8 tech tips to advance security and compliance

Mitigate risk, enforce security configuration and policy, and help your organization stay compliant with Red Hat® Enterprise Linux® security and compliance capabilities.

1 Manage standards-based compliance settings

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. Plus, if you have specialized regulatory compliance requirements, you can create a custom policy to meet your objectives.
Learn more about managing compliance

2 Automate security configuration with system roles

Red Hat Enterprise Linux system roles, powered by Red Hat Ansible® Automation Platform, allow administrators to use automation to install and manage security settings at scale in less time.
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.
Learn more about security automation

3 Centralize 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.

Find out more about identity management

4 Customize 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 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 policy with container-specific SELinux rules. This simplifies policy writing and reduces risk by eliminating the need to run containers with superuser privileges.

Experiment and learn more about policy lockdown

5 Patch systems with minimal downtime

Red Hat provides kernel live patches for common vulnerabilities and exposures (CVEs) rated critical or important for extended update support (EUS) releases at no extra cost. Kernel live patching (KLP) allows you to patch a running kernel to immediately address vulnerabilities without rebooting your system to minimize downtime without compromising security.
Experiment and learn more about KLP

6 Manage security and compliance at scale

Included in a Red Hat Enterprise Linux subscription, at no added cost, Red Hat Insights is a Software-as-a-Service (SaaS) offering that provides users with actionable security data about their deployments. Discover and address operational and vulnerability risks, scan your systems faster to determine which patches are missing, and prioritize which critical patches to apply first. You can create, modify, implement, and maintain security configuration policies across all your Red Hat Enterprise Linux systems from a single web interface. Additionally, you can execute, scale, and automate remediation plans from Red Hat Insights with a Red Hat Smart Management subscription.
Learn more about compliance

7 Record system activity to support compliance goals

Red Hat Enterprise Linux includes session recording, which has auditing and logging capabilities that let security administrators capture keystrokes and activities of a select group of users on a system. This data is recorded in the same system journal or log file as all other activities and can be analyzed and correlated using replay and pause capabilities included in the playback tool.
Experiment with session recording

8 Stop unauthorized applications from executing

Application allowlisting can reduce potential attack vectors and prevent rogue applications from executing on your system. The file access policy daemon (fapolicyd) offers built-in application allowlisting, which permits only approved executables to run on a system by a user. System administrators can configure fapolicyd with default policies or build their own to prevent modified or unauthorized applications from running.
Find out more about application allowlisting

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