The everlasting escape room:

Navigating your way through cloud security

Chris Toulson
Solution Architect,
Deutsche Bank

Johana Limka
Account Solution Architect,
Red Hat

Yuval Kashtan
Senior Principal Software Engineer,
Red Hat

Red Hat

What we'll discuss today

- Brief view
  - Operational Resiliency and Regulators
  - Business challenges
- Encryption
  - Cloud, Security
  - Segment, Identify, Encrypt
- Red Hat OpenShift
  - Practicalities with OCP
  - North-South (N-S) and East-West (E-W) cluster traffic encryption solution
  - Demo
- Move forward, faster

Cloud usage is being reshaped by emerging regulatory requirements

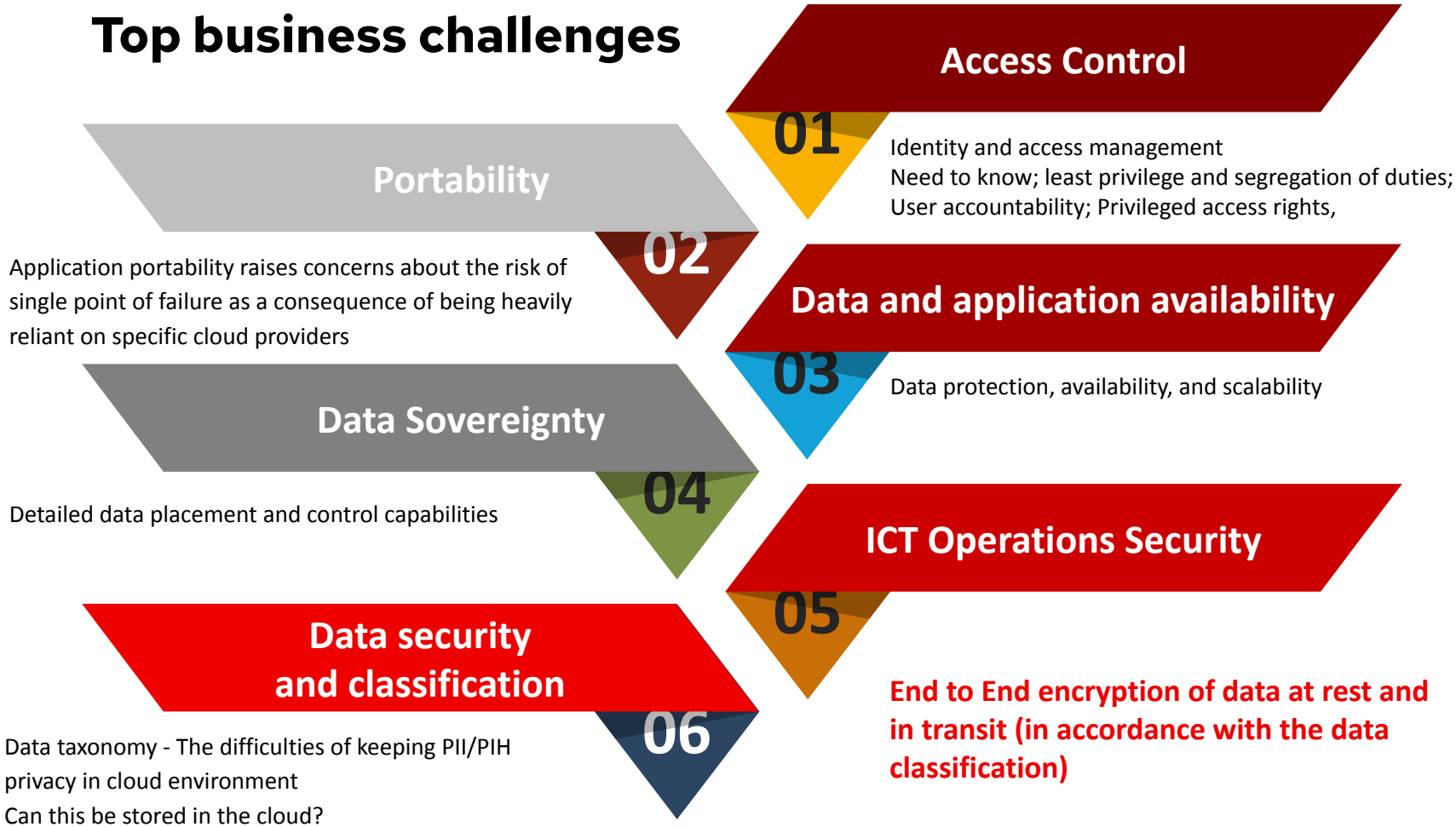
TBD — Cloud Sovereignty

TBD — Directive on Critical Infrastructure Resilience (CIR)

2024/2025 — Digital Resiliency (DORA), NIS 2

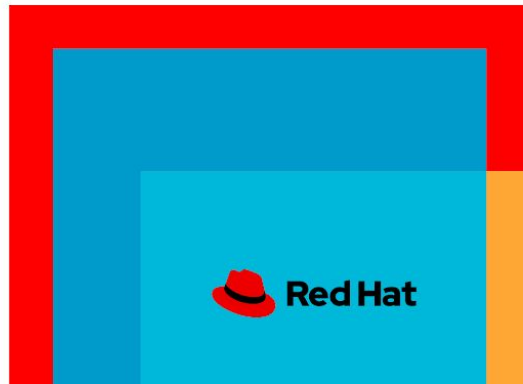
2018 — Data Privacy (GDPR)

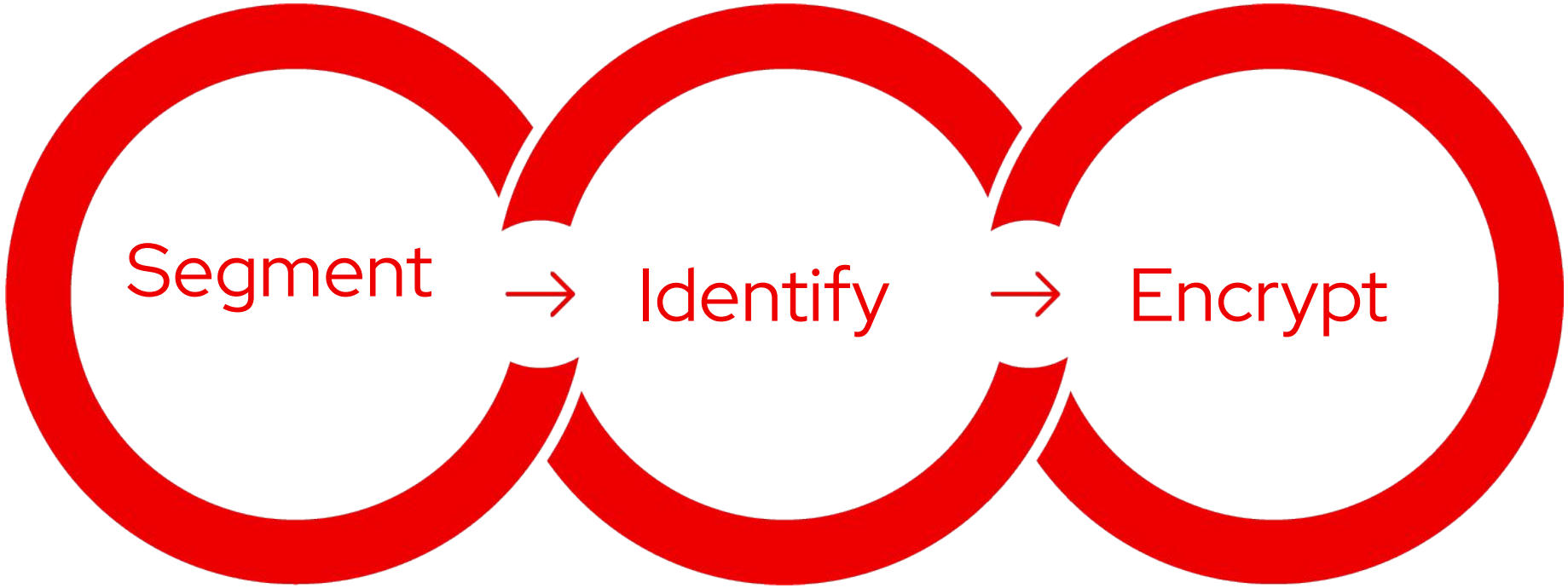
Top business challenges



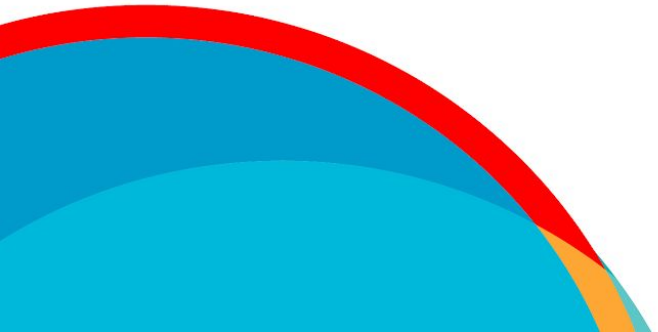
Cloud, Security

- Protection
- Types of Cloud
- Regulators
- Vulnerabilities
- Exposure
- Approach
- Externalise
- Guardrails
- Working in parallel




Segment
Identify
Encrypt

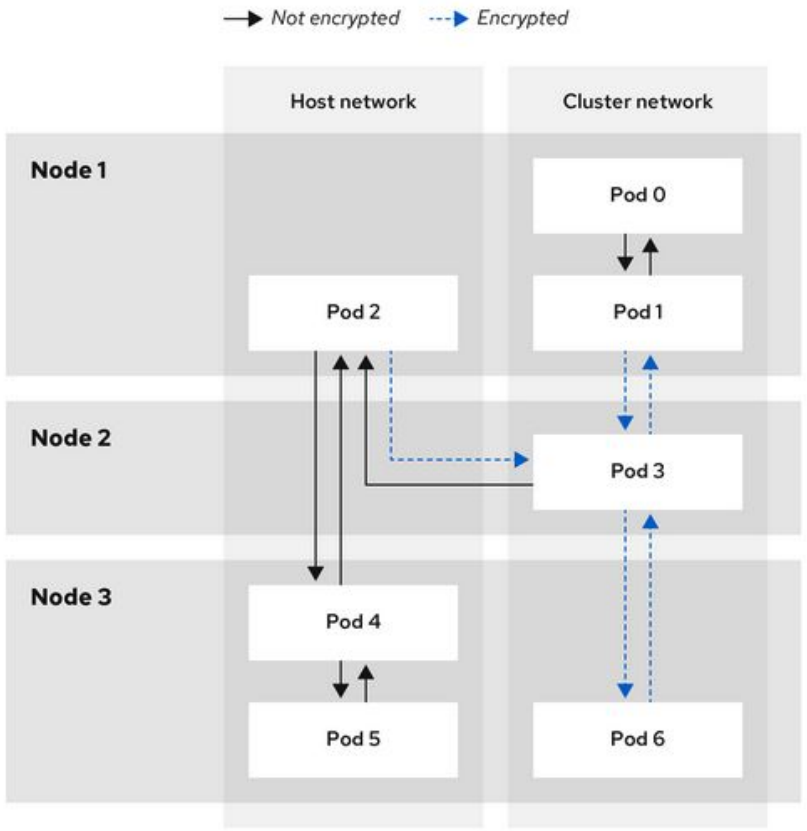
OpenShift Practicalities



Red Hat

OpenShift East-West IPsec

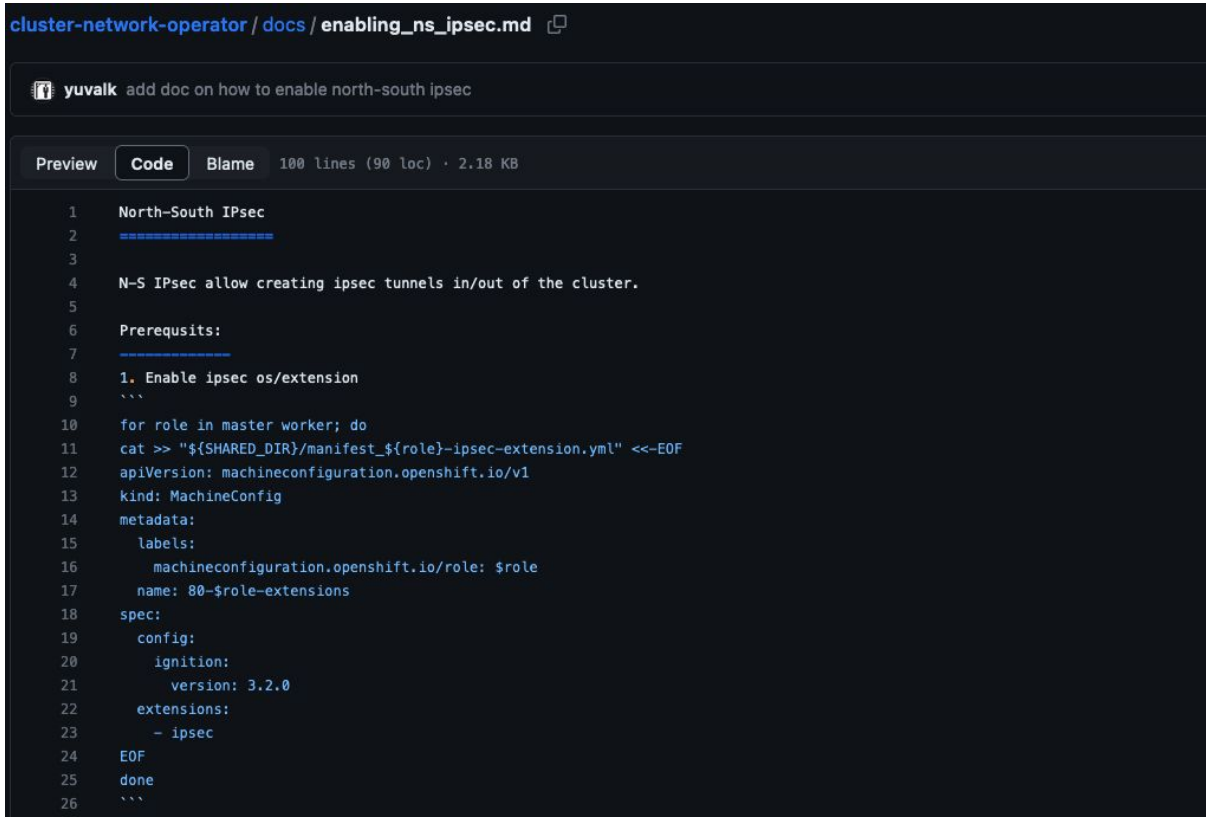
- ovn kubernetes SDN built in IPsec support
- Protect pod-to-pod traffic
- Fully self managed solution
- Simple enablement with a single, true/false config parameter



Red Hat

Announcing North-South IPsec

- 4.14 Technology Preview
- Same as RHEL Libreswan on host
- Customer managed



cluster-network-operator / docs / enabling_ns_ipsec.md

yuvalk add doc on how to enable north-south ipsec

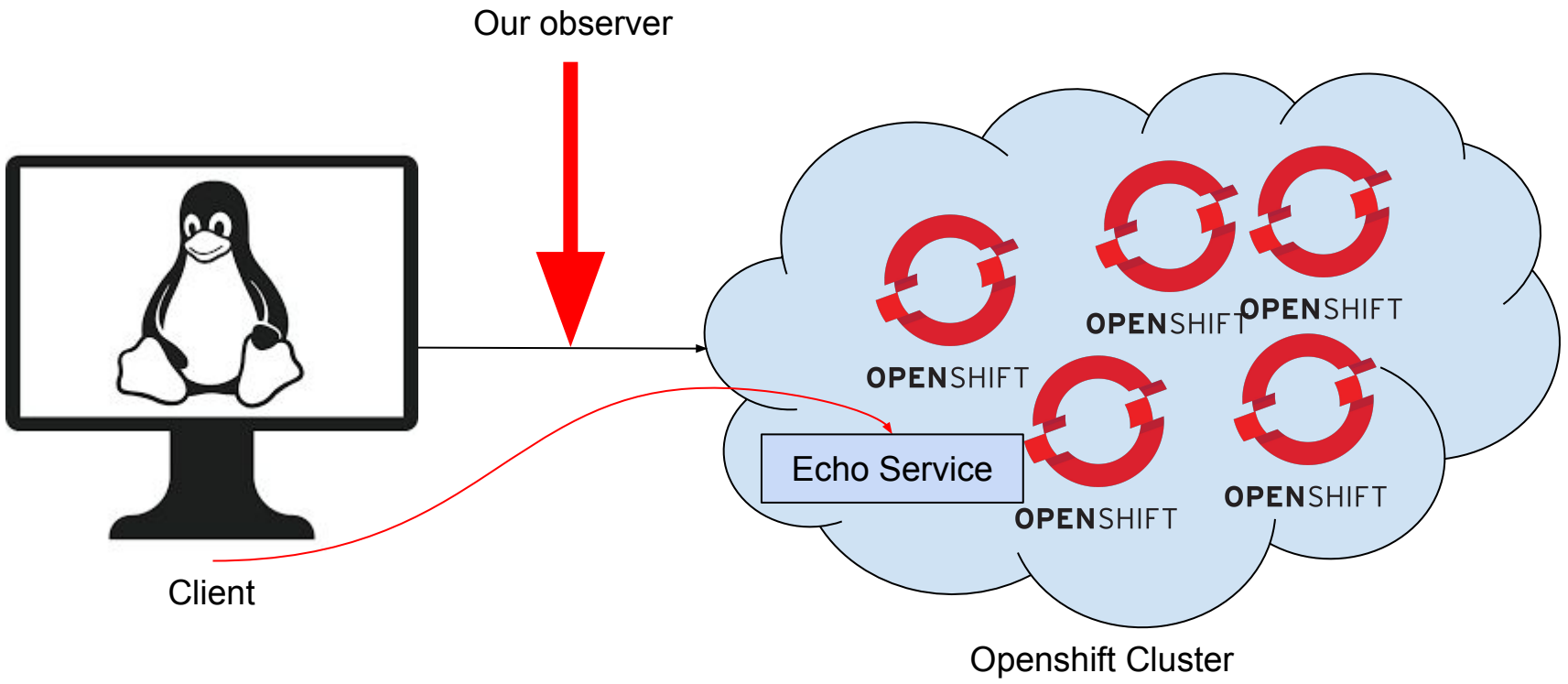
Preview | Code | Blame | 100 lines (90 loc) · 2.18 KB

```
North-South IPsec
=================

N-S IPsec allow creating ipsec tunnels in/out of the cluster.

Prerequsits:
============
1. Enable ipsec os/extension
```
```
for role in master worker; do
cat >> "${SHARED_DIR}/manifest_${role}-ipsec-extension.yml" <<-EOF
apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfig
metadata:
  labels:
    machineconfiguration.openshift.io/role: $role
  name: 80-$role-extensions
spec:
  config:
    ignition:
      version: 3.2.0
  extensions:
    - ipsec
EOF
done
```
```
```

Demo

Peering into the matrix - What are we going to see

- A simple echo service deployed on an openshift cluster
- Accessed from a RHEL VM
  - Without encryption can see cleartext traffic
  - With encryption network capture shows gibberish



Key takeaway

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology"

Bruce Schneier

Q&A

Red Hat Summit

Thank you


linkedin.com/company/red-hat


facebook.com/redhatinc


youtube.com/user/RedHatVideos


twitter.com/RedHat

Red Hat

In-Transit encryption

This slide is things I hope will be said before my part ;-)

Protect data as it travel between servers

Especially important for cloud where we have 3rd parties owning the network

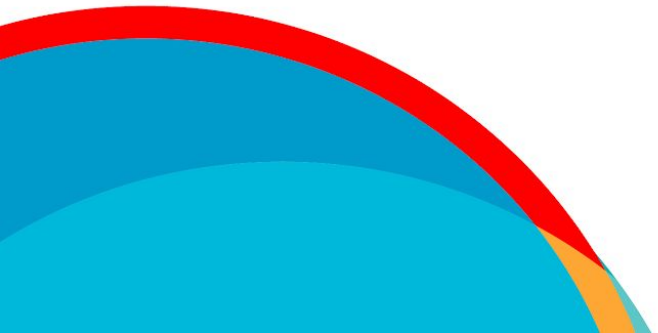
But is also important in many on-perm cases

To lower PII visibility and integrity

- If not I'll try to cover the missing parts

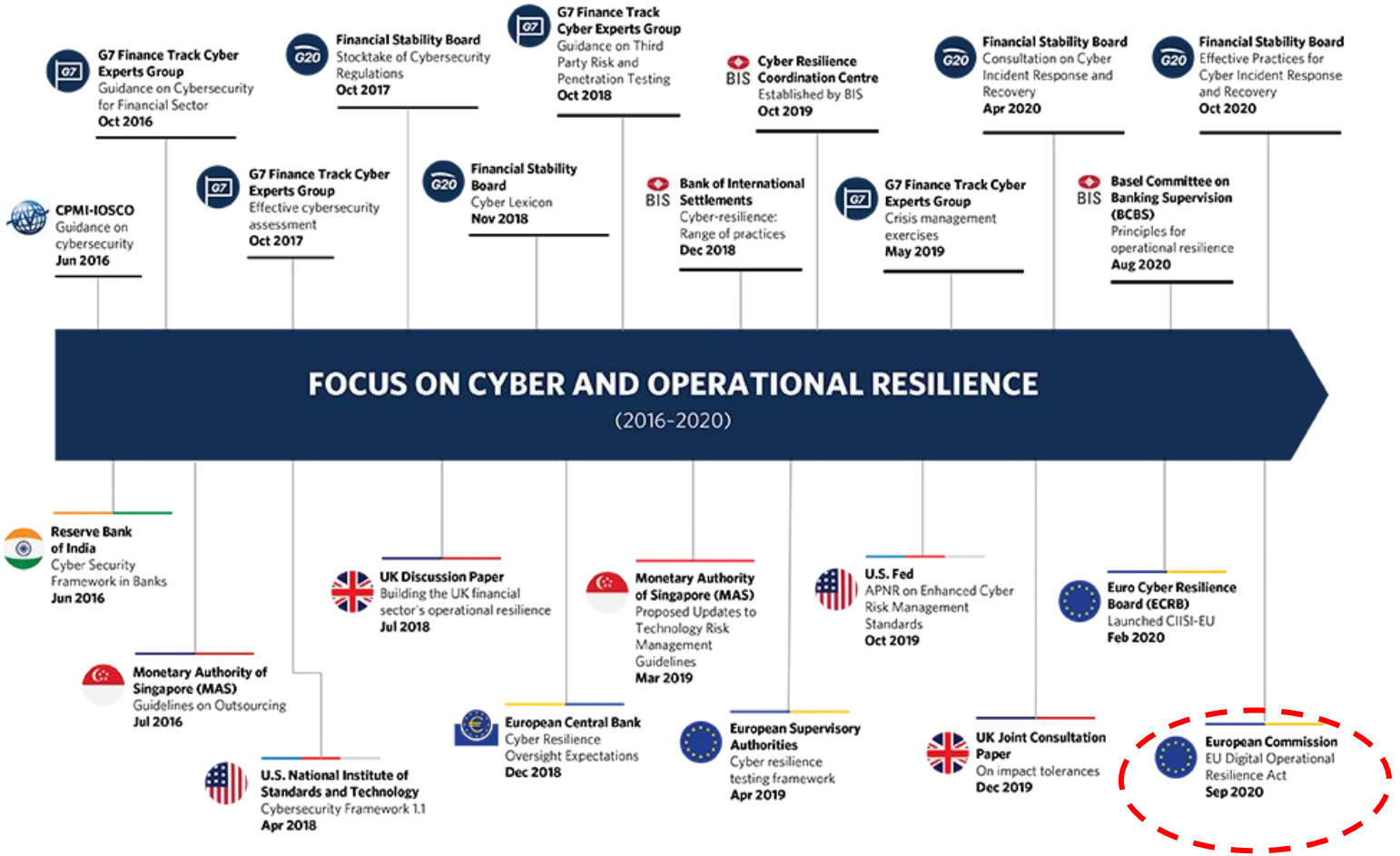
Examples

.



Red Hat

Cloud usage is being reshaped by emerging regulatory requirements



DORA adopted by the European Council on 28 Nov 2022

SOURCE: Marc Saidenberg, John Liver, and Eugene Goyne, "2020 Global Bank Regulatory Outlook: Four Major Themes Dominating the Regulatory Landscape in 2020" (EY, January 20, 2020), https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/banking-and-capital-markets/ey-global-regulatory-outlook-four-major-themes-dominating-the-regulatory-landscape-in-2020_v2.pdf.

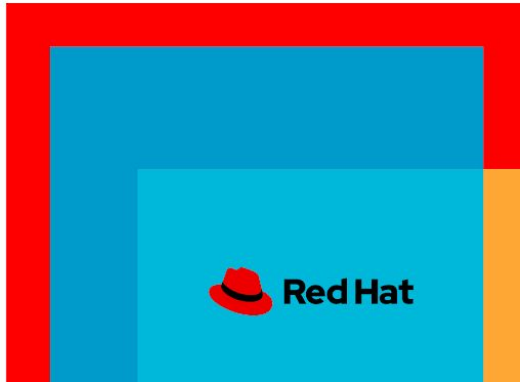
Draft Abstract

The everlasting Escape room - navigating your way through cloud security

When it comes to embracing the public cloud, Enterprises (especially heavily regulated ones) tend to get very creative, resulting in an often unique take on how they would ensure adoption fits within the security posture expected by the organisation and its regulators.

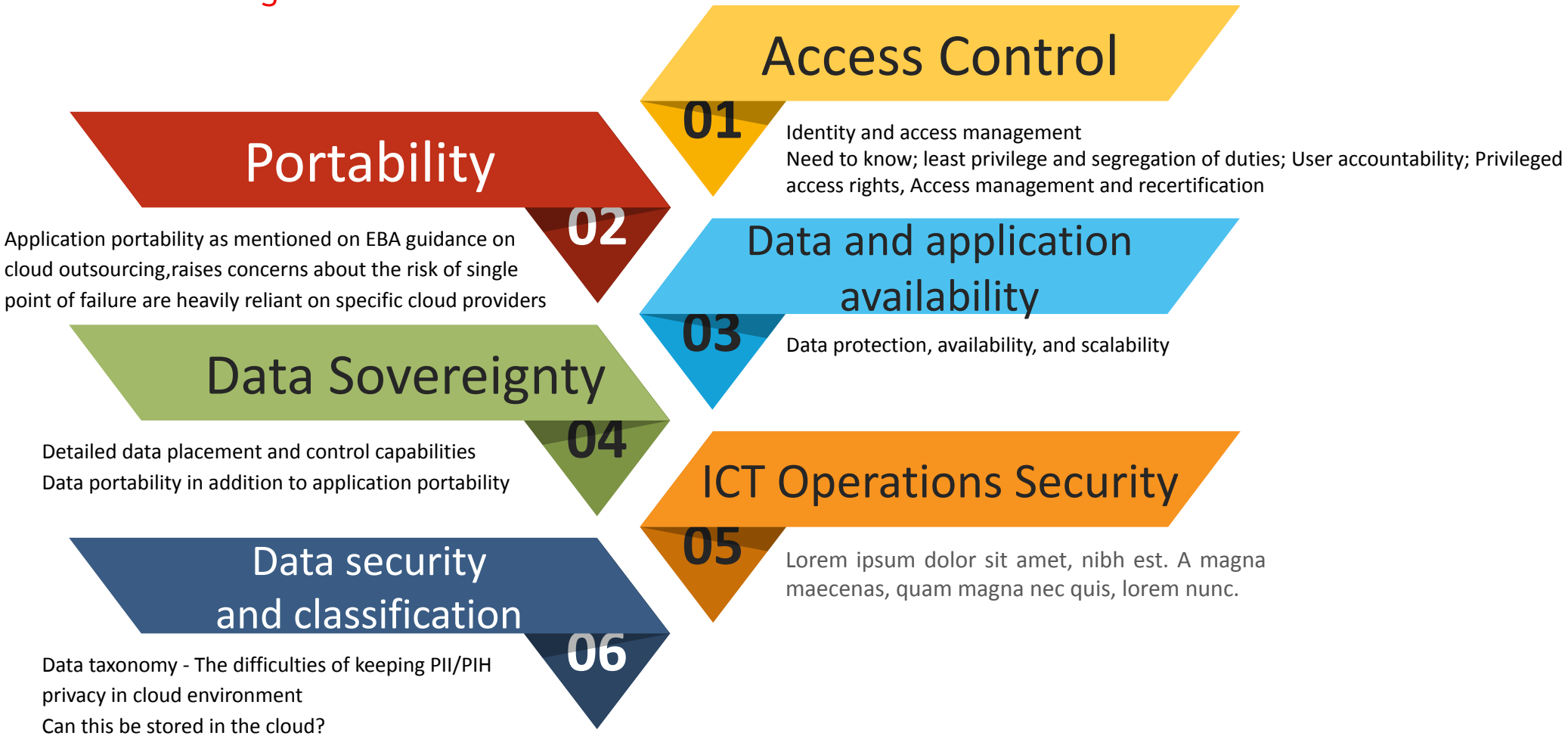
This often results in a very tightly controlled offering once security has been taken into account. Vendors such as Red Hat have a fundamental role in ensuring organisations are empowered to meet the security requirements.

Join us in our journey into public cloud adoption and experience the various challenges with some of the intricacies of deploying OpenShift into highly controlled environments.



Security and Compliance

Top business challenge



Cloud Security

Protection

Protection from the internet: public IPs, external LBs, FW rules
Protection from the underlying cloud provider
Protection from ourselves: segregation between apps/namespaces

Regulators & Cloud

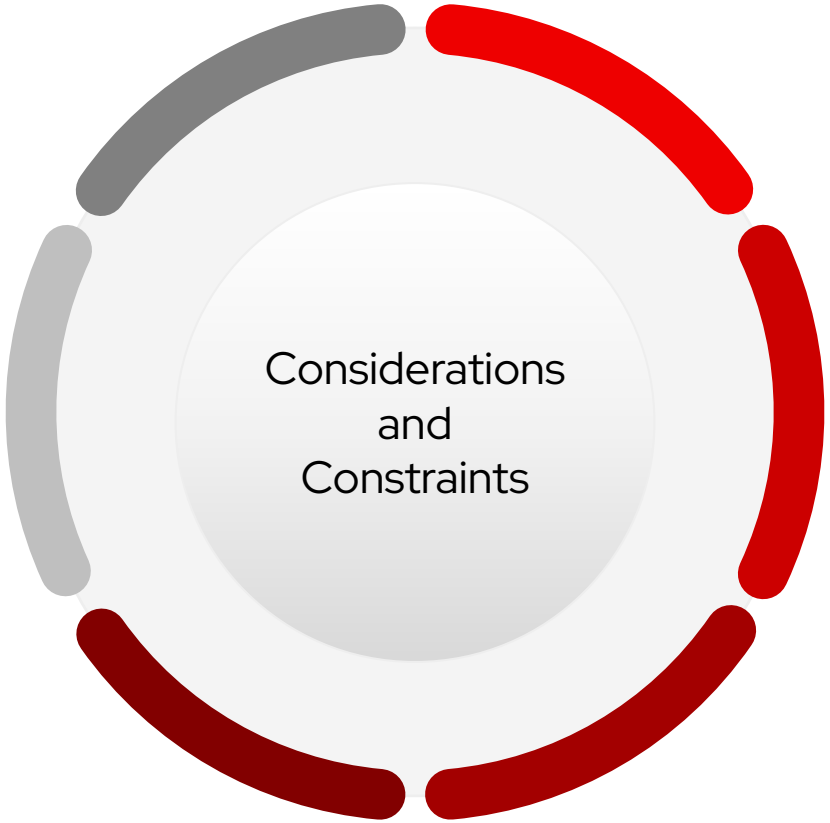
Cloud migration criteria for the applications
Requirements definition and interpretation

Approach

It's often a "no" by default approach and then working backwards

Teams treating OCP as another application rather than a platform or infrastructure provider when it comes to security and associated process

The key point is, everyone is typically working in parallel on the journey so it's a shifting landscape as the security posture matures and guardrails are introduced.
This is why it becomes an **everlasting escape room …**



Exposure

Implications of various network setups such as:
Direct facing applications/network
Indirect internet facing
Internal facing

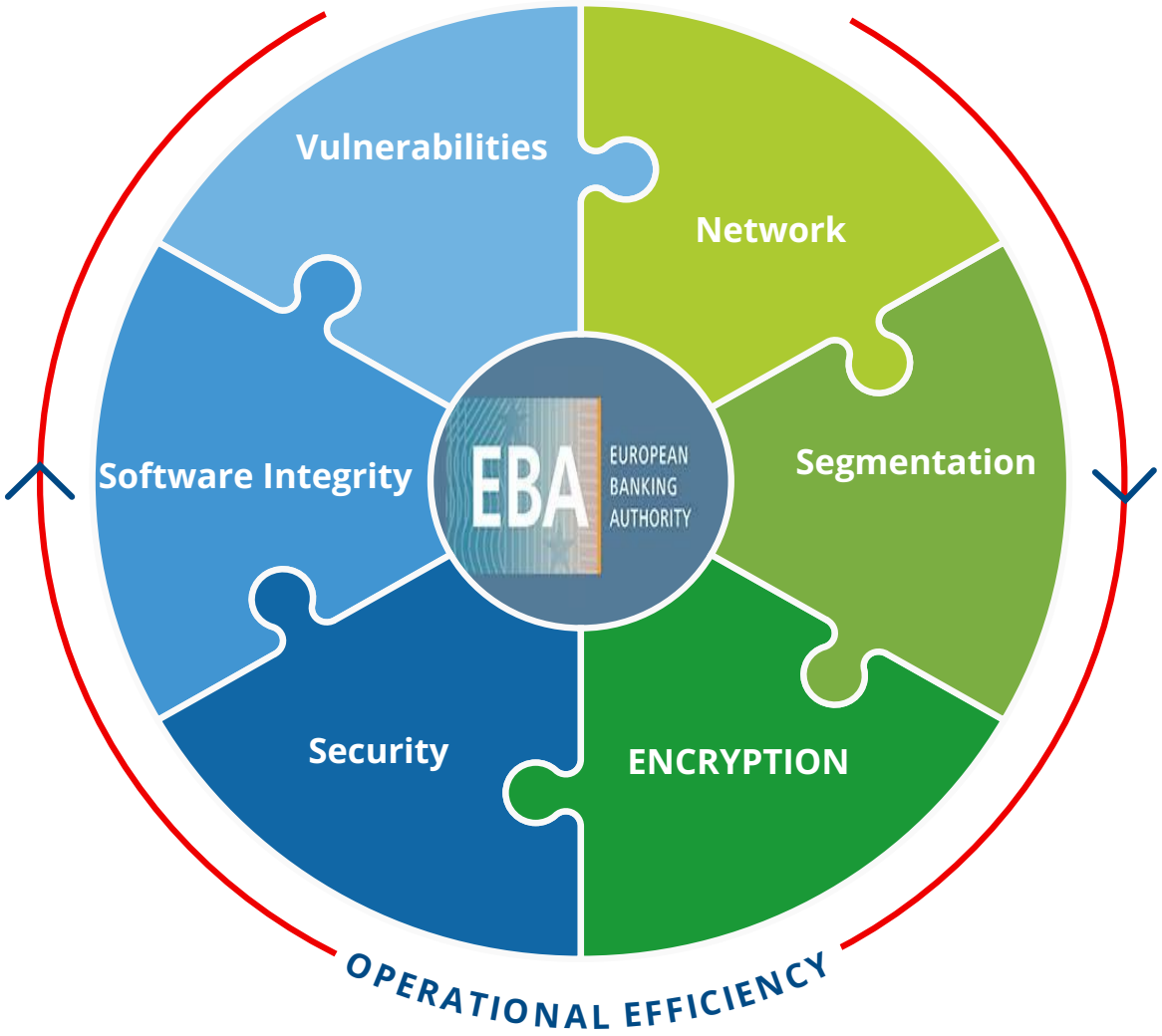
Vulnerabilities

Who owns the images?
Do timelines change in the cloud?
Who owns the remediations

Externalise

Externalise the management of certificates
Automate the management of all certificates
Understand the certs that remain inside the cluster and accept any associated risk
Externalise the management of secrets outside of the cluster
What are the build and runtime guardrails that are in place – for example Sentinel and Prisma

Operations Security and Compliance



Identification of potential vulnerabilities

Implementation of secure configuration baselines of all network components

Implementation of network segmentation, data loss prevention systems

Implementation of protection of endpoints including servers, workstations and mobile devices

Ensuring that mechanisms are in place to verify the integrity of software, firmware and data

Encryption of data at rest and in transit (in accordance with the data classification)

Operations Security and Compliance

Identification of potential vulnerabilities

Implementation of secure configuration baselines of all network components

Implementation of network segmentation, data loss prevention systems

Implementation of protection of endpoints including servers, workstations and mobile devices

Ensuring that mechanisms are in place to verify the integrity of software, firmware and data

Encryption of data at rest and in transit (in accordance with the data classification)

Cloud usage is being reshaped by emerging regulatory requirements

TBD — Cloud Sovereignty

TBD — Directive on Critical Infrastructure Resilience (CIR)

2024/2025 — Digital Resiliency (DORA), NIS 2

2018 — Data Privacy (GDPR)

Red Hat

Chris's slides