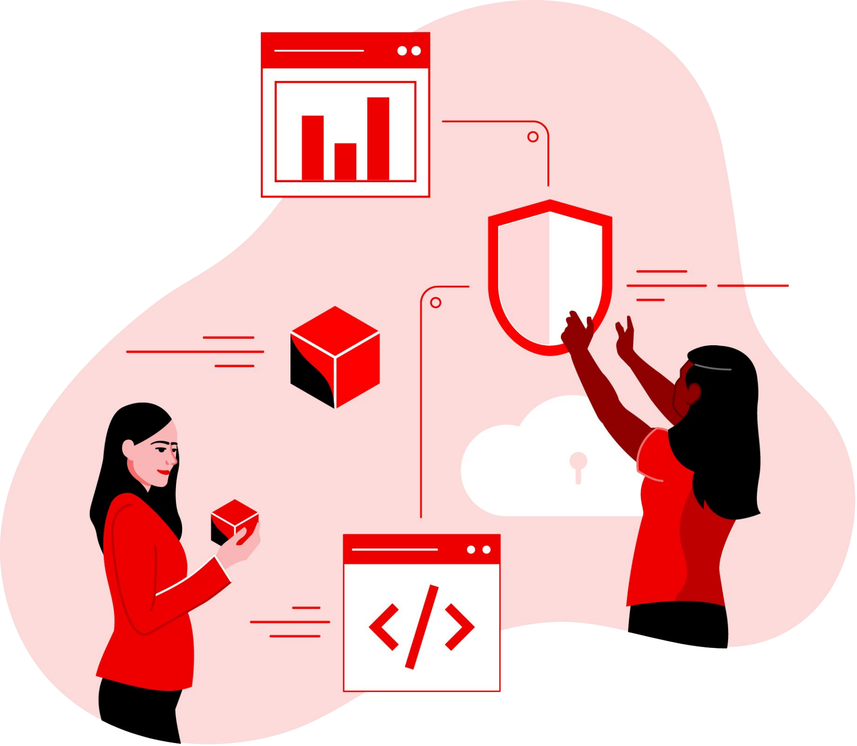
Build a **trusted** software supply chain with Red Hat



Red Hat

Software supply chain security considerations for a DevSecOps practice

Red Hat
Trusted Software
Supply Chain

Securing The Software Supply Chain for Speed and Trust

Henrik Løvborg

Tech Sales Leader

Software supply chain attacks: a matter of when, not if

Ransom paid but a mere fraction to the overall downtime and recovery costs of a data breach

742%

average annual increase in software supply chain attacks over the past 3 years[1]

45%

of organizations worldwide will experience supply chain attacks by 2025[2]

1 in 5

data breaches are due to a software supply chain compromise[3]

71%

YoY increase in cost of average ransom payment[4]

[1] State of the Software Supply Chain | [2] 7 Top Trends in Cybersecurity for 2022 | [3] Cost of a Data Breach 2022 - IBM Report | [4] Average Ransom Payment Up 71% This Year, Approaches $1 Million |

Just 7% are taking steps to review security risks in their supply chain [1]

94% of tech leaders say selecting the right security tools for their DevOps teams is challenging [2]

Security headcount and skills gap

Limited security expertise, standardize workflows to keep pace with releases

Security threats change quickly

Manually making sense of issues in the face of alerts, suffering burnouts

Security debt remains high

Tool sprawl, context switching results in fragmented visibility, long downtimes.

[1] State of the Software Supply Chain - Sonatype | [2] DevSecOps: Critical Risk Reduction Leads to Better Business Outcomes - IDC December 2021

Devs struggle to stay code compliant given high cognitive load[1]

Platform engineer for security and compliance into the SDLC to mitigate and reduce risks

Prevent & identify malicious **code**

Confidence in software integrity

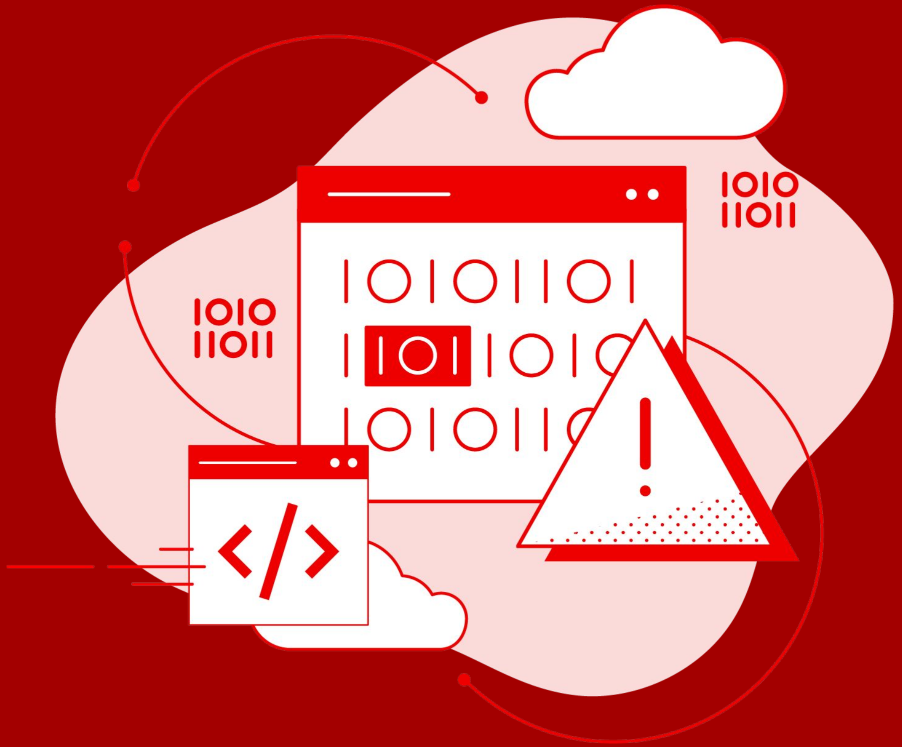
Safeguard **build** systems early

Adherence to regulation/compliance

Continuously **monitor** security at runtime

Enhanced trust with customers/stakeholders

[1] Salesforce productivity survey



Prevent and identify malicious code

Catch application releases with security vulnerabilities

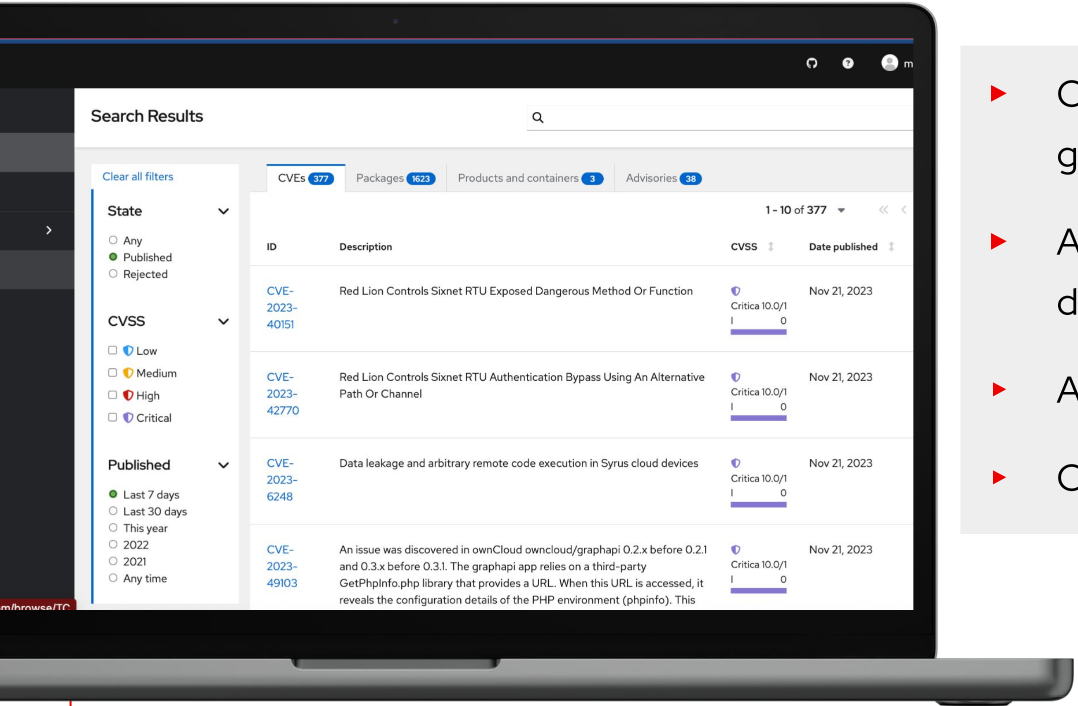
45% say software is released without going through security checks and/or testing[1].

- 3 of 5 organizations indicate their developers are using separate security tools[2].
- 65% of developers identified image scanning and vulnerability management as an important security use case[3].
- Over half of customers surveyed insist their developers use validated images[4].

[1][2] Walk the Line: GitOps and Shift Left Security - ESG Report | [3][4]State of Kubernetes Security Report 2022 - Red Hat Report

Code with integrated application security checks

Catch security issues early to avoid complexity of doing so in production



Search Results

Clear all filters

CVEs 377 | Packages 1623 | Products and containers 3 | Advisories 38

State

○ Any
● Published
○ Rejected

CVSS

□ Low
□ Medium
□ High
□ Critical

Published

● Last 7 days
○ Last 30 days
○ This year
○ 2022
○ 2021
○ Any time

1 - 10 of 377

ID	Description	CVSS	Date published
CVE-2023-40151	Red Lion Controls Sixnet RTU Exposed Dangerous Method Or Function	Critica 10.0/1 l 0	Nov 21, 2023
CVE-2023-42770	Red Lion Controls Sixnet RTU Authentication Bypass Using An Alternative Path Or Channel	Critica 10.0/1 l 0	Nov 21, 2023
CVE-2023-6248	Data leakage and arbitrary remote code execution in Syrus cloud devices	Critica 10.0/1 l 0	Nov 21, 2023
CVE-2023-49103	An issue was discovered in ownCloud owncloud/graphapi 0.2.x before 0.2.1 and 0.3.x before 0.3.1. The graphapi app relies on a third-party GetPhpInfo.php library that provides a URL. When this URL is accessed, it reveals the configuration details of the PHP environment (phpinfo). This	Critica 10.0/1 l 0	Nov 21, 2023

m/browse/TC

- Curate trusted content with security-focused golden solution templates and integrated checks
- Automated software composition scanning and dependency analytics
- Aggregated view with drill down on security health
- Cryptographic signing and verification

Safeguard build systems early

Account for all packaged components, dependencies

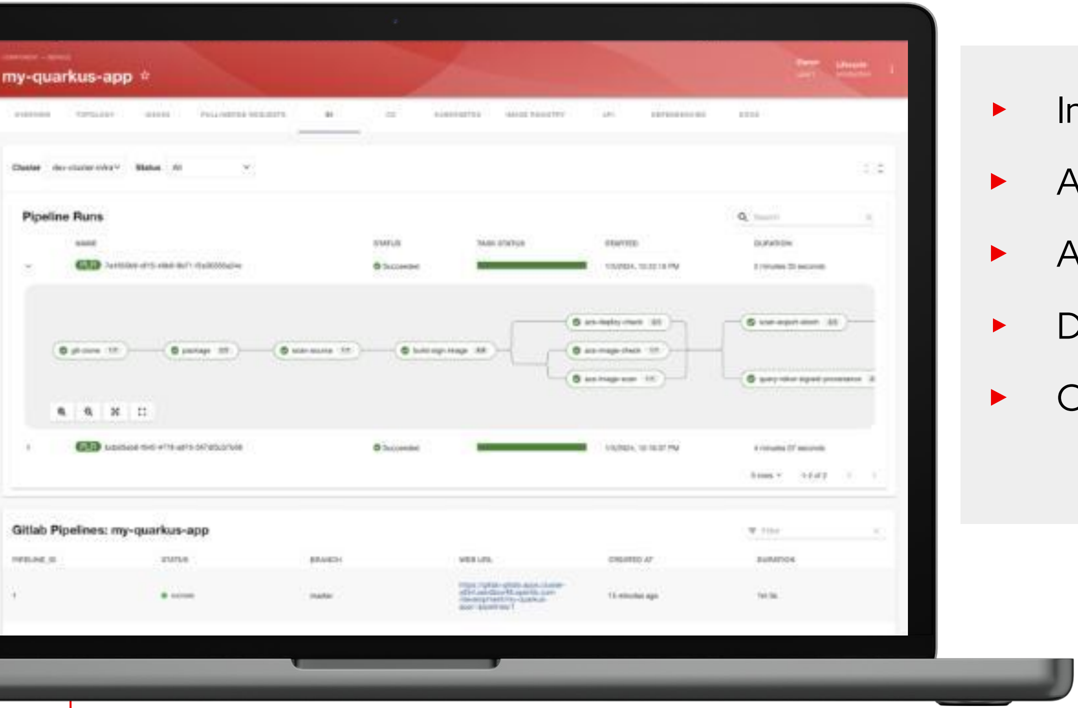
6 out of 7 project vulnerabilities come from transitive dependencies [1]

- Of the **1.2 billion** dependencies downloaded each month, **62%** had a transitive vulnerability[2]
- **73%** of organizations increased efforts to secure open source software only after an attack[3].
- **60%** of organizations will mandate Software Bill of Materials (SBOMs) by 2025[4]

[1][2]State of the Software Supply Chain - Sonotype Report | [3]Walk the Line: GitOps and Shift Left Security - ESG Report | [4]Gartner Report: Innovation Insight for SBOMs

Build with security focused CI/CD workflows

Efficiently track and trace security issues to remain industry compliant



- Integrated security guardrails across pipelines
- Auto-generated Software-Bill-of-Materials (SBOM)
- Attestations and provenance checks
- Deployment based on policies to a declared state
- Continuous image vulnerability scanning

Continuously monitor security at runtime

Isolate critical alerts from the noise in real-time

57% of surveyed worry the most about their runtime phase - for Day 2 operations[1]

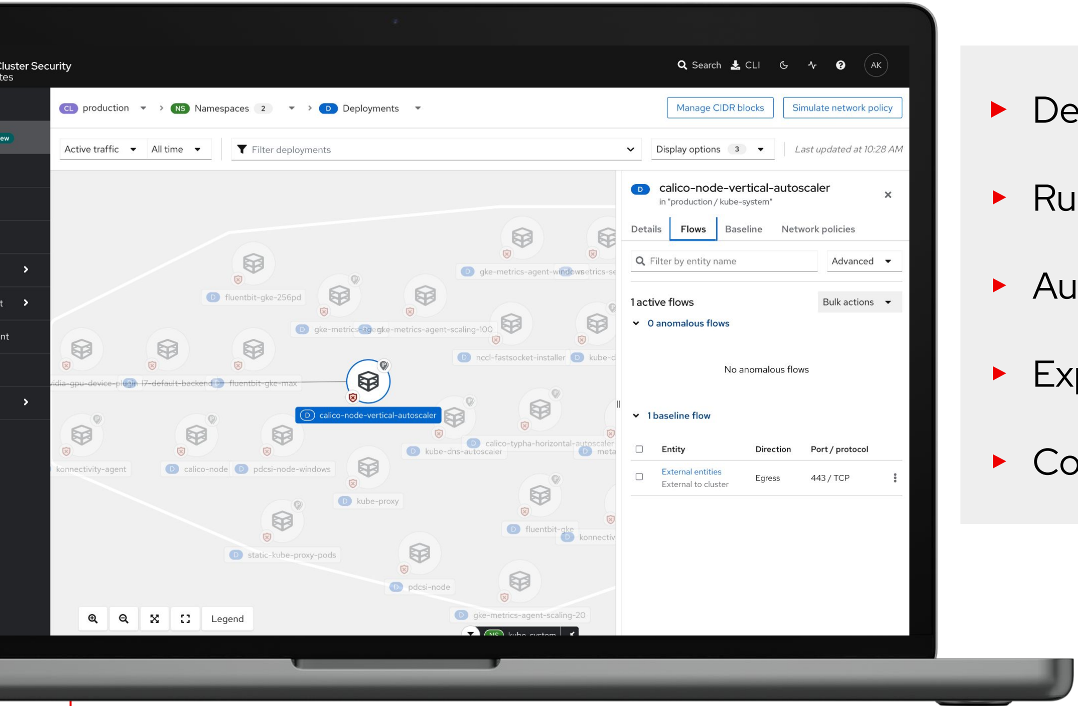
- Nearly **53%** of respondents have experienced a misconfiguration incident in last 12 months[2].
- **83%** say they are experiencing an increase in IaC template misconfigurations[3].
- But only **28%** say they are scanning production environments for misconfigurations[4].

[1][2] State of Kubernetes Security Report 2022 - Red Hat Report | [3][4] Walk the Line: GitOps and Shift Left Security - ESG Report

Red Hat
Trusted Software
Supply Chain

Monitor and identify runtime security incidents

Proactively reduce time to resolution for consistent user experiences



calico-node-vertical-autoscaler
in "production / kube-system"

Details | Flows | Baseline | Network policies

Filter by entity name — Advanced

1 active flows — Bulk actions

0 anomalous flows

No anomalous flows

1 baseline flow

□	Entity	Direction	Port / protocol
□	External entities External to cluster	Egress	443 / TCP

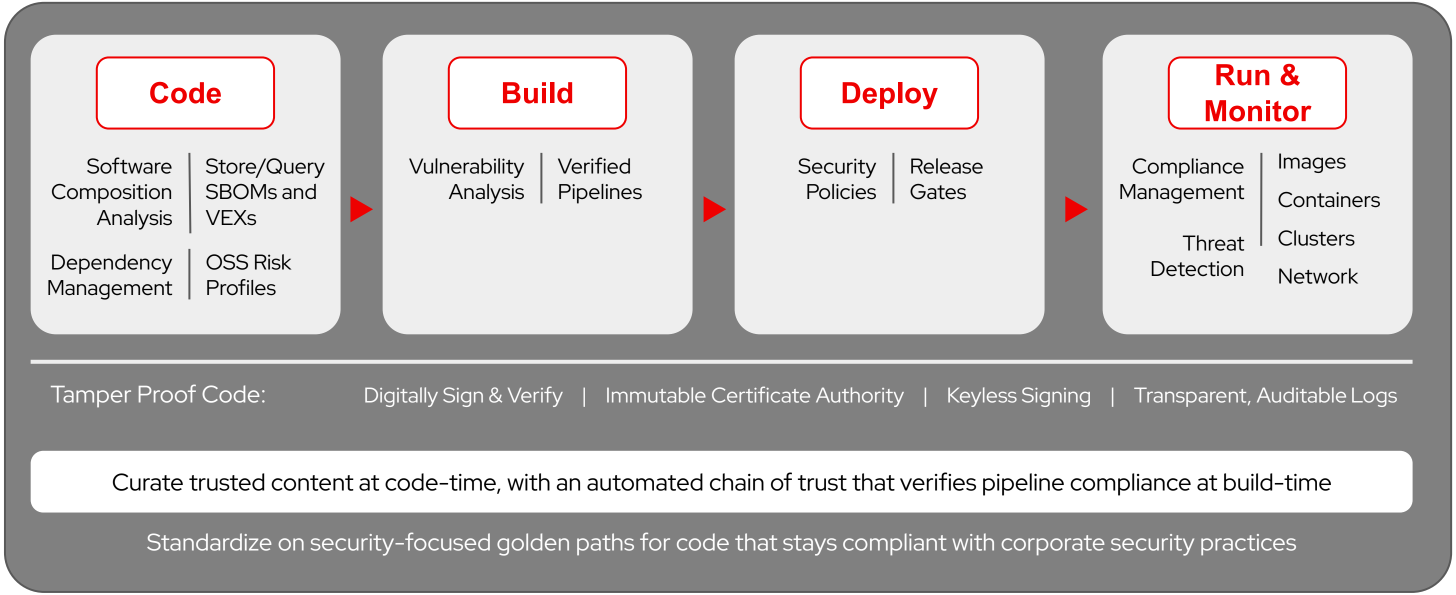
- ▸ Detect and respond to suspicious activity
- ▸ Runtime vulnerability scanning and management
- ▸ Audit for compliance across hundreds of controls
- ▸ Expedite incident response to reduce down times
- ▸ Continuous improvement from runtime to build

Red Hat

Code, build, deploy and monitor to a Trusted Software Supply Chain

Accelerate Innovation that Safeguards User Trust

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



Code

Software Composition Analysis | Store/Query SBOMs and VEXs

Dependency Management | OSS Risk Profiles

Build

Vulnerability Analysis | Verified Pipelines

Deploy

Security Policies | Release Gates

Run & Monitor

Compliance Management

Threat Detection

Images

Containers

Clusters

Network

Tamper Proof Code: Digitally Sign & Verify | Immutable Certificate Authority | Keyless Signing | Transparent, Auditable Logs

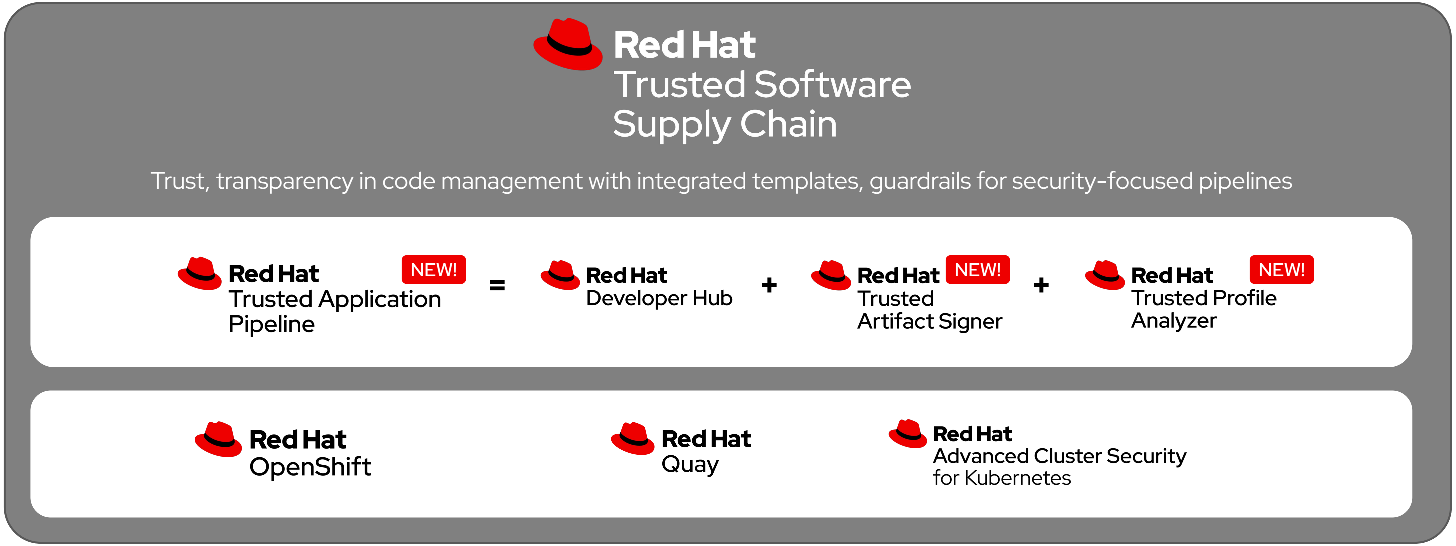
Curate trusted content at code-time, with an automated chain of trust that verifies pipeline compliance at build-time

Standardize on security-focused golden paths for code that stays compliant with corporate security practices

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

Shift Left Security in the Software Supply Chain

Protect the components, processes and practices early in your software factory



Red Hat
Trusted Software
Supply Chain

Trust, transparency in code management with integrated templates, guardrails for security-focused pipelines

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

Red Hat OpenShift

Red Hat Quay

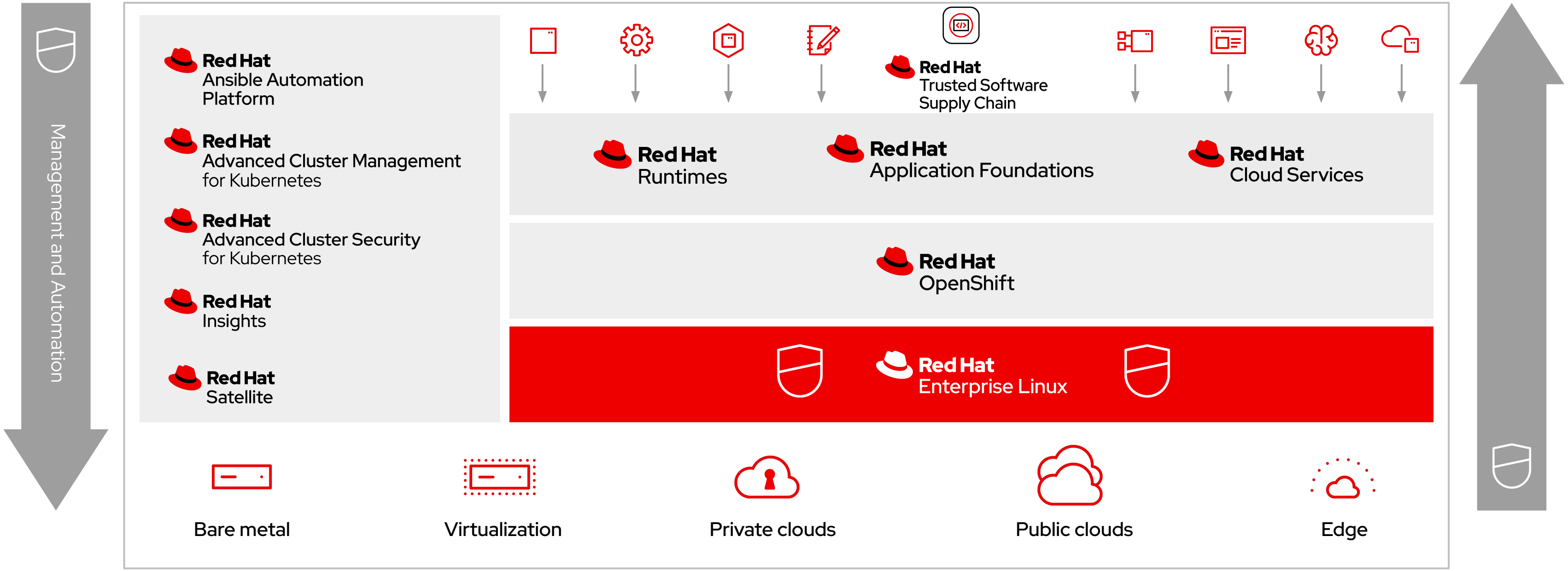
Red Hat Advanced Cluster Security for Kubernetes

Roadmap items are subject to change without notice

Note: **Red Hat Trusted Application Pipeline is a single product SKU that includes RHDH, RHTAS, RHTPA.*

Layered security throughout the stack and lifecycle

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


Management and Automation
Red Hat Ansible Automation Platform
Red Hat Advanced Cluster Management for Kubernetes
Red Hat Advanced Cluster Security for Kubernetes
Red Hat Insights
Red Hat Satellite
Red Hat Trusted Software Supply Chain
Red Hat Runtimes
Red Hat Application Foundations
Red Hat Cloud Services
Red Hat OpenShift
Red Hat Enterprise Linux
Bare metal
Virtualization
Private clouds
Public clouds
Edge

Enhance and extend security functionality

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

- Increase Trust
- Reduce Risk
- Improve Compliance
- Enhance Collaboration
- Increase Agility
- Improve Quality

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

Sign up today

- Choose Red Hat for your trusted software supply chain + DevSecOps
- Learn how Red Hat Trusted Software Supply Chain can help: **red.ht/trusted**

Demo

Thank you