Red Hat
OpenShift 4

Zero trust: 10 ways Red Hat OpenShift simplifies the journey

About M-22-09

In January 2022, the Office of Management and Budget (OMB) released a Federal strategy to move the U.S. Government toward a "zero trust" approach to cybersecurity (M-22-09)[1]. Among the objectives, agencies need to expose a Federal Information Security Modernization Act (FISMA)-moderate application to the internet, solely relying on Zero Trust principles for protection. Requirements include implementing minimum viable:

- Monitoring and infrastructure.
- Denial-of-service protections.
- Enforced access-control policy.
- Integration with an enterprise identity management system.

Enforce security policy at all layers in the application stack

Kubernetes layer and higher. Visibility and enforcement come from Red Hat Advanced Cluster Security for Kubernetes.

Make your application available over the internet with Zero Trust principles

Simplify your journey to zero trust with Red Hat® OpenShift® Platform Plus, a single hybrid cloud platform used to build, run, and manage applications at scale—integrated with the tools you need to implement a zero trust architecture in less time and with less risk. Here are 10 ways Red Hat OpenShift Platform Plus helps to meet the zero trust objectives introduced by M-22-09.

1 Use built-in auditing and monitoring

Red Hat OpenShift collects telemetry from workloads to make context-aware access decisions. You can configure Red Hat OpenShift to forbid bypassing telemetry collection. You can also integrate Red Hat OpenShift with your agency's existing enterprise log and activity monitoring tools, including Splunk.

2 Control configuration management

Red Hat OpenShift wraps each component—for example, application programming interface (API) server and software-defined network (SDN)—in a Kubernetes operator used for configuration, monitoring, and management. Administrators are subject to role-based access controls (RBAC) whenever they make a configuration change. You can also configure operators to prohibit configuration drift.

3 Inherit the security capabilities of Red Hat Enterprise Linux

These capabilities include SELinux mandatory access control (MAC), kernel capabilities, seccomp, namespaces, and control groups to prevent processes, malicious or not, from interfering with other processes on the same host. More protection comes from Red Hat Enterprise Linux® CoreOS, which reduces potential attack vectors by removing anything unnecessary to host, manage, and safeguard Red Hat OpenShift.

4 Use policy to help ensure that APIs are used and security-focused

Keep your APIs compliant by using Red Hat 3scale API Management, included with OpenShift Platform Plus, to define and enforce policies for traffic management, security, and use. Red Hat 3scale works with Red Hat OpenShift Service Mesh to protect micro-segmented applications.

5 Apply macro-segmentation to control which traffic enters or exits the internal services communication network

Malware or intruders cannot move from the enterprise network to the platform's internal SDN without going through the Ingress Operator in OpenShift, which acts as an enforcement point.

[1] *White House press release. "Office of Management and Budget Releases Federal Strategy to Move the U.S. Government Towards a Zero Trust Architecture,"OMB Briefing Room. Jan. 25, 2023.*

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

6 Apply micro-segmentation and restrict internal cluster communications

Limit network connections at different network layers between pods and services to those that are strictly necessary. Use Red Hat Advanced Cluster Security for Kubernetes, included with OpenShift Platform Plus, to detect and restrict network policy based on application ports and protocols. Create mTLS micro-segmented networks with OpenShift Service Mesh.

Layers below Kubernetes. Protection comes from Red Hat Enterprise Linux CoreOS.

7 Augment Red Hat Enterprise Linux resource management in Red Hat OpenShift Container Platform

Use Kubernetes-native APIs to restrict each project's resources or storage. Enforce resource quotas per project and across projects. Use Red Hat OpenShift Container Platform's managed service accounts to limit the potential for compromise or damage from attacks like rogue tokens. This capability also provides denial-of-service protections.

Richer access controls than standard Kubernetes

Controls automatically apply to microservices and microsegments.

Decisions consider context (e.g., time of day) using Red Hat SSO rules engine or Red Hat 3Scale.

Rich, built-in roles let you tailor authorization to specific business access needs.

8 Enforce supply chain controls and platform access for workloads

Configure Red Hat OpenShift and Red Hat Advanced Cluster Security to prevent deployment of services that require overbroad access and block deployment of images with known vulnerabilities. Require images to be signed before deployment. Prevent images from being pulled from external registries.

9 Consider the context of the request when granting or denying access

Delegate context-based access controls to Red Hat Single Sign-On (SSO), included in Red Hat OpenShift, to implement with its internal rules engine. These controls can be reflected back into Red Hat OpenShift's rich RBAC and policy tokens for access control.

10 Integrate your existing access control and identity provider services

Red Hat OpenShift supports multiple identity providers, including active directory, Lightweight Directory Access Protocol (LDAP), OpenID connect, and others. Enforce use of phishing-resistant multifactor authentication methods like smart cards, hardware tokens, biometrics, credentialing via public key infrastructure (PKI), and passwords, by delegating to Red Hat SSO using application or cluster proxies. Red Hat SSO enforces access policies for the platform and workloads hosted on the platform.

Find out more: redhat.com/civilian-agencies

About Red Hat

Red Hat helps customers standardize across environments, develop cloud-native applications, and integrate, automate, secure, and manage complex environments with award-winning support, training, and consulting services.

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

North America
1 888 REDHAT1
www.redhat.com

Europe, Middle East, and Africa
00800 7334 2835
europe@redhat.com

Asia Pacific
+65 6490 4200
apac@redhat.com

Latin America
+54 11 4329 7300
info-latam@redhat.com