Tech tips to advance security and compliance

Experience security and compliance capabilities that help you mitigate risk, enforce security configuration and policy, and stay compliant.

Configure custom, system-wide crypto policy

System-wide cryptographic policy provides a consistent way to implement and maintain standards-based compliance settings for your infrastructure. With one simplified command, you can select a built-in cryptographic policy and apply it consistently across the applications on your system. In addition, if you have specialized regulatory compliance requirements, you can create a custom policy to meet your objectives.

Automate security configuration with system roles

With Red Hat® Enterprise Linux® system roles, powered by Red Hat Ansible® Automation Platform, administrators can use automation to quickly install and manage security settings at scale. System roles are written to work with multiple Red Hat Enterprise Linux releases across various footprints, allowing administrators to use best practices for Red Hat solutions. With a single command or workflow, you can configure new security settings and maintain them on all your systems.

Centralize your authentication and authorization

Red Hat Enterprise Linux includes centralized identity management (IdM) capabilities that allow you to authenticate users and implement role-based access controls (RBAC) using a single, scalable interface that spans your entire datacenter. Identity management in Red Hat Enterprise Linux integrates with Microsoft Active Directory, lightweight directory access protocol (LDAP), and other third-party identity and access management solutions through standard application programming interfaces (APIs). You can also centrally manage authentication and authorization for services using certificate-based authentication and authorization techniques.

Lock down your containers with custom policies

Security-Enhanced Linux (SELinux) is an implementation of mandatory access control (MAC) in the Linux kernel. Red Hat Enterprise Linux containers run with SELinux enabled by default. This includes an additional layer of security in the operating system (OS) and prevents containers from breaking out and overwriting the underlying host OS or other containers on the system. Udica allows system administrators and container developers to analyze a running container and auto-generate a customized policy with container-specific SELinux rules. This simplifies policy writing and eliminates the need to run containers with superuser privileges, therefore reducing risk.
Red Hat is the world’s leading provider of enterprise open source solutions, using a community-powered approach to deliver high-performing Linux, cloud, container, and Kubernetes technologies.