



Cloud Security: Frameworks and Enforcement

SHAWN WELLS

Director, Innovation Programs, U.S. Public Sector

shawn@redhat.com || 443-534-0130

35 MINUTES, 2 GOALS

35 MINUTES, 2 GOALS

1. Cloud Security Lifecycle

- Government Certification & Accreditation Models
- Case Study: Westfield's MADFW/MITE

35 MINUTES, 2 GOALS

1. Cloud Security Lifecycle

- Government Certification & Accreditation Models
- Case Study: Westfield's MADFW/MITE

2. Enabling Security Technologies

- Security Content Automation Protocol (SCAP)
- Containers

WHAT IS THE CLOUD?

- Infrastructure as a Service (IaaS)
 - CIA C2S, NSA MACHINESHOP, ARC-P, Westfield's MITE

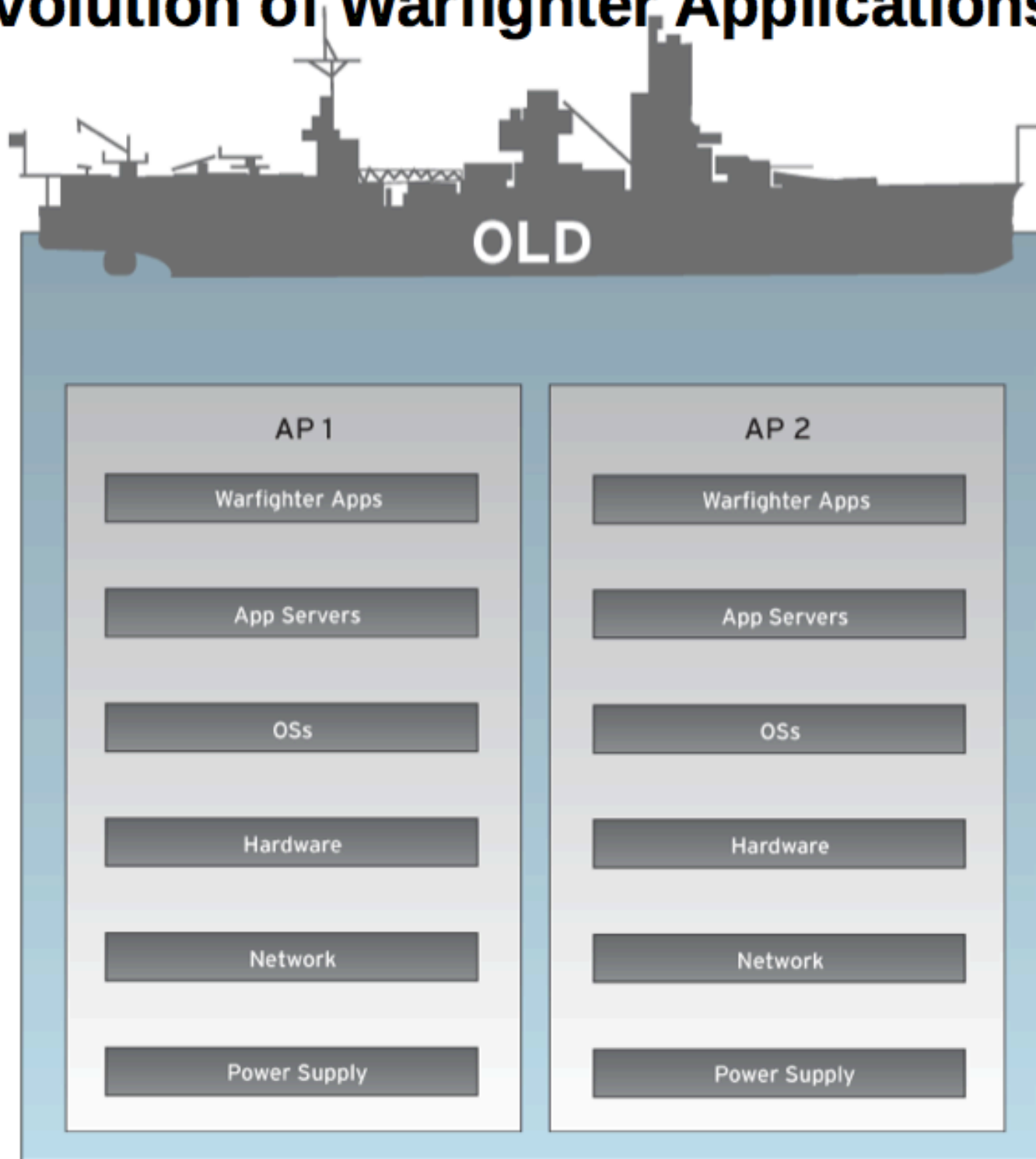
WHAT IS THE CLOUD?

- Infrastructure as a Service (IaaS)
 - CIA C2S, NSA MACHINESHOP, ARC-P, Westfield's MITE
- Platform as a Service (PaaS)
 - DLT CODEvolved, Autonomic ARCWRX

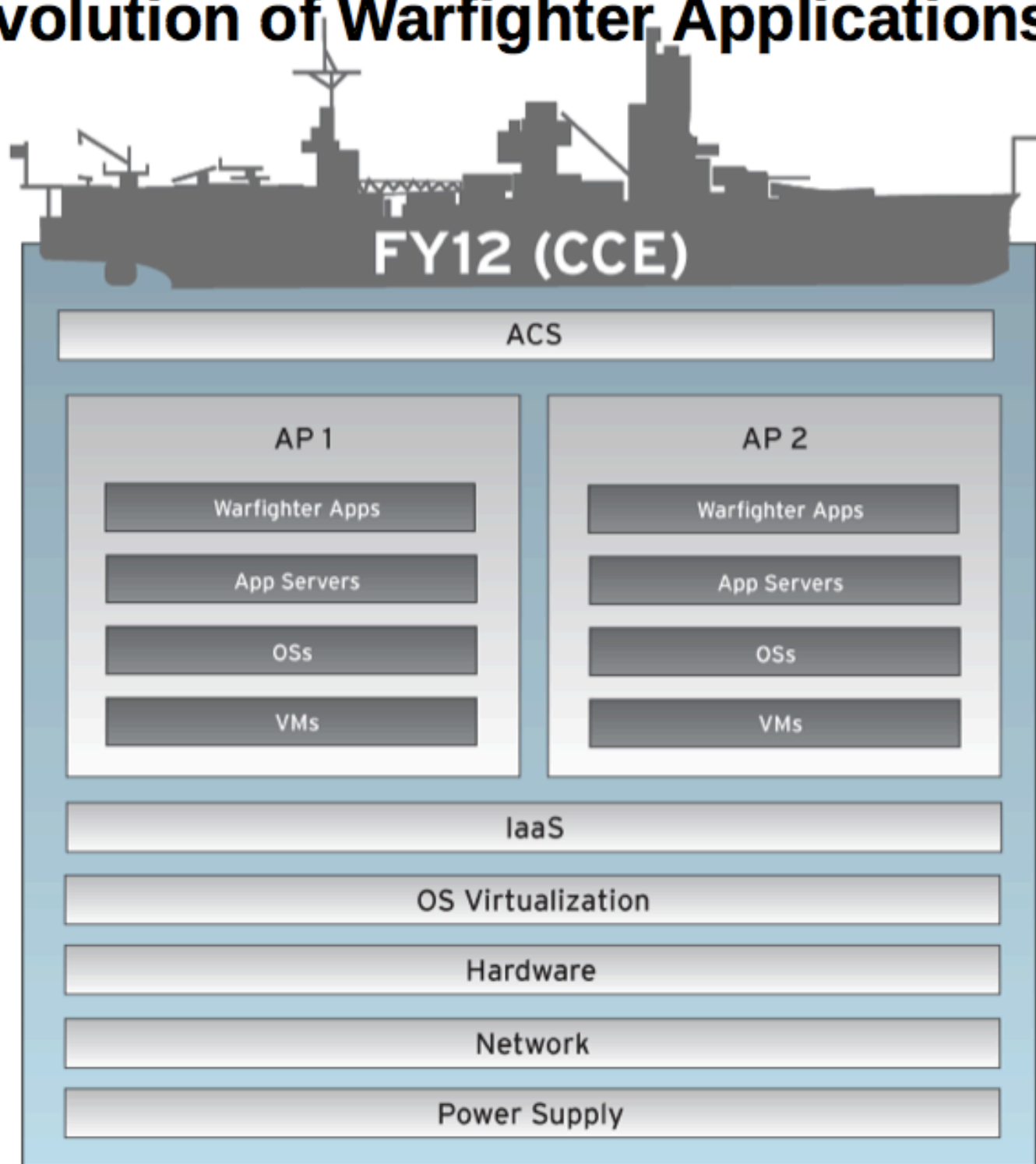
WHAT IS THE CLOUD?

- Infrastructure as a Service (IaaS)
 - CIA C2S, NSA MACHINESHOP, ARC-P, Westfield's MITE
- Platform as a Service (PaaS)
 - DLT CODEvolved, Autonomic ARCWRX
- Software as a Service (SaaS)
 - salesforce.com

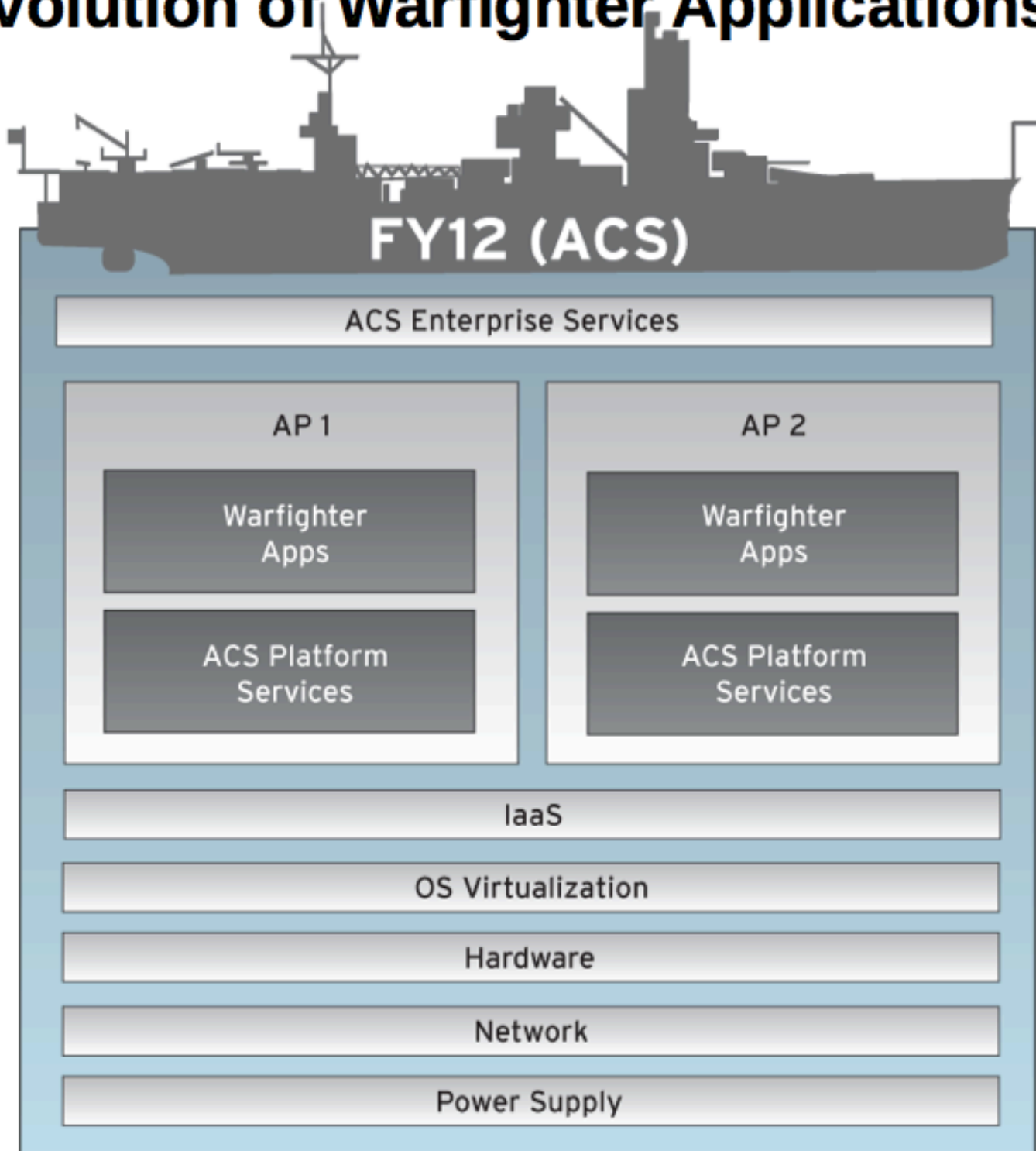
Evolution of Warfighter Applications



Evolution of Warfighter Applications



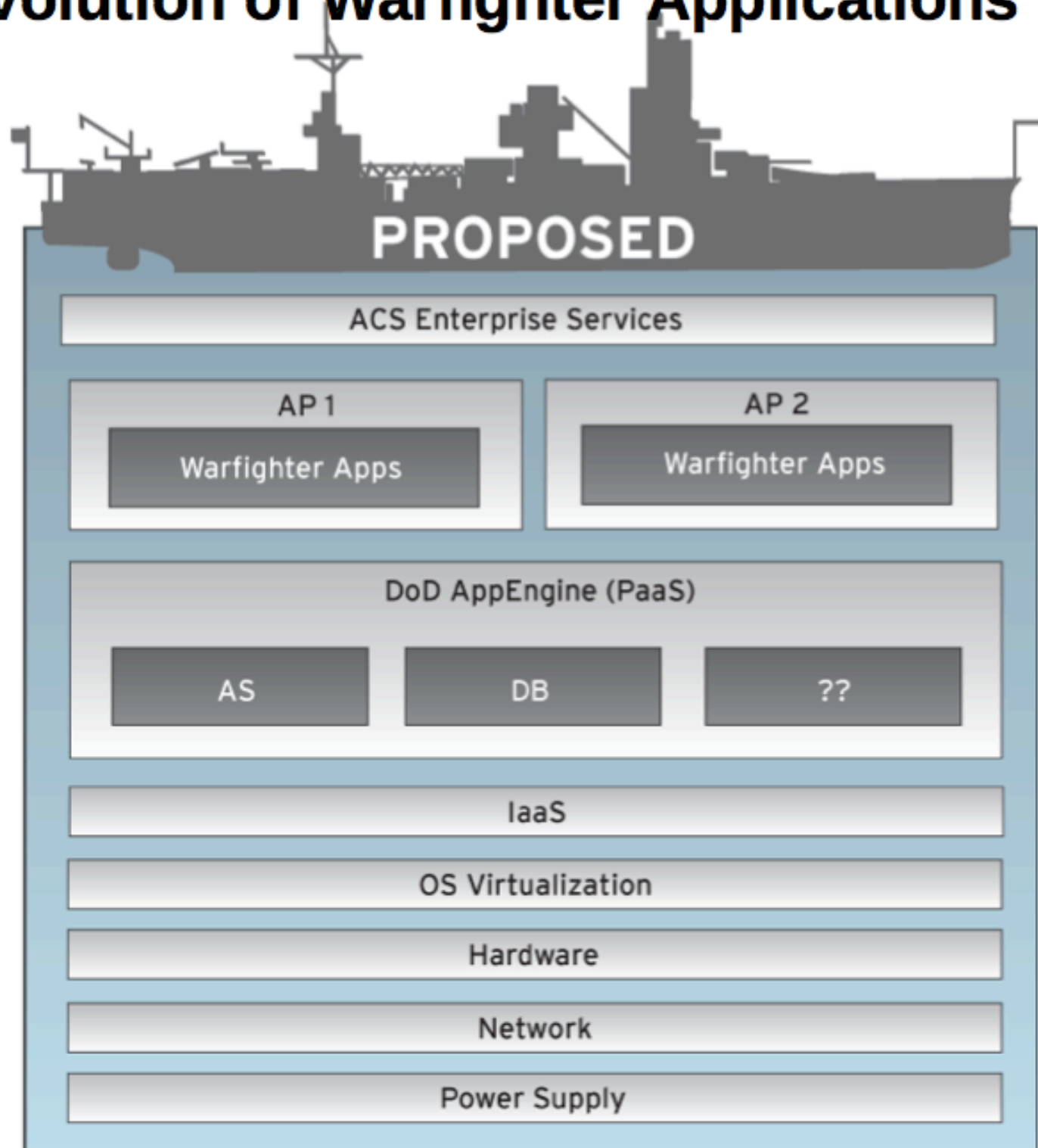
Evolution of Warfighter Applications



Evolution of Warfighter Applications

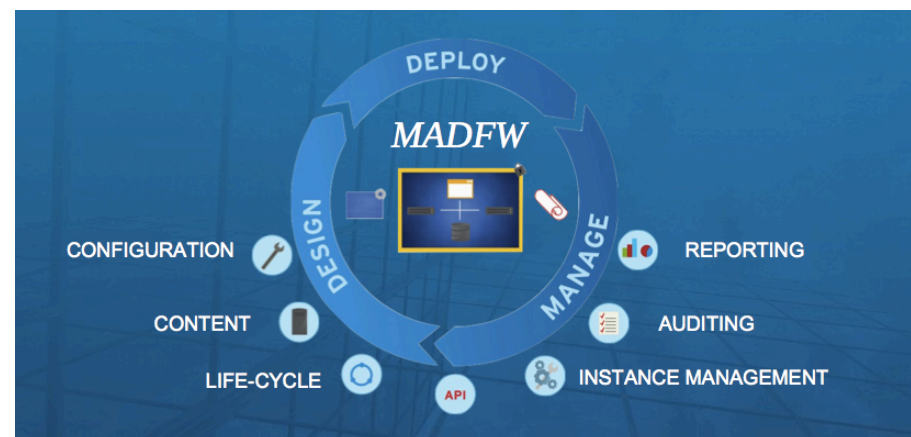
PLATFORM SERVICES	PAAS
App providers build to vendor products	App providers build to DoD standard
Changing middleware vendor requires work from all app providers	Changing middleware vendor is invisible to all app providers
Static scaling	Dynamic scaling
Makes it easier for app providers to build C&A'd environments	Removes need for app provider to build C&A'd environments
Build / deploy apps in months / years	Build / deploy apps in days
RHEL+JBoss, Windows+BEA Solaris+Oracle	Google AppEngine

Evolution of Warfighter Applications



IaaS Case Study: Westfield's MADFW

- Also known as MITE, falls under MID
- Development environment for ~117 tenants
- Anything beyond operating system is responsibility of tenant (applications, continuous monitoring, etc)
- ICD 503, High/Low/Low



Continuous Monitoring

- NIST 800-53, 800-137, and many other regulations require continuous monitoring
- We've been using the SCAP Security Guide
 - Large body of Linux security controls
 - Logically grouped into profiles (e.g. DoD STIG, FISMA Moderate, C2S...)

<https://fedorahosted.org/scap-security-guide/>

Contributors Include . . .



Control Tailoring

The screenshot shows a window titled "Tailoring 'Common Profile for General-Purpose Fedora Systems [TAILORED]'". The window contains a tree view of configuration items and two property panels on the right.

Tree View:

Title	Type	ID
[-] Guide to the Secure Configuration of Fedora rel...	Benchmark	FEDORA-19
[+] [✓] Introduction	Group	intro
[-] [✓] System Settings	Group	system
[-] [✓] Account and Access Control	Group	accounts
[-] [✓] Protect Accounts by Restricting Pa...	Group	accounts-res...
[+] [✓] Verify Proper Storage and Exist...	Group	password_st...
[-] [✓] Set Password Expiration Param...	Group	password_ex...
[✓] Set Password Maximum Age	Rule	accounts_ma...
[✓] Set Password Minimum Age	Rule	accounts_min...
[✓] Set Password Minimum Leng...	Rule	accounts_pas...
[✓] Set Password Warning Age	Rule	accounts_pas...
[+] [✓] Restrict Root Logins	Group	root_logins
[+] [✓] Installing and Maintaining Software	Group	software

Profile Properties:

- ID: common_tailored
- Title: Common Profile for General-Purpose Fedora Systems [TAILORED]

Selected Item Properties:

- Title: <no item selected>
- ID: (empty)
- Description: (empty text area)

Sample Output

XCCDF results

Rule Results Summary

pass	fixed	fail	error	not selected	not checked	not applicable	informational	unknown	total
7	0	4	2	0	4	0	0	0	17

Title	Result
Ensure gpgcheck Enabled In Main Yum Configuration	pass
Ensure gpgcheck Enabled For All Yum Package Repositories	pass
Direct root Logins Not Allowed	notchecked
Restrict Virtual Console Root Logins	error
Restrict Serial Port Root Logins	error
Restrict Web Browser Use for Administrative Accounts	notchecked
Ensure that System Accounts Do Not Run a Shell Upon Login	pass
Verify Only Root Has UID 0	pass
Root Path Must Be Vendor Default	notchecked
Prevent Log In to Accounts With Empty Password	fail
Verify All Account Password Hashes are Shadowed	pass
All GIDs referenced in /etc/passwd must be defined in /etc/group	notchecked
Verify No netrc Files Exist	pass
Set Password Minimum Length in login.defs	fail
Set Password Minimum Age	fail
Set Password Maximum Age	fail

Save XCCDF Result

Save ARF

Open HTML report

Save HTML report

Close

SCAP Content Repositories

NIST maintains SCAP content repository for U.S. Government. Plenty of non-Linux content!

<http://web.nvd.nist.gov/view/ncp/repository>

MADFW v2: PaaS (via containers)

- Think of the containers as boxes, nodes as the truck
- We don't care what's inside the box, it's just cargo



Multi-tenancy



RHEL

HYPERVISOR (RHEV, OpenStack, KVM, even VMWare...)

Multi-tenancy



system_u:system_r:svirt_t:s0:c379,c680

system_u:system_r:svirt_t:s0:c41,c368

RHEL

HYPERVISOR (RHEV, OpenStack, KVM, even VMWare...)

Multi-tenancy

```
root@server3:~  
File Edit View Search Terminal Help  
[root@server3 ~]# ls -alZ /var/lib/nova/instances/c7bab5f0-f61e-445e-ab62-2c6b6fd11e04/  
drwxr-xr-x. nova nova system_u:object_r:nova_var_lib_t:s0 .  
drwxr-xr-x. nova nova system_u:object_r:nova_var_lib_t:s0 ..  
-rw-rw----. qemu qemu system_u:object_r:svirt_image_t s0:c379,c680 console.log  
-rw-r--r--. qemu qemu system_u:object_r:svirt_image_t s0:c379,c680 disk  
-rw-r--r--. qemu qemu system_u:object_r:svirt_image_t s0:c379,c680 disk.config  
-rw-r--r--. nova nova system_u:object_r:nova_var_lib_t:s0 libvirt.xml  
[root@server3 ~]# ls -alZ /var/lib/nova/instances/104de82a-61a1-4d1b-9207-95174313ba21/  
drwxr-xr-x. nova nova system_u:object_r:nova_var_lib_t:s0 .  
drwxr-xr-x. nova nova system_u:object_r:nova_var_lib_t:s0 ..  
-rw-rw----. qemu qemu system_u:object_r:svirt_image_t s0:c41,c363 console.log  
-rw-r--r--. qemu qemu system_u:object_r:svirt_image_t s0:c41,c363 disk  
-rw-r--r--. qemu qemu system_u:object_r:svirt_image_t s0:c41,c363 disk.config  
-rw-r--r--. nova nova system_u:object_r:nova_var_lib_t:s0 libvirt.xml  
[root@server3 ~]# █
```

**WE CAN DO MORE
WHEN WE WORK
TOGETHER**

