# AUTOMATING SECURITY IN THE CLOUD AND DATACENTER

**The views expressed in this presentation are those of the author(s) and do not necessarily reflect the official policy or position of the Air Force, the Department of Defense, or the U.S. Government.**

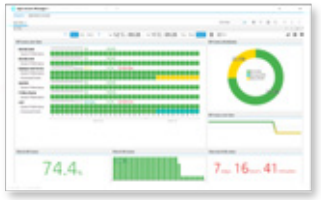
Jeff Hart
Chief Technologist
M2 Technology

# Automated Security = Automated Everything

Provisioning Users, Servers, Applications, Network Devices, Storage

Patching

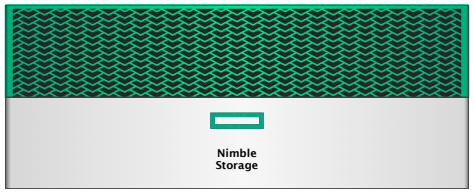
Configuration Management

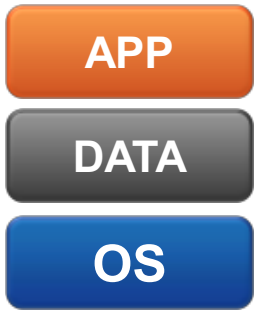


Testing – Functional, Load, and Security

Reporting

Service Management Processes





M2 TECHNOLOGY

# Automated IT and Security Operations

- IT Automation is Good
- Security Automation is Better
- DevSecOps is Best

- Automation requires testing
- Automation needs protection

Automating security improves security posture and reduces costs

*Gratisography*

M2 TECHNOLOGY

# Why Automated Security and DevSecOps?

## Better | Cheaper | Faster

**Projects using same automation as HmC:**

- Reduced release intervals from 6 months to 6 weeks with findings dropping from low three digits to a handful
- Data center operator reduced system fielding time from 4 days to 3 hours
- Increased test coverage by 400% even with a 50% staffing reduction

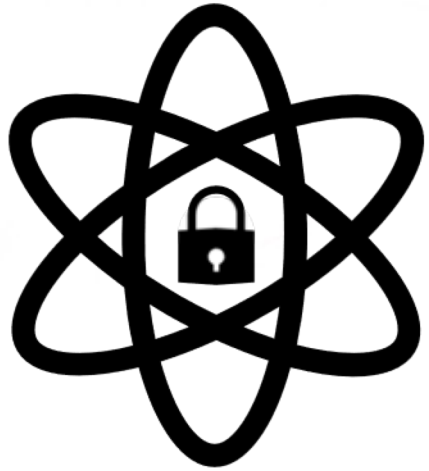
**Kessler Run**

- Credited with $391M in real life cost savings by deploying capability in 4 months instead of an estimated 5 years using traditional waterfall
- 90% of approximately 850 RMF controls inherited from platform, leaving about 40 controls at the application layer to be addressed
- First DoD organization to achieve Continuous Delivery to SIPR

# Start With a Secure Enclave

**100% Virtual Environment**

- Begin with host only network
- Load virtual NGFWs
- Build out virtual network infrastructure

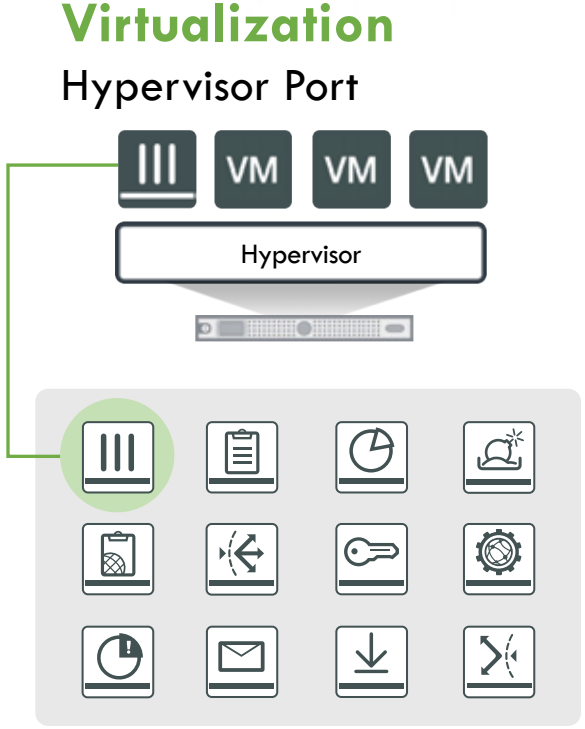


**Hybrid Environment**

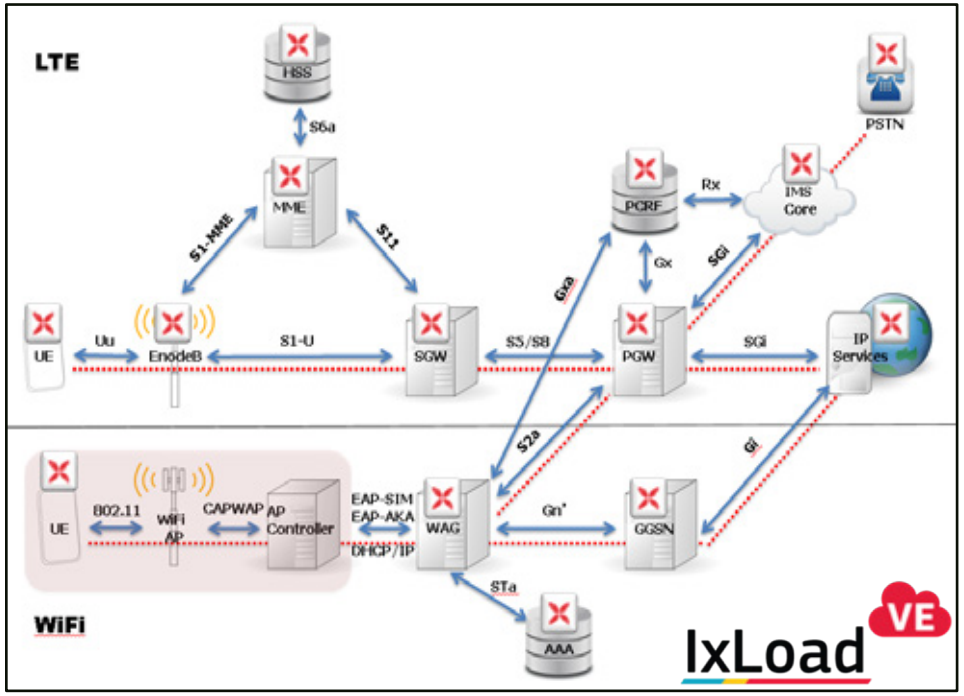
- Create virtual firewall / virtual domain on physical NFGWs
- Create physical to virtual NIC mapping
- Connect virtual switches / routers to virtual NICs

# Network Function Virtualization

Security stacks can now be completely constructed with virtual appliances – NGFW, IDS/IPS, Packet Capture, AAA servers, etc.

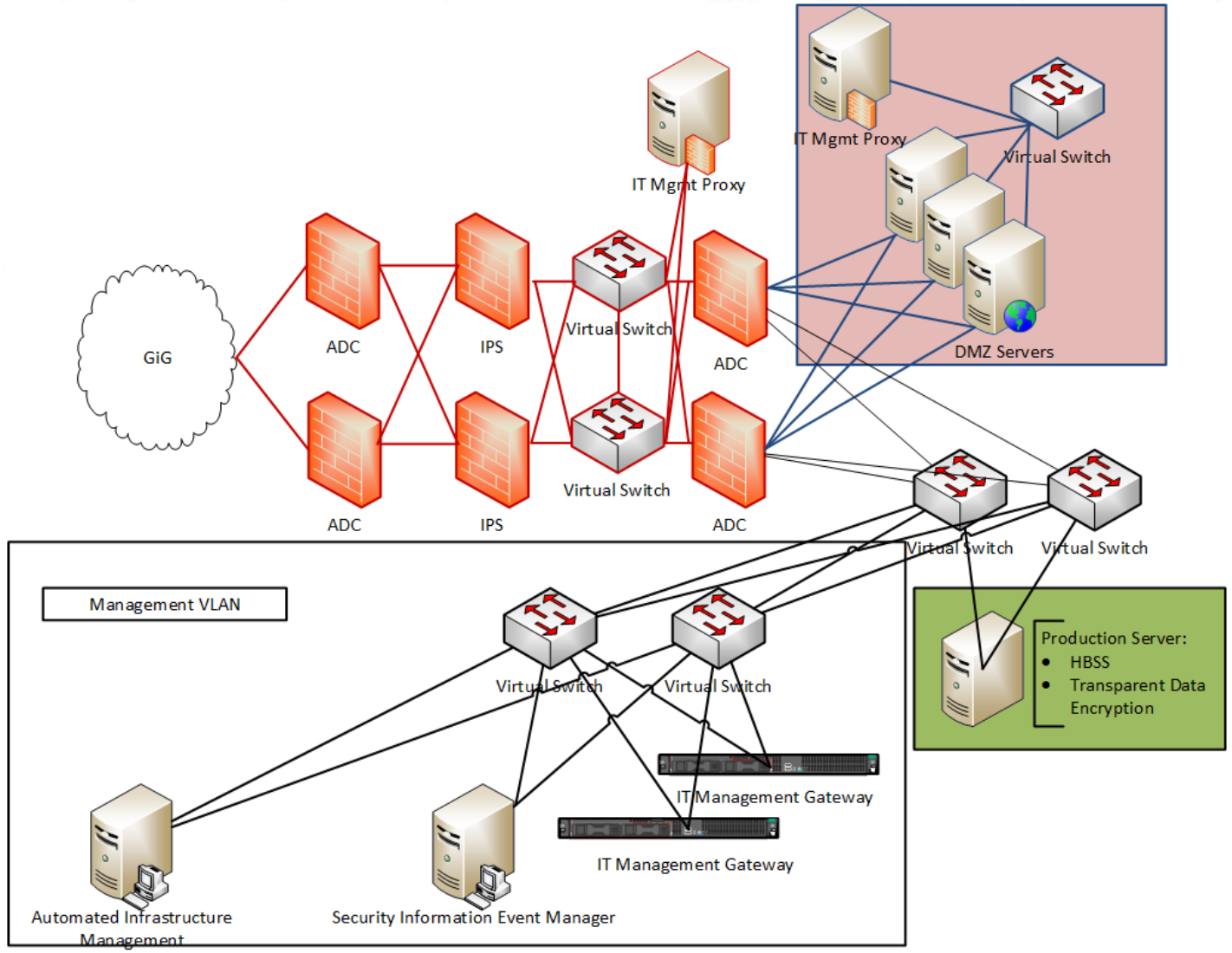



Virtual test devices are available for functional, load, and security testing



# Build out virtual network infrastructure

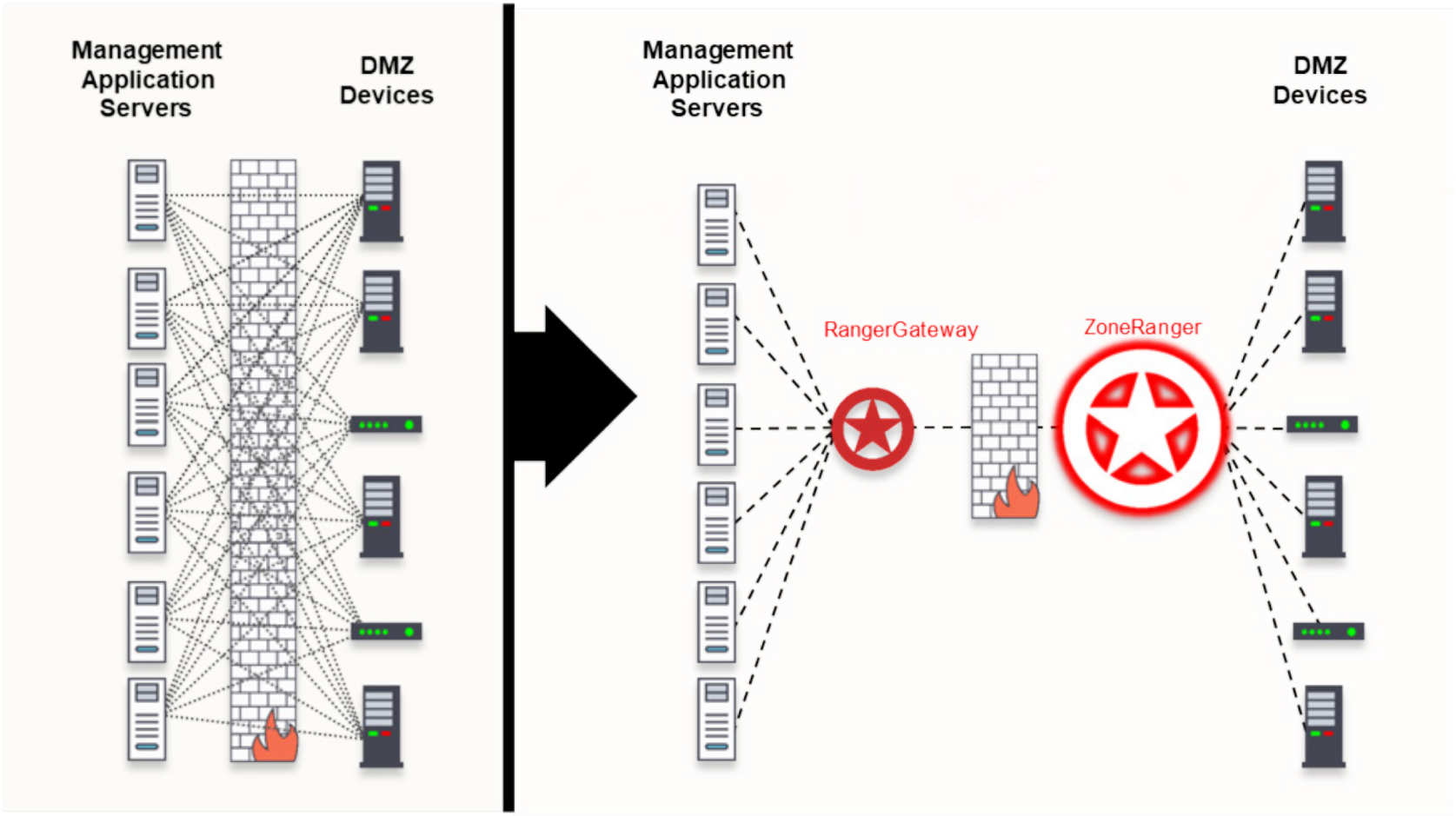
Complete Security and Management Stacks Before Deploying Applications



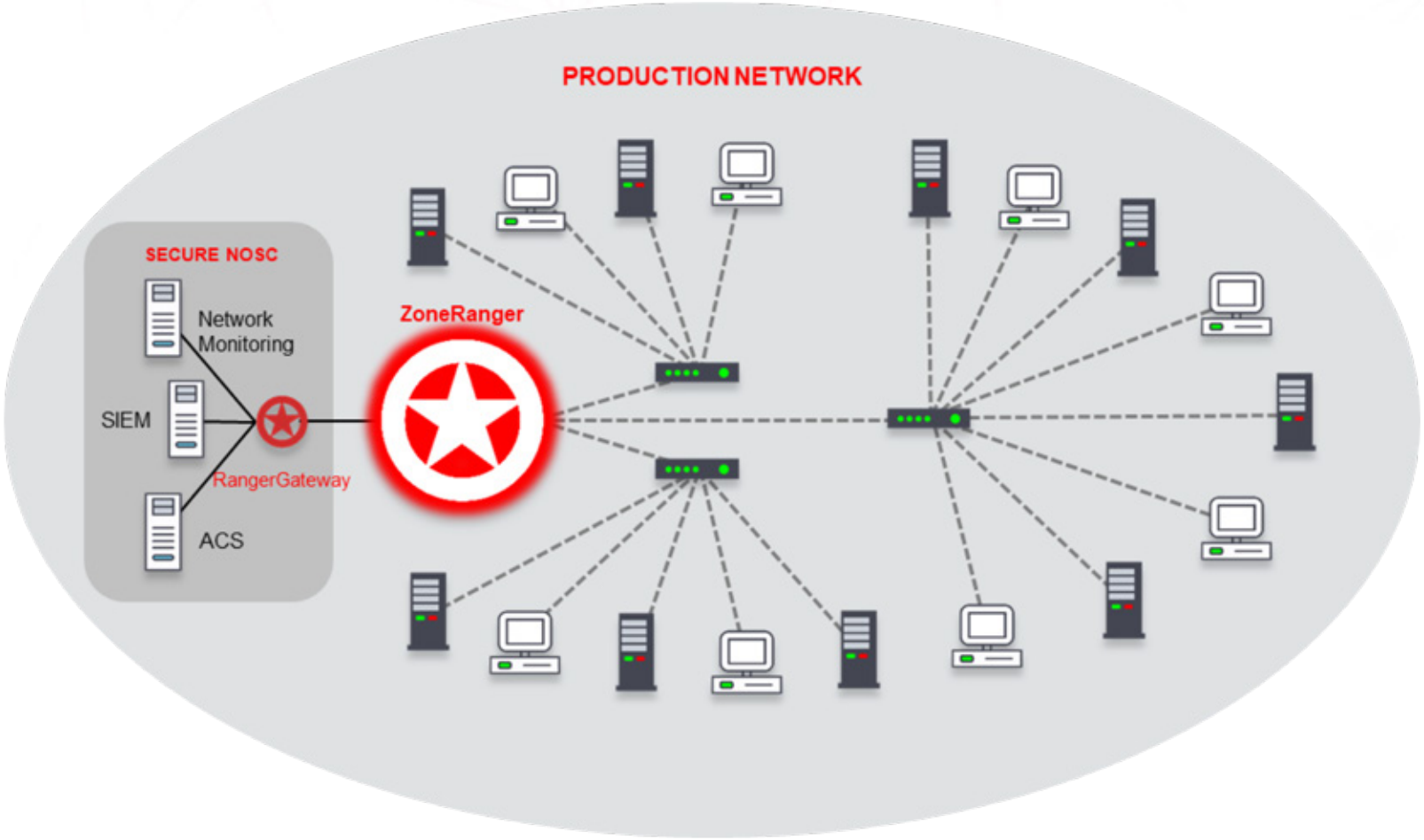
# Simplify IT Command & Control

## IT Management Proxies

- Collapses firewall openings
- Removes firewall CAB decisions when making changes in IT Management
- Extend continuous monitoring to all enclaves, including log files
- Centralize 2FA management



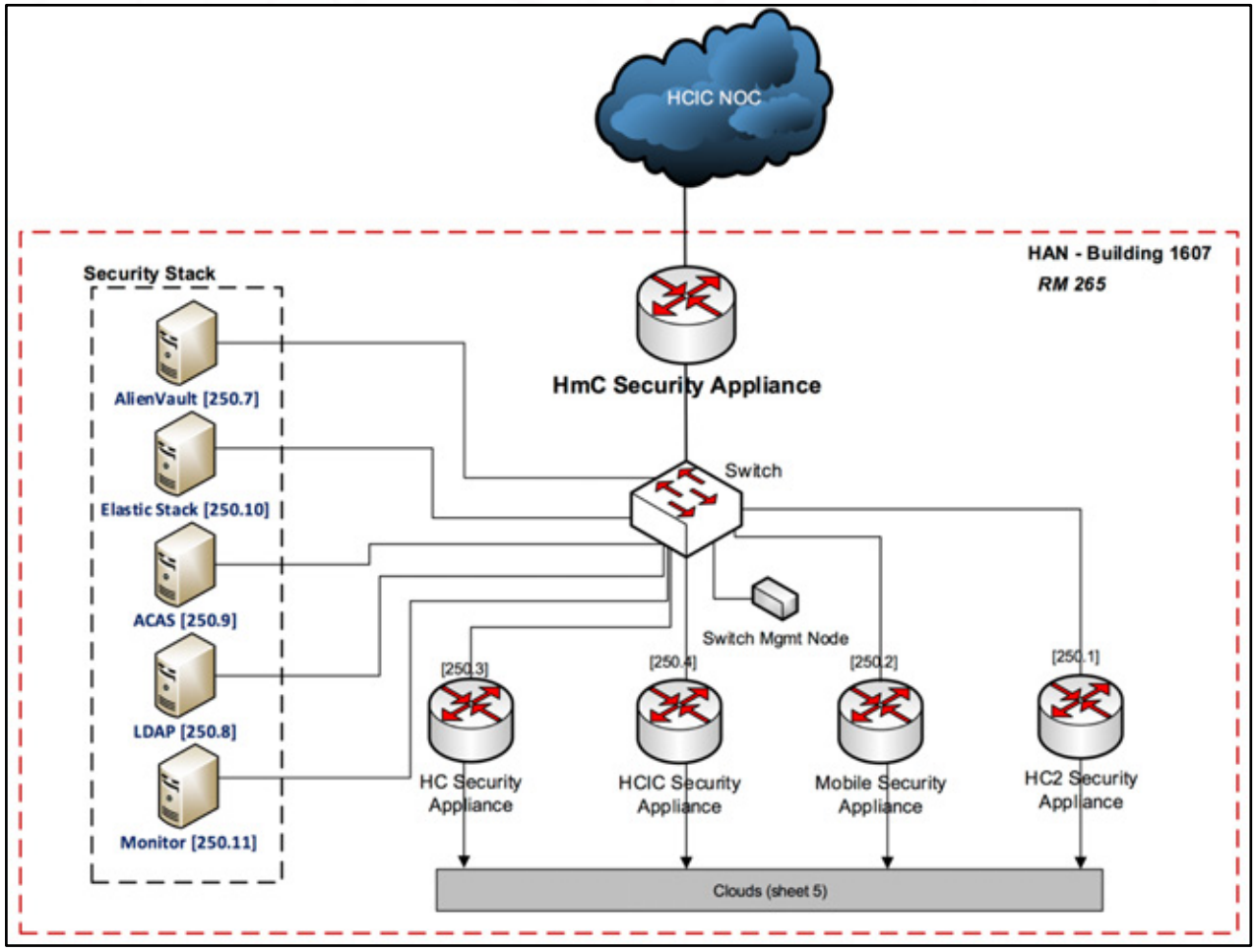
# Secure IT Command & Control




- Secure IT Command & Control across multiple enclaves
- Restrict management consoles to physically secure environments
- Simplify ACL management

IT Management Proxies deployed as Management Application Proxies

# HmC Security Stack




- Intrusion Detection System (IDS)
- Intrusion Protection System (IPS)
- Security Information and Event Management (SIEM)
  - includes crowd-sourced rules engine
- Vulnerability scanning
- Log aggregation & analytics
- Automated alarms and alerts
- System monitoring
  - resources, performance

HmC has demonstrated automating both virtual and physical security appliances

# HmC Automated Security

- Baked into design & execution
- Application quality
- Configuration discipline & management
- Source Code Analysis
- Industry Best Practice Lockdown
- Vulnerability Scans
- Penetration Testing
- Patch Management
- Policy Enforcement
- Monitoring Configuration & Analysis
- Entire Ecosystem into Design
- Validate Alternatives in Real Time

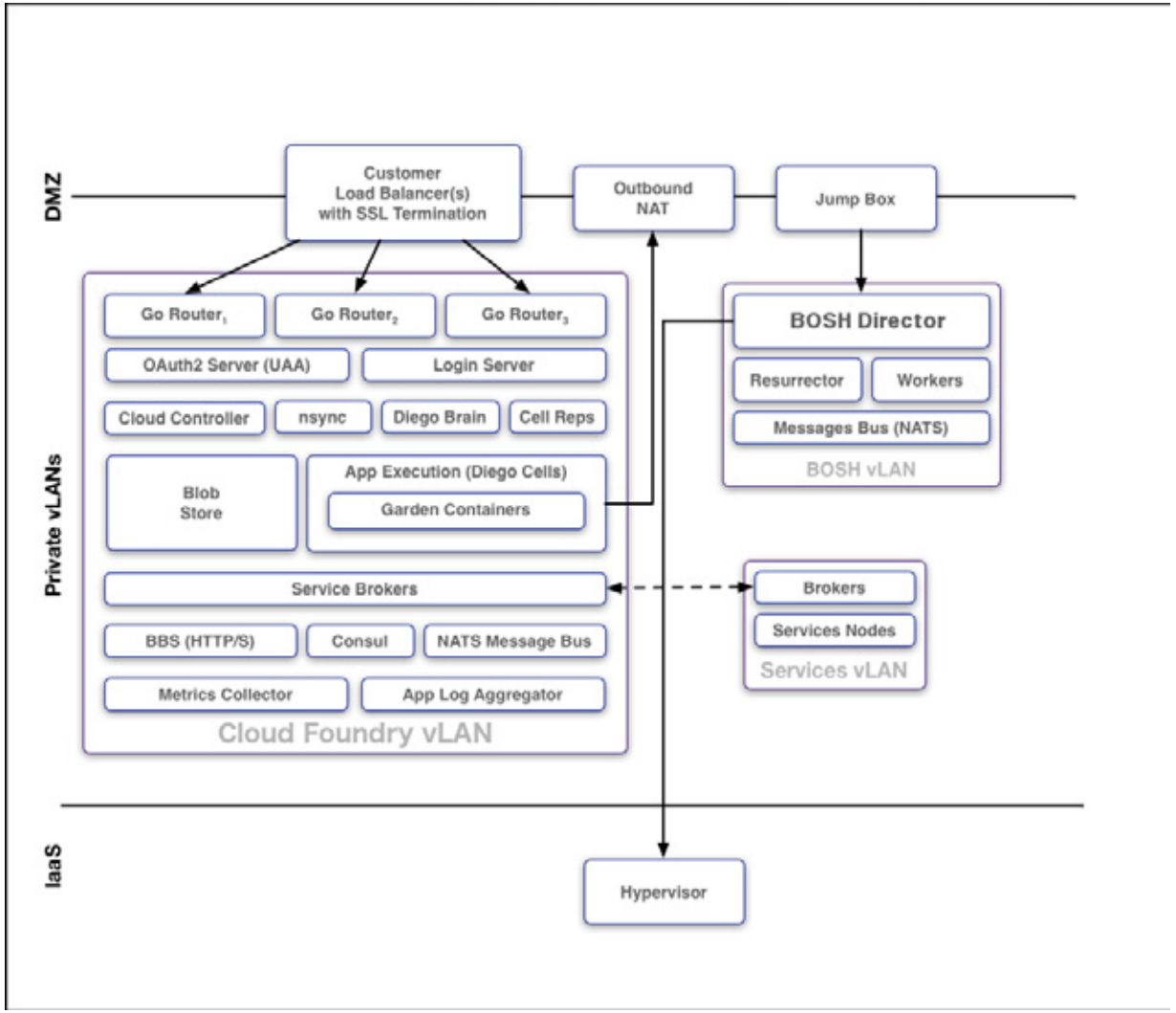
M2 TECHNOLOGY

# Pivotal Cloud Foundry Security

## Cloud Native Security

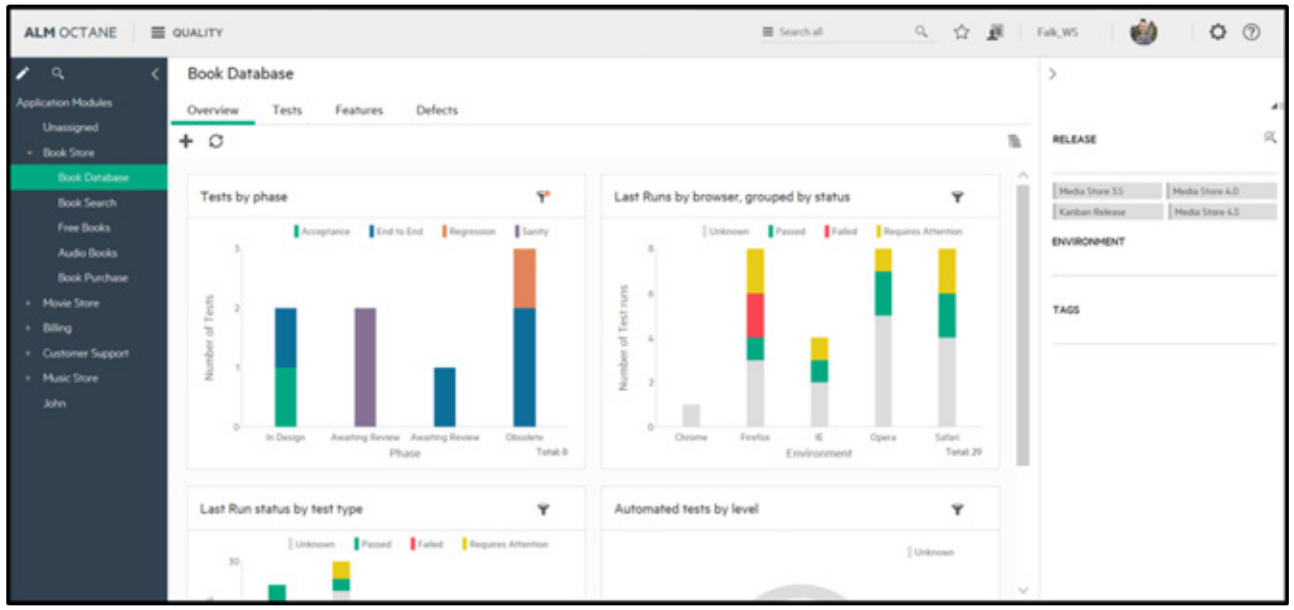
## Repair | Repave | Rotate

- Minimize network surface area
- Encrypt connections
- Isolate applications and data in containers
- Role based access control



M2 TECHNOLOGY

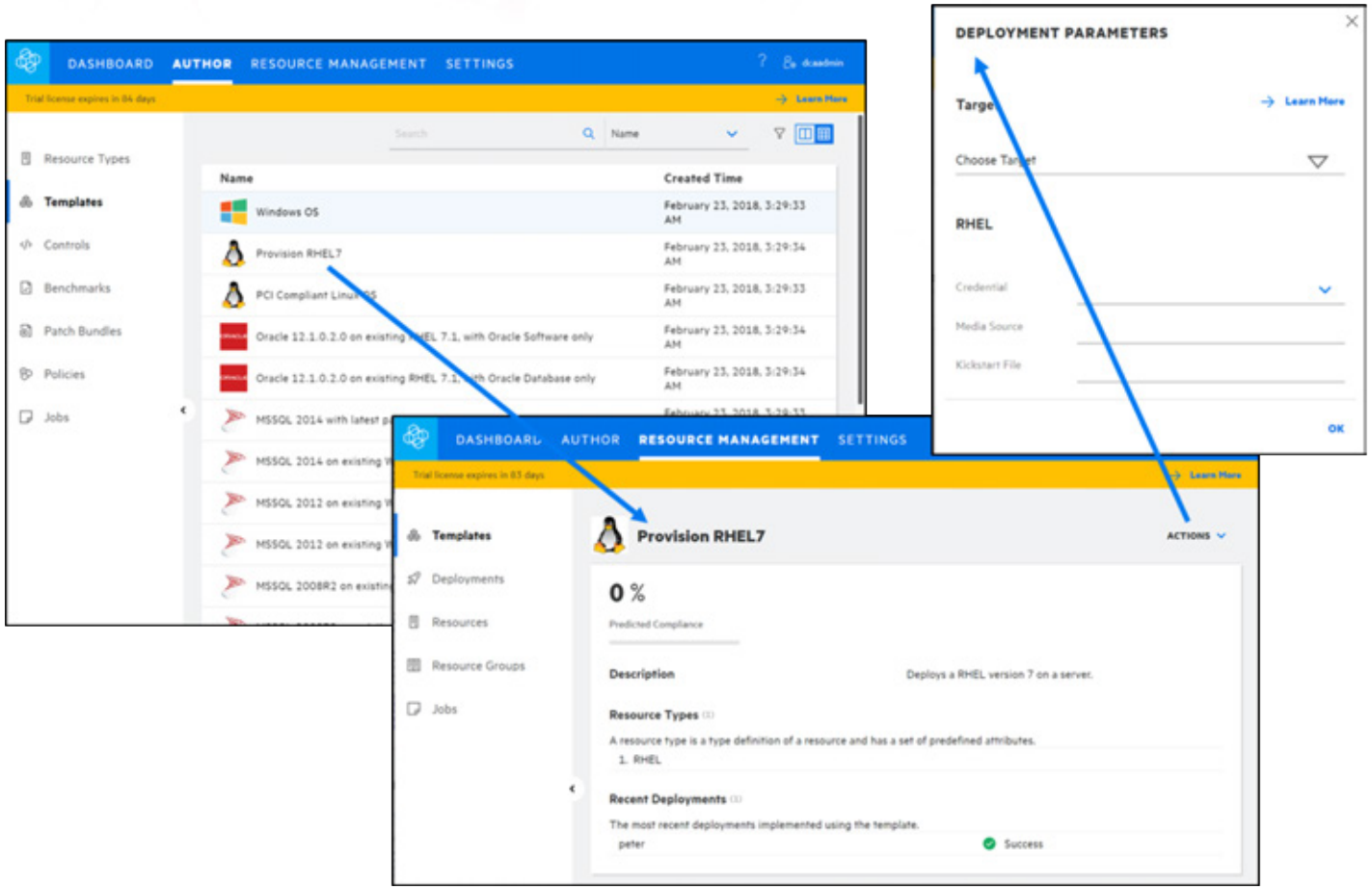
# Automated Testing From Day 1




Functional | Load | Security

- Test early & often
- Safe automation requires test and development environments
- Optimal use case for cloud computing – stand up and spin down
- Fire drill test environment first
- Testing is foundational for TDD and CICD

# Deploy Application in Secured Enclave

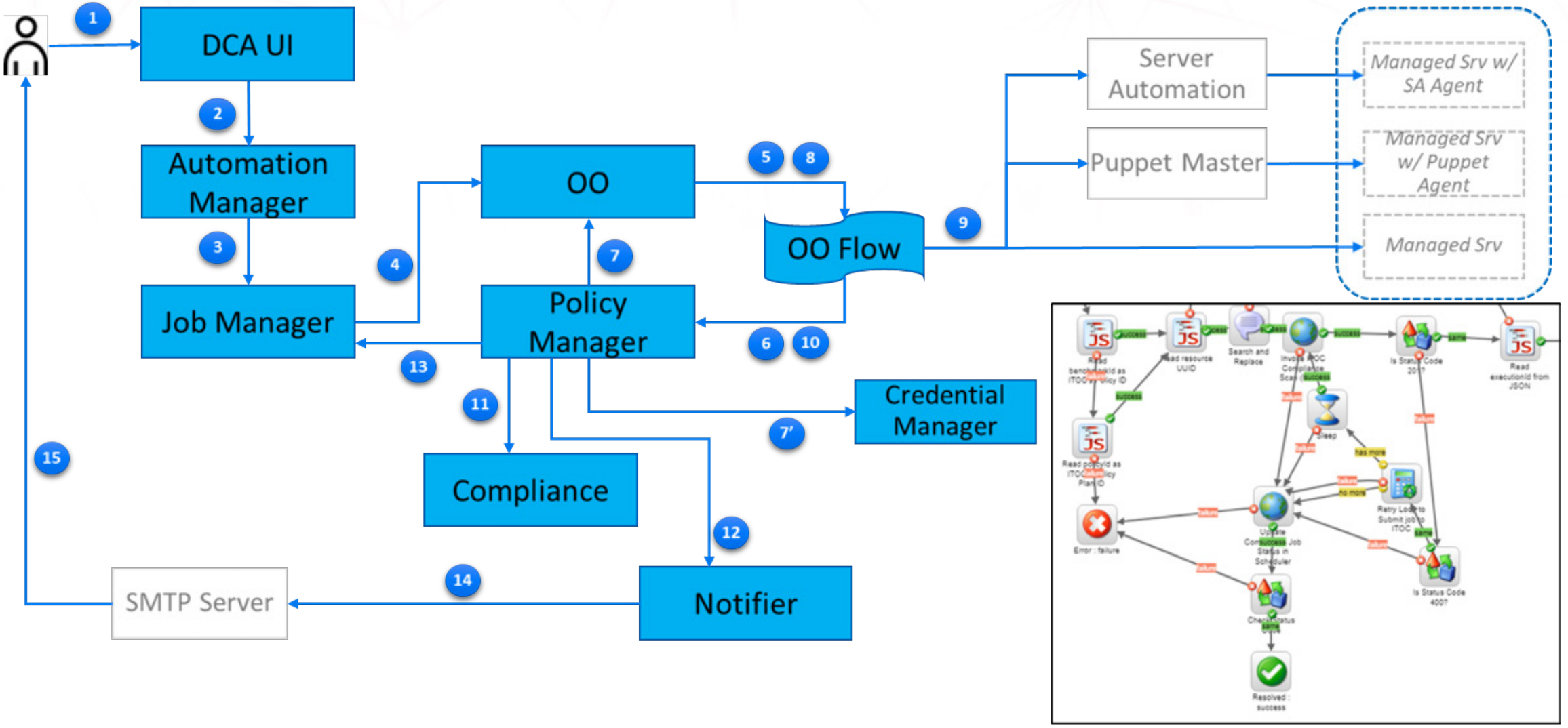



Orchestration driven network, server, and application automation

Leverage available automation tools such as

- Chef
- CONS3RT
- Nutanix Calm
- Micro Focus Data Center Automation
- Pivotal Cloud Foundry Concourse
- Puppet
- VMware vRealize Automation
- Windows System Center

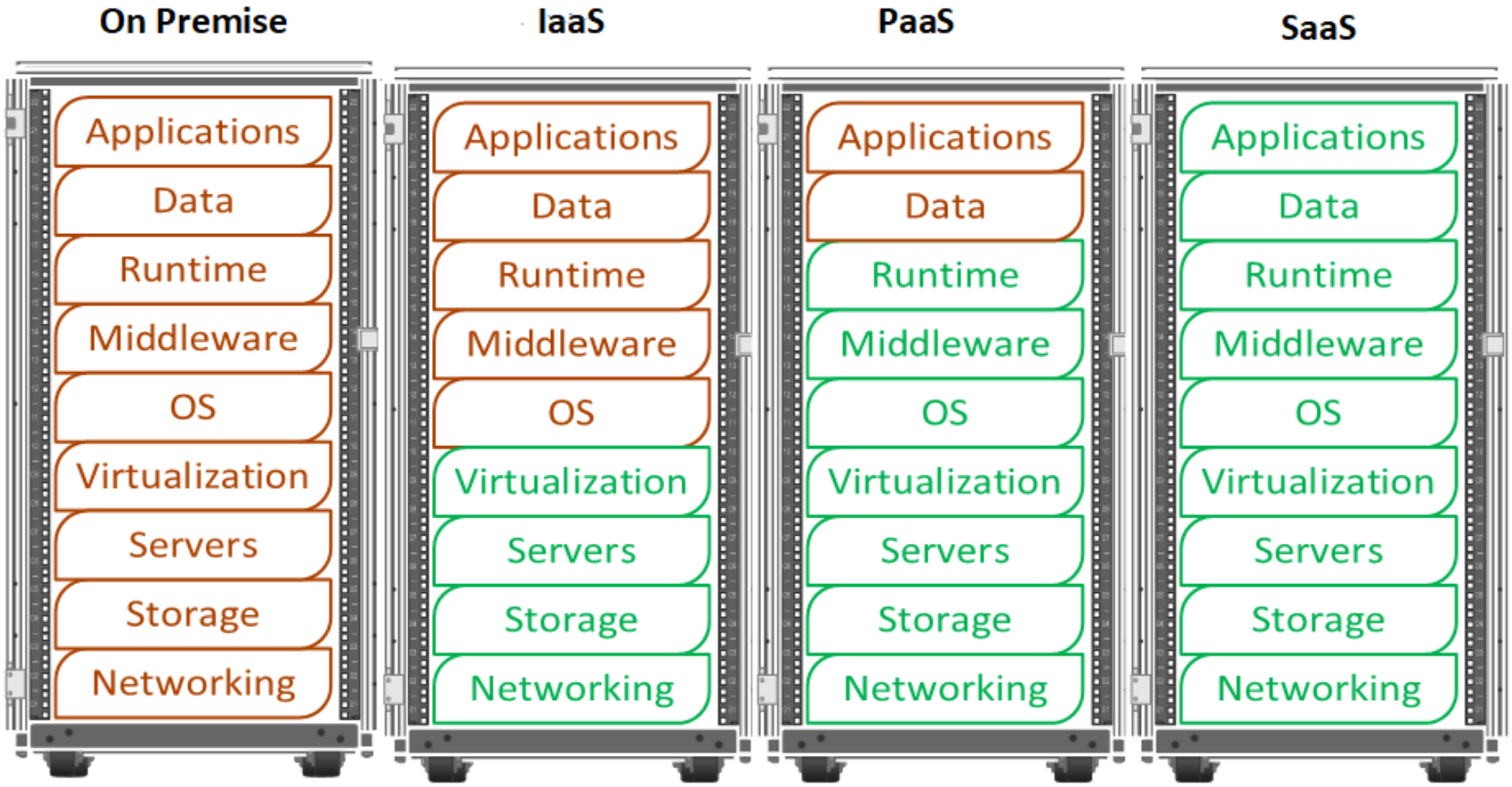
# Automate Patch & Compliance



M2 TECHNOLOGY

# Standardize Everything "Below the Code"

- Quicker time to field capabilities
- Reduce cost
- Fewer Errors
- Significant cost avoidance opportunities



M2 TECHNOLOGY

# PaaS Examples

- Platform examples
  - Docker Enterprise Edition
  - Microsoft Universal Windows Platform
  - Pivotal Cloud Foundry
  - Red Hat JBoss Middleware Application Platform, Openshift
  - ServiceNow
- Self hosted PaaS / Application Platform
  - Maximum flexibility
  - More resource intensive – people and equipment
- Self managed PaaS / hosted IaaS
  - HmC – IaaS with automation and orchestration
  - Still people resource intensive
- Hosted PaaS
  - Allows focus on the code, maximum return on people investment
  - Pivotal Cloud Foundry
  - ServiceNow

M2 TECHNOLOGY

# More Information

## Containers

https://training.play-with-docker.com/ - free, self-paced with labs

https://www.edx.org/school/red-hat - free MOOC, $99 for certification

## HmC

Jackpine hosts regular HmC 101, 201, and 301 lunch and learns via DCS and join.me

## Openshift

https://learn.openshift.com/ - free online, self-paced with pre-configured Openshift instance

# Way Forward

- Brutally honest evaluation of organizational capacity
- Begin by leveraging available automation tools in your environment
- Identify your gaps in automated testing; current Air Force requirements include static and dynamic code security analysis
- Pick one security function or application to start, preferably on the small side
- Not every solution is suited for every situation
- Continue the conversation with industry and peers

Jeff Hart
jeff.hart@m2ti.com
202.595.1917