Being secure with open platforms

Cybersecurity Symposium
June 18, 2024

Nadhan (E.G.Nadhan)
Global Chief Architect Leader
Red Hat

Red Hat

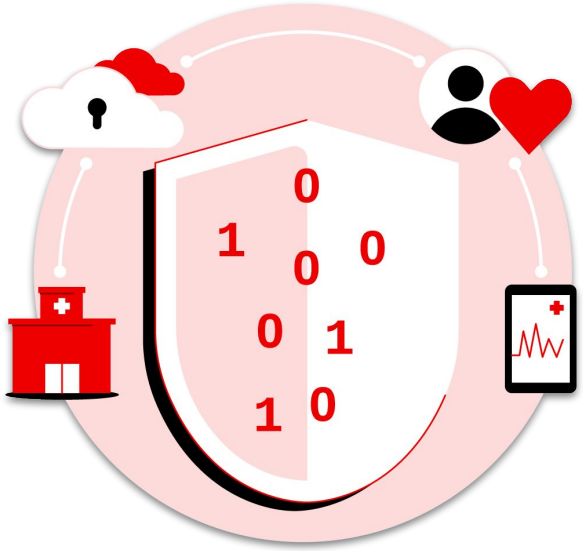
Red Hat Product Security

The functions and services which provide end to end assurance that Red Hat offerings are securely developed, maintained, and compliant

Red Hat

Market Expectations

Influencing Red Hat's Security Strategy



Government Regulation

Red Hat integrates new guidance, standards, and policies from world governments. We work closely with government agencies and customers who need to adhere to heightened security requirements

Supply Chain Concerns

We can attest to how securely we build and manage our offerings using industry standards such as SLSA[1]. We continue to focus on ways to harden our productization pipelines.

Industry Alignment

Red Hat continues to lead in the creation and adoption of updated formats, standards, and integration from industry groups such as NIST[2], First[3], and OpenSSF[4].

Vulnerability Management Emphasis

Our security engineers continue to improve the processes by which we address and disclose vulnerabilities with engineering teams, partners, and customers.

[1] SLSA: Supply chain Levels for Software Artifacts https://slsa.dev/
[2] NIST:National Institute of Standards and Technology https://www.nist.gov/
[3] FIRST: Forum of Incident Response and Security Teams https://www.first.org/
[4] OpenSSF: Open Source Security Foundation https://openssf.org/

Customer Expectations

Delivering Outcomes to Manage Risk

Compliance

Being able to demonstrate that Red Hat's portfolio meets or exceeds industry security requirements

SDL

Red Hat has a secure development lifecycle (SDL) and continues to mature secure development practices; including supply chain security

Incident Response

We continue to provide superlative incident response in analyzing and closing vulnerabilities

SBOM

Our portfolio can consistently build and deliver a software bill of material (SBOM) for each offering using our consolidated component registry

Our services work together to build trusted offerings and **decrease risk**

Under which principles of security do we operate?

Defense in depth	Failure or compromise of a single layer or component of a system should not compromise the system as a whole
Secure by design	Security is not an add-on, afterthought, or checklist
Secure by default	The default system configuration should have all reasonable security controls enabled and all services and features not needed for basic operation disabled
Separation of duty	No one person, entity, or system identity should have full control or access to all elements of a policy, process, or system
Least privilege	Individuals, system identities, roles, entities, or execution contexts, be they human or automation, should be scoped to include only the access to resources required to complete the assigned and expected task or business duties
Transparency	The open source principle of transparency should also apply to security issues and data, including designs, algorithms, and source code, all of which should be freely available when reasonable
Understand the threat	Effective defense of a system must consider the nature of the actual threat or risk that is being mitigated or defended against so the appropriate responses are utilized

Red Hat portfolio security overview

Presenter's Name
Title

Presenter's Name
Title

Red Hat

Hybrid cloud computing can be complex

How do you maintain security and compliance across multiple, different environments?

Challenges:

- Data is spread across workloads.
- Each cloud needs to meet compliance requirements for the specific workloads running.
- Compliance standards and the security environment change, sometimes very quickly.

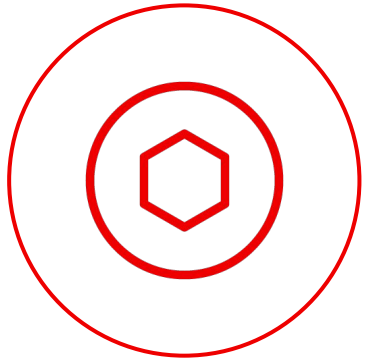
Red Hat

Open standards and open source are key to managing complexity

Organizations want open technologies

Linux is the primary operating system in datacenters and key enabler of public clouds.

Linux containers are the preferred deployment option for cloud-native applications.

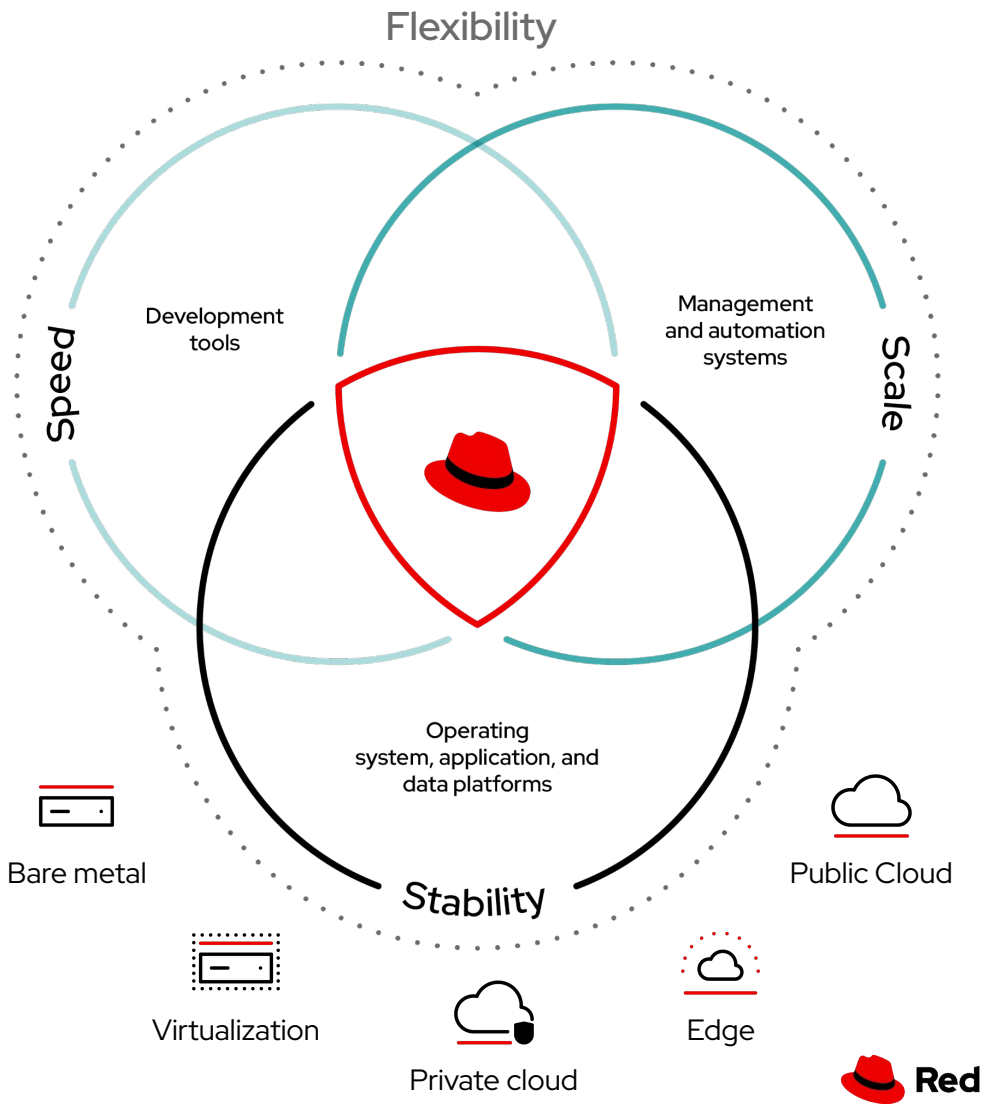


Kubernetes is the leading industry standard for managing containerized workloads.

Red Hat Open Hybrid Cloud Strategy

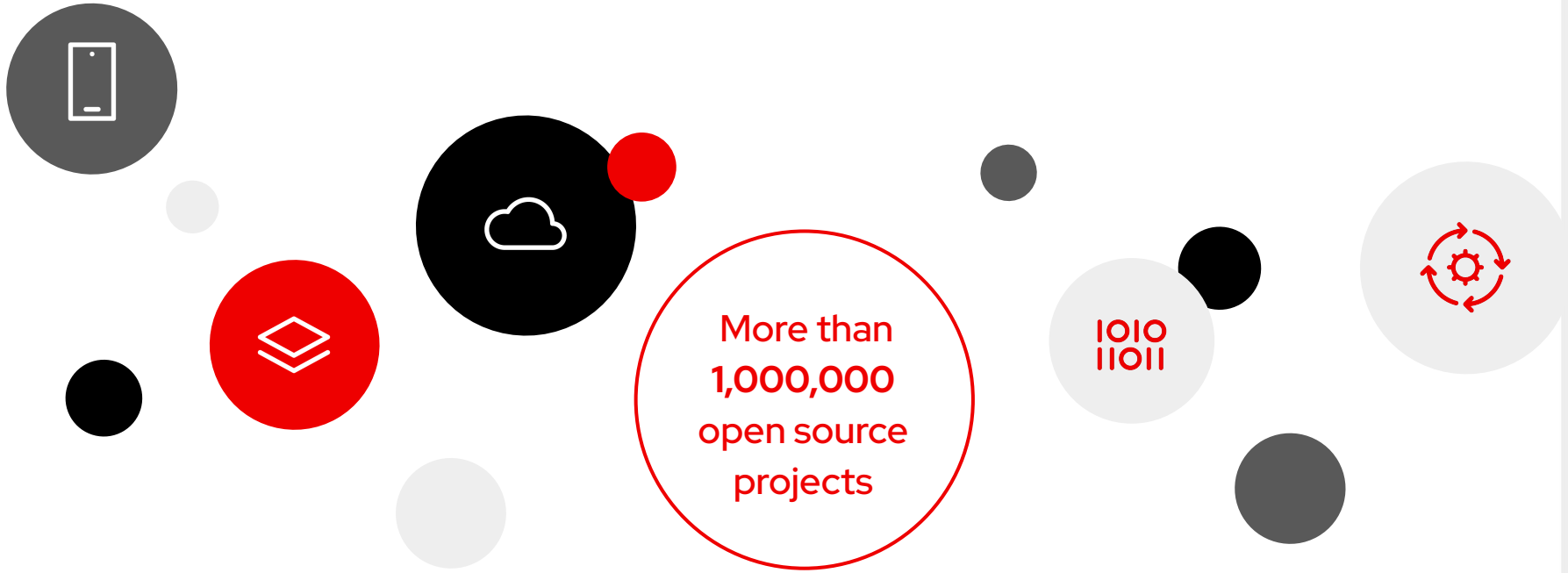
Open hybrid cloud is Red Hat's® recommended strategy for **transforming applications, infrastructure, and processes in order to deliver** a *flexible* and *security-focused* cloud experience with the stability, speed, and scale required for digital business transformation.

It helps customers deliver innovation faster in a hybrid world.



Open source + open standards = open hybrid cloud

Run and manage applications anywhere using hardened open source technologies

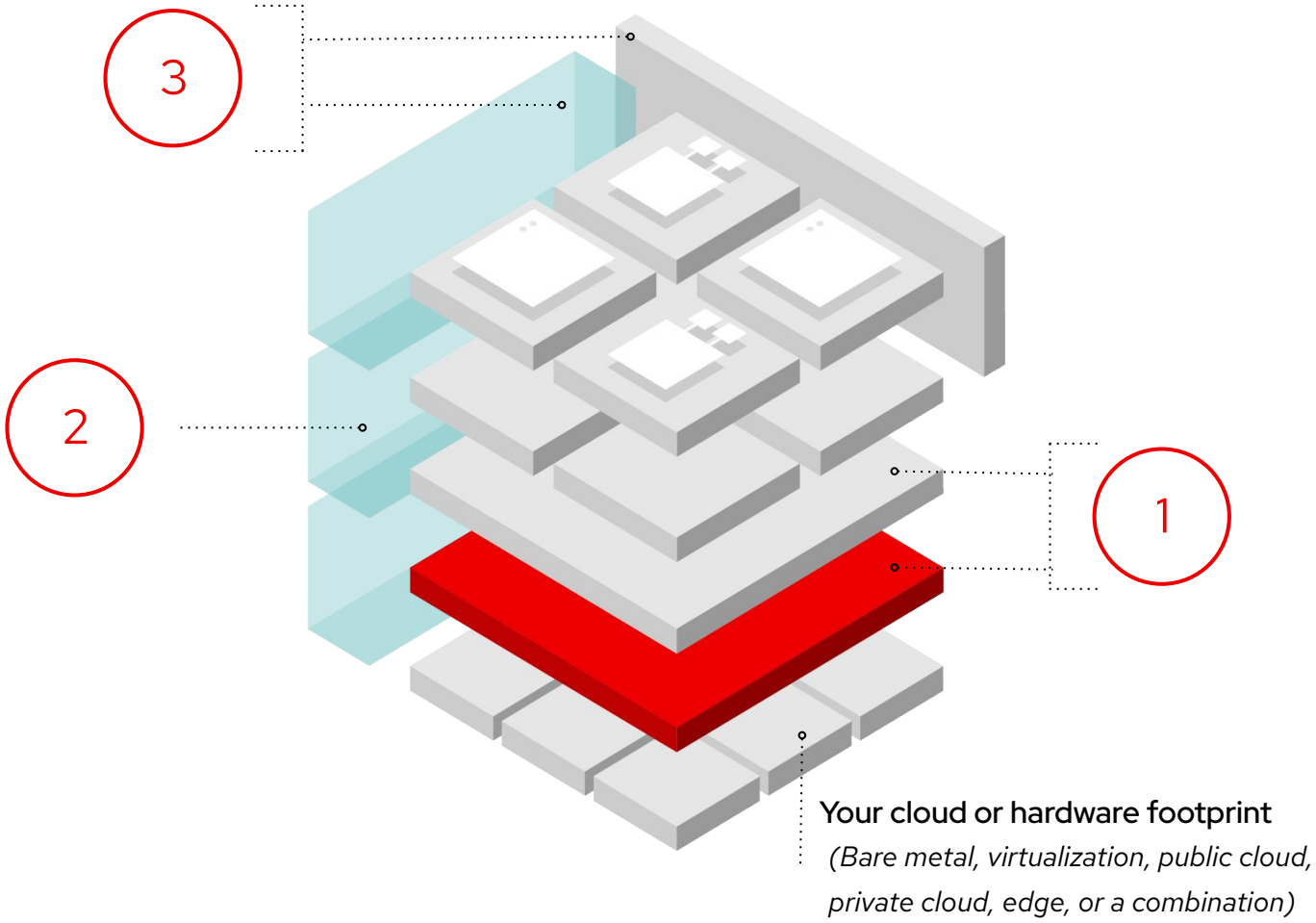


Challenges:

- Unmanaged community software can be more vulnerable to attack.
- Significant time and resources to create a trusted baseline of software from various community projects.
- Burden of support falls on developers.

Red Hat

Red Hat's three-part layered approach to hybrid cloud security:

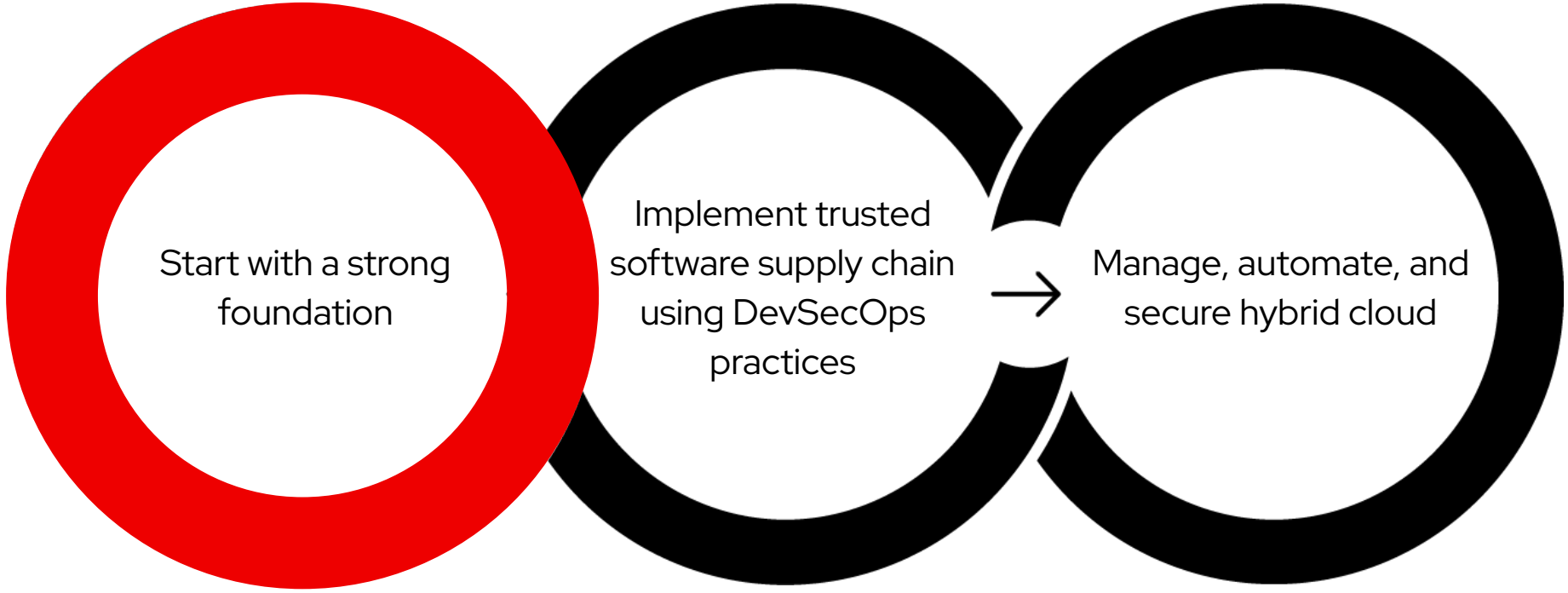


1. Start with a strong foundation
2. Implement trusted software supply chain on top of a hybrid cloud using DevSecOps practices
3. Manage, automate, and secure a hybrid cloud

Red Hat

Red Hat's approach to hybrid cloud security - part one

Build a security-focused hybrid cloud

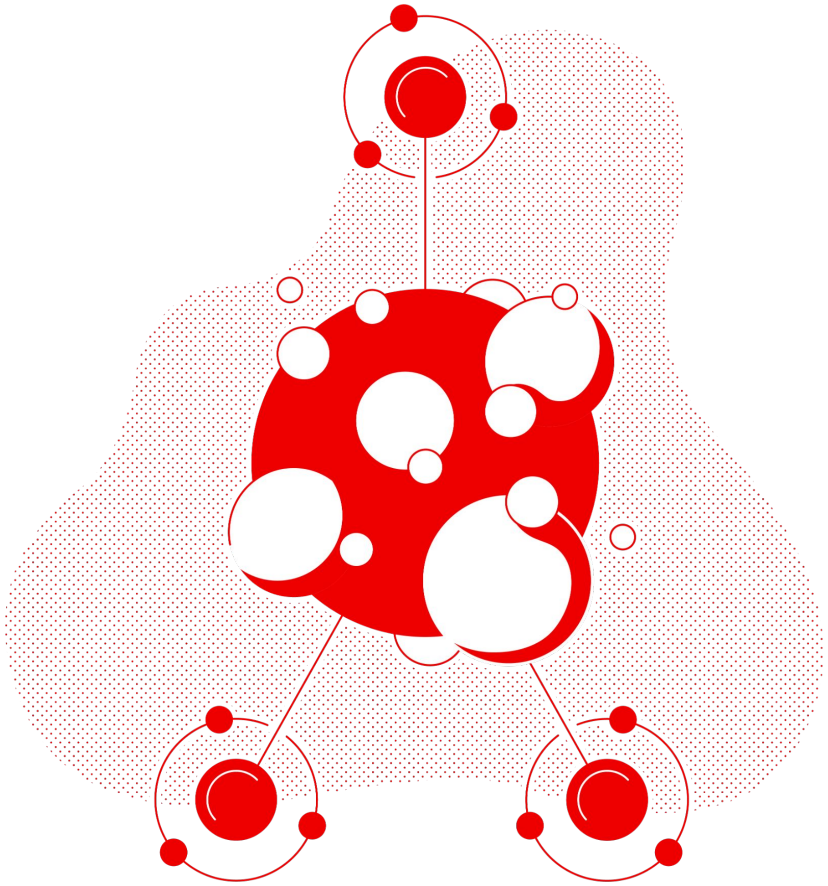


Red Hat

Build a strong security-focused hybrid cloud foundation with **enterprise-ready**, open source software that has a documented, reproducible supply chain.

Red Hat

A patchwork of unmanaged open source can be messy



- Repositories can be anywhere.
- Distribution tends to be unsigned and in community repositories. (And if signed, who holds the keys?)
- Safeguards may exist, but to what standard?
- Upstream repositories are prime targets for supply chain attacks.
- “Release early, release often” can lead to significant changes.

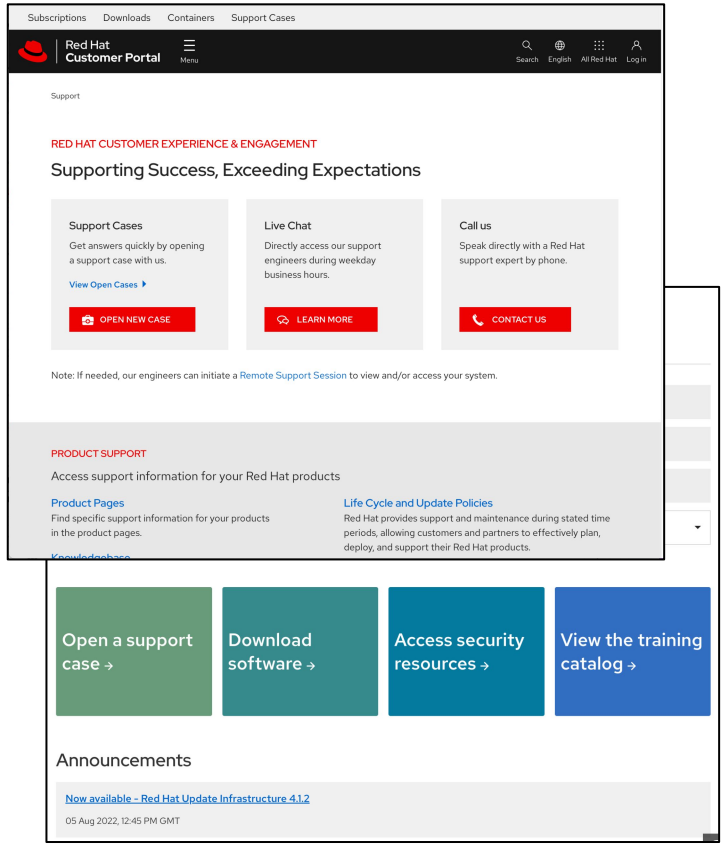
Red Hat: Providing trusted open source software for the enterprise

- All code is stored in internal repositories.
- Strong distribution mechanisms with signed packages.
- Strong safeguards against tampering.
- Minimal modifications over product lifetimes protects from unwanted and potentially risky upstream code changes.

Red Hat

24x7 authoritative security guidance for open source software

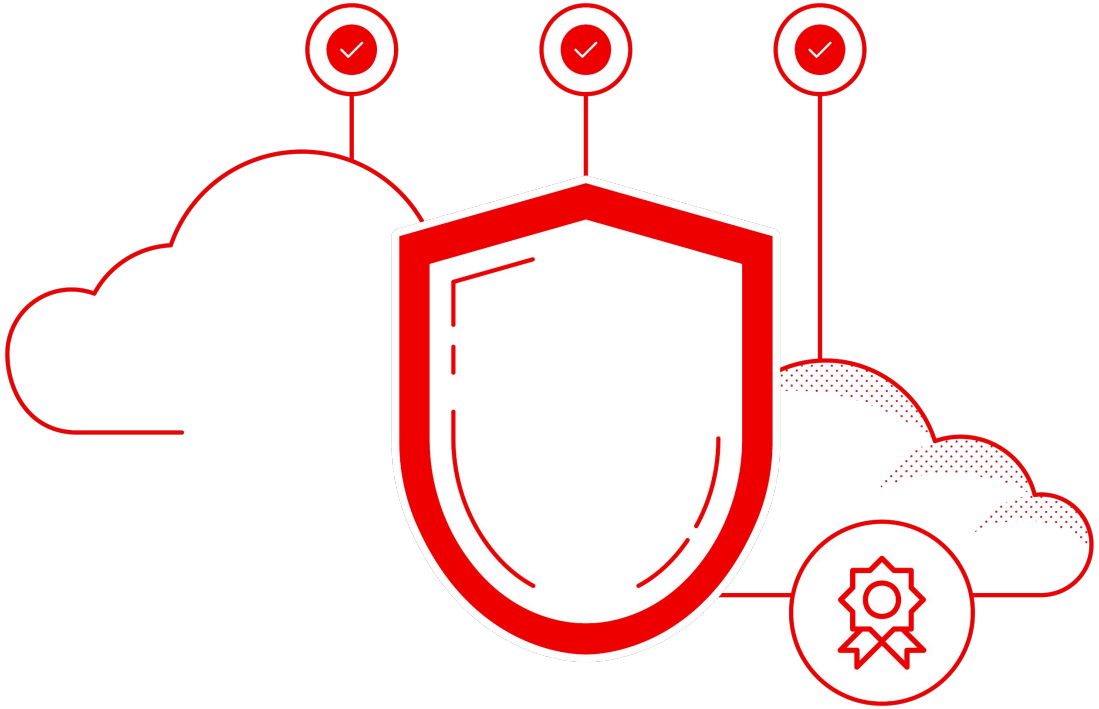
Red Hat Product Security works around the clock to provide guidance, stability, and security updates for open source



1. Investigating and verifying issues
2. Identifying affected products
3. Evaluating impact
4. Determining any necessary remedial actions

Red Hat

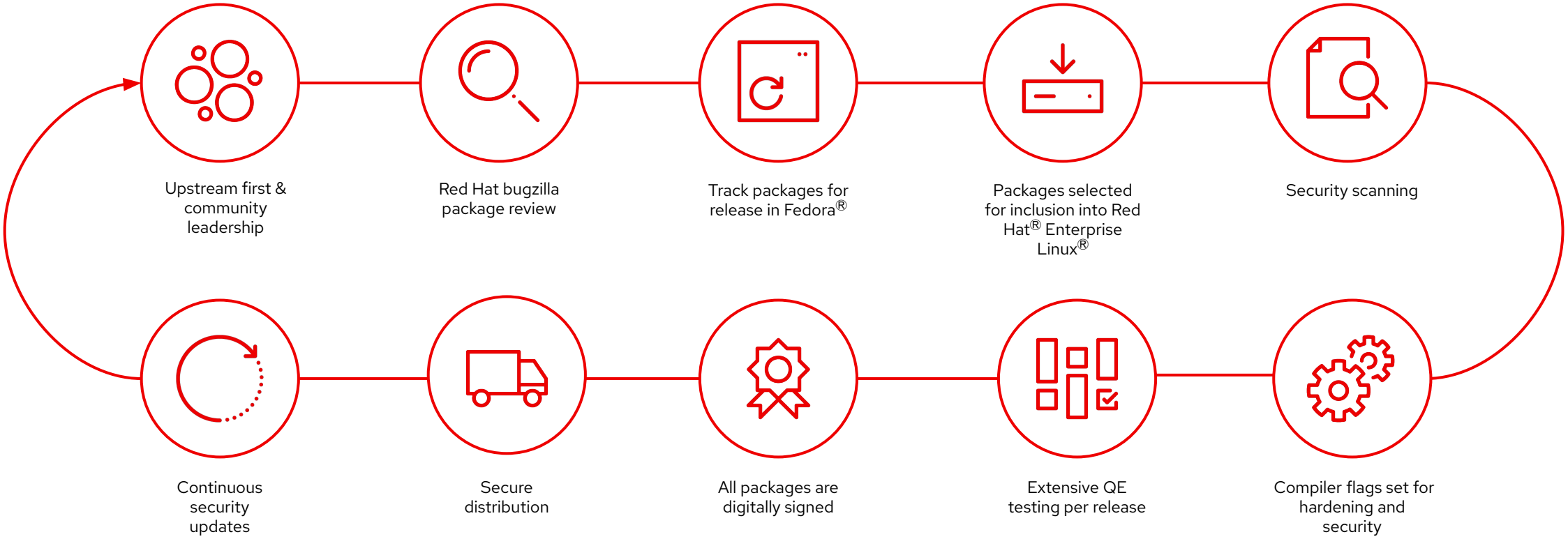
Verified security certifications help meet regulatory requirements



- Benefit from Red Hat's market-leading commitment to security certifications
- Strong, independent FIPS validation of cryptography for Red Hat Enterprise Linux
- Security claims validated by Common Criteria certification program

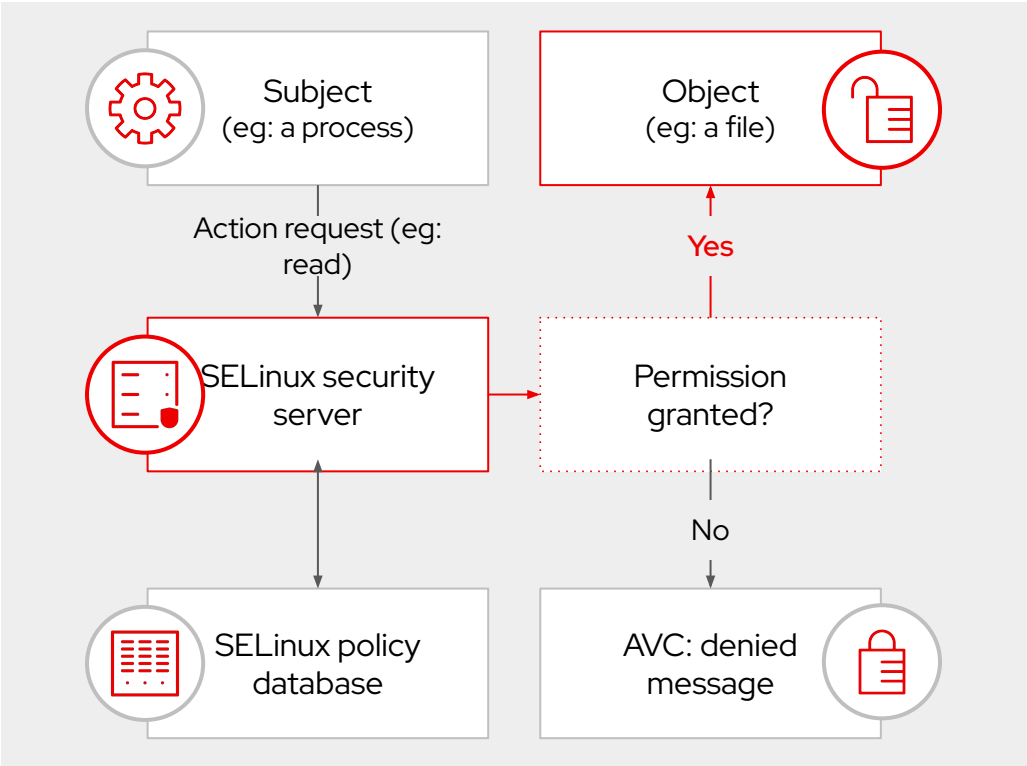
Red Hat's software supply chain security

Reducing risk and making open source consumable for the enterprise



Red Hat

It all begins with Red Hat Enterprise Linux



Trusted operating system for the enterprise:

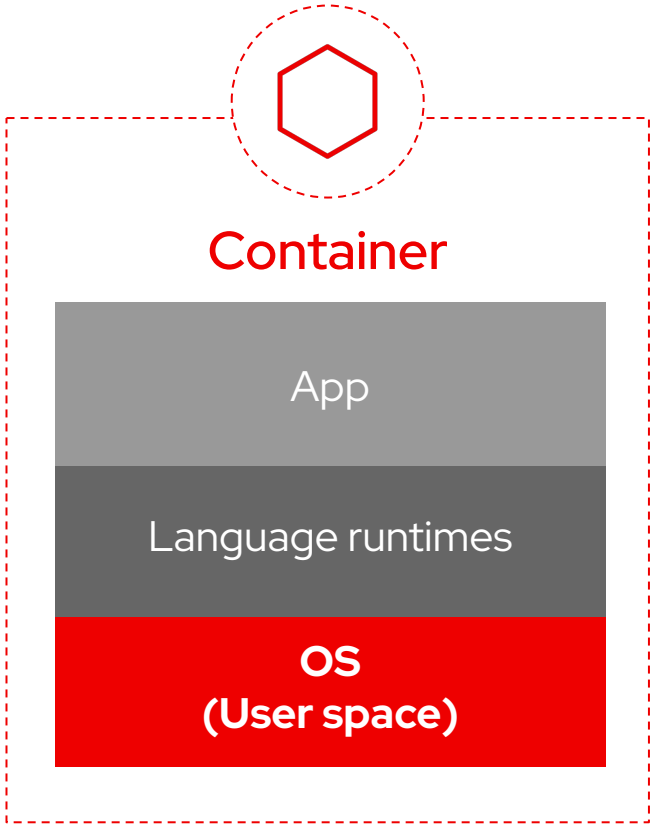
- Advanced resource access (SELinux, ACLs, FAPolicyd)
- Advanced process management, including Linux Containers (podman)
- Identity and Access Management: Centralized Identity Management
- H/W and S/W identity and cryptographic attestations (via SecureBoot, TPMs, IMA, RH signing)
- Derivative operating systems via image builder, RHCOS to further minimize attack surface

Live demo

Red Hat

Get the same trusted content packaged as Linux containers

Red Hat Universal Base Image (UBI)



Trusted:

- Libraries
- Packaging format
- Core Utilities
- Security Response
- Patching
- Performance Response
- Technical Support
- More

Red Hat

Red Hat's approach to hybrid cloud security - part two

Security in application development using DevSecOps practices

Red Hat

First step: Adopting a DevSecOps mindset is essential

Built over an enterprise open source foundation to protect the software factory

55% DevSecOps leaders agree that a culture of shared ownership between application development and security teams is critical[1]

78% have initiatives that increase collaboration between DevOps and Security teams[2]

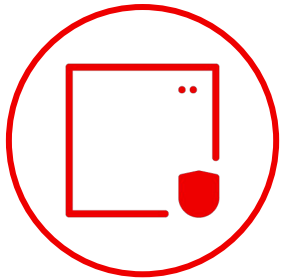
92% of IT leaders point out that enterprise open source solutions are important as their business accelerates application workloads to the open hybrid cloud[3]

[1]DevSecOps: Critical Risk Reduction Leads to Better Business Outcomes - IDC December 2021 | [2]State of Kubernetes Security Report 2022 - Red Hat Report | [3]State of Enterprise Open Source 2022 - Red Hat Report

Secure the use of source code and transitive dependencies

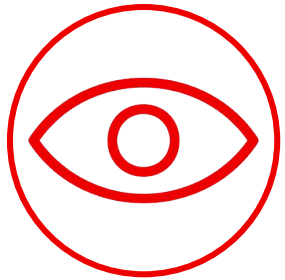
Software supply chain security considerations for the software development lifecycle

Prevent & identify malicious **code**



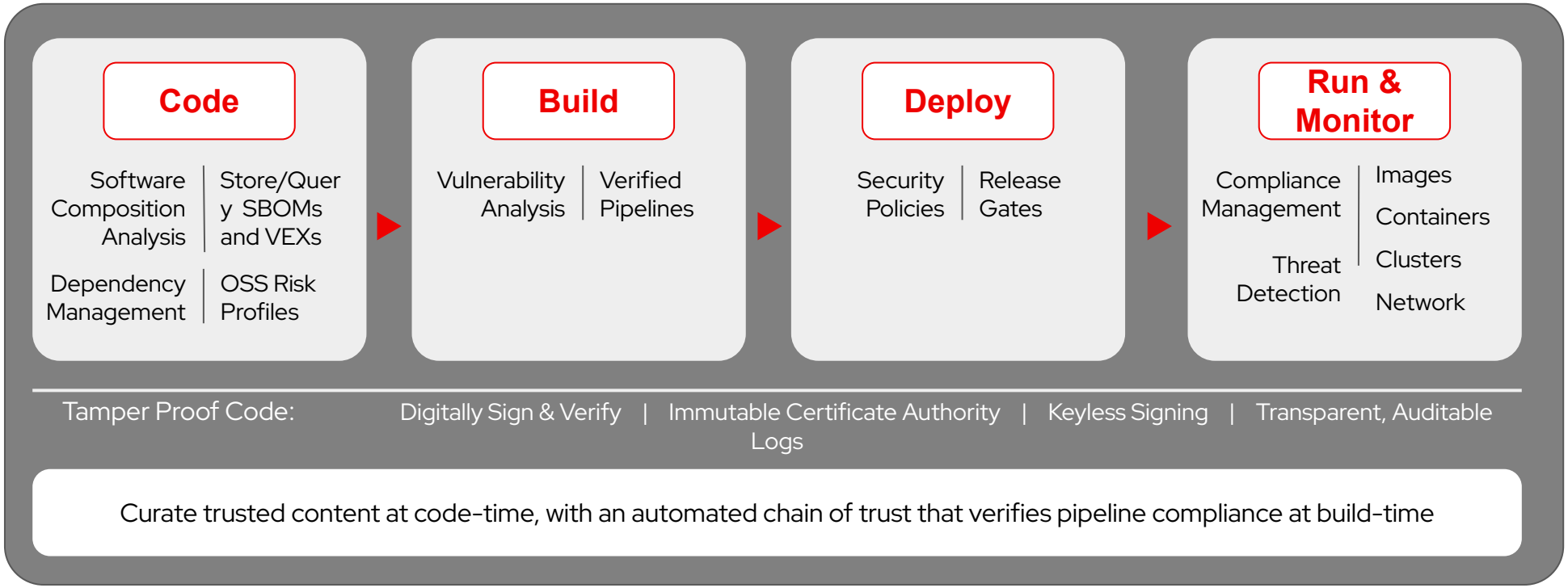
Safeguard **build** systems early

Continuously **monitor** security at runtime



Accelerate Innovation that Safeguards User Trust

Delivered with integrated security guardrails at every phase of the software development lifecycle



Build and deploy platform, pipeline and applications as-code to an auditable, declarative state that's continuously monitored

Other unified diagram options

NDA REQUIRED

Red Hat Trusted Software Supply Chain

Shift Left Security early in the Software Supply Chain

Red Hat
Trusted Software
Supply Chain

Developer self-service with pre-integrated security guardrails: artifact signatures, attestations & SBOMs

Red Hat Trusted Application Pipeline Q1* = **Red Hat** Developer Hub + **Red Hat** Trusted Artifact Signer Q1 + **Red Hat** Trusted Profile Analyzer Q1

Red Hat OpenShift

Red Hat Advanced Cluster Security for Kubernetes

Red Hat Quay

**Red Hat Trusted Application Pipeline* is a single product SKU available in Q1.
Includes Red Hat Developer Hub, Red Hat Trusted Artifact Signer, Red Hat Trusted Profile Analyzer capabilities with its own installer*

Red Hat® Open Hybrid Cloud Platform

Red Hat OpenShift Platform Plus

Red Hat OpenShift Container Platform

Red Hat OpenShift Kubernetes Engine

Red Hat Advanced Cluster Management for Kubernetes	Red Hat Advanced Cluster Security for Kubernetes	Red Hat Quay	Red Hat OpenShift Data Foundation
Multicluster management	**Cluster security**	**Global registry**	**Cluster data management**
Observability | Discovery | Policy | Compliance | Configuration | Workloads	Declarative security | Container vulnerability management | Network segmentation | Threat detection and response	Image management | Security scanning | Geo-replication Mirroring | Image builds	RWO, RWX, Object | Efficiency | Performance | Security | Backup | DR Multicloud gateway
Manage workloads	**Build cloud-native apps**	**Data-driven insights**	**Developer productivity**
Platform services	Application services*	Data services*	Developer services
• Service mesh | Serverless • Builds | CI/CD pipelines • GitOps | Distributed Tracing • Log management • Cost management	• Languages and runtimes • API management • Integration • Messaging • Process automation	• Databases | Cache • Data ingest and preparation • Data analytics • AI/ML	• Developer CLI | IDE • Plugins and extensions • CodeReady workspaces • CodeReady containers

Kubernetes cluster services

Install | Over-the-air updates | Networking | Ingress | Storage | Monitoring | Log forwarding | Registry | Authorization | Containers | VMs | Operators | Helm

Kubernetes (orchestration)

Red Hat Enterprise Linux — **Linux (container host operating system)** — Red Hat Enterprise Linux CoreOS

Physical — Virtual — Private cloud — Public cloud — Edge

* Red Hat OpenShift® includes supported runtimes for popular languages/frameworks/databases. Additional capabilities listed are from the Red Hat Application Services and Red Hat Data Services portfolios.

** Disaster recovery, volume and multicloud encryption, key management service, and support for multiple clusters and off-cluster workloads requires OpenShift Data Foundation Advanced

Enhance and extend security functionality

Build on Red Hat functionality through our **security partners** to better secure the entire DevOps life cycle.

Application analysis	**Identity & access management**
SAST, SCA, IAST, DAST, Image risk	Authn, Authz, Secrets Vault, HSM, Provenance
Compliance	**Network controls**
Regulatory compliance, PCI-DSS, GDPR	CNI plugins, policies, traffic controls, service mesh
Data controls	**Runtime analysis & protection**
Data protection and encryption	RASP, production analysis
Audit and monitoring	**Remediation**
Logging, visibility, forensics	SOAR, automatic resolution

CYBERARK, sysdig, aqua, SYNOPSYS, TIGERA, paloalto NETWORKS, NeuVector, snyk, anchore, THALES, portshift, tufin, TREND MICRO, IBM, Lacework, StackRox

Red Hat platform security

Secure host, container platform, namespace isolation, k8s and container hardening

Red Hat

Comprehensive DevSecOps

Red Hat, along with its partner ecosystem, can help organizations apply DevSecOps practices in both containerized and traditional environments.

Secure open hybrid cloud technologies

Red Hat

- Infrastructure
- Containers and kubernetes
- Automation and management
- Application development
- Hosted offerings

+

Enhance and extend

Partner ecosystem

- Certified containers and operators
- Secure the entire lifecycle
- Automate security operations center
- IBM collaboration

Culture, process, and implementation

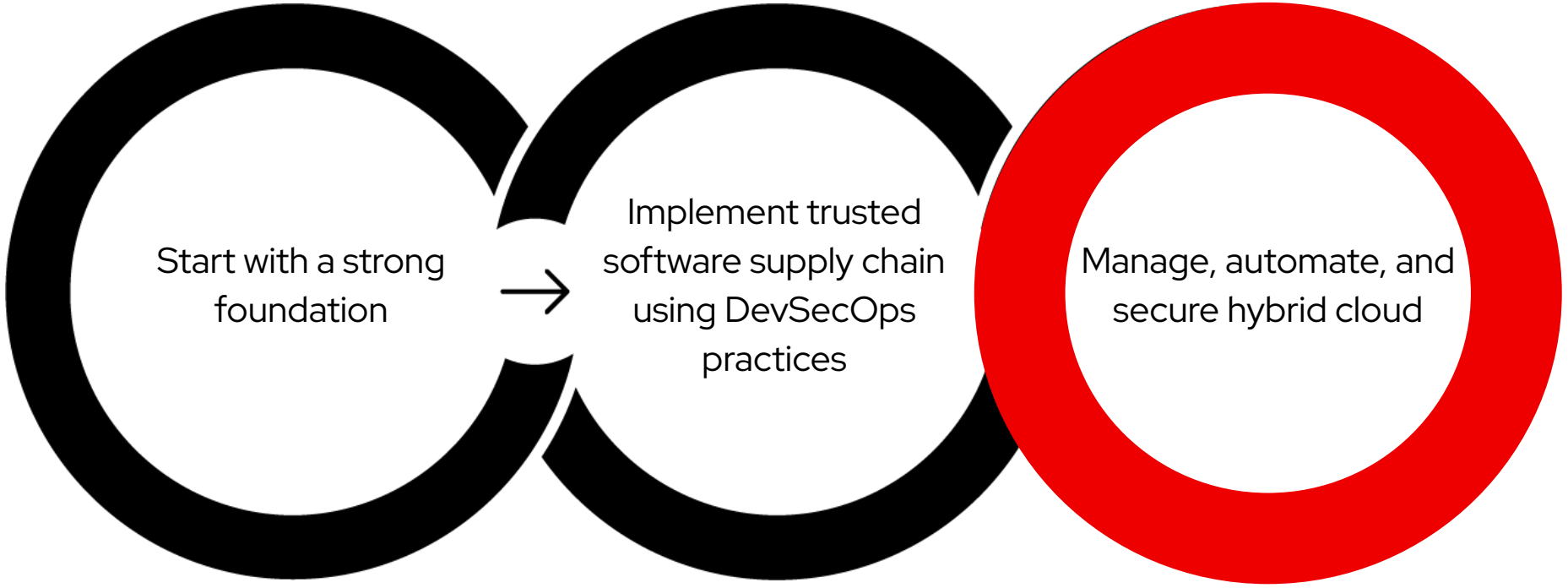
Red Hat Consulting | Red Hat Open Innovation Labs | Managed services and partner consulting

Red Hat Training and Certification

Red Hat

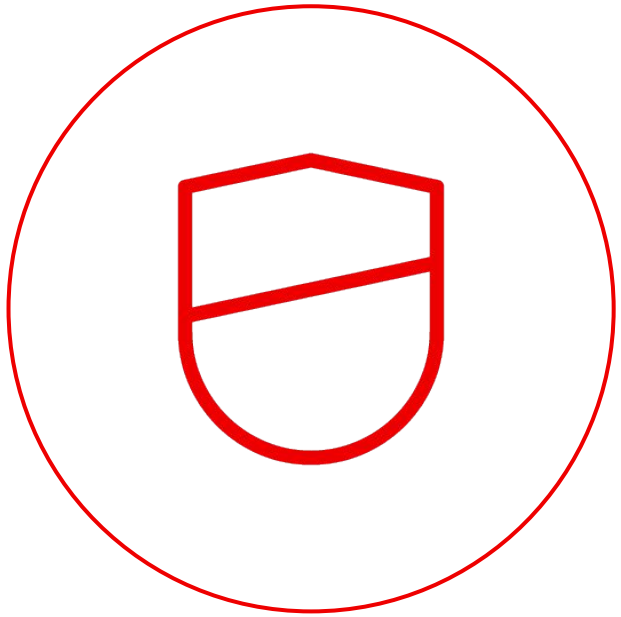
Red Hat's approach to hybrid cloud security - part three

Manage, automate, secure, and control your security-focused hybrid cloud



Red Hat

How to keep up with security and compliance in the hybrid cloud?

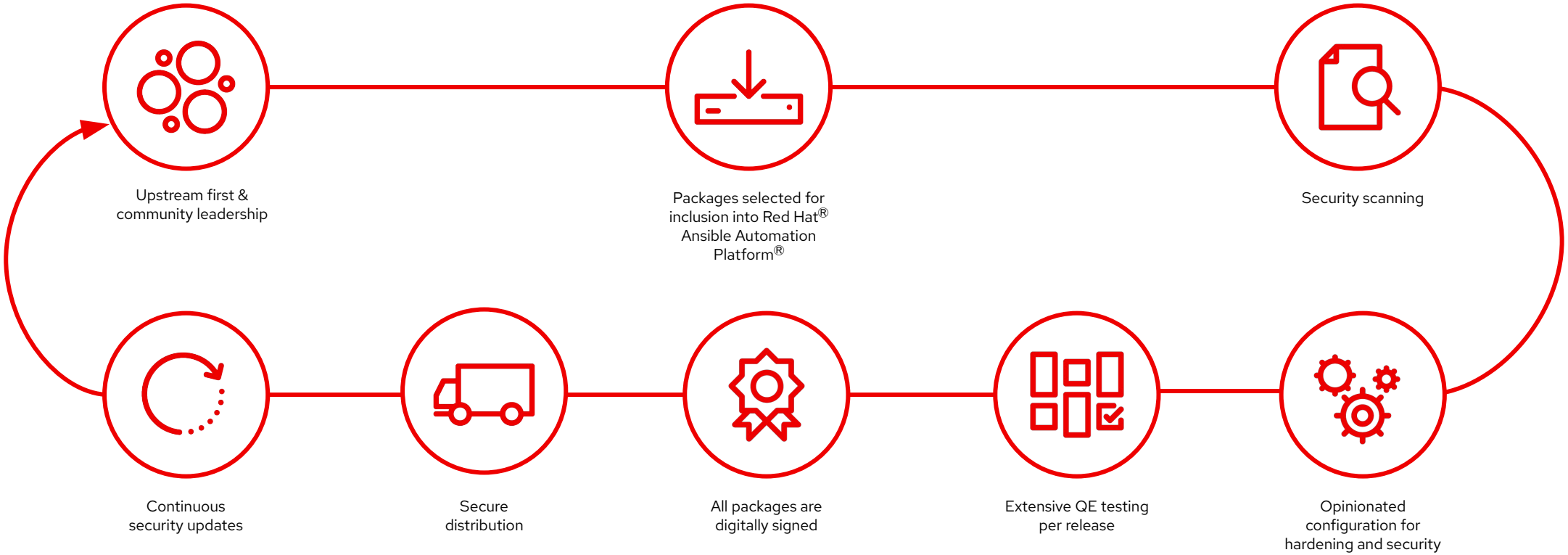


Implement an **enterprise-wide automation strategy** to keep pace with dynamic risk and compliance requirements

Red Hat

Applied: **Ansible's** software supply chain security

Reducing risk and making open source consumable for the enterprise



Red Hat

Extending Security to Ansible Content

Trust, Accelerate, Simplify

Enforce a secure supply chain for developer content

- Reduce security risks by limiting unverified content sources that may contain malicious or incorrect code
- Ensure an unbroken chain of custody of automation content code

"Peace of mind" with Certified Collections

- Digitally signed by Red Hat
- 100+ Collections across 55+ Red Hat partners technical support via TSANet
- Includes many Red Hat products (RHEL, OpenShift, Satellite, Insights and more)

Secure critical content with Private Automation Hub

- Enables developers to use approved Ansible content freely and easily
- An on-premise means to provide Ansible execution environments and Collections privately and securely at scale

Red Hat

Manage, automate, and secure hybrid cloud

Automate, monitor, and remediate to maintain security with these technologies:

Red Hat
Ansible Automation Platform

Enterprise framework to build, deploy, and manage IT automation at scale.

Red Hat
Insights

Continuously analyze platforms and applications to help manage hybrid cloud environments.

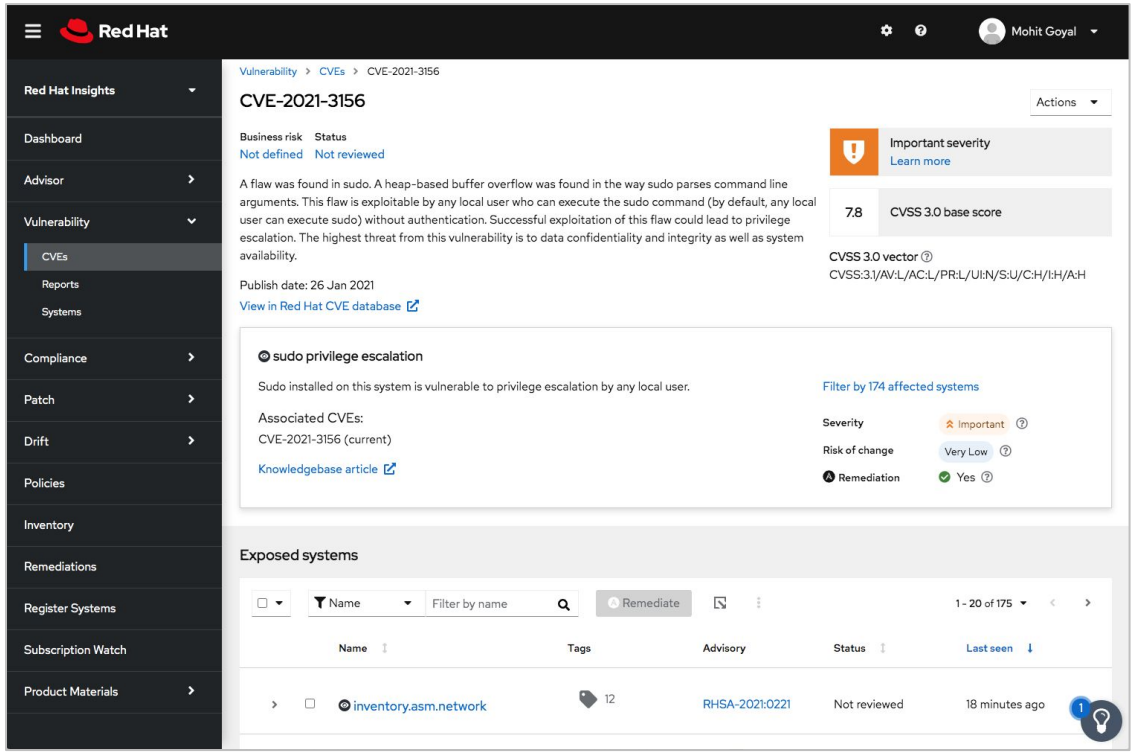
Red Hat
Advanced Cluster Management

End-to-end visibility and control for your Kubernetes cluster.

Red Hat
Advanced Cluster Security

Helps integrate security into each phase of the container life cycle—build, deploy, and run.

Scalable vulnerability management for RHEL with Red Hat Insights



- Included with your Red Hat Enterprise Linux subscription
- Manage, remediate, and report on RHEL CVEs
- Configure, deploy, and monitor OpenSCAP policies
- Use executive reports for at-a-glance reporting on exposures
- Tailor rules made easier via simple interface

Red Hat

Red Hat Ansible Automation Platform:

The capabilities you need across your IT footprint.

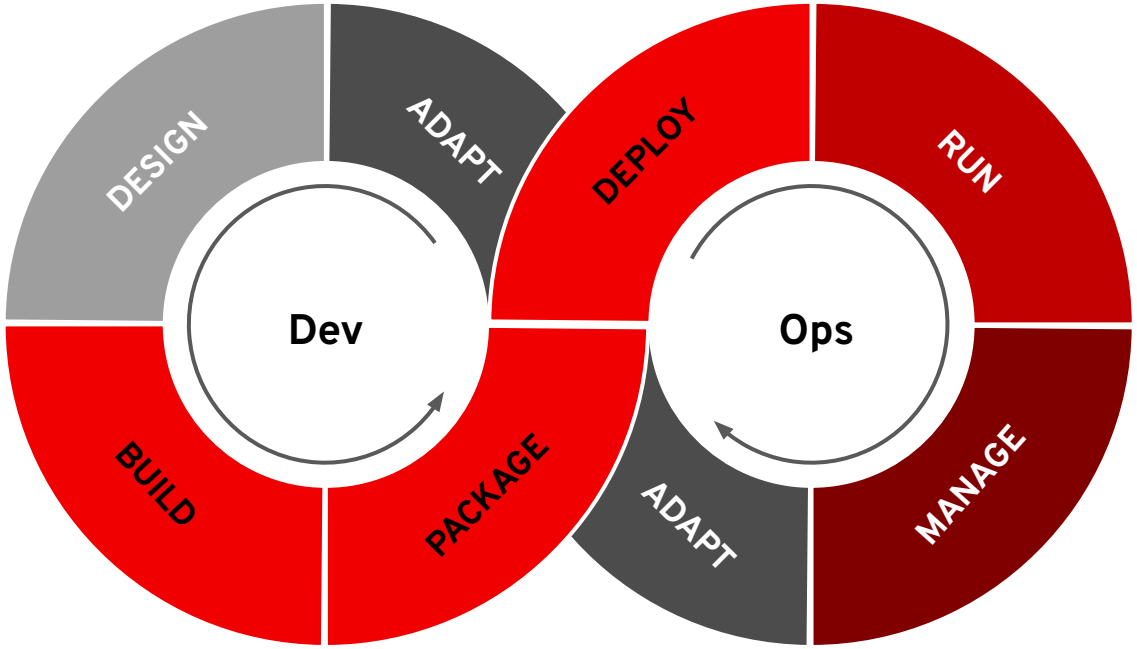
Applications	Network	Cloud	Security	Infrastructure	Edge
▸ DevOps ▸ CI/CD ▸ GitOps	▸ Configuration management ▸ Infrastructure awareness ▸ Network validation	▸ Orchestration ▸ Operationalisation ▸ Governance	▸ Investigation enrichment ▸ Threat hunting ▸ Incident response	▸ Deployment ▸ Provisioning ▸ Management	▸ Extend security ▸ Scalability ▸ Interoperability

Red Hat Advanced Cluster Security: Use Cases

Security across the entire application lifecycle

POLICY-AS-CODE

- Image scanning
- Host scanning
- Serverless scanning
- Configuration scanning
- Compliance checks, auditing, reporting, remediation
- CI/CD integration and automation
- Artifact attestation



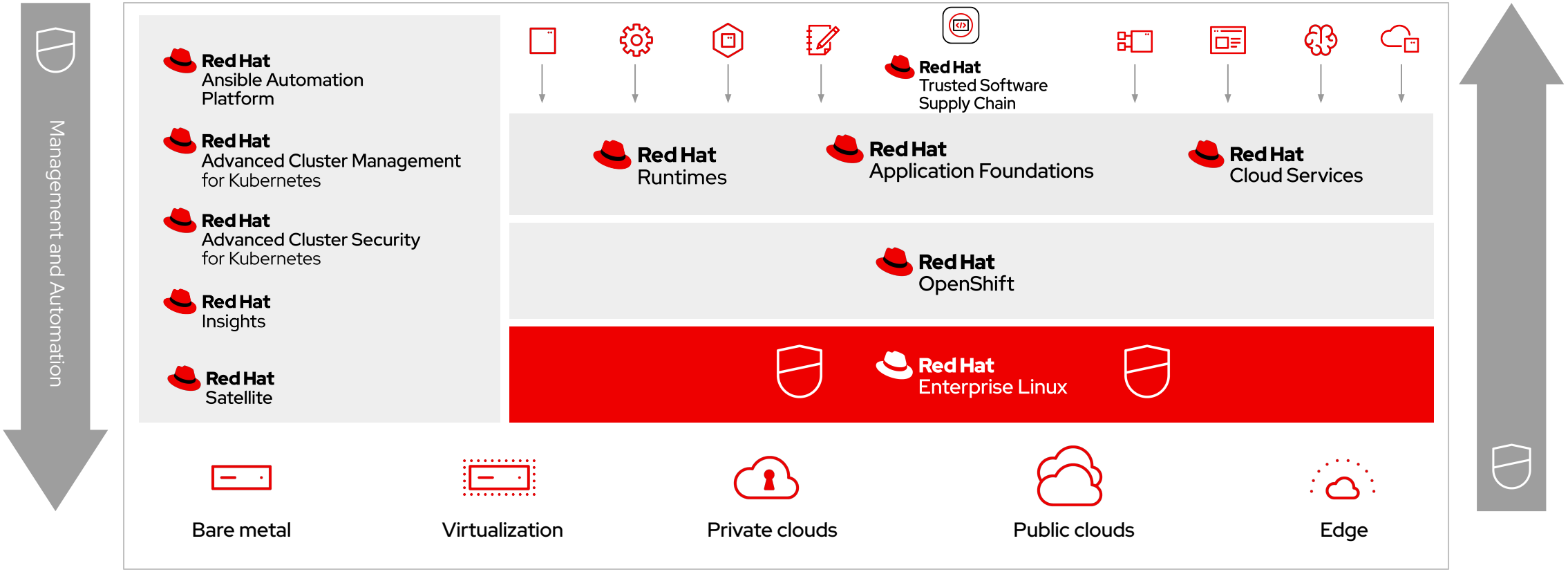
- Runtime threat detection
  - ✓ Process allowlisting
  - ✓ Anomaly detection
  - ✓ Policy-based detection
- Runtime vulnerability management
- Incident response
- Integrations
  - ✓ SIEM
  - ✓ Registries, CI/CD, runtimes, notification tools
- Feedback loop

VISIBILITY (images, deployments, network flows, processes, secrets use)

CONTAINERS AND K8S (on-premises, cloud/hybrid, edge)

Layered security throughout the stack and lifecycle

Build, deploy, and run applications on top of a hybrid cloud using DevSecOps practices



Red Hat

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.

linkedin.com/company/red-hat

youtube.com/user/RedHatVideos

facebook.com/redhatinc

twitter.com/RedHat

Red Hat