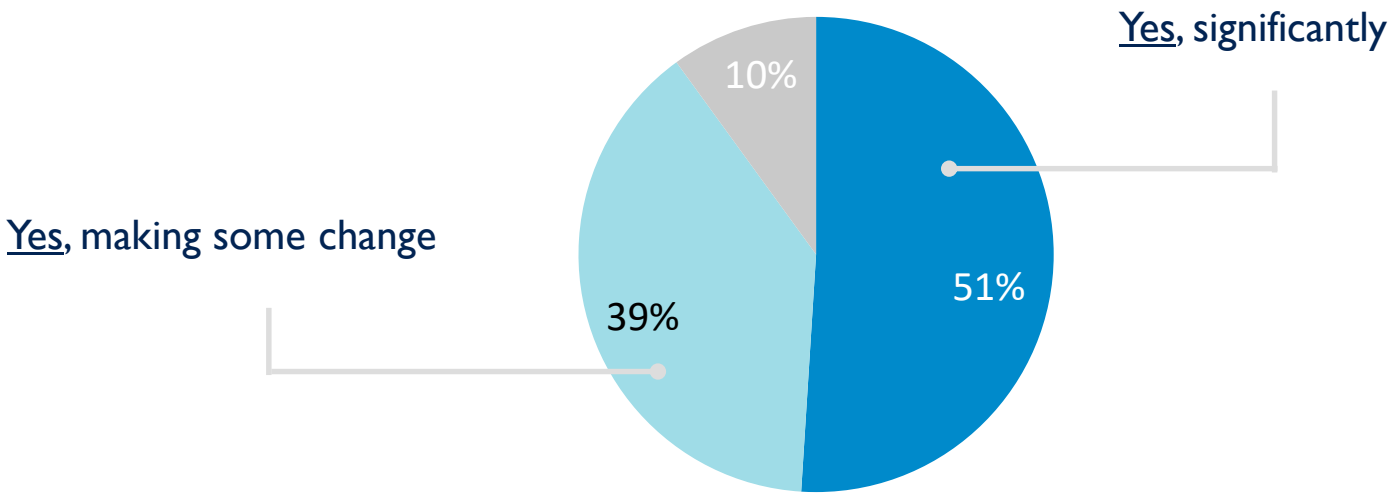
anticipate that their industries will be disrupted by digital trends to a great or moderate extent.



say their organizations are adequately preparing for the disruptions to come.

90% of CEOs are Changing How They Use Technology

Question	Are you changing how you use technology to assess and deliver on wider stakeholder expectations?



GENERAL DYNAMICS
Mission Systems

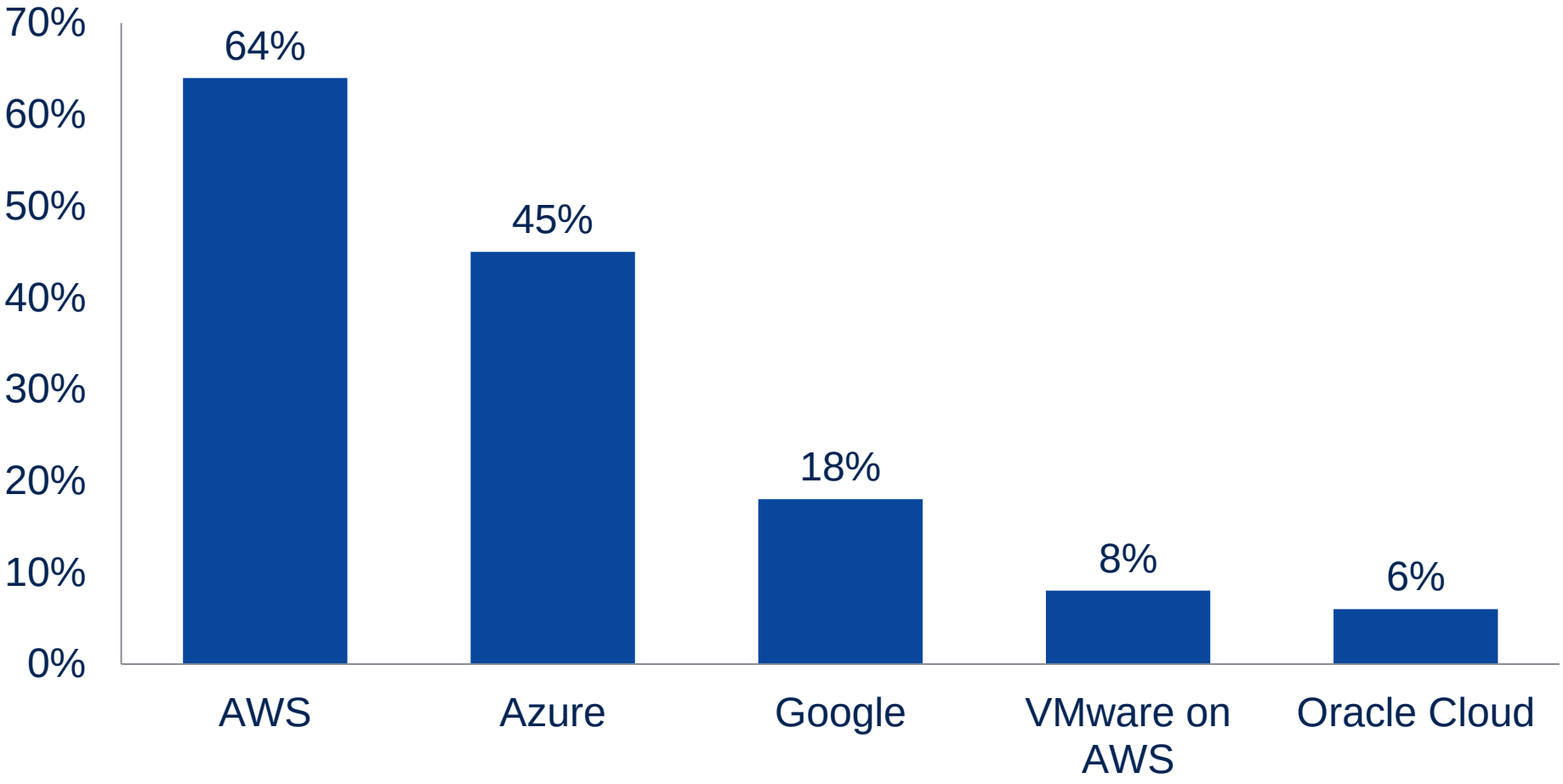
General Cloud Trends

- Ubiquitous
  - 96% of enterprises use the cloud
- Multi-Cloud
  - 81% of enterprises have a multi-cloud strategy
  - Each with an average of 3-5 clouds in use
- Top cloud challenges in 2018
  - Security
  - Managing costs:
    - 1/3 of cloud spend is wasted
    - Focus on optimization

Cloud Trends in the U.S. Government

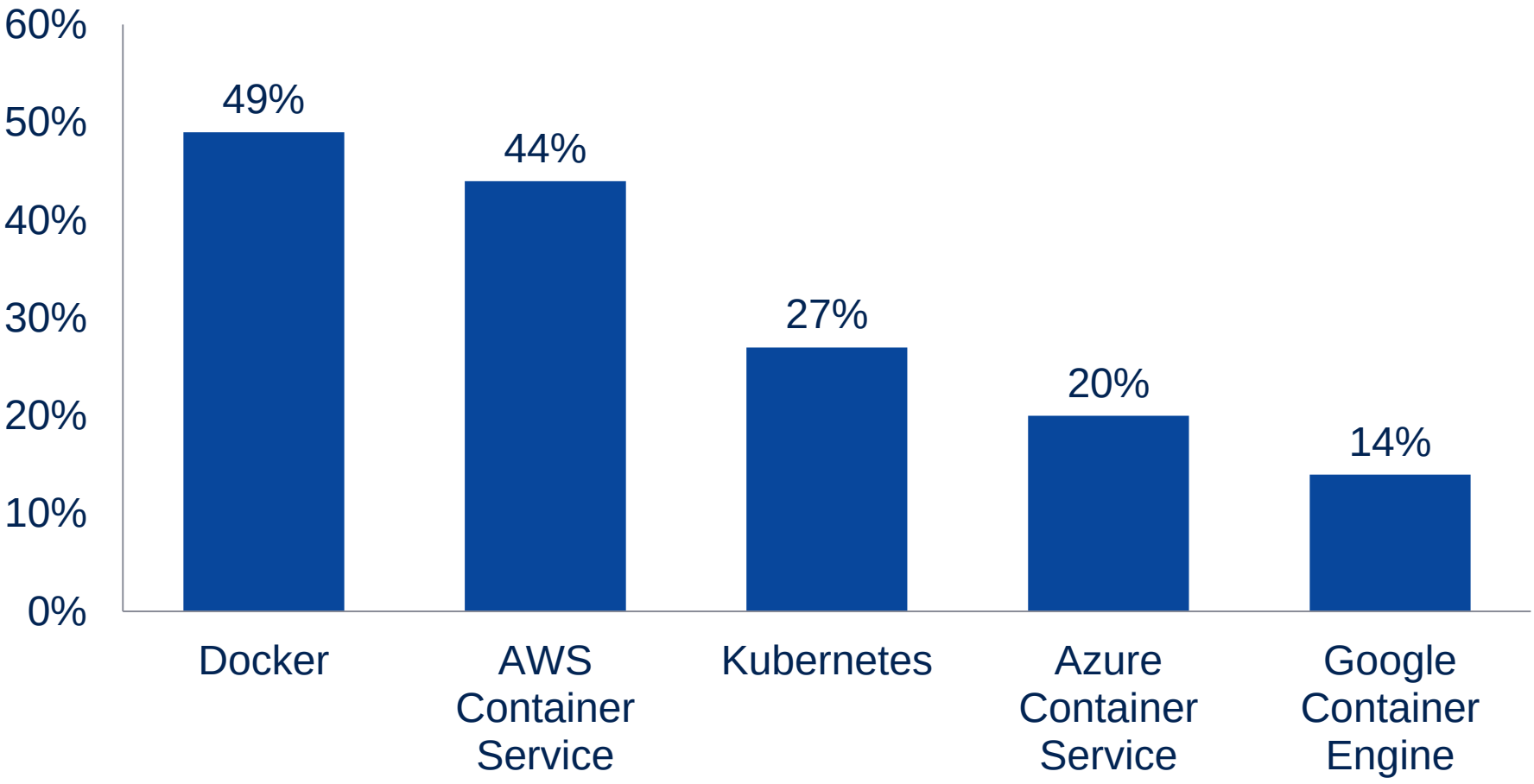
- Executive Order, 05MAY17
  - Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
  - *"Agency heads shall show preference in their procurement for shared IT services, to the extent permitted by law, including email, **cloud**, and cybersecurity services."*
- DoD CIO Memo, 03MAY18
  - Fourth Estate Application and System Cloud Migration
  - *"…[virtualized] workloads resident in Fourth Estate data centers will migrate to **milCloud 2.0**…by the end of the second quarter FY2019…all remaining workloads migrating by the end of 4Q FY 2020."*
  - Impacts >100 data centers

Cloud Trends – Public Cloud Adoption Rates



GENERAL DYNAMICS
Mission Systems

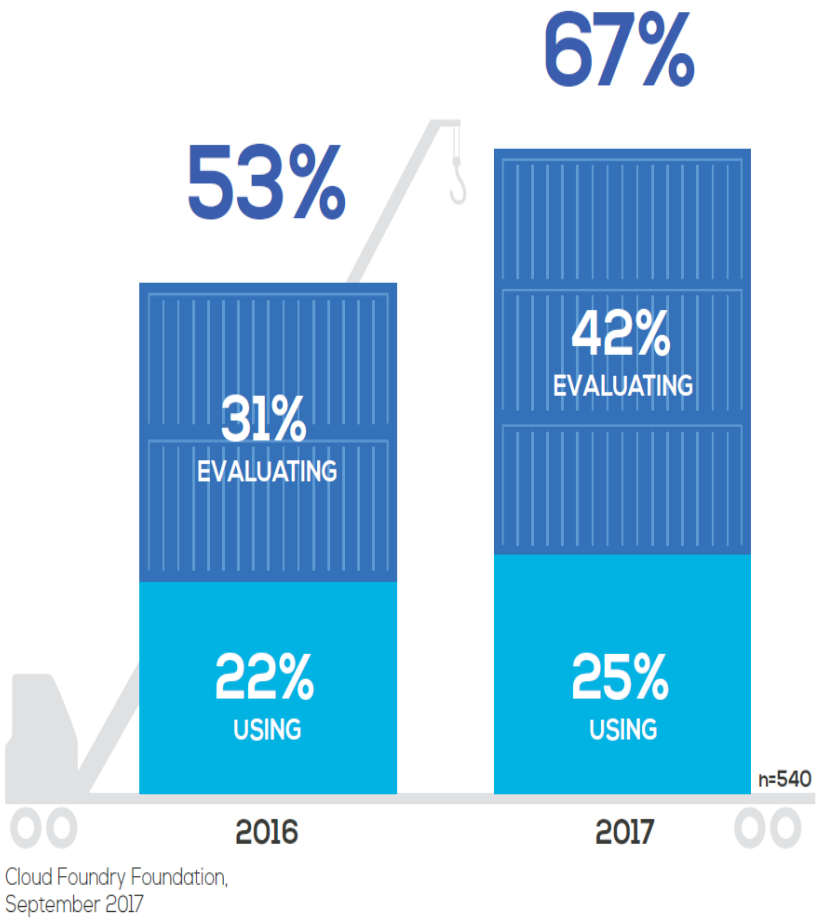
Cloud Trends – Container Engine Market Penetration



GENERAL DYNAMICS
Mission Systems

Container Technology Adoption Rates

- Healthy growth in enterprises evaluating container technology
- Deployment to the production environment is growing at a slower rate
- Managing container resources is cited as a factor in deploying the technology

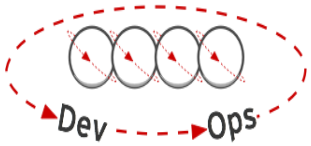


Cloud Foundry Foundation, September 2017

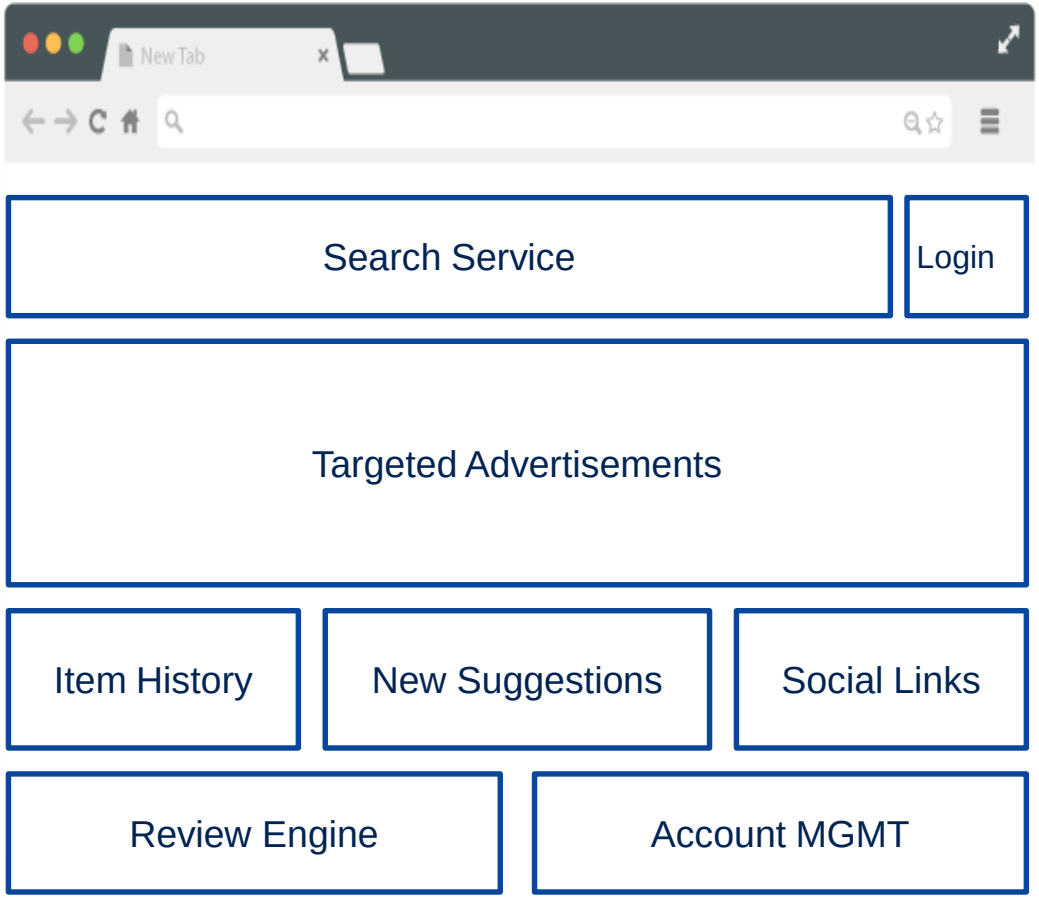
Enabling Microservices with Red Hat® OpenShift®

Production Trends

Development Process	Application Architecture	Deployment & Packaging	Application Infrastructure
Waterfall	Monolithic	Physical Servers	Datacenter
Agile	N-Tier	Virtual Servers	Hosted
DevOps	**Microservices**	**Containers**	**Cloud**



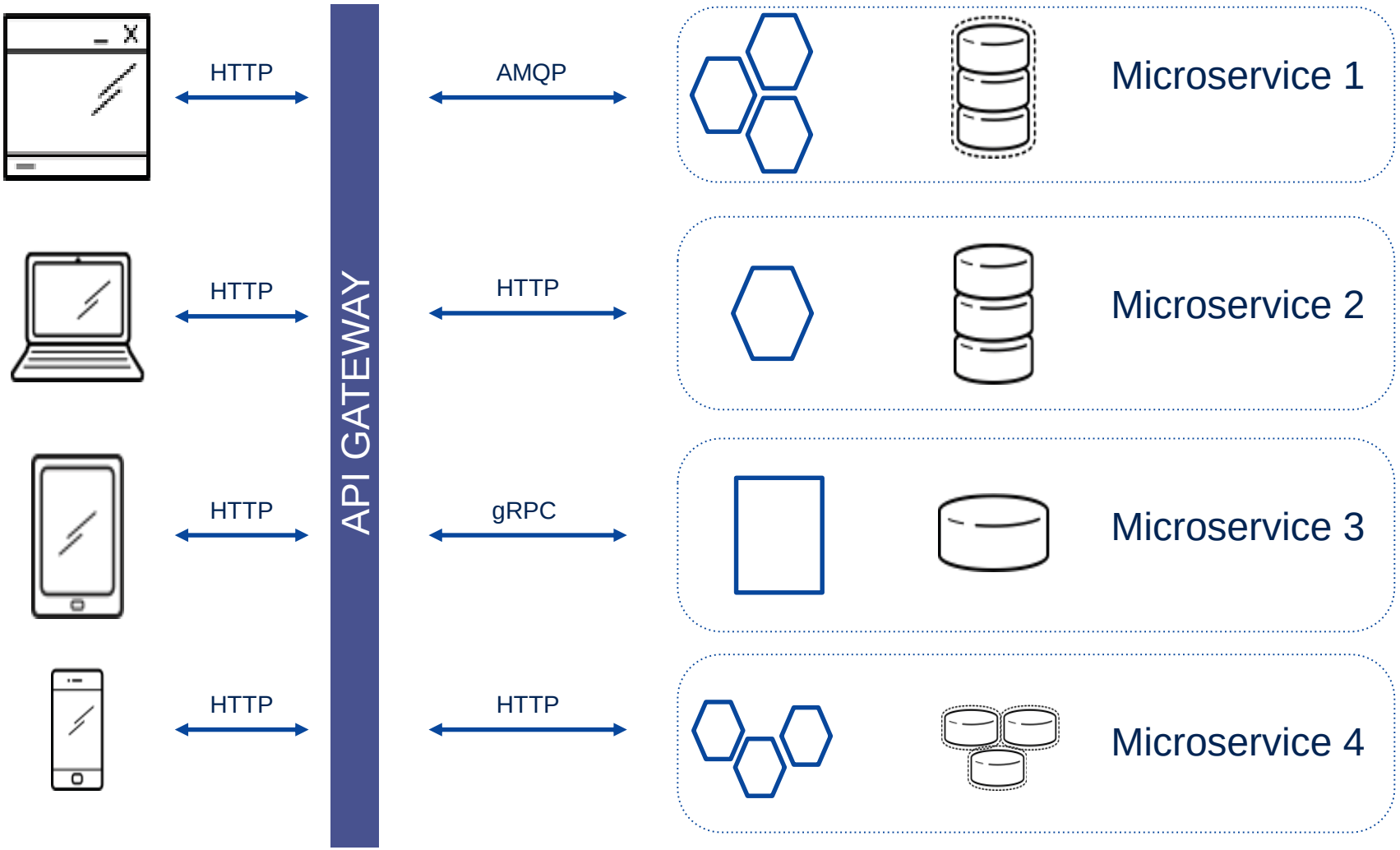
Modern Web Apps



Modern webapps are composed of multiple backend services

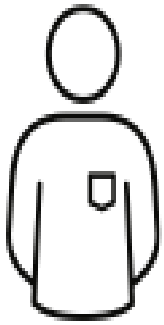
These can be composed in different technologies and languages.

Microservice Architectures



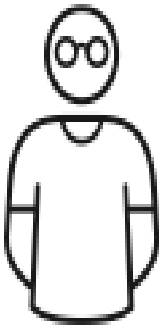
What are Containers?

It Depends Who You Ask



OPERATIONS

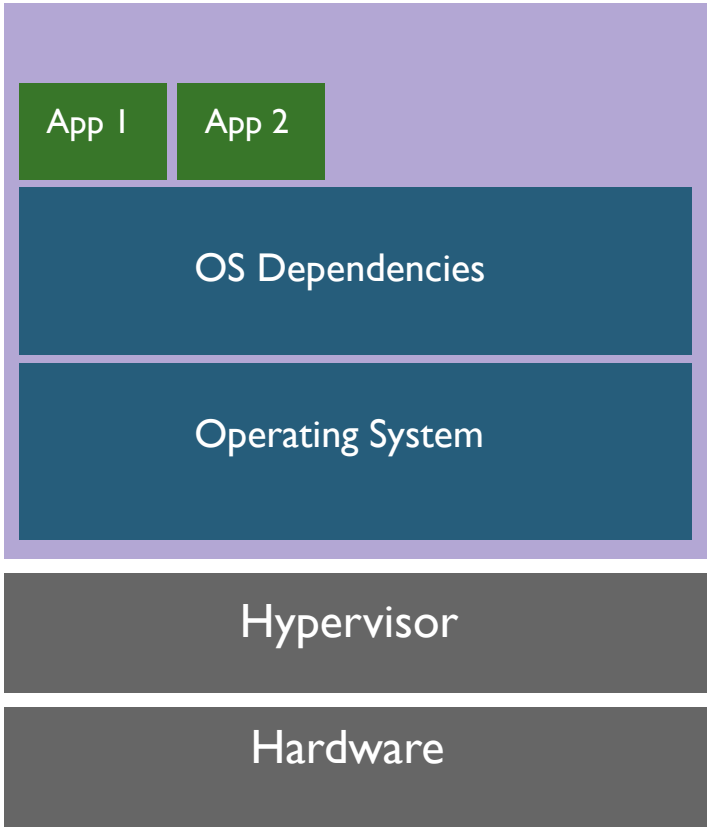
- Application processes on a shared kernel
- Simpler, lighter, and denser than VMs
- Portable across different environments



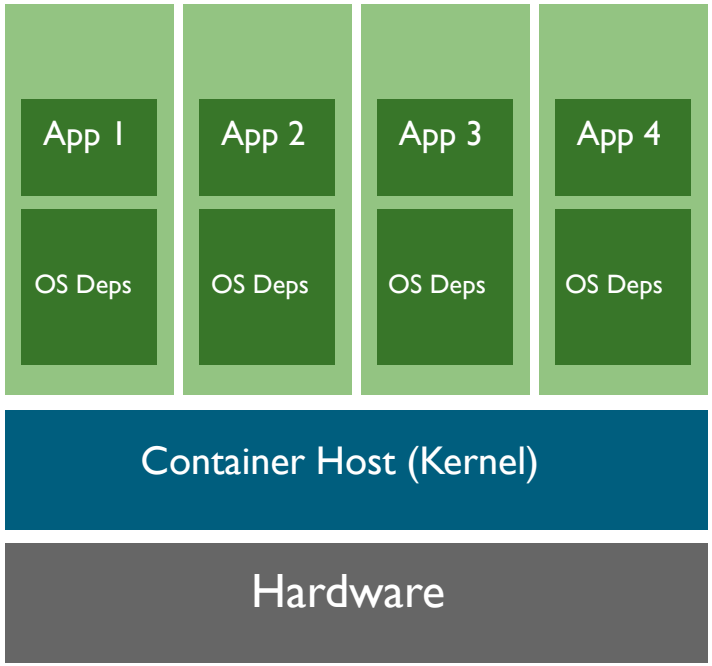
DEVELOPERS

- Package apps with all dependencies
- Deploy to any environment in seconds
- Easily accessed and shared

Virtual Machines vs. Containers



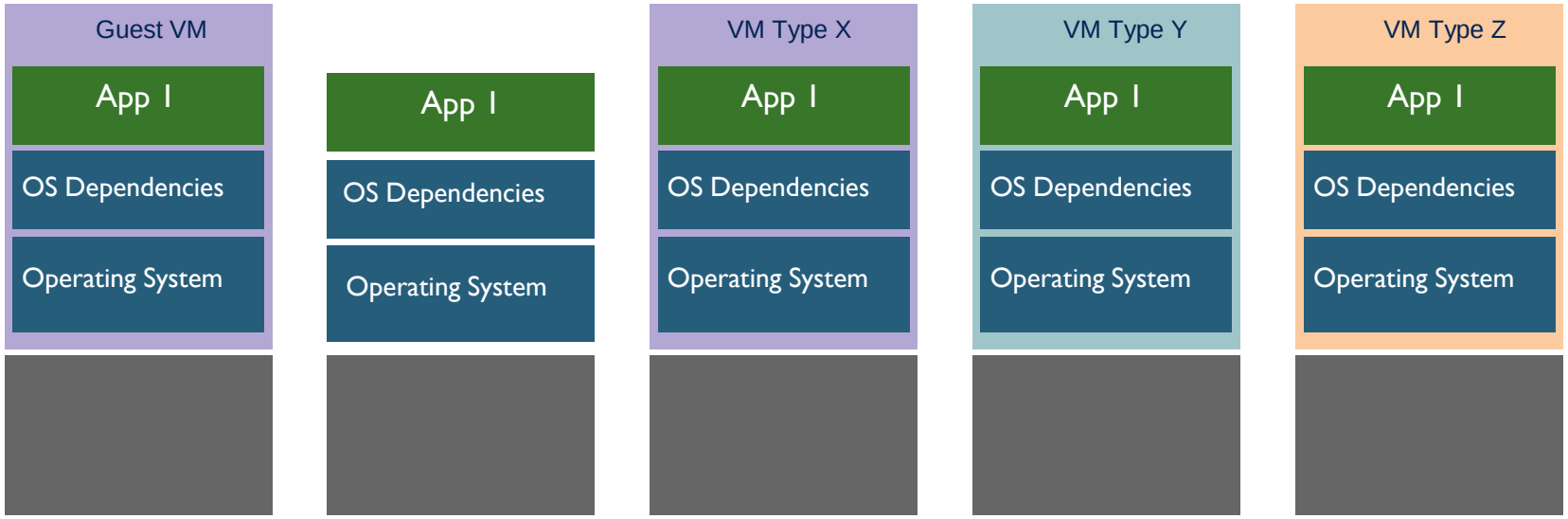
VMs



Containers

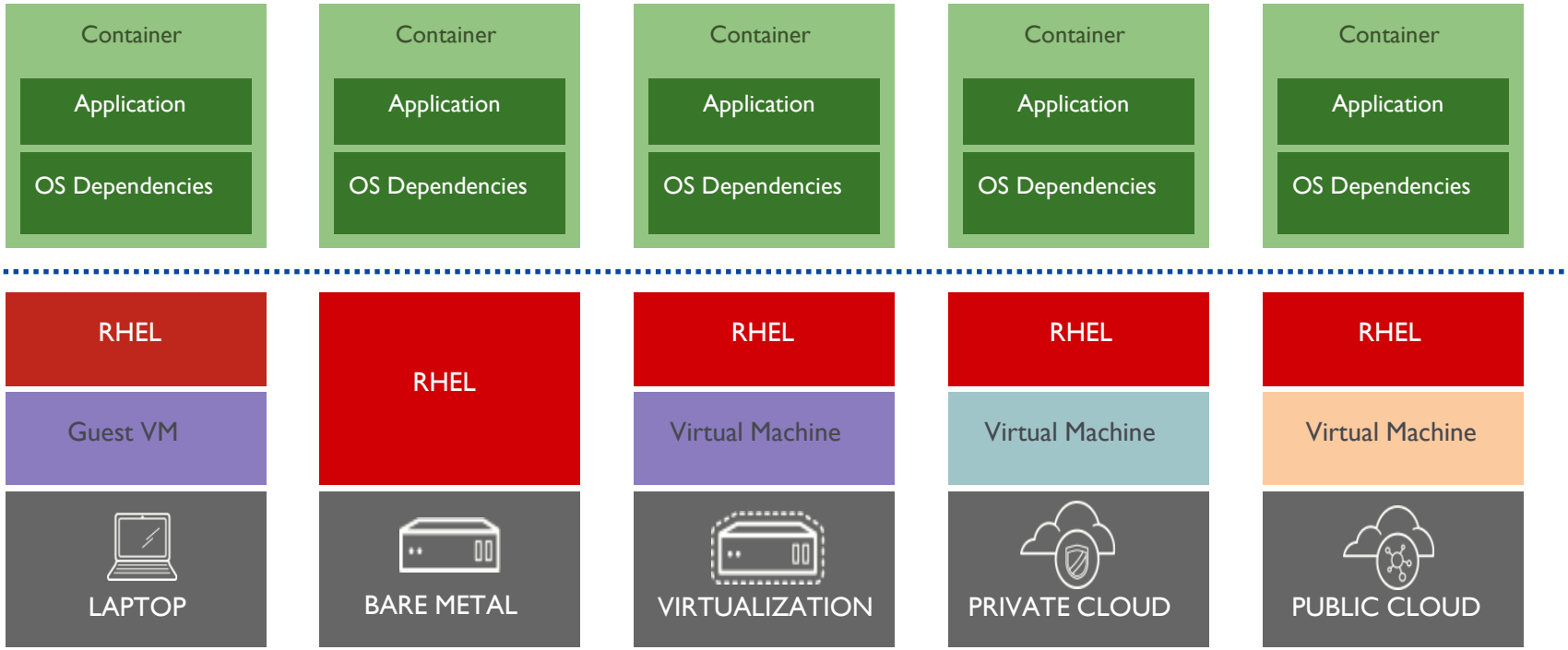
Application Portability with VMs

Virtual machines are NOT portable across hypervisors and do NOT provide portable packaging for applications



Application Portability with Containers

RHEL Containers + RHEL Host = Guaranteed Portability
Across Any Infrastructure



How do we secure containers?

CONTROL

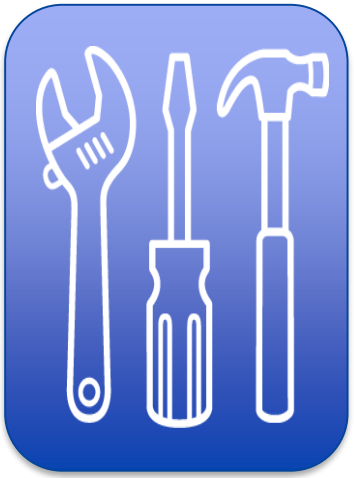
Secure the Pipeline & the Applications

Container Content	CI/CD Pipeline
Container Registry	Deployment Policies

DEFEND

Secure the Infrastructure

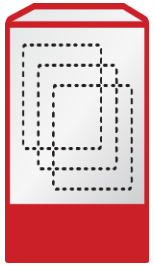
Container Platform	Container Host Multi-tenancy
Network Isolation	Storage
Audit & Logging	API Management



EXTEND

Leverage the Ecosystem

RED HAT® ENTERPRISE LINUX



RED HAT® ENTERPRISE LINUX
Red Hat® CoreOS

THE FOUNDATION FOR SECURE, SCALABLE CONTAINERS

A stable, reliable host environment with built-in security features that allow you to isolate containers from other containers and from the kernel.

Minimized host environment tuned for running Linux containers while maintaining the built-in security features of Red Hat Enterprise Linux..

- Secure OS
- Kernel & User namespaces
- Cgroups
- Capabilities
- R/O Mounts

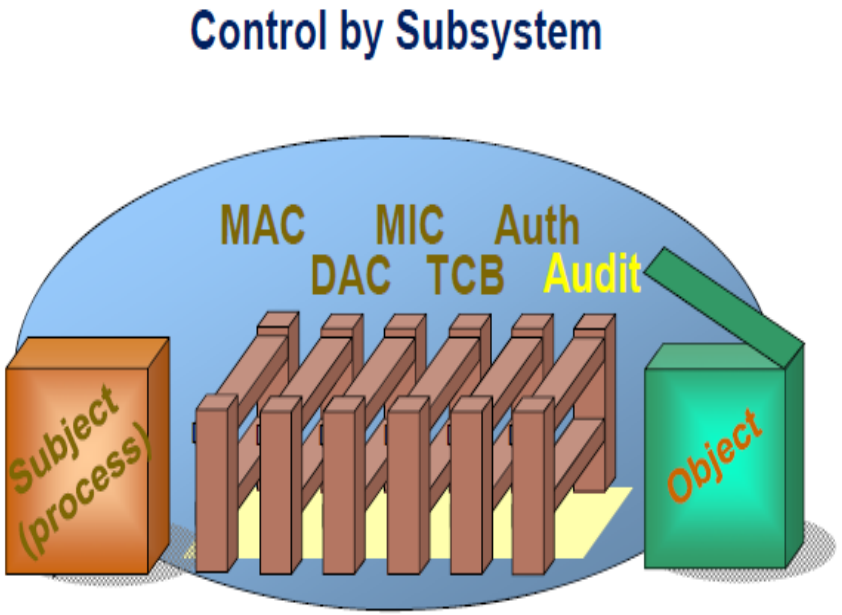
GDMS' PitBull Technology: Enabling Multilevel Security (MLS)

What is PitBull®?

- A trusted operating system (OS)
- A trusted OS refers to how much trust the OS assigns/allows the user
- All trusted OSes employ a security reference monitor that allows/ disallows actions based on mathematical comparison of **subject clearance** vs. **object sensitivity label**
- PitBull® started in 1988 on Compartmented Mode Workstations (CMWs)
- PitBull® is a Linux based OS with sensitivity levels or security labels supporting 32,767 classification levels and 4,095 compartments
- Security labels based on MITRE MTR10649, Revision 1 (DDS-2600-6216-93)
- PitBull® does not require SELinux, but leverages the same Linux Security Modules (LSM) framework SELinux uses

PitBull® Security Goal

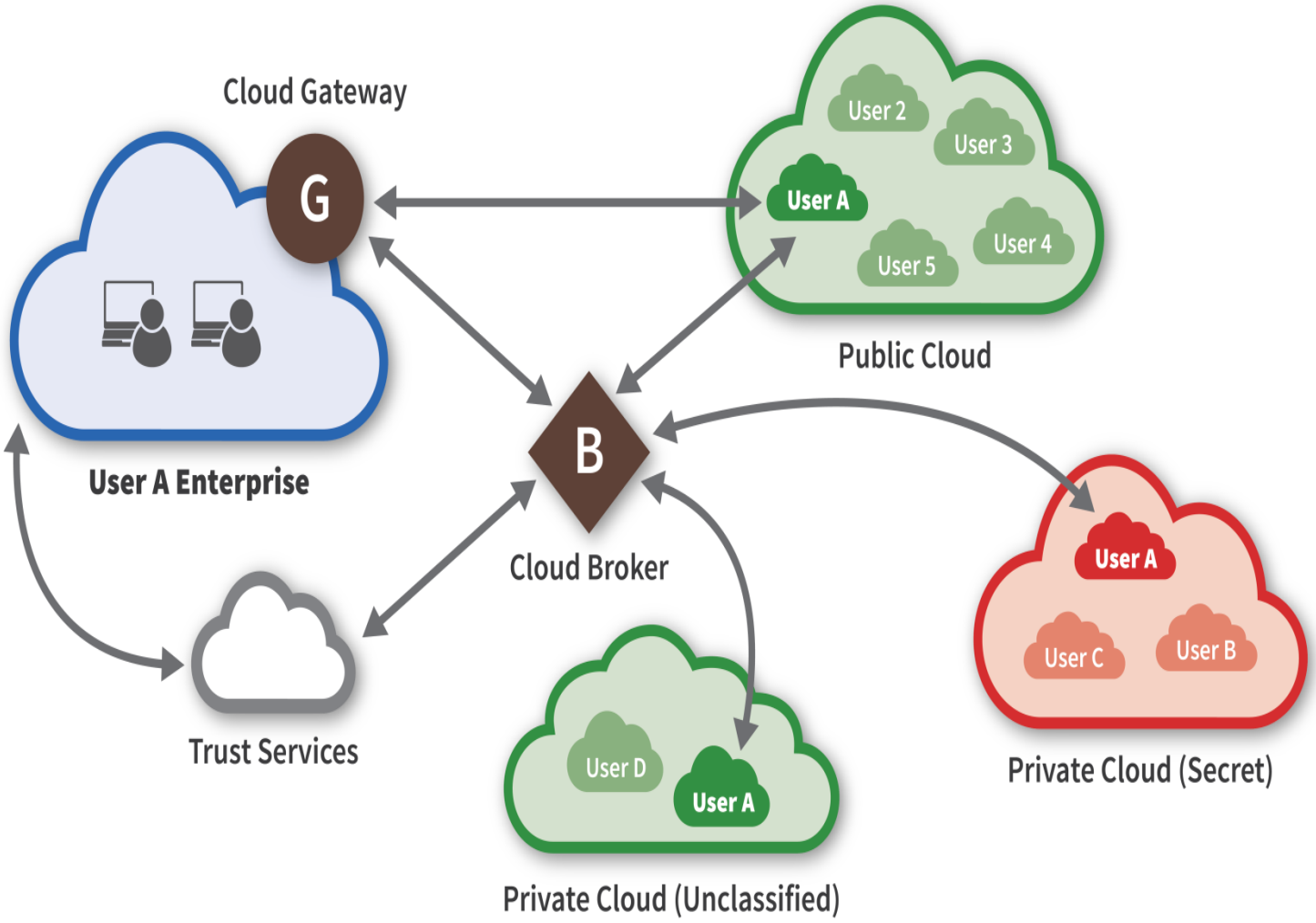
- Overall Goal of PitBull security:
  - limit damage by rogue programs
  - limit damage by administrators and rogue users
  - control data flow
- How PitBull does that:
  - compartmentalizes system (MAC)
  - grants processes minimal privileges
  - grants users minimal authorizations
  - protects Trusted Computing Base



GENERAL DYNAMICS
Mission Systems

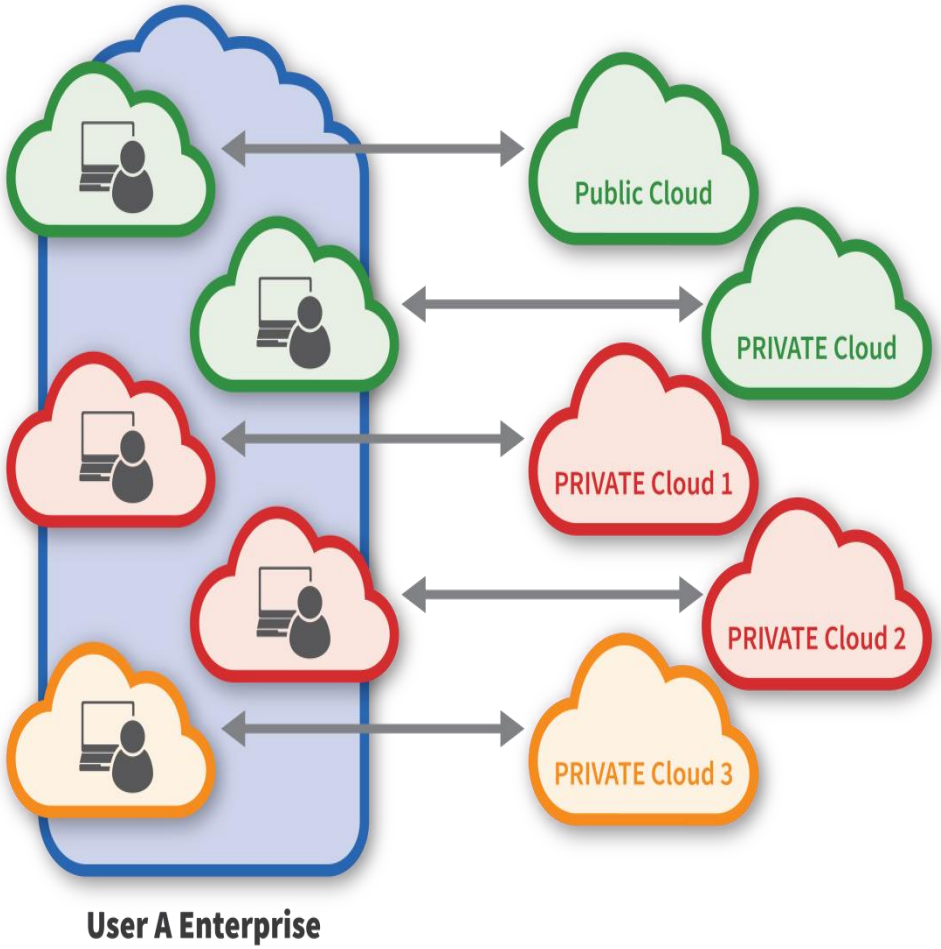
Secure Clouds – Multilevel Security (MLS) Use Case

Cloud Security – Shared Resources



GENERAL DYNAMICS
Mission Systems

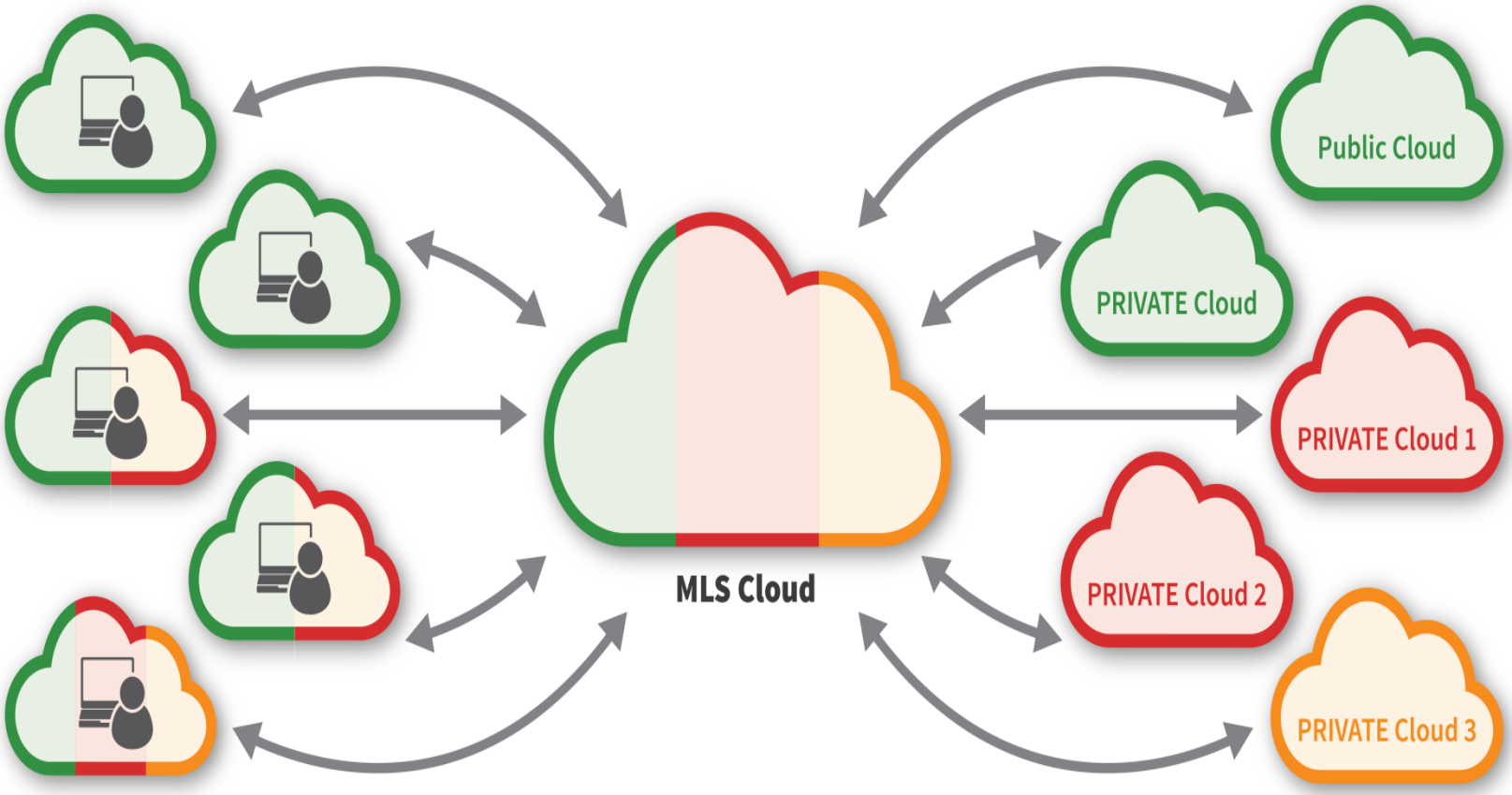
Secure Clouds Today – One Level at a Time



- Access to one security level
- Data fusion is difficult
- Clouds don't exist for all security levels, compartments, COIs, releasabilities
- Inefficient use of resources

GENERAL DYNAMICS
Mission Systems

MLS Cloud with PitBull and OpenShift



GENERAL DYNAMICS
Mission Systems

MLS Container Benefits

- Easy development and delivery of system components
- Flexible scaling of systems via container management
- More effective use of hardware resources
  - Dense service packing on hardware with containers
  - Eliminating parallel hardware strings required for non-MLS security architectures
- Users to operate in a single, integrated data environment with strong security controls
  - Access to services and data across multiple compartments, security levels, communities of interest, and departments
  - Rich fusion environment across security levels

MLS Cloud Solutions

- Red Hat®'s OpenShift® provides secure container support and orchestration for clouds and microservices
- GDMS' PitBull provides a Multilevel Security trusted operating system with a proven 25+ year track record
- Red Hat® + GDMS Strategic Partnership brings a juggernaut in compute infrastructure together with the leader in MLS trusted computing and security
- What can we do for you?

Market Trends in Data Security

- Data breaches increasing public awareness
- Regulations in Government, Finance, and Healthcare markets
- Cybersecurity insurance
- Corporate IP theft is a high-priority issue

Security and privacy by design

Severe penalties

- Moving to the Cloud implies “losing Control of our Data”
- Nation-state cyber-security threat is critical
- Insider threat high priority
- Data leaks and breaches risk reputation and careers

Shared Problems, Common Needs

Problem Space	Desired Capability
1. Can't protect my data in a modern enterprise environment	• Protection of IP and high value assets regardless of where it resides (multiple clouds, data center, enterprise) • Controlled access anytime, anywhere, from any device (managed, unmanaged, BYOD: enterprise, partners, customers) • Dynamically adjust to changing business requirements
2. Can't tell where, when, or how my data is being used	• Proper use of IP and high value assets by employees and external collaborators • Revoke access as dictated by business needs • Lock down access to lost files or leaked information
3. People want to effectively do their jobs, even if it means bypassing security measures	• Proactive prevention of intentional and unintentionally leaks of information (e.g., Shadow IT) • Low friction, nonintrusive protections and administration
4. Need enhanced governance of a borderless enterprise (cloud)	• Visibility, control, and enforcement of cloud-based services • Threat protection against data loss, user behaviors • No drop in compliance