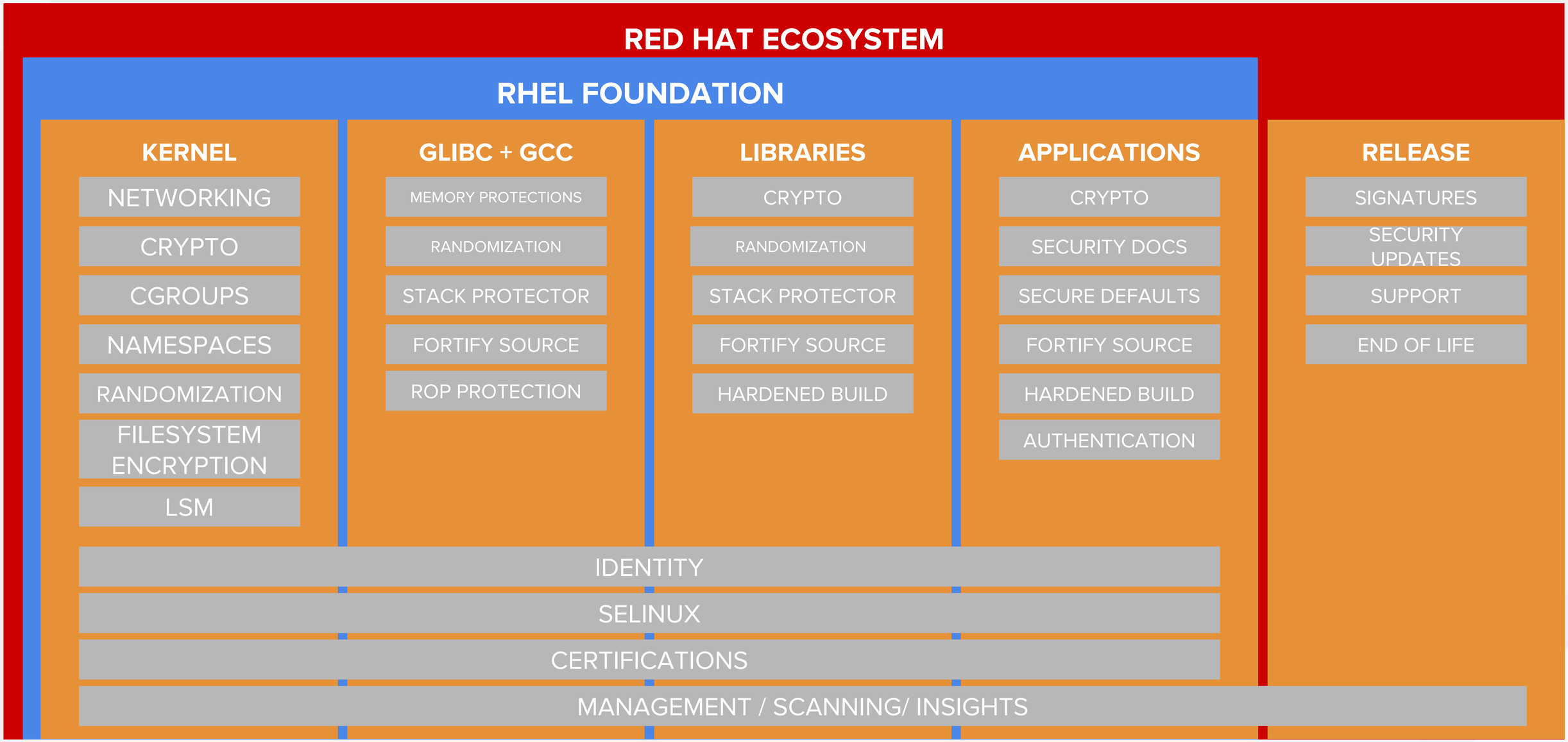
RED HAT SECURITY ROADMAP

Josh Bressers
Security Strategist
@joshbressers

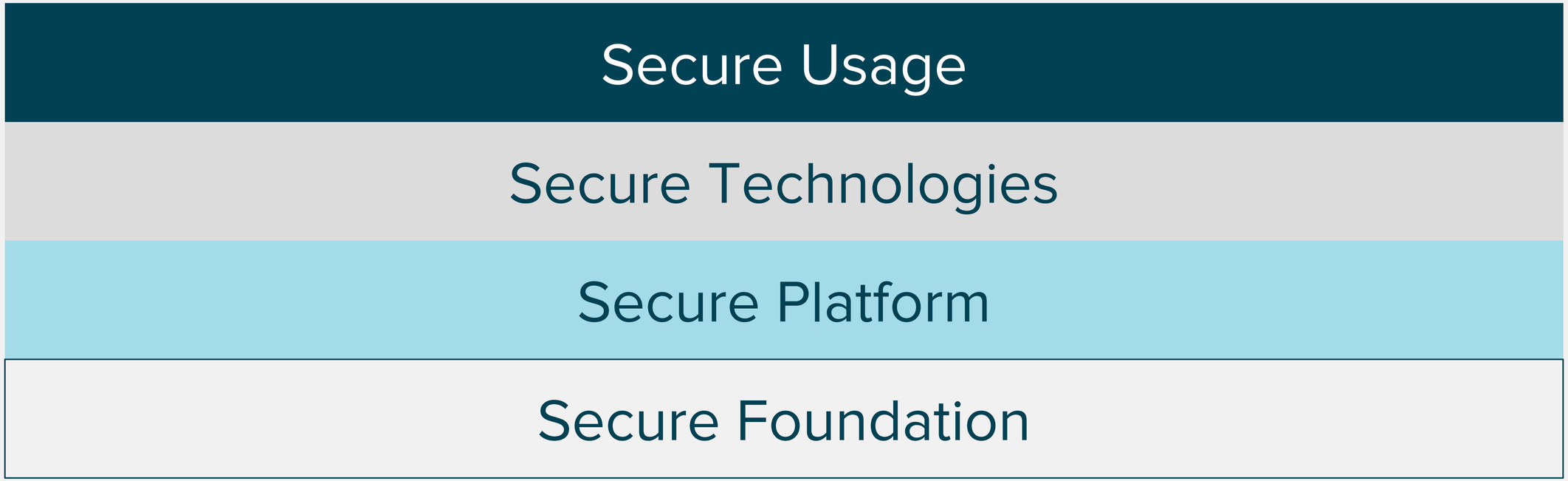
ROADMAP

NOT CRYSTAL BALL

RED HAT, SECURITY COMPANY?



SECURING THE WHOLE STACK



FOUNDATION

CRYPTO

MAINTENANCE	DEPRECATION	VISION
● Security updates ● Bug fixes ● Certifications ● Modify defaults ● Minor features	● Watch research ● Proactive deprecation	● New algorithms ● Better system management ● Library improvements

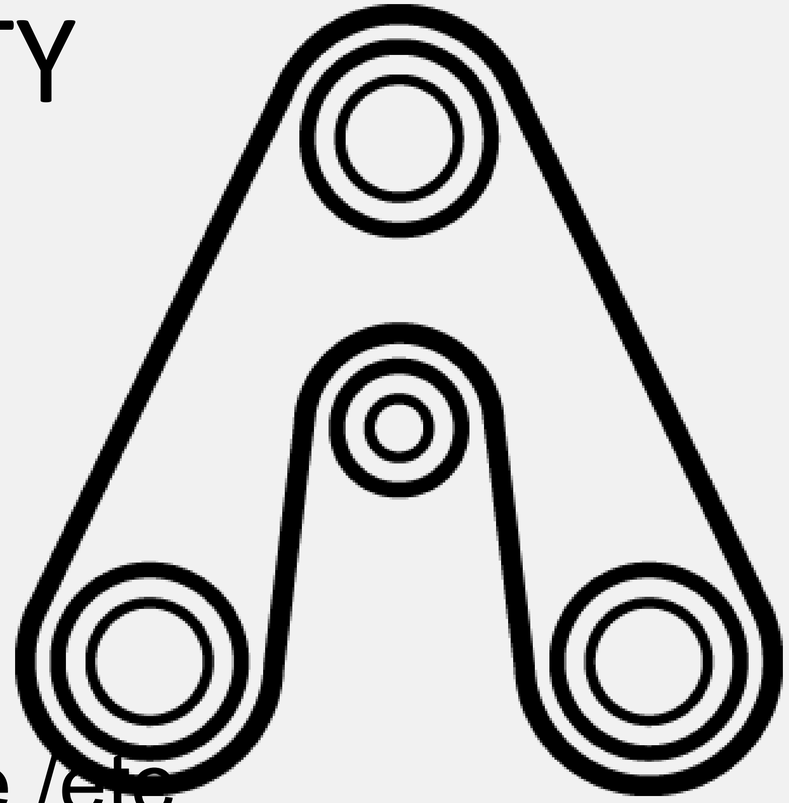
CERTIFICATION & COMPLIANCE

	MAINTAIN	INVEST
Product Compliance	● FIPS ● Common Criteria ● SCAP	● OSPP 4 ● Faster certifications ● Easier to use and deploy
Procedural Compliance	● PCI ● HIPAA ● SOX	● Continuous monitoring ● Guidance ● Better defaults ● SCAP profiles

DETER THREATS

- gcc/glibc security enhancements
  - ROP, MPX
  - Memory protections
  - Better warning
- Boot Time Security
  - TPM
  - Secure Boot
- Whitelisting

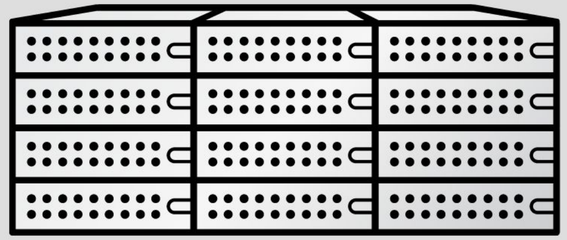
RUNTIME SECURITY



- Selinux
- Container Isolation
- USBGuard
- Systemd
  - Private /tmp
  - Protected /usr /home /etc

NETWORK SECURITY

- Encryption
  - IPsec L3 encryption tunnels with hardware offload
  - MACSec L2 encryption for Hosts and VMs
    - reduces the need for full mesh of L3 IPsec tunnels at the application level.
- Network Isolation
  - with overlay tunnels using VXLAN, GRE, MPLS.
  - HW offload with NICS available as well



STORAGE

Encryption

SELinux Enablement

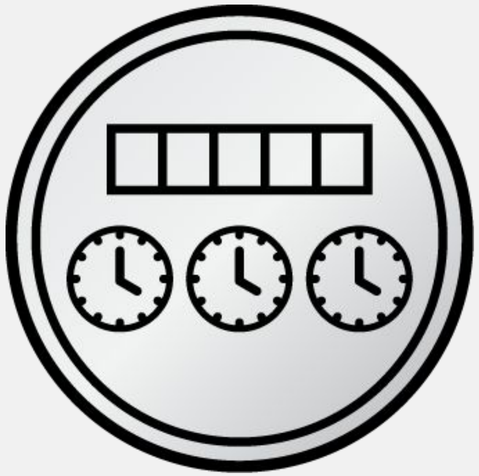
Network Bound Disk Encryption

Resource Segregation (RADOS)

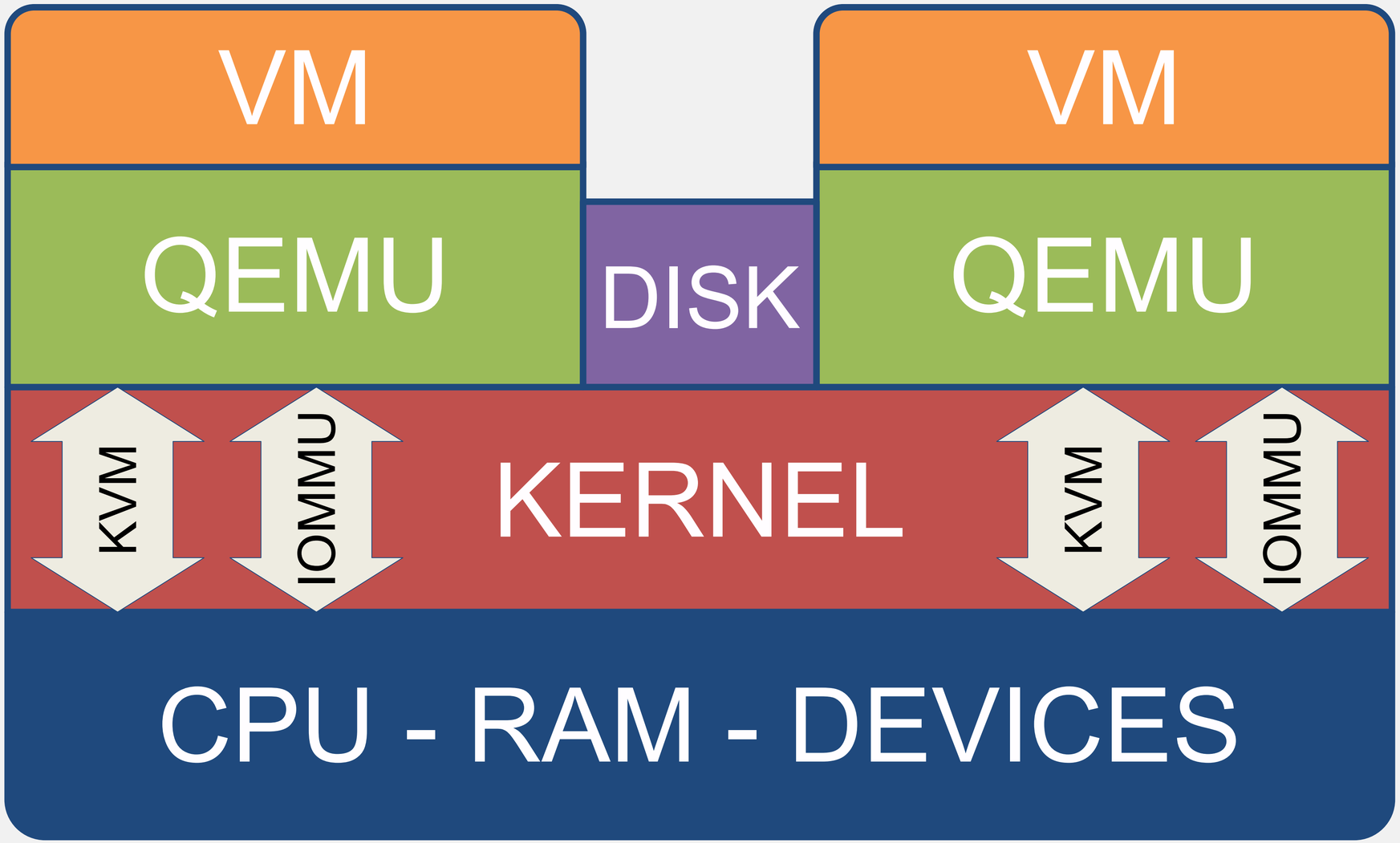
FEATURES

ENVIRONMENT INSPECTION

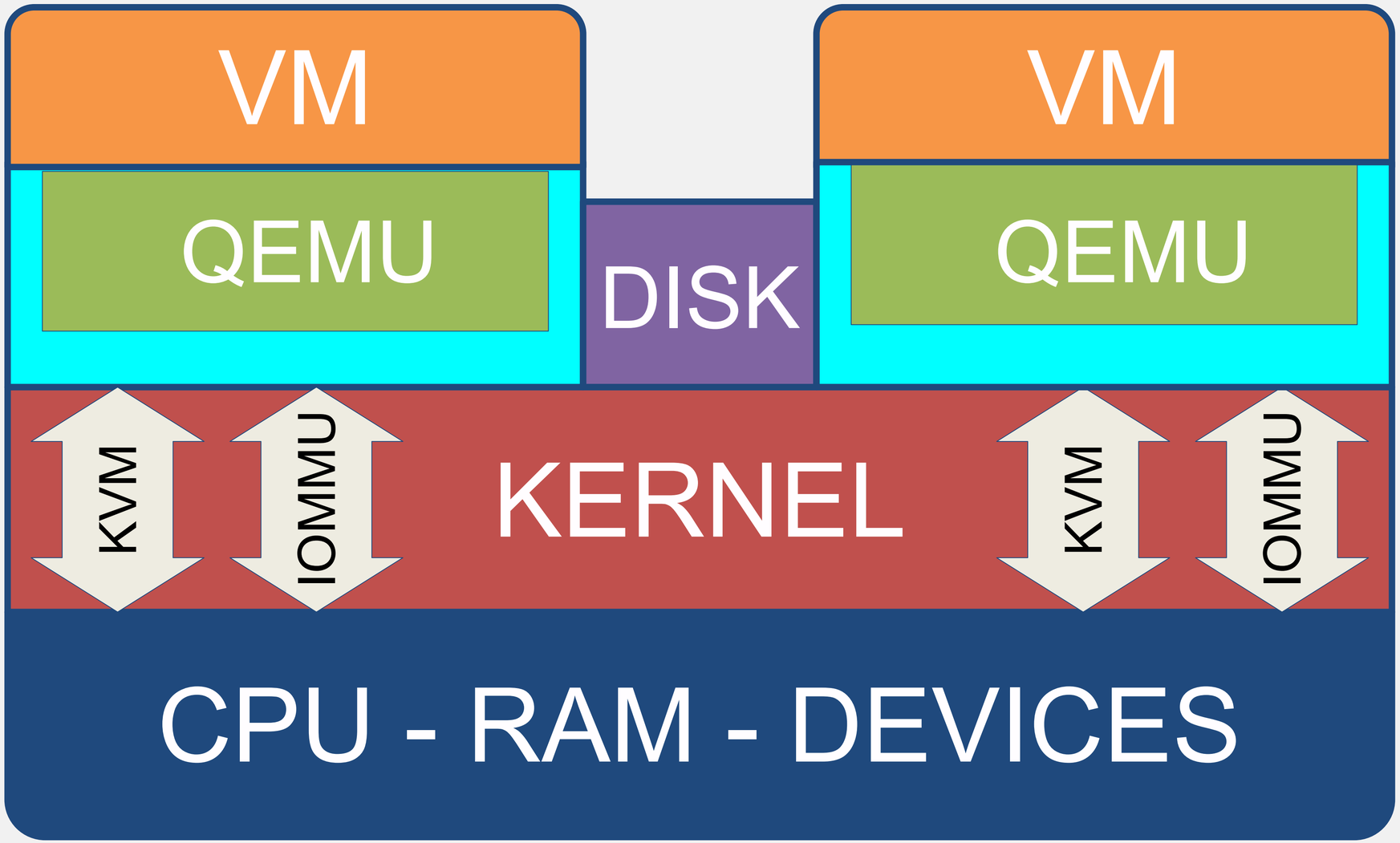
- Measuring the runtime environment
  - Common Logging
  - Audit



KVM WITHOUT SVIRT



KVM WITH SVIRT

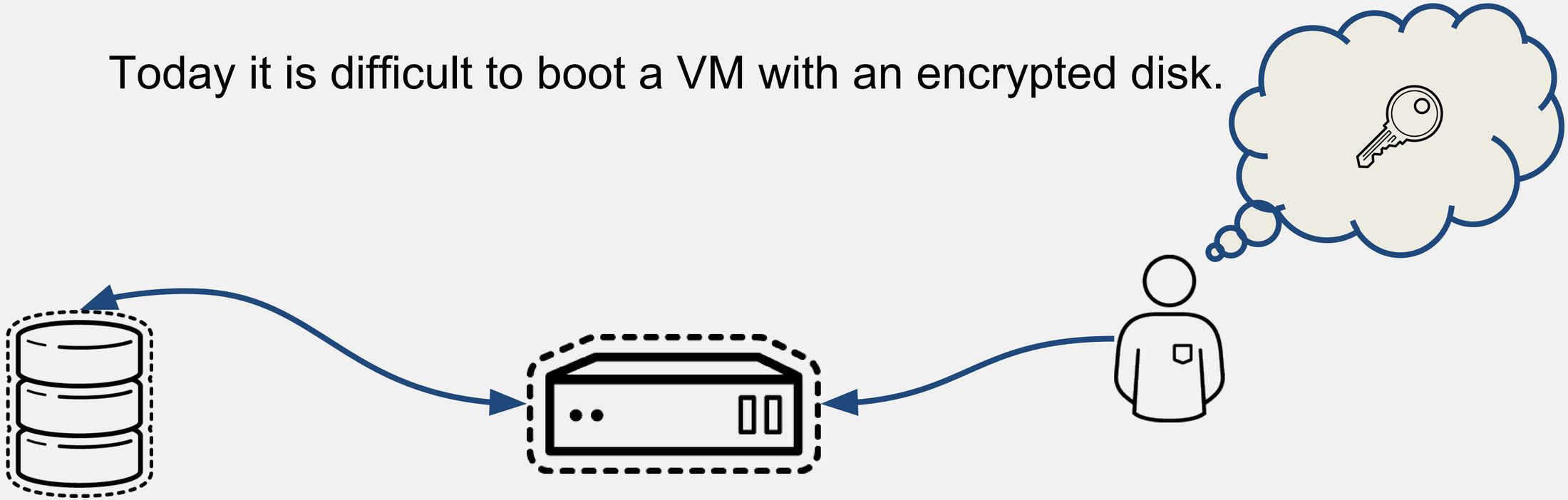


MIDDLEWARE

- JBoss EAP 7.1
  - Elytron security subsystem
    - Replaces PicketBox/JAAS
    - Single security subsystem for configuring Management and Application security
  - Common Criteria Certification
- RH-SSO (Keycloak) 7.1
  - SSSD integration with RHEL IdM
  - Node.js client
  - OpenID Connect Certification
- API Management
  - Integrate 3scale into our portfolio

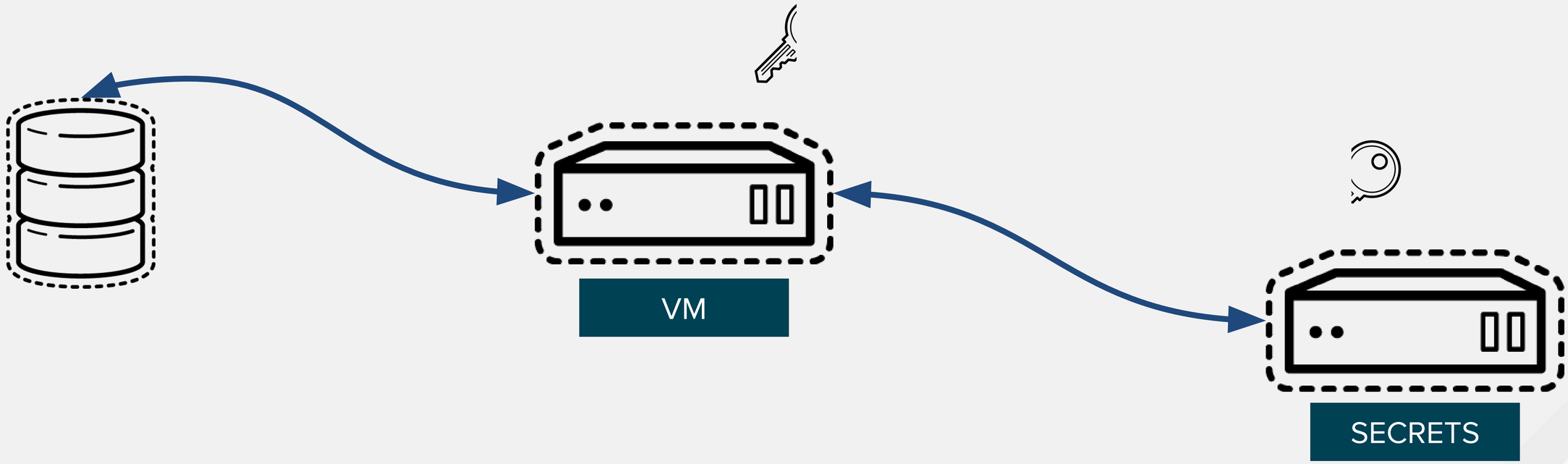
NETWORK BOUND DISK ENCRYPTION

Today it is difficult to boot a VM with an encrypted disk.



NETWORK BOUND DISK ENCRYPTION

What if we could store the secret in the network?
Very defined security use cases, separated keys from unlocking material



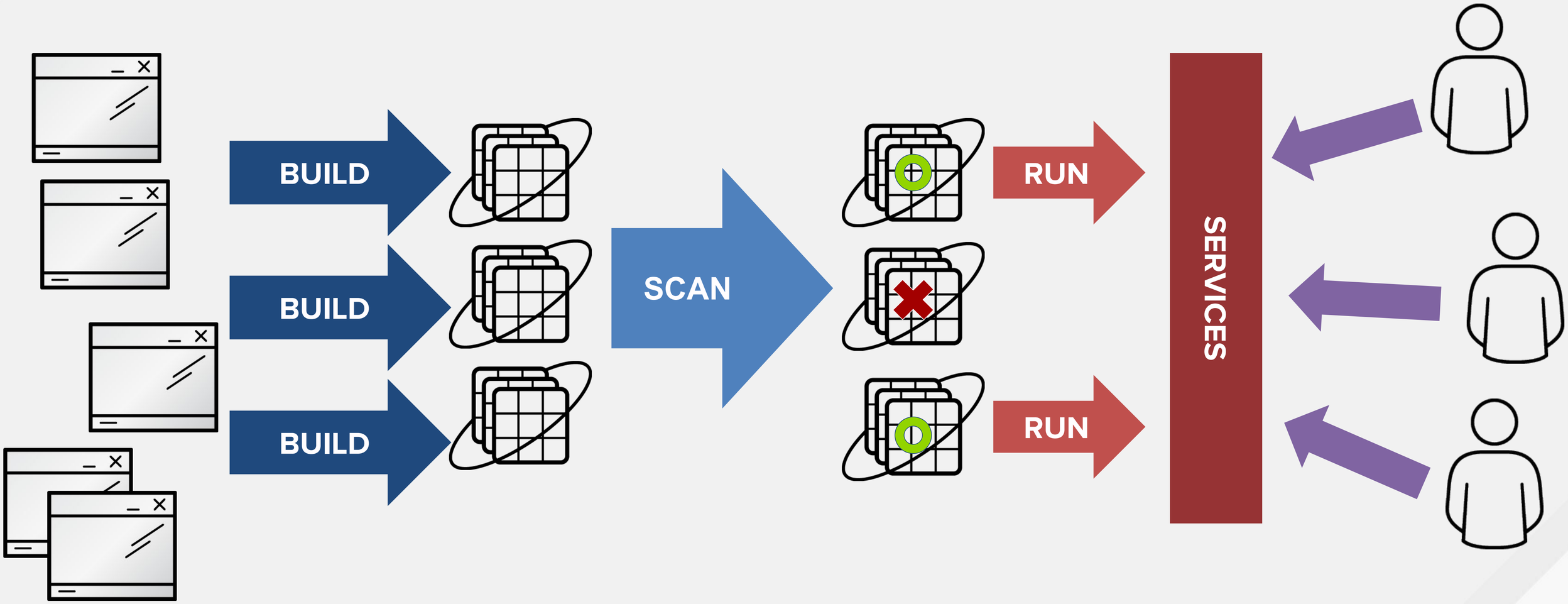
CONTAINER SECURITY

SCANNING
CFME, ATOMIC SCAN

SIGNING
BUILDING TRUST

CONTAINMENT TECHNOLOGY
PROTECTING THE CASTLE

CONTAINER SCANNING



SCAP

- SCAP workbench
- Ever improving rules
- Compliance verification
- SCAP Certification

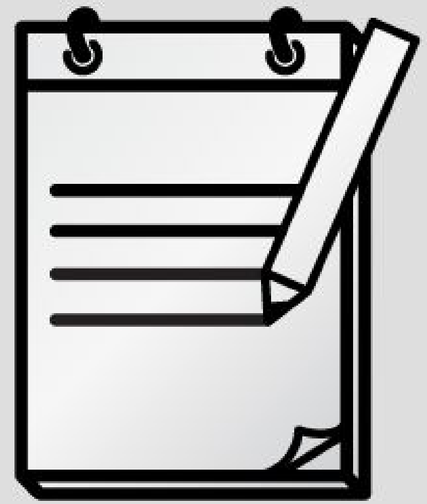
Lab

Practical OpenSCAP: Security, standard compliance, and reporting

RELEASE

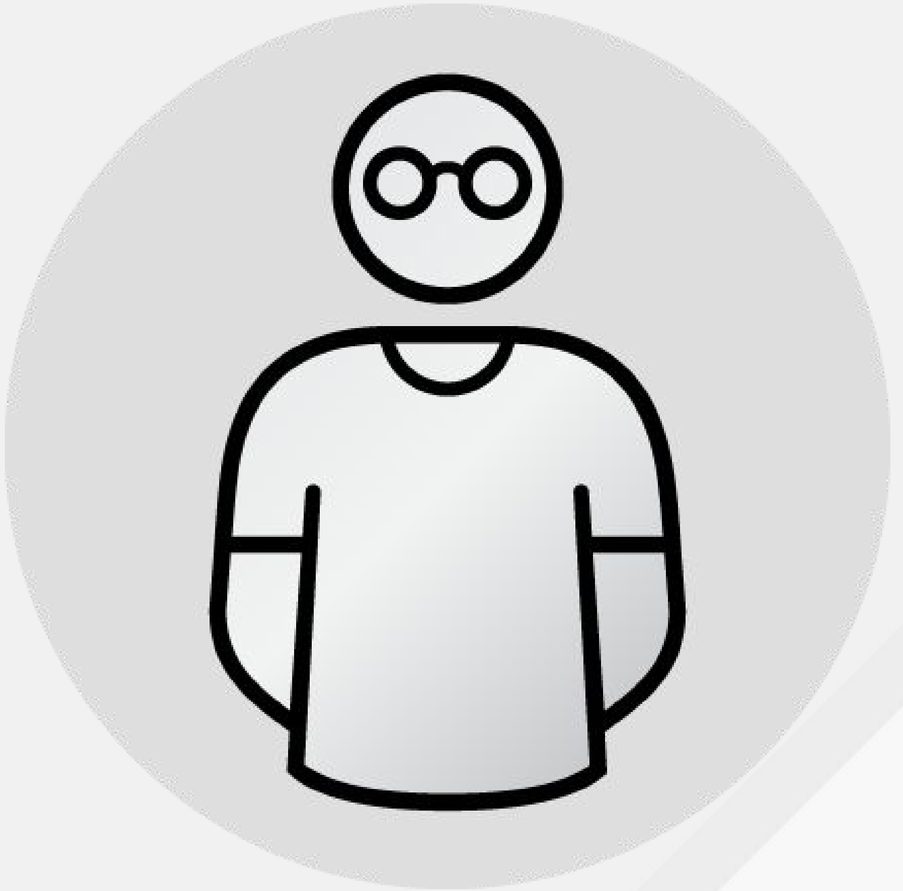
DOCUMENTATION

- Security problems and solutions
  - Red Hat Portal
- Security HOWTOs
  - Red Hat online guides
- Compliance and remediations rules
  - SCAP Security Guide

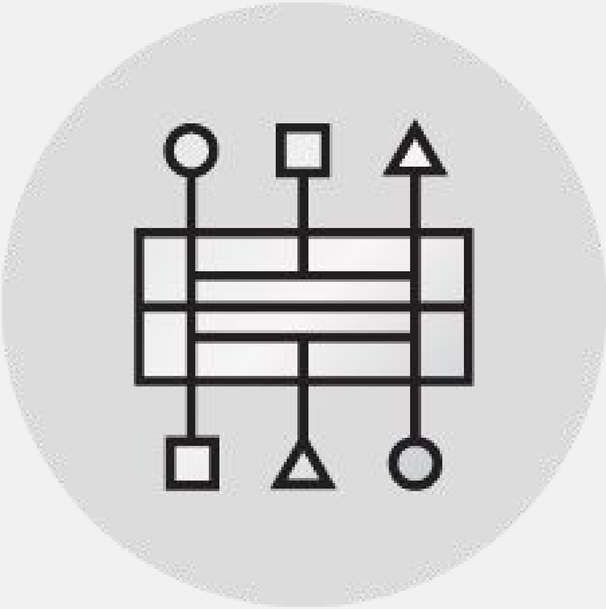


RESPONSE

- Responsible adult in the room for high touch issues
- Delivery of Ansible playbooks along with Labs & Insights rules
- Evolve with the security environment



VULNERABILITY DATA

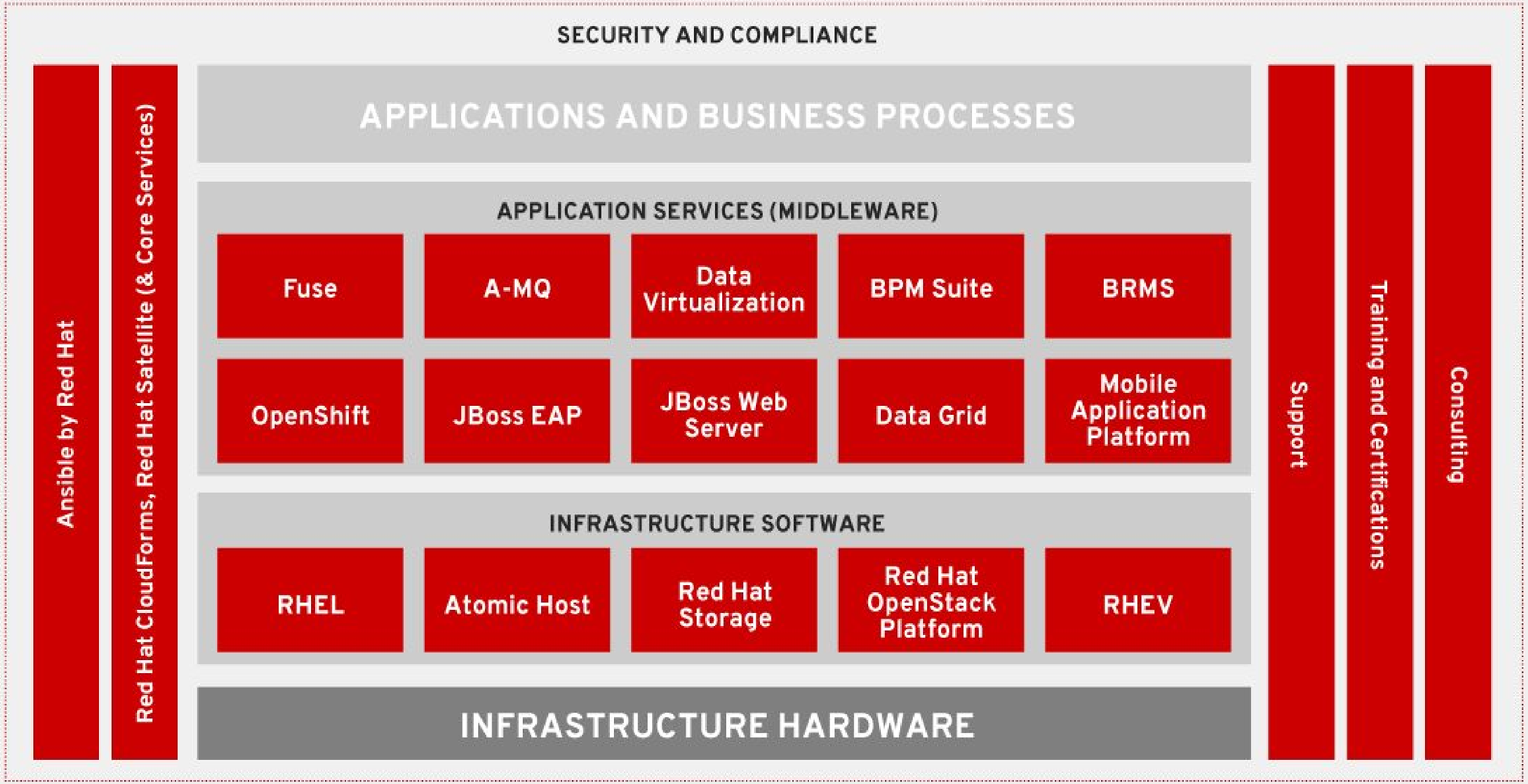


- Vulnerability service API
- SWID
- Full portfolio OVAL support
- CVSSv3
  - CVSSv2 until 2017

MANAGEMENT & IDENTITY

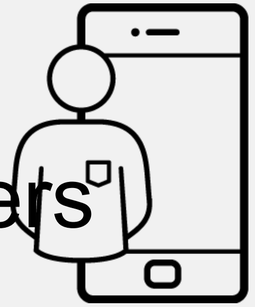
MANAGEMENT

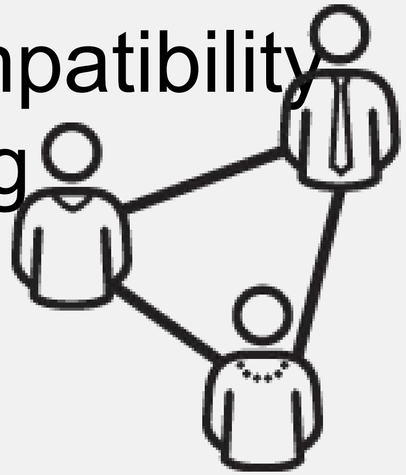
Patching - Inspection - Configuration Management

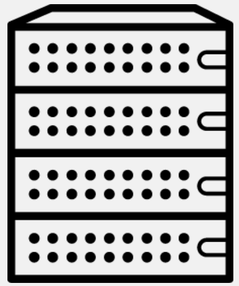


IDENTITY

- SSSD and IPA in containers
- Better AD support
- Cached authentication
- Smart Card authentication
- Better SSSD compatibility
- Session recording







SMART ANALYSIS

- Red Hat Insights
  - Machine learning / Anomaly detection
- CloudForms
  - Smart State Analysis
- Audit
  - Human understandable audit trail
  - Audit analysis functionality

WHERE DO WE GO NEXT?

- Focus on containers
- Compliance is coming!
  - Brace yourselves
- Monitoring industry direction
- Invent the future

- Tell us what **you** need

Secure your seat at these security sessions

Secure your enterprise software supply chain with containers
Tuesday, 10:15 AM - 11:15 AM, Room 2005

Red Hat security roadmap
Tuesday, 11:30 AM - 12:30 PM, Room 2005

Are you listening to what SELinux is telling you?
Tuesday, 3:30 PM - 4:30 PM, Room 2005

Identity management for cloud and hybrid cloud environments with Red Hat and Microsoft
Tuesday, 4:45 PM - 5:45 PM, Room 2005

Security Enhanced Linux for Mere Mortals
Tuesday, 4:45 PM - 5:45 PM, Room 2006

Cryptography: What every application developer needs to know
Tuesday, 4:45 PM - 5:45 PM, DevNation Room 132

Practical steps implementing Red Hat identity management solution
Wednesday, 10:15 AM - 11:15 AM, Room 2005

End-to-end OpenSCAP for automated compliance
Wednesday, 11:30 AM - 12:30 PM, Room 2005

Middleware security: Authentication, authorization, and auditing services
Wednesday, 3:30 PM - 4:30 PM, Room 2005

Container security reality check: The container is only the beginning
Wednesday, 4:45 PM - 5:45 PM, Room 2006

Running a policy-based cloud with Cisco Application Centric Infrastructure, Red Hat OpenStack, and Project Contiv
Wednesday, 4:45 PM - 5:45 PM– 2005

Red Hat identity and access management vision, solution, and roadmap
Thursday, 10:15 AM - 11:15 AM, Room 2005

Understanding security risks and mitigation across the virtualization stack
Thursday, 11:30 AM - 12:30 PM, Room 2005

Compliance, security automation, and remediation with CloudForms, Satellite, and Ansible
Thursday, 3:30 PM - 4:30 PM, Room 2005