Zero Trust: How OpenShift simplifies the journey

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). 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.

This brief identifies 10 ways Red Hat OpenShift Platform Plus helps to meet zero trust requirements published by the Office of Management and Budget