Red Hat Enterprise Linux security and compliance

Secure foundation for running open hybrid cloud workloads

Red Hat Enterprise Linux helps you get more secure, compliant, and audit-ready by supporting the top security and compliance requirements for an OS:

- Modern, multi-layered security capabilities to reduce risk
- Automated patching and remediation to minimize downtime
- Secure development lifecycle processes and validation
- Built-in compliance tools to meet security standards
- Consistent security controls across the hybrid cloud
- Workload security in public cloud environments

Securing the operating system is key

The number and sophistication of security exploits are ever-increasing, which means having security built into every part of the infrastructure is critical. Operating systems (OS)—as the foundation on which all applications run—need a depth and breadth of security capabilities to protect against vulnerabilities and meet compliance requirements.

Red Hat® Enterprise Linux® provides a more secure foundation from which you can scale existing applications and roll out emerging technologies consistently across bare-metal, virtual, cloud, and edge footprints. Its built-in security and compliance capabilities help:

- **Mitigate -** Manage security and reduce the risk of a breach before your data, systems, or reputation is exposed.
- **Secure -** Automate security controls and maintain them over time, at scale and with minimal downtime.
- **Comply -** Streamline compliance standards for organizations with highly regulated environments.

Mitigate the risk of exposing your data, systems, or reputation

Critical security upgrades and patches - Increase uptime and resilience with live kernel patching and remediation of security vulnerabilities. Quickly address critical and important security issues without reboots to ensure uptime for critical apps.

Application allowlisting (fapolicyd) - Prevent unauthorized access by allowlisting trusted programs to run on a machine or network. Take advantage of predefined policies or customize your policies to detect or prevent modified applications from running.

Supply chain security - Reduce software lifecycle risk with more secure development practices that include static code analysis across the entire code base. This can minimize security flaws before shipping and improve the upstream open source project.

Scalable vulnerability management - Integrates scalable security configuration and vulnerability management using Red Hat Insights. Customize security policies, apply them across systems, monitor for exposure, and remediate if necessary.

Automate security controls at scale and maintain them over time

Secure hardware root of trust - Use hardware-based root of trust to ensure that the software on your systems has not been modified or tampered with. Provide consistent hardware security configurations for external hardware tokens including smart cards and hardware security modules (HSMs).

Network Bound Disk Encryption (NBDE) - Automate the unlocking of encrypted systems on-premises or in the hybrid cloud without manually managing encryption keys. This extra layer of data protection ensures they are only available when they are secure.

Modernized and scalable encryption - Keep data secure with system-wide consistent and customizable cryptography settings for addressing compliance requirements. Manage cryptography across the system with an easy one-command method.

SELinux mandatory access controls - Equip files, processes, users, and applications with granular access controls to minimize the risk of inappropriate privilege escalations. Customize access by application or container. This level of control enforces data confidentiality and integrity, as well as protects processes from untrusted inputs.

Centralized identity management - Manage the authentication and authorization of users via role-based or policy-based access control at scale across the environment. Easily integrate with other identity and access management solutions or directories.

Meet compliance requirements and streamline audits

Verified security certifications - Support customer compliance mandates. Red Hat's intent is for minor releases of Red Hat Enterprise Linux to be independently validated against FIPS standards, and every EUS release to achieve Common Criteria Certification.

Built-in compliance tools - Perform configuration and vulnerability scans on a local system to validate compliance. Generate reports and OpenSCAP baselines, then use automation to remediate non-compliant systems. Integrate with Red Hat Smart Management and Red Hat Insights for managing compliance at scale.

Session recording - Record administrative activity as a viewable file to meet security auditing requirements or provide playback to assist with post-incident troubleshooting. Easily customize which users or groups you want to record.

System roles - Automate security configuration and maintain consistency across systems over time to ensure security and compliance at scale. Deploy and manage Red Hat Enterprise Linux security with fewer resources than ever before by using roles for SELinux, certificates, NBDE, session recording, SSH, crypto policy, and more.

Experience all Red Hat Enterprise Linux has to offer

Contact your Red Hat sales representative or click to learn how Red Hat Enterprise Linux can help you manage security and compliance across your hybrid cloud infrastructure.

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