

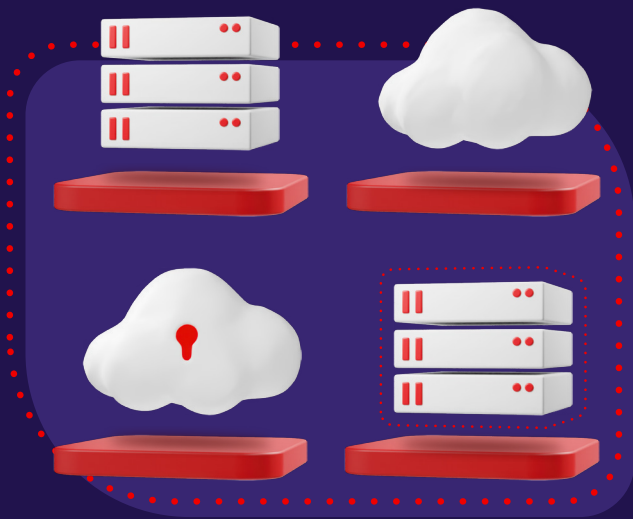


Managing infrastructure at cloud scale



Learn how to stay
security focused with
Red Hat Enterprise Linux

Table of contents



Introduction

Page 3

Chapter 1

Handle complexity with consistency

Page 5

Chapter 2

Linux: The operating system for the hybrid cloud

Page 8

Chapter 3

Red Hat Enterprise Linux: A security-focused solution

Page 9

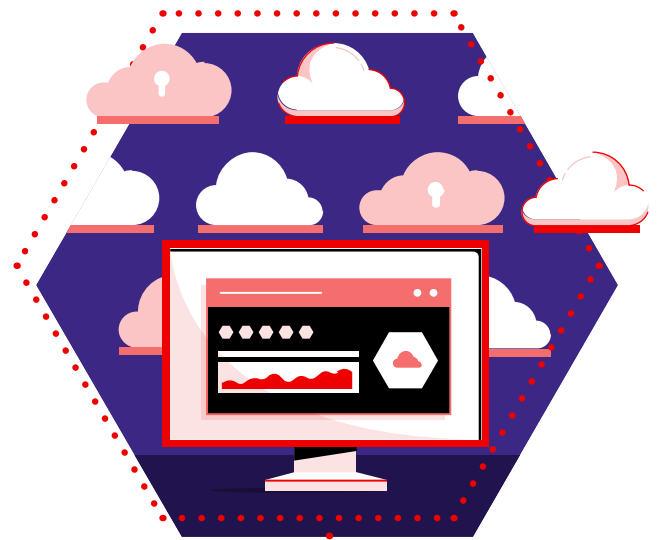
Get started

A more effective approach

Page 12



Introduction



The scalability and efficiency of cloud architectures and the potential for cost savings continue to draw organizations toward public, private, and hybrid cloud environments. In fact, a hybrid approach is used by 73% of respondents in recent Red Hat research.¹ Each environment added brings new complexity, and today that complexity is inseparable from security risk.

Attackers now use AI to find and exploit vulnerabilities faster than most teams can patch them. Between 2020 and 2025, the mean time to exploit a new vulnerability fell from 44 days to negative 7 days, which means exploits often appear about a week before a vulnerability is publicly disclosed.² The volume of new Common Vulnerabilities and Exposures (CVEs) being reported has climbed just as sharply. In the 1st quarter of 2026, there were 15,176 new Common Vulnerabilities and Exposures (CVE) records reported, or about 166 a day—a 19% increase over the 4th quarter of 2025, which saw 12,796 CVEs, or 140 per day.³

Most organizations cannot keep pace. In a recent study, 37% of vulnerabilities in large organizations remain unpatched after 12 months.⁴ The gap between how fast threats arrive and how fast teams can respond is widening dramatically.

A consistent operating platform across clouds and on-premise systems helps teams apply patches, address security threats, and apply policies faster. Specialized workloads, such as custom AI applications that require dedicated stateful graphics processing unit (GPU) architectures, can still use purpose-built environments while sharing a common foundation for compliance, vulnerability management, centralized oversight, and resource access.



¹ Red Hat e-book. "[State of Linux in the public cloud](#)." 13 April 2026.

² Kutscher, Jurgen, "[M-Trends 2026: Data, Insights, and Recommendations From the Frontlines](#)." Google Cloud, 23 March 2026.

³ "[CVE Program Report for Q1 2026](#)." CVE.org, 12 May 2026.

⁴ "[2026 Vulnerability Statistics Report](#)." Edgescan, accessed on 22 Sept. 2026.

Managing infrastructure at cloud scale is not only about controlling cost and complexity. It is about building a strong, reliable foundation, treating security as a primary focus, and implementing automation so teams can react to vulnerabilities in hours rather than months. An inconsistent or fragmented infrastructure often leads to direct security exposures.

To close the gap between the speed of new security threats and the speed of response, organizations need an approach that lets teams take advantage of multiple cloud platforms while keeping the underlying operating system (OS) consistent, reliable, and security focused. Red Hat® Enterprise Linux® can provide that foundation for hybrid cloud infrastructure.



Find out more about how Red Hat Enterprise Linux can support evolving infrastructure. Watch a video on the [Red Hat Enterprise Linux cloud experience](#).⁵

Complexity doesn't just increase—it multiplies

Each component, cloud, platform, and OS adds overhead for management, maintenance, and security. In time, teams can become overwhelmed with even basic tasks.

44 days to negative 7 days

The mean time to exploit a new vulnerability fell from 44 days in 2020 to negative 7 days in 2025, so exploits now often appear before public disclosure.²

166 vulnerabilities a day

By the 1st quarter of 2026, an average of 166 vulnerabilities were published every day, a 19% increase over the Q4 2025 average.³

37% left unpatched

According to a recent study, 37% of vulnerabilities in large organizations remain unpatched after 12 months.⁴

See it. Stage it. Ship it.

Overcome complexity with Red Hat Enterprise Linux. Instead of stitching together multiple tools from different vendors, choose a single, integrated workflow that moves from detection to remediation. Running Red Hat Enterprise Linux with Red Hat Satellite and Red Hat Ansible Automation Platform allows for detection through remediation in an optimized workflow.

⁵ Red Hat Youtube. "[Cloud-optimized Red Hat Enterprise Linux](#)." 13 Nov. 2025.

Chapter 1

Handle complexity with consistency

Consistency is essential for managing the complexity of a multicloud environment.

Standardizing on a consistent platform across environments can make infrastructure easier to manage, operate, and govern with a continual focus on security. Consistency in an OS does not require forcing every workload onto identical infrastructure. Some workloads, such as custom AI applications that need dedicated stateful GPU architectures or patient healthcare databases subject to strict data-privacy regulations, for example, call for a unique setup.

Consistency means establishing a reliable operating environment with a security focus for compliance, enhanced protection from vulnerabilities, and ease of management. Standardizing on a common foundation keeps services, data controls, and security policies tightly aligned, allowing teams to manage everything from a central control plane and share resources across teams without extensive staff retraining.

Consistent features and services

When an organization's systems run on the same OS across multiple environments, the features and services teams use are common and share a consistent user interface across those environments. In a hybrid environment that spans public and private clouds, edge locations, and on-premise infrastructure, or any combination of these, a lack of standardization creates multiple variations in services, user experience, and other unique operations and workflows that slow down progress.

This might include:



Mismatched tooling: Security and monitoring tools native to a single cloud platform are unavailable or behave differently in another.



Feature gaps across environments: A service available in your public cloud isn't supported at remote edge locations or on-premise datacenters.



Fragmented patch management: Security patches and vulnerability updates are applied on different schedules across different platforms, leaving isolated systems exposed.



Forced rework: Application workflows built for on-premise infrastructure fail to run in the public cloud without custom modifications.

When the features and services that an organization's system depends on are outside of its control, the complexity of running that system and managing it with an adequate security focus increases.

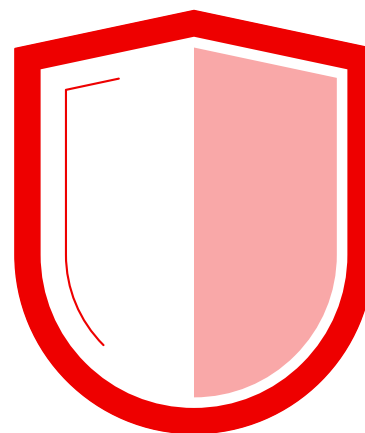


Consistent compliance and security focus

Security management is a primary requirement for any system. From OS to applications, a plan for security needs to be a priority from the start, and a team's compliance and security focus should be proactive so it continues to meet evolving requirements.

With components spread across different environments, keeping them synchronized is challenging. As compliance requirements evolve, teams may have to update configurations across infrastructure separately, and each provider's services and configurations can have differences that must be tracked and managed. In an environment facing 166 newly published vulnerabilities a day,³ managing security and compliance manually in multiple OSes quickly becomes unsustainable.

A centralized approach to controlling configuration, so that every environment consistently meets the same security and compliance requirements, is the practical way to keep that overhead manageable.



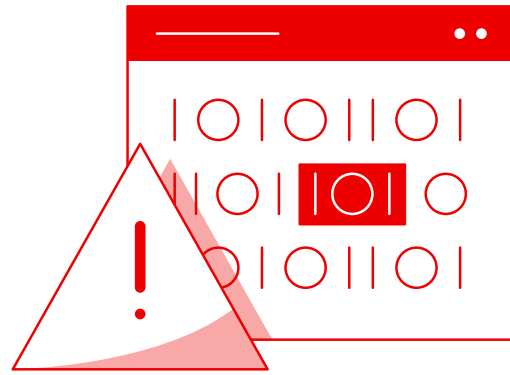
As workloads shift to open hybrid cloud, a security-focused foundation for the applications and processes matters more than ever. Built to meet today's expectations for security and compliance, Red Hat Enterprise Linux provides that foundation.

Consistent data control

If an organization discovers an unauthorized release of data, finds that data resides in a noncompliant cloud, or simply wants to move an application between clouds, getting that data out of the cloud can be difficult and expensive if it's running on a cloud-native OS provided by the cloud provider.

The need for greater control over data has led jurisdictions to enact laws that require organizations to meet strict standards for handling personal, financial, and other data. Regulations such as the California Consumer Privacy Act (CCPA) and the European Union's General Data Protection Regulation (GDPR) have resulted in billions of dollars in fines for major organizations. Even without the threat of penalties, data needs to be controlled effectively, and a consistent environment for managing it makes that far simpler by allowing portability from one environment to another as needed.

Data control is also becoming more regional. As data sovereignty requirements grow, Red Hat continues to expand support for sovereign cloud deployments, helping organizations keep data within the jurisdictions they are required to use. For organizations that need to control their digital infrastructure, data, and supply chain in a sovereign cloud, Red Hat Enterprise Linux provides the open source OS foundation that sovereign cloud environments require: transparent, auditable, portable, and free from proprietary cloud lock-in.

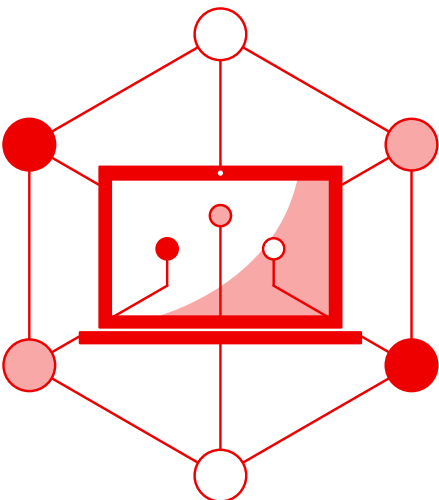


Consistent governance and visibility

Adding an application or user to an environment is usually fairly simple. However, in a complex hybrid cloud environment, this often leads to cloud sprawl, where forgotten workloads linger and the unmonitored users and accounts attached to them multiply quickly.

The result is higher costs for compute, storage, and bandwidth, along with potentially increased security exposure. It is not unusual for cloud environments to hold hundreds of accounts belonging to people who have left the company. Dormant development servers, for example, can carry significant risk and can be compromised without anyone noticing. Visibility into what is running, and what is consuming resources, is the 1st step to controlling it. Red Hat Lightspeed (formerly Red Hat Insights) provides that visibility across hybrid cloud environments, so teams can apply rules to govern each environment and gain consistent control over systems.

A consistent management approach across the many environments in any IT infrastructure is the key to managing cloud sprawl.⁶



Chapter 2

Linux: The operating system for the hybrid cloud

The starting point for controlling complexity, simplifying management, and reducing risk exposure across environments is a standard operating environment (SOE).

Building a modern hybrid cloud environment requires the infrastructure to be easily manageable while keeping workloads stable, available, and as secure as possible. For many organizations the answer is clear. More than 90% of companies in the U.S. Fortune 500 rely on Red Hat.⁷ Organizations running Red Hat Enterprise Linux in the cloud get the same benefits they get on premise, and when running on one of the hyperscalers, Red Hat Enterprise Linux is jointly engineered and optimized to run most efficiently on their unique underlying infrastructure.

An organization's Linux choice determines who owns security oversight

To realize the benefits of the cloud, it matters which Linux distribution an organization chooses. Cloud providers offer different Linux distributions through their marketplaces, and each comes with its own procurement model, operational cost, support model, and integrations. In a multicloud environment, those differences add up.

Determining who owns OS security is a critical decision in any hybrid cloud strategy. When organizations rely on community distributions or cloud-provider builds, the burden falls entirely on internal teams to configure the OS, vet software dependencies, and coordinate vulnerability responses across environments.

If developers pull unapproved packages to meet deadlines, they introduce untracked security risks. An enterprise open source Linux distribution transfers that burden to a trusted vendor who continuously audits, signs, and maintains the entire software supply chain from the core OS through the application layer.

Cloud-native Linux distributions are designed to work best inside a single cloud, and their security capabilities often stop at the edge of that cloud. Standardizing on Red Hat Enterprise Linux provides centralized, cloud-agnostic control, so compliance rules, cryptographic policies, and remediation workflows stay identical whether they run on Amazon Web Services (AWS), Microsoft Azure, Google Cloud, Oracle Cloud Infrastructure (OCI), a regional cloud provider, a private cloud, or on premise.

By standardizing on Red Hat Enterprise Linux, organizations migrating workloads to the cloud can reuse existing processes, configurations, and skills across environments.

Find out more about how organizations are using Linux in public cloud environments in the [2026 State of Linux in the public cloud e-book](#).¹

⁷ Red Hat client data and Fortune 500 list, July 2026.

Chapter 3

Red Hat Enterprise Linux: A security-focused solution

Red Hat Enterprise Linux provides a consistent foundation, plus the built-in management and security features to run it confidently across clouds.

Red Hat Enterprise Linux helps teams address the challenges hybrid cloud environments introduce. It supports unified workload migrations, streamlines management, and helps proactively prepare for security threats.

Cloud-optimized for major hyperscalers

Cloud-optimized Red Hat Enterprise Linux offerings are jointly engineered, integrated, and supported images for Red Hat Enterprise Linux across AWS, Google Cloud, Microsoft Azure, and OCI. These cloud-optimized offerings are tailored to specific hyperscalers' unique environments, providing users with pretuned, ready-to-run images to build, deploy, and manage workloads in the cloud. They provide users a stable, consistent surface to deploy and build on without having to worry about the underlying technology.

Simplified access in public cloud marketplaces

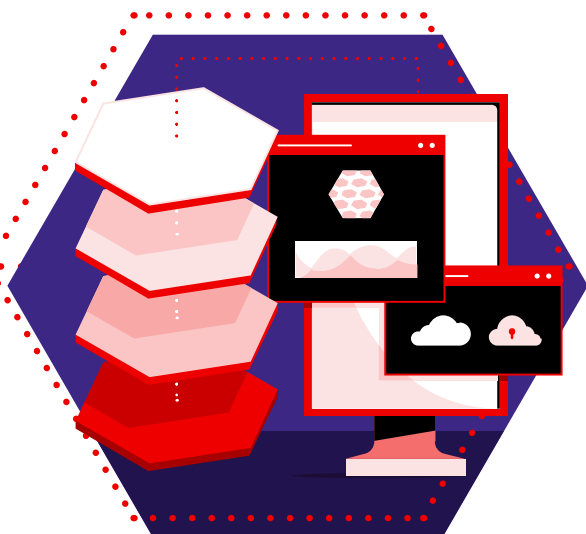
Red Hat Enterprise Linux is available through public cloud marketplaces, which simplifies both purchasing and deployment. Organizations can draw down from their cloud provider committed spend programs including the Private Pricing Agreement (PPA) with AWS, the Microsoft Azure Consumption Commitment (MACC), Google Cloud committed use discounts (CUDs), and Oracle's Universal Credit model. Because these purchases draw down commitments that have already been made, budget that was already set aside can be put to work, procurement can be consolidated, and separate approval cycles can be avoided.

Alternatively, an organization can move an existing Red Hat Enterprise Linux instance from on premise to the cloud with [Red Hat Cloud Access](#). Choose from pay-as-you-go options, annual subscriptions, or work with Red Hat or a certified partner to develop a custom plan tailored to an organization's needs.

Learn more:



[Red Hat Enterprise Linux for AWS](#)
[Red Hat Enterprise Linux for Microsoft Azure](#)
[Red Hat Enterprise Linux for Google Cloud](#)
[Red Hat Enterprise Linux for OCI](#)



Security focus built in from the start

Rather than treating security as a series of reactive fixes, Red Hat Enterprise Linux integrates comprehensive security capabilities from the start. This built-in approach mitigates risks across 3 primary pillars:

Modern deployment and immutability



Image mode for Red Hat Enterprise Linux: Manage the OS as an immutable container image using familiar continuous integration and continuous delivery (CI/CD) pipelines, preventing configuration drift and reducing vulnerability exposure.



Red Hat Hardened Images: Minimal container baselines that reduce user-space footprint and attack surface by default. Available at images.redhat.com.

System defense



Red Hat Lightspeed: Proactively identifies vulnerable systems across your hybrid environment and contextualizes risk based on live workloads.



Security-Enhanced Linux (SELinux) active by default: Applies strict access controls in enforcing mode out of the box, containing application breaches and stopping lateral network movement.



System-wide cryptographic policies: Standardizes security settings across system libraries to phase out aging, insecure protocols automatically.

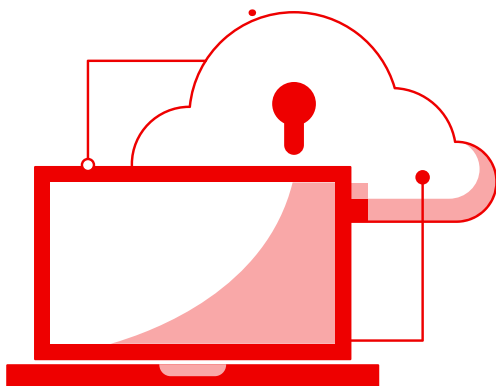
Secure supply chain and post-quantum cryptography (PQC) preparedness



Signed packages and trusted libraries: Every RPM Package Manager (RPM) and application dependency is cryptographically verified prior to installation, maintaining software supply chain integrity from the OS to the application code.



Post-quantum preparedness: Incorporates National Institute of Standards and Technology (NIST)-approved quantum-resistant cryptography, helping organizations proactively protect sensitive data against long-term decryption risks.⁸



Ease of management

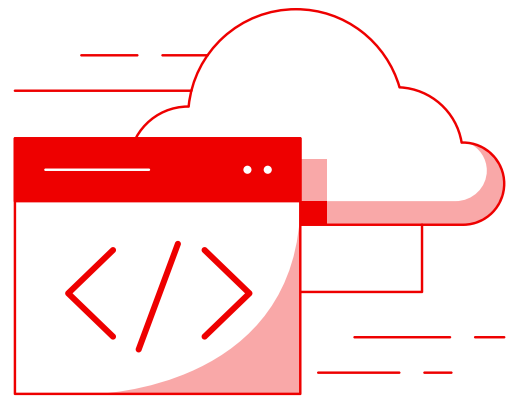
Standardizing on Red Hat Enterprise Linux across infrastructures provides a consistent operating foundation supported by an extensive ecosystem of certified hardware, software, and cloud providers. Advanced tools from Red Hat automate and streamline application management, from provisioning and scaling to policy enforcement and decommissioning.

In a complex infrastructure, simply knowing what is running across multiple clouds and locations is challenging, and maintaining and updating all of it can consume too many team resources. [Red Hat Lightspeed](#), included with Red Hat Enterprise Linux, collects analytics about each environment to help identify and fix issues before they become incidents.

Flexibility and consistency

Red Hat Enterprise Linux is designed for consistent performance and a security focus across environments, whether in the cloud, on premise, or at the edge. Using the same OS across deployments provides the same user experience for all workloads.

Workloads should run wherever best meets the need for performance, scale, and compliance. Red Hat Enterprise Linux is engineered to perform as part of a large partner ecosystem, giving organizations freedom from cloud vendor lock-in. Standardizing on it lets organizations maintain skills, standards, processes, and management tools, so when needs change, it lowers the friction and cost of that change. Red Hat Enterprise Linux offers long-term support so teams can keep critical workloads on a given release for an extended amount of time and upgrades can be planned based on an organization's own schedule. Organizations with differing needs can opt for the [Red Hat Enterprise Linux Extended Life Cycle, Premium](#) or [Red Hat Enterprise Linux Long-Life Add-On](#) subscriptions to support their critical workloads as required.



Innovative developer tools

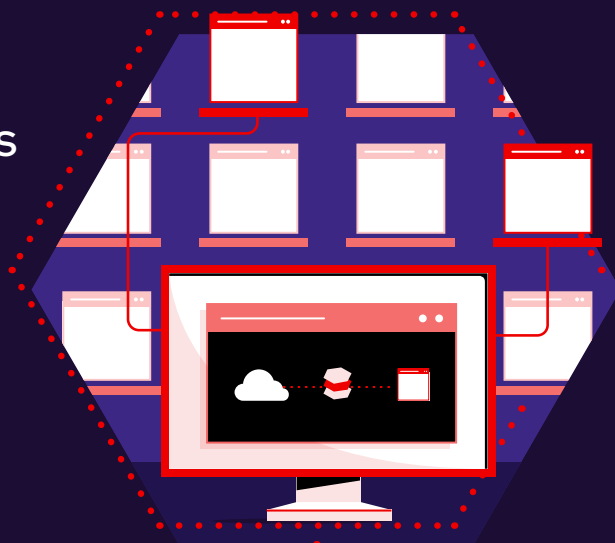
Red Hat Enterprise Linux includes access to the Red Hat Knowledgebase, how-to videos, demonstrations, get-started guides, and documentation. Red Hat Universal Base Image (UBI) provides a stable Red Hat Enterprise Linux userspace for container projects, and application streams provide current versions of popular languages and tools. Developers can also use Red Hat Enterprise Linux as a container host with tools such as Podman, Skopeo, and Buildah.

Get started

A more effective approach

Modern organizations operate across multiple environments. Choose an OS that unifies them.

No matter what combination of environments an organization's infrastructure includes, the key to success is a foundational OS that is consistent and reliable wherever workloads run, and that lets teams approach security consistently across environments.



Ready to streamline operations and build a security-focused environment? Talk to a Red Hatter about building cloud infrastructure on Red Hat Enterprise Linux.



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.

f facebook.com/redhat
X twitter.com/RedHat
in linkedin.com/company/red-hat

redhat.com

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

Copyright © 2026 Red Hat, LLC. Red Hat, the Red Hat logo, Ansible, and OpenShift are trademarks or registered trademarks of Red Hat, LLC or its subsidiaries in the United States and other countries. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries. All other trademarks are the property of their respective owners.