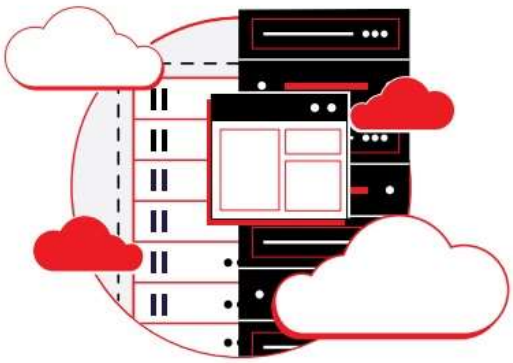
Red Hat Enterprise Linux security and compliance



Securing the operating system is key

Due to the ever-increasing number and sophistication of security exploits, security built into every part of the infrastructure is critical. It's vital that an operating system (OS), as the foundation for all applications, has the depth and breadth of security capabilities to protect against vulnerabilities and meet compliance requirements.

Red Hat® Enterprise Linux® provides consistent controls across bare-metal, virtual, hybrid cloud, and edge computing environments to help mitigate risk when developing on and then deploying applications into production. It is important for the OS to support an auditable and secure

development life-cycle process that includes specific supply chain security capabilities.

Compliance-ready solutions for the real world

The growing number of compliance mandates around securing IT resources will only continue to increase the need for tighter security controls. We know that when it comes to compliance, customers in highly regulated industries such as financial, government, and retail, require their products to meet stringent security baselines and involve their compliance officers in decisions even as foundational as the OS.

Requests for Federal Information Processing Standard (FIPS) and Common Criteria are widespread and often a key driver for purchases for customers with highly regulated environments. Red Hat Enterprise Linux has built-in security hardening standards that streamline audit or reporting requirements. We are committed to frequent FIPS and Common Criteria evaluations, enabling independent parties to verify our security claims.

Reduce risk, enforce security controls, and comply with standards

Red Hat Enterprise Linux helps you mitigate your risk of being exposed to vulnerabilities using automated and repeatable security controls.

Mitigate – Manage security and reduce the risk of a breach before your data, systems, or reputation is exposed. Red Hat Enterprise Linux:

- Expands vulnerability coverage to remediate the latest exploits.
- Provides transparent and efficient security patching.
- Strengthens supply chain security with secure build processes and risk analysis.
- Scans and remediates vulnerabilities.
- Run applications in more secure sandboxes without full access to the rest of your system.

Secure – Automate security controls and maintain them over time, at scale and with minimal downtime. Red Hat Enterprise Linux:

- Provides built-in layers of security to defend against myriad threats.
- Minimizes reboots when patching for increased uptime and resilience.
- Implements a system-wide cryptography baseline.
- Provides hardware root of trust to verify integrity of the system.
- Streamlines and scales security across the hybrid datacenter.

Comply – Streamline compliance standards for organizations with highly regulated environments. Red Hat Enterprise Linux:

- Meets regulated industry standards with independently validated and certified solutions.
- Delivers compliance tools as part of the OS to easily deploy security baselines at scale.
- Captures audit logs of user activity for security event and incident management.

Feature highlights

Consistent access controls – Applies security configuration and access controls consistently across bare-metal, virtual, Kubernetes and container environments, and all types of clouds.

Modernized and scalable encryption – Keeps data security with system-wide consistent and customizable cryptography settings for addressing compliance requirements. Easy one-command method of managing the security of cryptography across all of Red Hat Enterprise Linux.

Multilayer breach defense – Provides multiple levels of security including vulnerability scanning and remediation, Security Enhanced Linux (SELinux) mandatory access controls, rootless containers, and application allow lists.

Critical security upgrades and patches – Minimizes downtime and reboots with live Kernel patching and remediation of critical and important security vulnerabilities.

Supply chain security – Provides more secure software life-cycle development practices with static code analysis across the entire code base to minimize security flaws before shipping and improving the upstream open source.

Verified security certifications – Supports customer compliance mandates. Every minor release of Red Hat Enterprise Linux is independently validated against FIPS standards, and every EUS release achieves Common Criteria Certification.

Built-in compliance tools – Streamlines compliance by providing built-in security configuration baselines, OpenSCAP for compliance scanning and integration with Red Hat Smart Management and Red Hat Insights for managing compliance at scale.

Secure hardware root of trust – Provides consistent hardware security module configuration for smart cards and hardware security modules (HSMs) to use hardware to measure software to verify that your systems have not been modified.

Centralized identity management – Manages the authentication and authorization of user actions and role-based access control at scale across the environment. Integrate with other identity and access management solutions and record changes made to the system by privileged users through session recording, auditing, and logging data.

Scalable compliance with Red Hat Insights – Integrates scalable security configuration through OpenSCAP using Red Hat Insights. Take advantage of CVE analysis, an expert rule database of security configuration, compliance checking, and remediation.

Experience all Red Hat Enterprise Linux has to offer

Contact your Red Hat sales representative, talk to a Red Hatter, or download a free product trial and find out how Red Hat Enterprise Linux provides you the control, confidence, and freedom to manage security and compliance consistently across your entire hybrid cloud infrastructure.