Optimize Linux security with Red Hat

The business value of Red Hat Enterprise Linux

IDC found that organizations that standardized on Red Hat Enterprise Linux realized significant security benefits, including:[1]

- 33% more efficient security teams.
- 46% quicker to complete security updates.
- 47% quicker to respond to security vulnerabilities.

Not all Linux distributions approach security the same way

In the world of IT infrastructure security, new threats emerge daily and compliance regulations are continuously added. Standardizing on a security-focused foundation is essential to safeguarding applications, processes, and workloads. While all Linux® distributions are rooted in open source, each takes a different approach to security.

When choosing a Linux distribution to standardize on, it is important to consider how well prepared you will be to mitigate new risks and meet the latest requirements. How are the distribution's security capabilities developed? How efficiently can you apply the distribution's protections in your environments? How will the distribution support and enhance your security posture beyond the point of sale, to safeguard your infrastructure from emerging threats now and into the future?

As a hardened operating system (OS) rooted in over 30 years of Linux experience, offered by a technology leader trusted by more than 90% of Fortune 500 organizations,[2] Red Hat® Enterprise Linux extends a *defense in depth* security strategy to solution development, configuration and management, and support. This overview explores how each of these elements contribute to a strong security posture, and work together to form a trusted, security-focused OS.

Red Hat Enterprise Linux is built for business-critical security and reliability

Red Hat is built on an open source foundation by a global, decentralized, and transparent community of international engineers that put security at the forefront of technology. Red Hat Enterprise Linux integrates a security focus from the outset, allows for easier application of security capabilities at build time, and supports users through continuous vigilance and remediation of emerging threats.

Security-focused software development lifecycle

When selecting a Linux distribution, it is important to consider what standards were followed during the development phase.

Red Hat prioritizes security during the development lifecycle, aligning with the National Institute of Standards and Technology (NIST) Secure Software Development Framework (SSDF), Open Worldwide Application Security Project (OWASP) guidance, and International Organization for Standardization (ISO) standards.

Red Hat Product Security fosters continuous security improvements in Red Hat's productization pipelines while supporting the systems and teams that work to assure the confidentiality, availability, and integrity of Red Hat's products and services. For the many Red Hat customers working in highly regulated industries, software supply chain security assurance is a requirement prior to deployment.

1 IDC White Paper, sponsored by Red Hat. "The Business Value of Standardizing on Red Hat Enterprise Linux." Document #US52594324, Sept. 2024.

2 Red Hat client data and Fortune 500 list, June 2024.

facebook.com/redhatinc
twitter.com/RedHat
linkedin.com/company/red-hat

redhat.com

Security built into production

The best Linux platform for your organization is a distribution that equips your team to efficiently apply protections based on best security practices. Red Hat incorporates multiple layers of security mechanisms within its Linux platform, including secure-by-default configurations, least privilege access controls, and automation.

One of the capabilities that Red Hat Enterprise Linux users can use to build security into their images from the start are the various security profiles that offer default configurations. These security baselines are based on best practices and allow administrators to apply configuration at build time, making sure their deployment meets compliance and corporate security policy requirements. This not only lowers risk, but also mitigates human error during what would otherwise be manual tasks after the build.

Red Hat Enterprise Linux helps customers achieve security goals

When the University of Sussex needed to migrate business-critical servers to a fully supported operating system, it worked with IT consultancy firm WM Promus to adopt Red Hat Enterprise Linux—reducing its risk of a cyber attack and earning a significant government certification for demonstrating a high degree of operational security.

"The university has a massive IT estate. Moving to Red Hat Enterprise Linux minimized disruption and meant the team could mitigate risks quickly."[3]

Eileen O'Mahony,
General Manager, WM Promus

A roadmap to address future threats

Having a strong security posture means being prepared for future threats and able to comply with emerging requirements. Some Linux distributions may require users to take on this preparation independently, leaving them to look for community solutions.

Red Hat Enterprise Linux is backed by a product and development team that actively observes for new threats and develops approaches to preparing for them. These Red Hat experts are active members of the security community, with many involved in the OpenSCAP project, an open source framework for security and compliance monitoring of Linux systems.

Adherence to global demands for regional compliance

Another important consideration when selecting a Linux distribution is whether it will be able to support the various compliance mandates that your teams and customers will require. Does it support a range of common cybersecurity validations and certifications, or will your team need to figure that out afterwards?

Over the years, Red Hat has made significant investments to make sure that Red Hat Enterprise Linux is best able to help organizations meet the strict global security requirements of their region and to position them to take advantage of security best practices as efficiently as possible. With over 100 offices in more than 40 countries, the team at Red Hat understands that there are a multitude of compliance regulations that differ from country to country.

To meet regional compliance demands, Red Hat has achieved a wide array of validations and certifications for its products and solutions, including Red Hat Enterprise Linux.

Efficient deployment methods

Meeting security requirements and following necessary best practices can place a burden on security teams. Scanning, validating, and attestation can be time-consuming, and require a high level of effort from multiple teams.

Image mode, a deployment method for Red Hat Enterprise Linux, takes a container-native approach to building, deploying, and managing the OS. This means security teams can apply container security tools, from those for scanning and validation to cryptography and attestation, to the base elements of the OS, making their jobs far less complex. This approach not only lowers risk, but also increases efficiency.

3 Red Hat case study. "WM Promus helps university boost efficiency and security." 23 Oct. 2024.

Proactive risk management

Your operating system should make it simple and efficient for your teams to maintain ongoing awareness of potential threats and security-related issues.

Red Hat Lightspeed, an end-to-end system management solution integrated with Red Hat Enterprise Linux, helps Red Hat Enterprise Linux users self-identify and report issues, prioritize risks based on the potential effect to their business, and even trigger the next action in an automation toolchain. Red Hat Lightspeed can scan for Common Vulnerabilities and Exposures (CVEs), and help to prioritize remediation actions based on the risk type, severity, and effect.

It can help your teams be proactive by auditing regulatory compliance with OpenSCAP policies, correct noncompliant systems, and generate compliance reports. You can also use Red Hat Lightspeed to rapidly detect active malware signatures in systems across your hybrid cloud environment.

Ongoing security support

Choosing which Linux platform to standardize on will have implications for your organization for many years to come. As such, it is essential to explore what type of support you can expect after deployment, and further into the future.

Red Hat Enterprise Linux users can operate with confidence, knowing they are backed by 10 years of updates and support for major releases, and access to the Red Hat Customer Portal, which delivers information about ongoing security vulnerabilities and the critical steps teams can take to mitigate their effect. Red Hat's Product Security Incident Response Team (PSIRT) helps users understand the risk and effect of emerging CVEs, and provides guidance for remediation.

Trusted partnerships and a history of collaboration

Red Hat works with many industry-led coordinated responsible disclosure programs. With a long, documented history of participating in security organizations such as Forum of Incident Response and Security Teams (FIRST), Open Source Security Foundation (OpenSSF), Oasis, and others, Red Hat remains a global partner in security collaboration.

As 1 of 6 organizations globally to hold a special role as a Root participant with the CVE organization, Red Hat partners with CVE.org on their mission to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities. In addition to the Root role, Red Hat is also a CVE Numbering Authority (CNA), which lets Red Hat assign CVE IDs to vulnerabilities and publish CVE records. This means that by the time a Red Hat Enterprise Linux user is notified of a new CVE, a team of security experts who are intrinsically familiar with the platform has already been actively involved in the search, assessment, and investigation into any necessary remediation steps.

Community sharing

Even users of other Linux distributions will likely benefit from Red Hat's security practices. In keeping with the open source ethos, Red Hat believes in community collaboration when it comes to rapid response, patching, and mitigation strategies for vulnerabilities that affect the Linux system, in order to maintain the reputation of Linux as a highly security-focused OS.

The Red Hat team collaborates with teams around the world in the development of open source security practices. Some examples of this include the creation of OpenSCAP, membership in OpenSSF, and contributions to OSV.dev.

This collaboration also extends to Red Hat code, which is open to community members to inspect, audit, review, and contribute to.

Optimize Linux security with Red Hat

When you standardize on Red Hat Enterprise Linux, you are backed by a company that believes in security by design. Learn more about how Red Hat can help your organization build on a security-focused Linux platform.

About Red Hat

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers develop cloud-native applications, integrate existing and new IT applications, and automate and manage complex environments. A trusted adviser to the Fortune 500, Red Hat provides award-winning support, training, and consulting services that bring the benefits of open innovation to any industry. Red Hat is a connective hub in a global network of enterprises, partners, and communities, helping organizations grow, transform, and prepare for the digital future.

North America	Europe, Middle East, and Africa	Asia Pacific	Latin America
1 888 REDHAT1 www.redhat.com	00800 7334 2835 europe@redhat.com	+65 6490 4200 apac@redhat.com	+54 11 4329 7300 info-latam@redhat.com

facebook.com/redhatinc
twitter.com/RedHat
linkedin.com/company/red-hat

redhat.com