

Container & Data Security

Best Practices

HOW ENCRYPTION HELPS



Data = ciphertext + key

WHEN SHALL I USE ENCRYPTION?



Cost of implementation < risk reduction

Understanding Risk

What Do We Care About?



Prioritization

Not all risks are equal in the eyes of the organization. We require a mechanism or process to not only identify, but prioritize which risks they want to tackle first.



Mitigation

When a risk is simply too great to live with, organizations must be enabled to mitigate those risks to levels acceptable to the business.

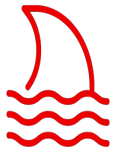


Acceptance

Sometimes, the risk presented is minor enough that remediating is more costly than simply leaving it alone. A risk can only be accepted by the appropriate business owner.

Understanding Risk

A Holistic Definition



Threat

Any malicious or ignorant action that causes damage, loss of operations, or theft.

Comprised of a Threat Actor and a Threat Vector.



Impact

An estimate of the harm that would be caused if a threat were to be realized.

Can be measured in many ways, e.x financials, operational downtime, environmental, reputational, etc.



Likelihood

The probability that a given threat event will occur over time.

There is a proportional relationship between time elapsed and likelihood increasing.



Quick Math!

Risk can be measured either qualitatively or quantitatively.

Qualitative risk analysis is based on a risk analyst's perception or judgment, while quantitative risk analysis is based on verified and specific data.

Quantitative risk is usually calculated via the following formula:

(threat x likelihood x impact)

Risk analysis for encrypting containerized Elastic Search

- **Need full text search capability of Elastic Search**

- **Data must be encrypted**

- ☐ Protect from provider access
- ☐ Comply to GDPR requirements that operators must not be able to somehow read/extract data in plaintext

- **Which level of encryption is possible?**

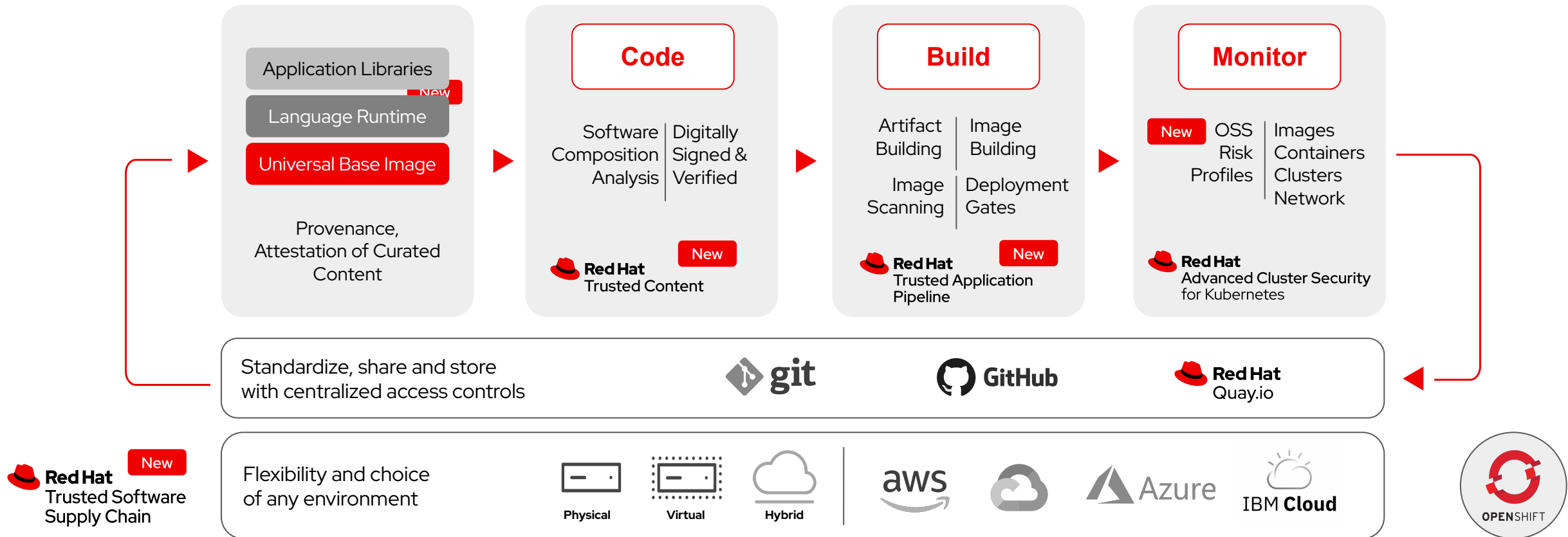
- ☐ App-Level ? ☐ No full text search in Elastic Search!
- ☐ Database-Level ? ☐ Not supported by Elastic Search!
- ☐ Filesystem ? ☐ YES! Possible natively on OpenShift via Persistent Volume Encryption or at the Application level
- ☐ OS-Level ? ☐ YES! Possible natively on OpenShift via Disk Encryption and/or Container Image Encryption
- ☐ Hardware-Level ? ☐ Would still allow operators to read plaintext within OS
- ☐ Platform-Level ? ☐ YES! Only PVCs of deployment get encrypted. Encryption done via CSI-Proxy

Container Security

Best practices

- Reduce attack surface with a container optimized operating system
- Use automated and policy-driven configuration management across your fleet
- Implement least privilege with fine-grained role based access control (RBAC)
- Encrypt platform data in transit and at rest
- Use automated compliance, risk assessment and remediation solutions
- Reduce deployment risk with admission control policies that
 - Minimize admission of privileged pods, pods with host capabilities
 - Prevent admission of pods with critical vulnerabilities

Code, build, and monitor with a Trusted Software Supply Chain

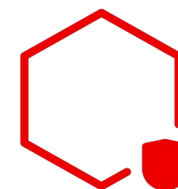


Kubernetes is the standard
for application innovation...



- ▶ Microservices architecture
 - ▶ Declarative definition
 - ▶ Immutable infrastructure

...and Kubernetes-native
security is increasingly critical



- ▶ Secure supply chain
- ▶ Secure infrastructure
- ▶ Secure workloads

DevOps

DevSecOps

Security

Detect

Trusted content

Container registry

Build management

CI/CD pipeline

Vulnerability Analysis

App Config Analysis

APIs for CI/CD pipeline

Protect

Kubernetes platform lifecycle

Identity and access management

Platform data

Deployment policies

Image Assurance

Compliance Assessments

Risk Profiling

RBAC

Respond

Container isolation

Network isolation

Application access and data

Observability

Runtime Behavioural Analysis

Auto-suggest Network Policies

Threat Detection

Red Hat Container Security Use Cases



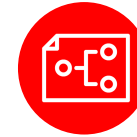
Vulnerability Management

- Scan images for known vulnerabilities
- Find vulnerabilities in running deployments and learn how to fix them
- Enforce policies based on vulnerability information in CI/CD workflows
- Defer CVE or mark as False Positives
- RBAC for approving deferrals



Compliance

- Assess compliance with CIS Benchmarks, and PCI-DSS, HIPAA, and NIST SP 800-190 reference architectures
- Get actionable insights to improve compliance posture
- Show proof of compliance with instant reports and dashboards



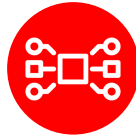
Risk Profiling

- Rank your deployments according to their security risk for prioritization
- Go beyond CVE scores, and understand the true risk of vulnerabilities based on information derived from Kubernetes
- Track improvements in your security posture to validate impact of your actions



Configuration management

- Identify configuration risks such as network exposures, privileged containers, processes running as root, and noncompliance to align with industry best practices
- Check for misconfigurations of your application deployments in CI/CD workflows.
- Analyze Kubernetes RBAC settings



Network segmentation

- Visualize active vs allowed network traffic to identify risky traffic
- Enable security teams to audit network policies and recommend better policies
- Simulate new, secure network policies and their impact
- Baseline network traffic to alert when it deviates from known-good network activity



Runtime detection & response

- Identify anomalous runtime activity using process allowlists and baselining
- Use pre-built policies to detect common threats such as crypto mining, privilege escalation, and various exploits
- Respond to threats with real time alerts or use Kubernetes-native controls to kill and restart suspicious pods

Where can/shall I apply encryption on the stack?



Application



Platform



Database

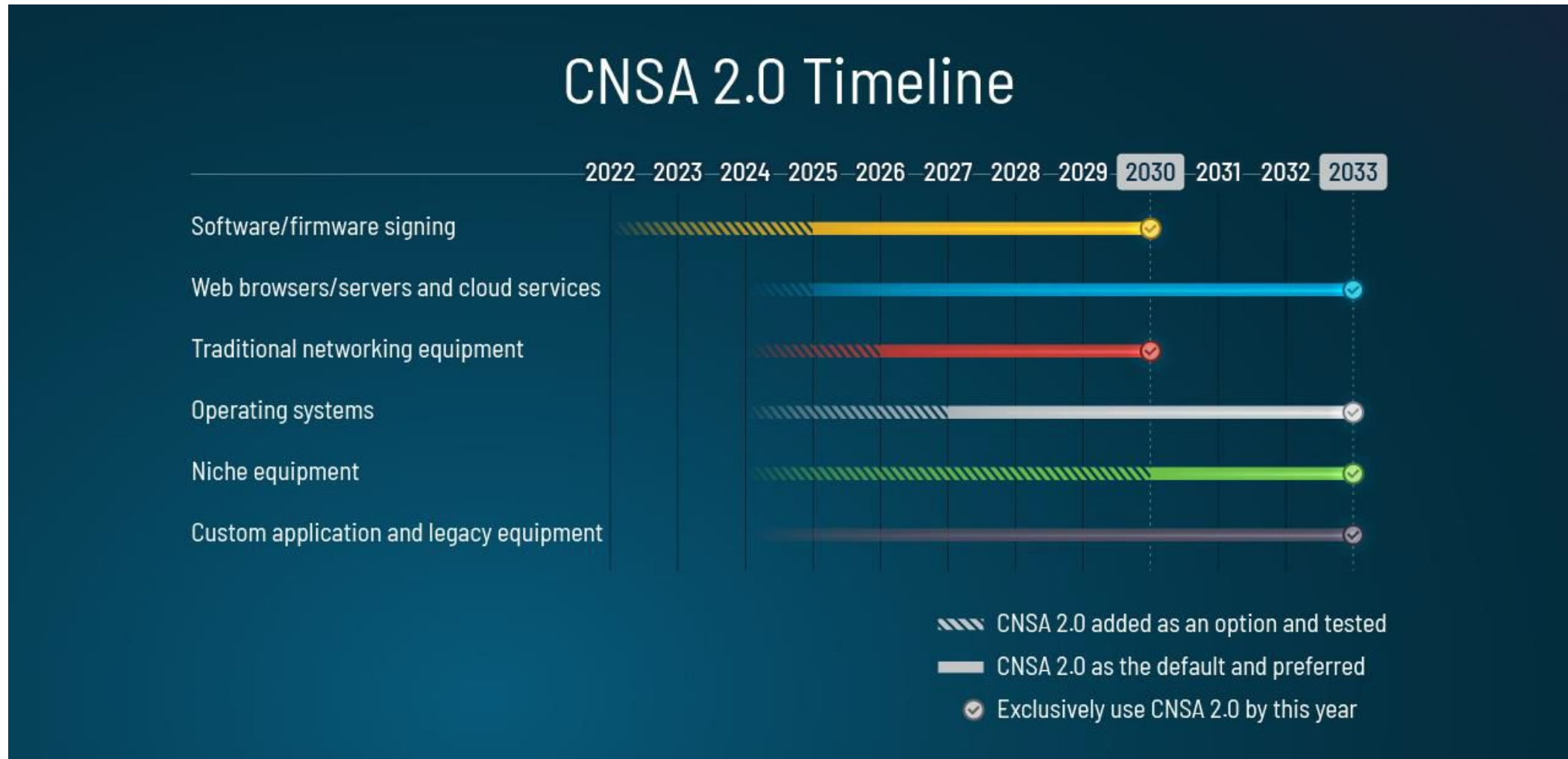


Filesystem / Operating System

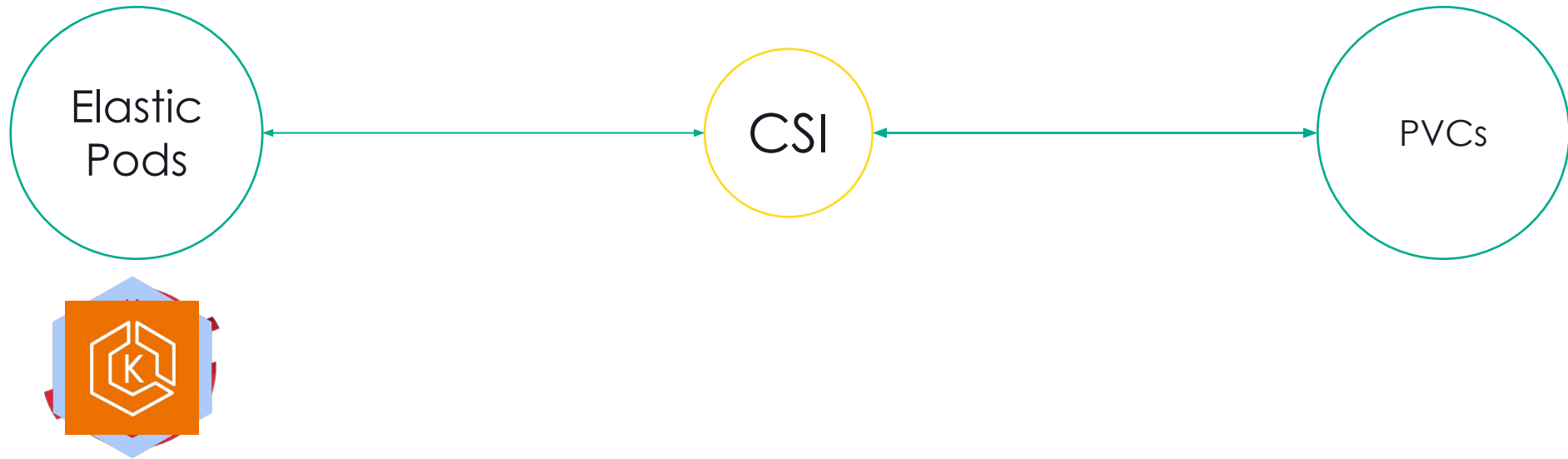


Hardware

Quantum Risk



Ensure portability of encrypted data



Questions & Answers