Red Hat Summit: Connect Warszawa

Security in the era of AI

Kirsten Newcomer

Sr. Director, OpenShift & Security Product Management
Red Hat

Red Hat

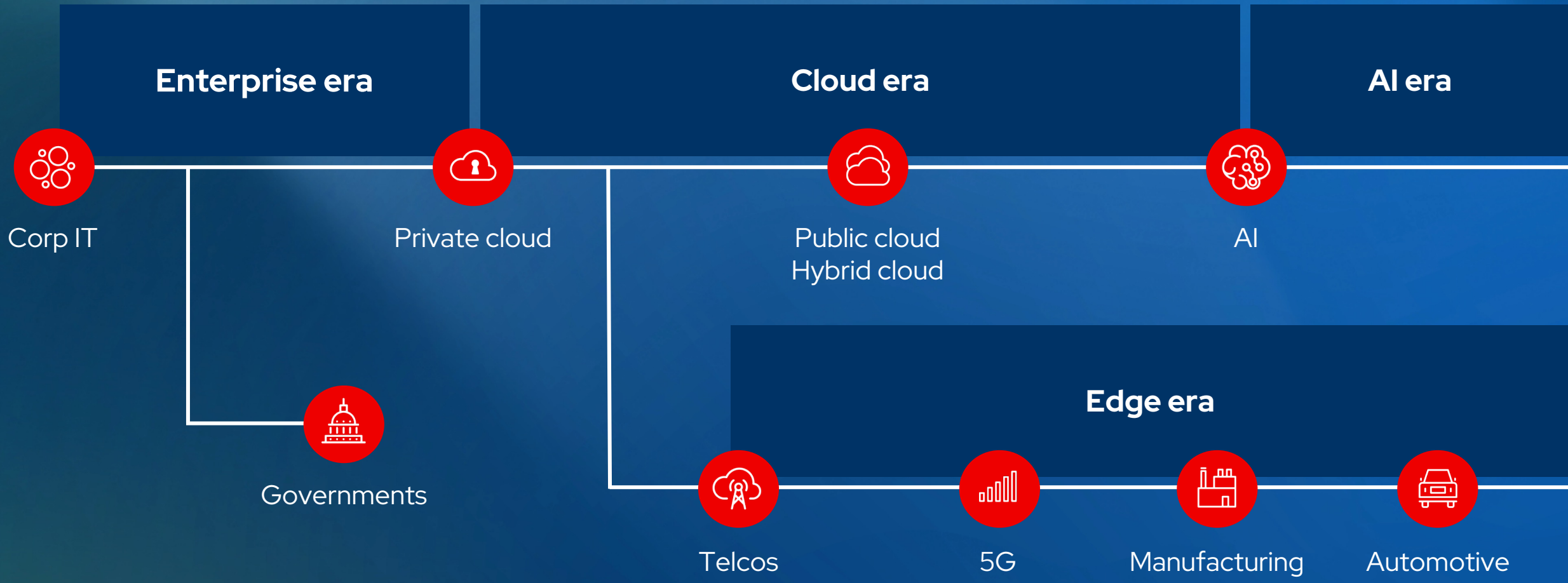

What’s challenging your
IT operations?


What’s driving
your innovation?

Generative AI era

You are here

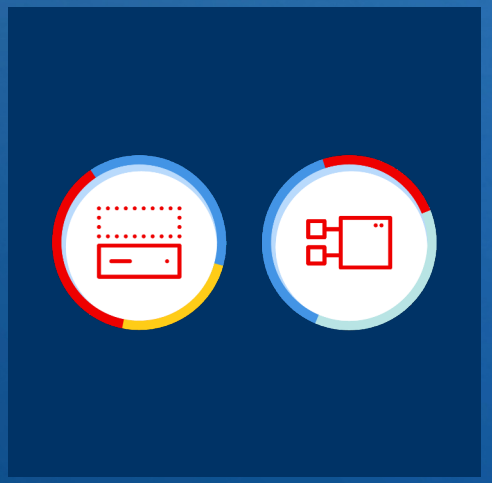
Every previous era has grown and expanded with “open”



Red Hat enables open hybrid cloud

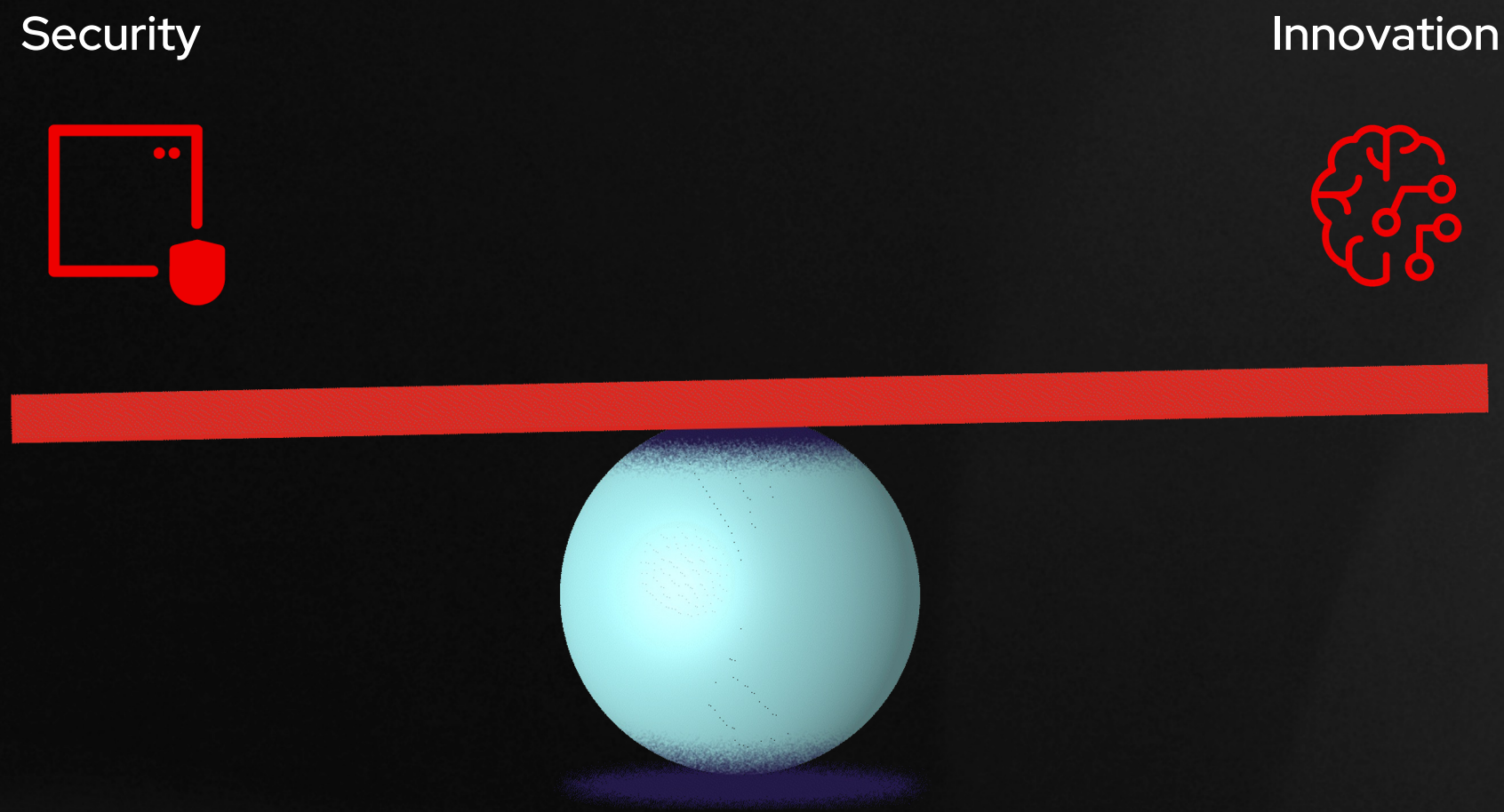
Any cloud

Secure automated infrastructure

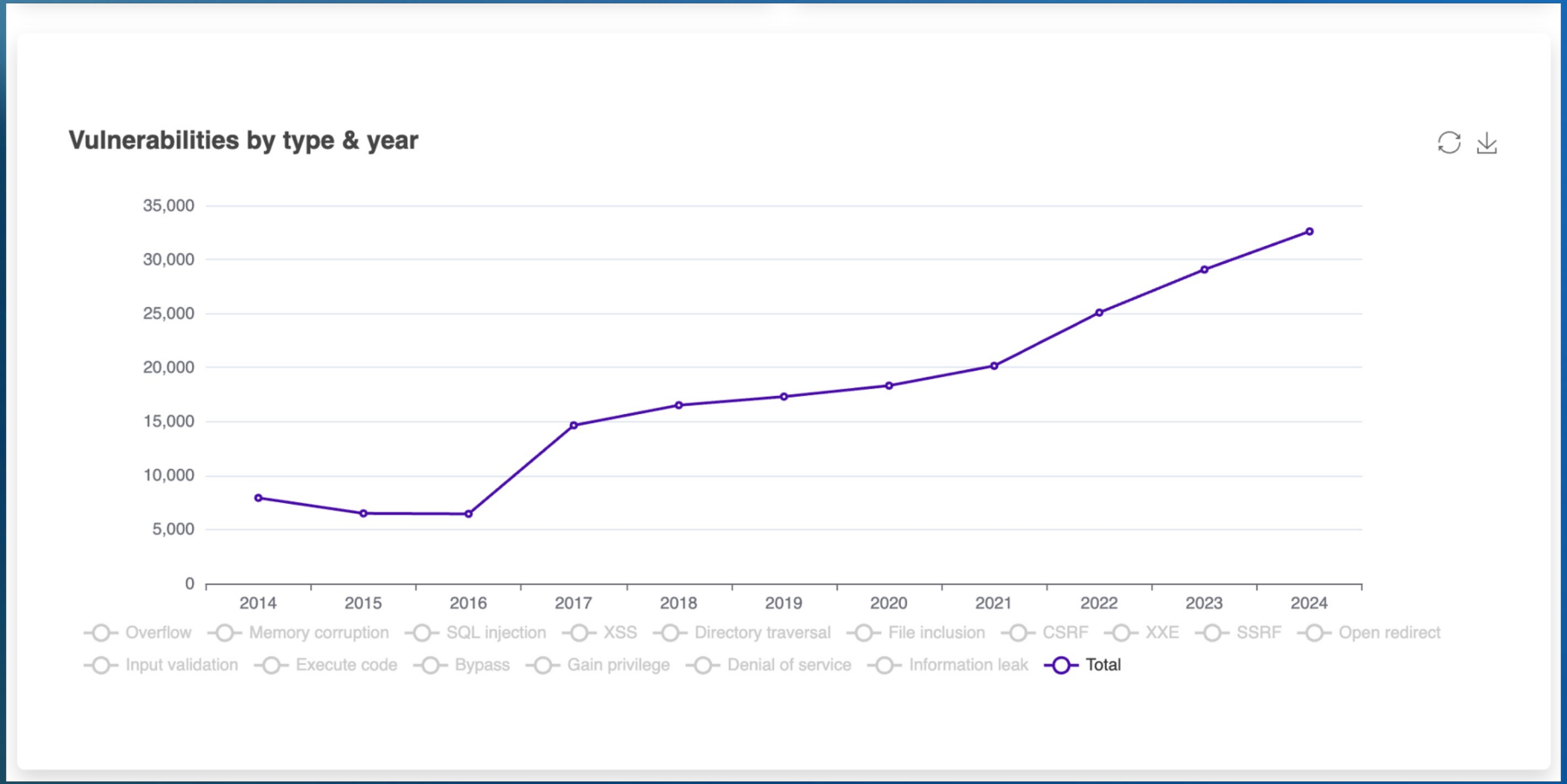


Any Application
(AI, cloud native, traditional, edge)

Team collaboration


Security
Innovation

Every era brings new security challenges



Every era brings new security challenges

The Digital Operational Resilience Act (DORA)

Every era brings new security challenges

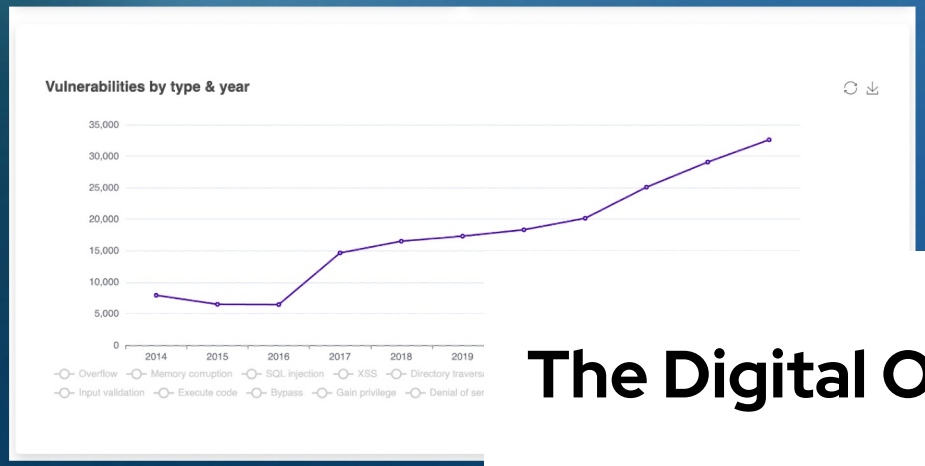
EU AI Act: first regulation on artificial intelligence

The use of artificial intelligence in the EU will be regulated by the AI Act, the world's first comprehensive AI law. Find out how it will protect you.

Every era brings new security challenges

Jailbreaking Generative AI

Security is more important than ever



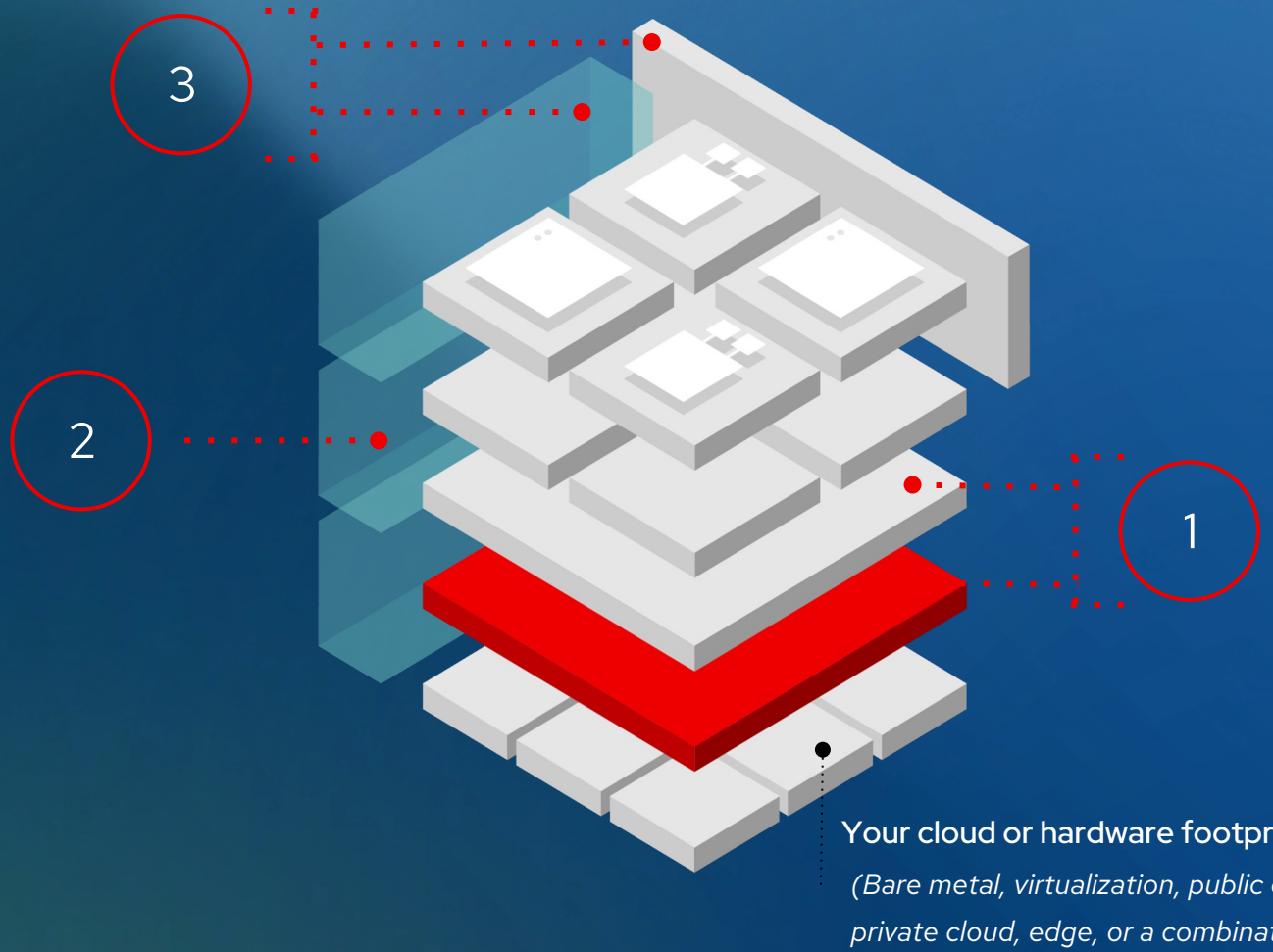
The Digital Operational Resilience Act (DORA)

EU AI Act: first regulation on artificial intelligence

The use of artificial intelligence in the EU will be regulated by the AI Act, the world's first comprehensive AI law. Find out how it will protect you.

Jailbreaking Generative AI

Red Hat's three-part approach to Security in the age of AI



1. Start with a strong foundation with built-in security capabilities
2. Implement trusted software supply chain using DevSecOps practices
3. Automate, automate, automate to manage and secure the stack

Red Hat Enterprise Linux security benefits

Secure foundation for running workloads in the open hybrid cloud

Modern, multi-layered security capabilities to reduce risk

Built-in compliance tools to meet security standards

Automated patching and remediation without downtime

Consistent security controls across the hybrid cloud

Secure development life cycle processes and validation

Workload security in any public cloud environments

Securely build, deploy and run applications at scale

Cloud-native or AI/ML

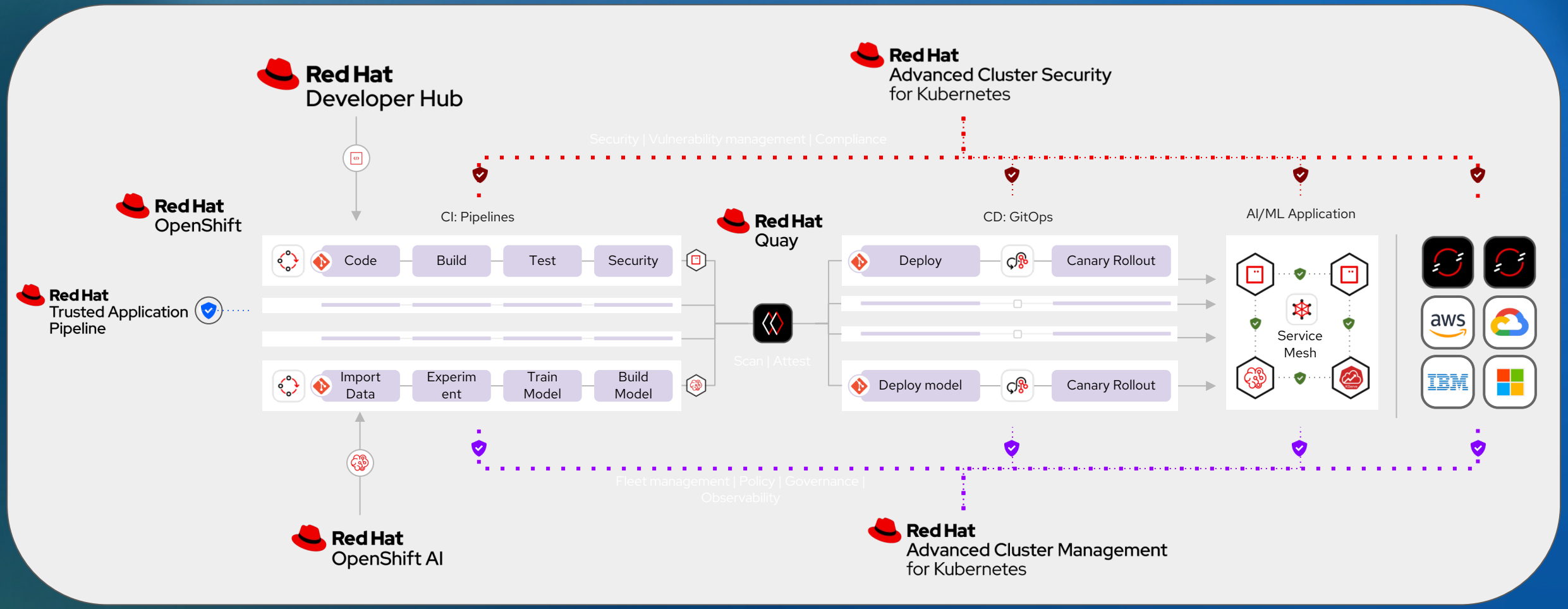
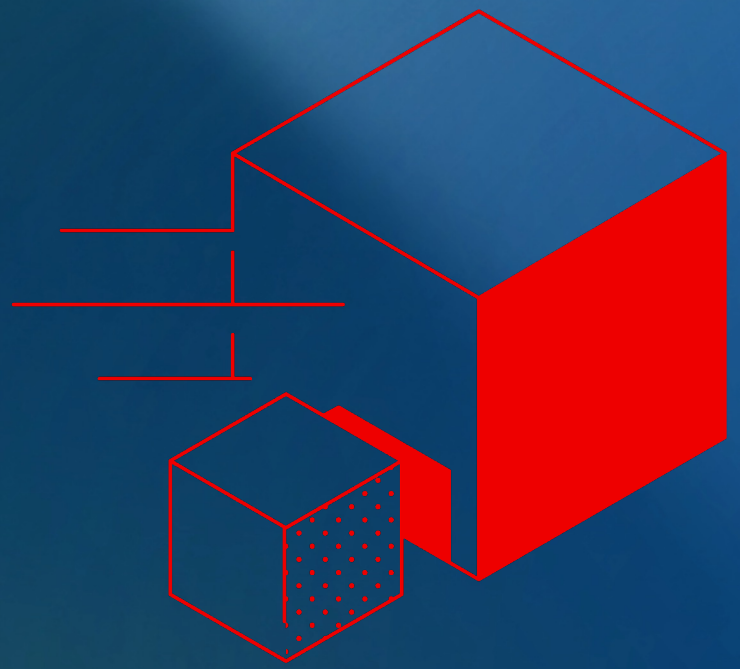


Image mode for Red Hat Enterprise Linux

Combining the power of RHEL with the benefits of containers



All RHEL users benefit from standardization

Simplify operating system (OS) portability across hybrid cloud environments

DevOps teams can reduce platform and application friction

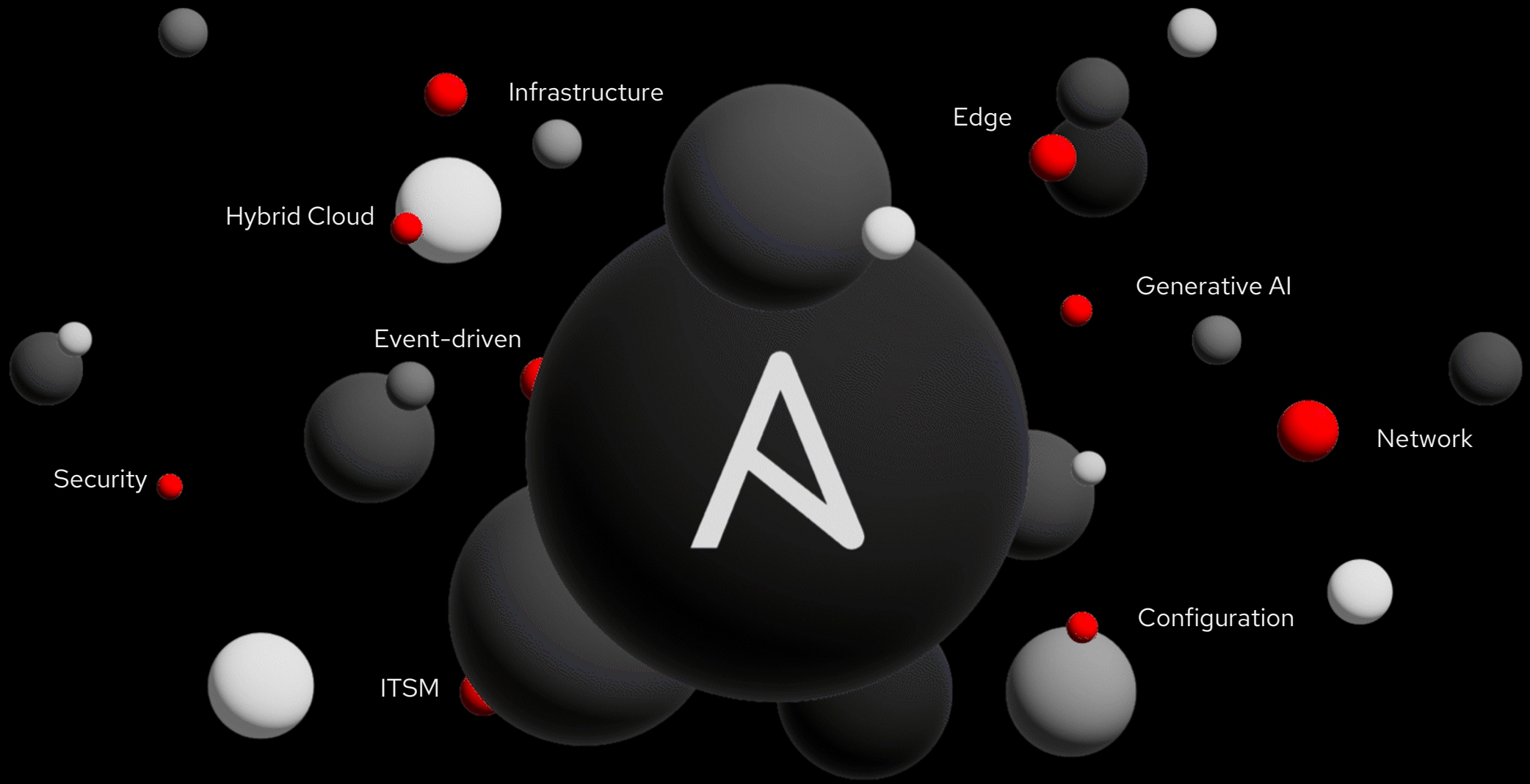
Integrate the operating system into continuous integration and continuous delivery (CI/CD) and GitOps workflows

Security teams can make their jobs far less complex

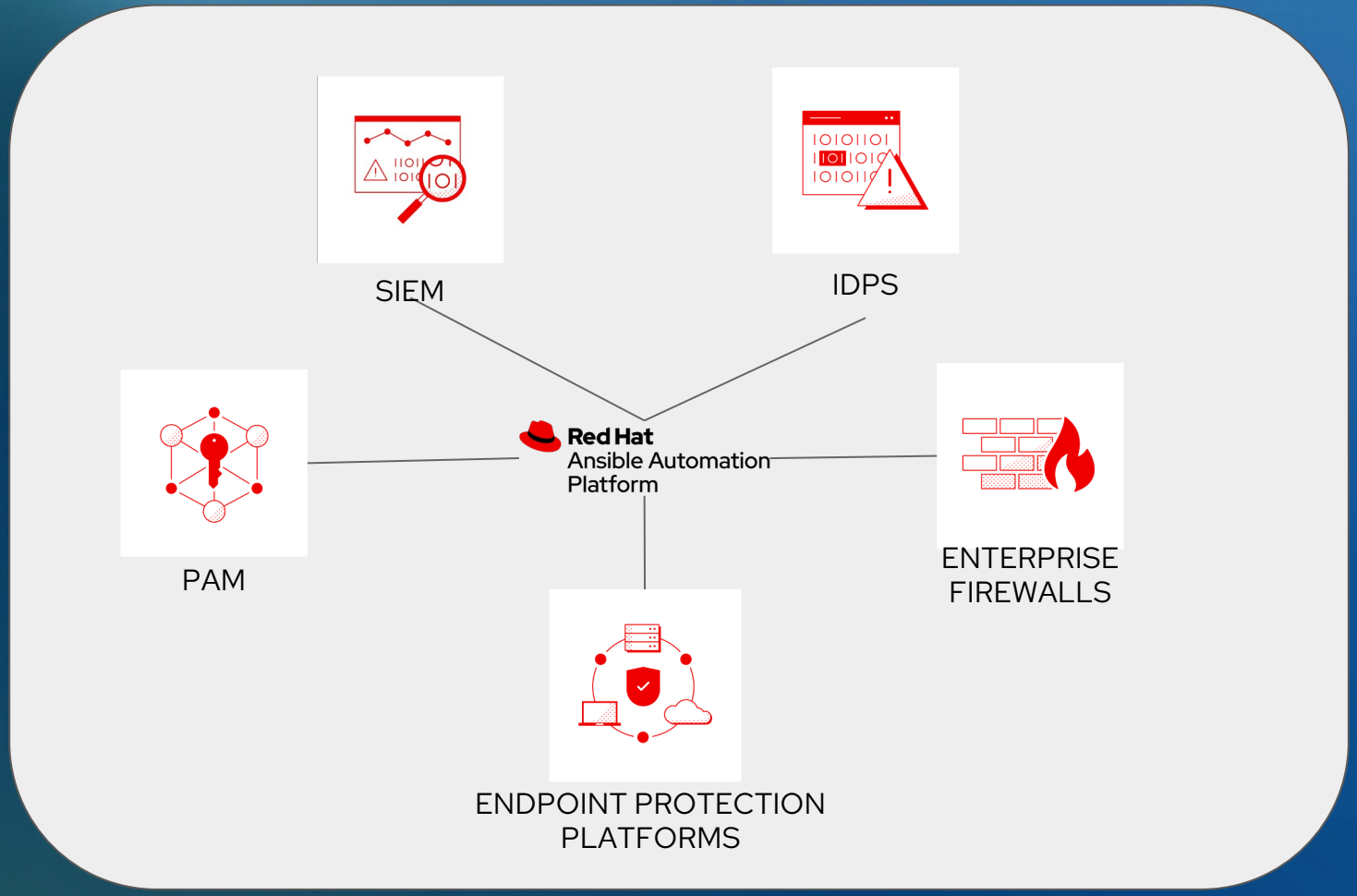
Apply container security tools to the base elements of the operating system

Solution providers can more easily deliver offerings

Build, test, and distribute Red Hat Enterprise Linux-based applications more easily


Infrastructure
Edge
Hybrid Cloud
Generative AI
Event-driven
Network
Security
Configuration
ITSM

Ansible enables security automation



- ✓ Governance, Risk + Compliance (GRC)
- ✓ CI/CD integration
- ✓ DevOps + inventory lifecycle mgmt
- ✓ GitOps
- ✓ Remediation, from datacenter to edge to cloud

OpenShift delivers automated operations

And an opinionated, pre-hardened deployment

Machines

Machines are complex for ops

Make machines easy
(like containers)

Configuration

Config change is risky

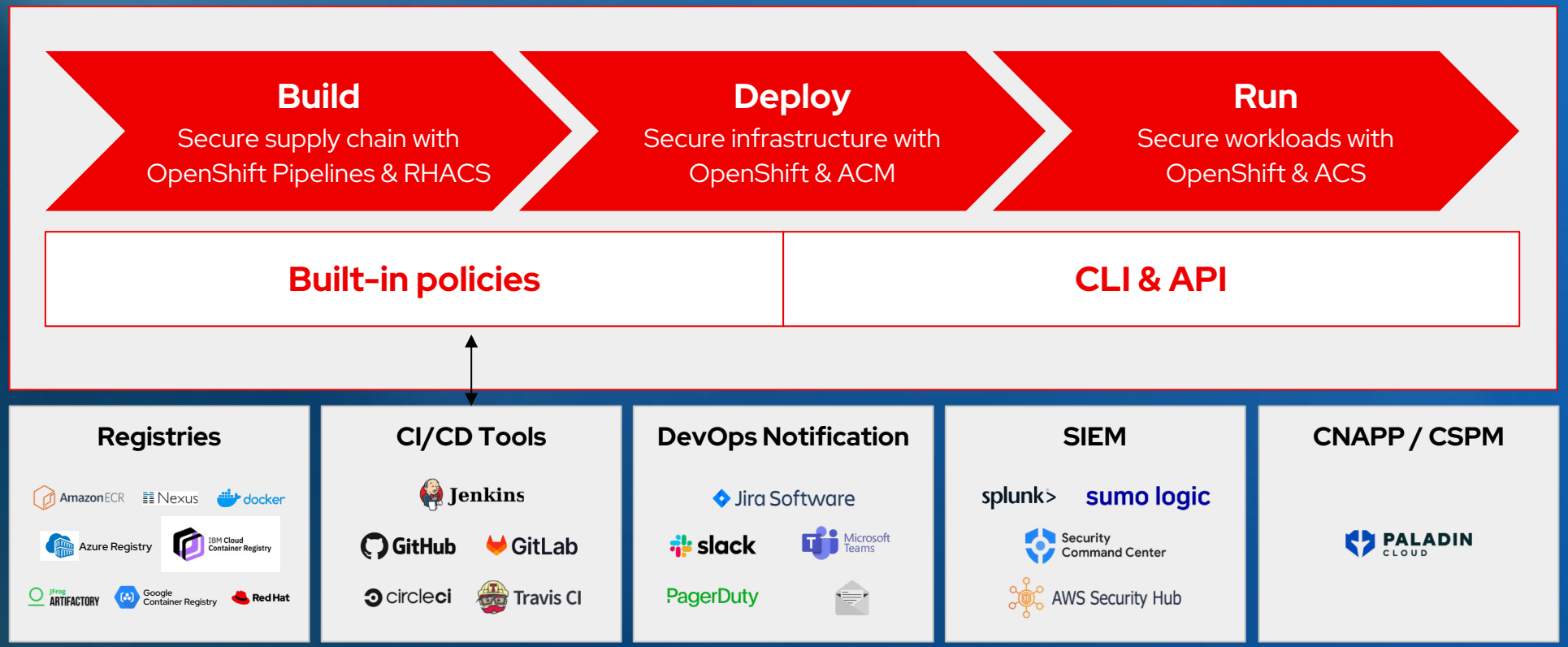
Make config management
and config change
easy and safe

Lifecycle

Software lifecycle is hard

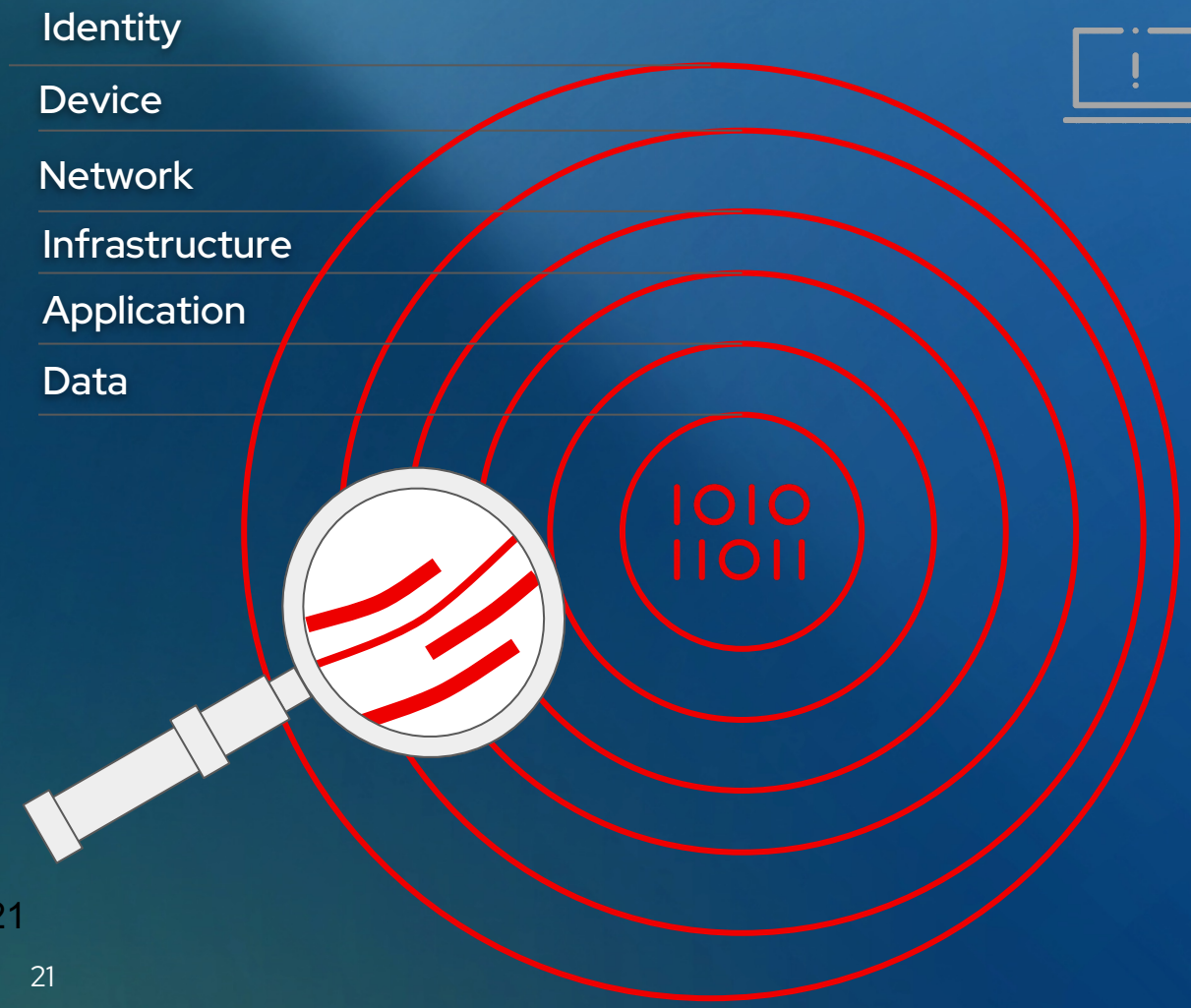
Automate software
lifecycle on Kube

OpenShift enables DevSecOps



Red Hat delivers Defense in Depth and enables Zero Trust

These are complementary approaches – you need both for effective security



Zero Trust is about tightly managing access:

- Who is on each side of the gateway - Identity
- What is allowed through the gateway - Identity
- How Is the gate itself protected - Integrity

Defense in depth is about prevention and mitigation:

- Security controls that create boundaries - proof of identity required to pass
- Security controls for containment, mitigation - Isolation
- Security tools for fast detection, response, and remediation in the event of a breach - Observability

21