Why your operating system still matters

8 ways Linux supports modern IT and business goals

Red Hat

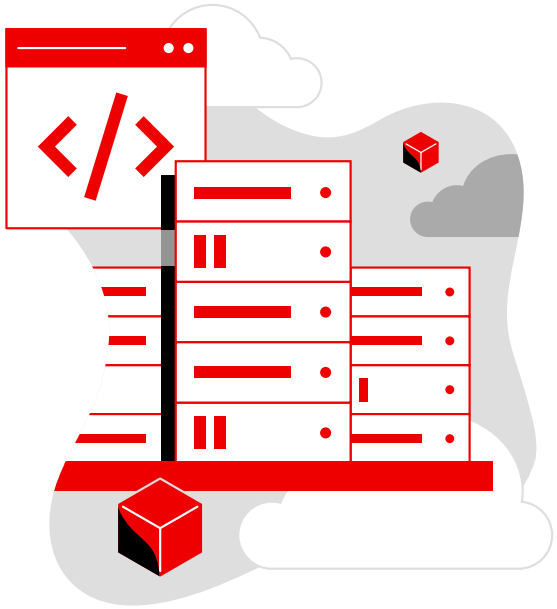
Contents

Your operating system is an essential part of modern IT

Operating systems have always been a key component in IT environments.

First developed in the 1950s, operating systems have continuously evolved to meet changing demands. Early operating systems focused primarily on batch processing and simple task scheduling, executing 1 job at a time. However, with the introduction of time-sharing systems in the 1960s, multiple users could interact with a computer simultaneously. Consequently, the following decades saw the emergence of operating systems like UNIX, which introduced modularity and portability to computing environments.

During the 1980s, Increased sales and adoption of personal computers introduced operating systems to the general public. The invention of graphical user interfaces (GUIs) revolutionized the way users interacted with computers, making computing accessible to a broader audience.



As the demand for server-based computing grew, **Linux®** emerged as a powerful, scalable operating system for enterprise datacenters worldwide. First released in 1991, the Linux kernel offered a free, open source alternative to UNIX that anyone could run, study, share, and modify. Linux is now one of the world's most popular operating systems and provides an ideal platform for modern, innovative IT.

The 2000s delivered **virtualization technologies**—followed by **containers**—that led to more efficient hardware resource use and a shift toward **cloud computing**. As a result, operating systems took on new management roles to support flexible application deployments and resource optimization.

Today, the influence of operating systems extends beyond core datacenters to include emerging technologies like **edge devices** and the **internet of things (IoT)**. Operating systems provide efficient data processing at the network edge to reduce latency and enhance performance in use cases ranging from smart cities to autonomous vehicles.

This e-book provides an overview of why the operating system—and specifically the Linux operating system—still matters today and how it meets modern IT and business demands.

8 reasons your operating system still matters today

As organizations adopt increasingly distributed, cloud-based IT environments, the importance of the operating system continues to grow.

87% of organizations have a multicloud strategy in place, and 50% of enterprise workloads run in a public cloud today.[1] Your operating system can serve as a unifying foundation across on-site and cloud infrastructure, diverse hardware and software, and traditional and cloud-ready applications. Security, management, portability, and life cycle planning all start with your operating system. Standardizing on a single operating foundation across your datacenter and cloud environments can simplify your IT operations, enhance flexibility, improve security, and support innovation.

As one of the world's most popular operating systems, many organizations choose Linux for their IT foundation. In fact, Linux held a 65.6% share of net new physical deployments and an 82.8% share of net new virtualized deployments in the worldwide server operating systems market in 2022.[2]

Organizations run a wide range of production and development workloads—including IT and web infrastructure, customer relationship management, and enterprise resource management—on Linux operating systems.[3] This chapter discusses the ways that your Linux operating system supports your applications, processes, and IT environment to deliver value across your entire organization.

In this chapter:

1 *Flexera. "**Flexera 2023 state of the cloud report**." March 2023.*

2 *IDC Market Share. "Worldwide Server Operating System Environments Market Shares, 2022: Steady Growth Persists." Document #US51038623. July 2023.*

3 *IDC White Paper, sponsored by Red Hat. "**Red Hat Enterprise Linux: $1.7 Trillion a Year Boost for Customers**." Document #US48931522. March 2022.*

1 Operating systems connect hardware, applications, and users.

As a fundamental layer in your software stack, your operating system supports interactions between hardware and applications and provides essential services and resources.

Your operating system abstracts the underlying hardware components to allow applications to run on diverse infrastructure without modifications for specific systems. It also manages resources—including central processing units (CPUs), memory, storage, and networking—to optimize system performance and prevent conflicts between multiple running applications. Operating system command-line interfaces (CLI) and GUIs let you interact more intuitively with the computer and its applications. Security features like user authentication, access controls, and encryption protect data and resources from unauthorized access. And error and exception handling capabilities prevent system crashes and enhance system reliability and overall user experience.

Modern operating systems like Linux usually implement two modes—kernel mode and user mode—to determine which privileges are available to which applications, components, and users. Via kernel mode, trusted core software components—like the **operating system kernel** and some device drivers—can perform privileged operations, directly use hardware resources, and access restricted system memory.

All other software—including user applications, libraries, and tools—run in user mode with limited access to system resources. These applications can only access the user space, isolated memory regions that prevent applications from interfering with critical operating system components.

Build your IT foundation on trusted expertise

While Linux can serve as a stable operating foundation for all of your IT workloads, many different Linux distributions are available, each with different tools, services, and support policies. Because your business relies on your IT foundation, your choice of Linux vendor is important and strategic.

Look for a trusted Linux vendor with the experience and expertise needed to support your business. Key aspects include:

- A production-grade Linux distribution that focuses on customer needs.
- Continuing contributions to and leadership within the Linux kernel.
- A collaborative community of customers, partners, and experts.
- A proven record of commercial support with long life cycles and security maintenance.

2 Operating systems ensure hardware and software compatibility.

Operating systems manage hardware resources like storage, networking, and peripherals to increase system stability and hardware-software compatibility.

Applications and hardware resources communicate via device drivers. Operating systems manage these drivers—ensuring proper installation, loading, and operation—to increase system stability and compatibility between applications and underlying hardware components. For example, during system initialization, your Linux operating system detects newly connected or integrated resources, identifies known devices, and locates and loads the corresponding drivers. Operating systems also provide hardware abstraction layers that let applications interact with hardware devices without knowing underlying hardware details. These standardized interfaces simplify application development and enhance portability across different hardware configurations.

Chipsets, storage, and networking are areas where device drivers and operating system management are essential. Many compute-intensive workloads like artificial intelligence and machine learning (AI/ML) can benefit from hardware acceleration in chipsets. Operating systems can make the features and acceleration from graphics processing units (GPUs), systems on chips (SoCs), and field-programmable gate arrays (FPGAs) available to these workloads.

Operating systems also provide access to data stored on hard drives in a stable and reliable manner. They manage file organization and storage using optimized methods to minimize data fragmentation, prevent naming conflicts, and ensure consistency across applications.

Finally, operating systems orchestrate network-related functions to deliver reliable connectivity and efficient data exchange between systems within a network. Using a network stack, operating systems manage the integration of network protocols to provide end-to-end communication over diverse networks. They configure and manage network devices like network interface cards (NICs) and wireless adapters to support and speed data transmission between applications. They also implement network security measures, including firewalls and encryption protocols, to help protect against unauthorized access and data breaches.

Gain choice with a certified partner ecosystem

Testing and certifications ensure that third-party products work reliably with your operating system. Look for a Linux vendor that partners with industry-leading hardware, software, and cloud vendors to give you more choice, innovation, and stability. Check that your chosen vendor's partner ecosystem includes the products and services that you currently use and plan to use in the future.

3 Operating systems enhance platform reliability and stability.

Operating systems detect and handle software and hardware errors to provide a stable, reliable platform for applications and users.

Applications are at the core of many digital businesses, and downtime is often unacceptable. Many operating systems include advanced error-detection mechanisms that capture and manage runtime errors during application execution. These mechanisms help to prevent system-wide crashes, disruptions, and data corruption. Plus, operating systems monitor critical applications and system files through file integrity checks, checksums, and digital signatures to ensure that only authorized and unmodified code is executed.

Hardware errors are also a concern. By detecting and managing hardware errors like memory faults, disk errors, and processor malfunctions, operating systems can increase system stability and prevent catastrophic failures. Working with the error correction code (ECC) and cyclic redundancy checks (CRC) protection built into memories and storage devices, operating systems can identify and manage faulty hardware to improve the reliability of data stored and used by applications. Error detection and correction mechanisms like journaling or checksums help operating systems quickly and accurately retrieve data for applications and users.

Understanding and fixing problems on a system level is also important. Operating systems provide logging and diagnostic tools that record information about errors and system events to assist troubleshooting and proactive maintenance operations. Using these tools, system administrators can analyze error patterns, identify potential vulnerabilities, and take corrective actions to maintain the overall stability and reliability of the system.

Improve stability with predictive analytics and proactive remediation tools

Managing complex IT environments can be complicated and time-consuming. Look for a Linux distribution that includes advanced management and automation tools to help you proactively manage your entire IT environment. Unified tools that work across infrastructure footprints and monitor all systems in your environment can help you find issues before they impact business operations. At the same time, tools that focus on operations, security, and business outcomes let you see the organizational impact of issues and changes and help to prioritize remediation actions.

4 Operating systems boost IT operational efficiency.

A consistent operating system can serve as a unified foundation across IT footprints, allowing you to standardize and streamline operations, increase efficiency, and improve security.

Modern IT environments often consist of multiple infrastructures and architectures. In fact, 85% of organizations operate multiple deployment environments, and 31% deploy applications in 5 or more environments.[4] For example, you may use both on-site datacenters and public cloud providers and deploy workloads on servers, workstations, and edge devices based on a variety of hardware architectures like x86, Arm, and IBM Power.

Consistency is critical in these diverse environments. Standardized operating environments let you develop common procedures, policies, and configurations that simplify day-to-day operations and management tasks. This delivers many benefits for IT organizations:

- **Interoperability.** Using a common operating system promotes interoperability and integration across diverse infrastructure. You can deploy, manage, and troubleshoot distributed applications across massive environments with less complexity.
- **Scalability.** Uniform operating system deployments simplify scaling of IT services and environments because new infrastructure can replicate existing, validated configurations.
- **Security.** Standardized operations environments make it easier to consistently enforce security policies—including regular patching, updates, and compliance audits—across environments, reducing the risk of security vulnerabilities.
- **Availability.** Using a consistent operating system across hybrid cloud environments streamlines issue resolution to reduce system downtime.

Standardize for efficiency

Your operating system can serve as a consistent, standardized foundation across all infrastructures and architectures. Choose a Linux vendor that offers multiple operating system variants optimized for different deployment environments while maintaining overall consistency. Ensure that the included and associated management and automation tools work in the same manner across all variants. Standardizing on 1 of these distributions can help you create cohesive, unified operating environments that streamline infrastructure management, enhance IT efficiency and productivity, and improve security.

4 F5 Networks. "2023 State of application strategy report." March 2023.

5 Operating systems protect your infrastructure, applications, and data.

Operating systems defend against threats that can compromise the integrity, confidentiality, and availability of your infrastructure, applications, and data.

The Linux kernel includes many security capabilities to help protect your infrastructure, applications, and data. For example, Linux operating systems contain the authentication and authorization tools needed to implement zero trust architectures. Authentication via usernames, passwords, biometrics, or security tokens identifies the individuals or applications that want to access IT systems and assets. Authorization and access control mechanisms like Security-Enhanced Linux (SELinux) define the permissions and privileges granted to these users, groups, or applications. Together, these tools help prevent unauthorized access to sensitive resources and system configurations.

Other key operating system security features include:

- **Encryption.** Built-in encryption technologies can protect confidential files and sensitive data both at rest and in transit across networks. For instance, Red Hat® Enterprise Linux uses system-wide cryptographic policies to configure and apply predefined cryptographic controls to systems and applications automatically. It also supports CPU-assisted encryption of virtual machine workloads for confidential computing.
- **Application allowlisting.** This capability establishes an index of approved applications and executable files that are permitted to run on a system by a specific user.
- **Hardware root of trust.** Hardware-based root of trust, remote attestation, and measured boot technologies verify system integrity and ensure that systems have not been modified or tampered with.
- **Security scanning.** Compliance and vulnerability scanning tools like Open Security Content Automation Protocol (OpenSCAP) can simplify audits, find and remediate misconfigured systems, and help you maintain compliance.
- **System logging.** Auditing and logging capabilities can record events and activities within a system. Administrators can then review and analyze these events, identify sources of security breaches, and implement corrective measures.

Build a foundation for zero trust

Zero trust architectures apply security to each asset, rather than managing security exclusively at the network perimeter. While Linux itself includes the core capabilities needed to build zero trust architectures, some distributions add features and tools that simplify zero trust adoption. Look for a Linux distribution that is offered via a trusted software supply chain and includes system-wide encryption settings, hardware root of trust capabilities, built-in compliance scanning, and policy-based identity management tools.

Read **the overview** to learn more.

6 Operating systems manage application and workload performance.

Operating systems manage CPU and memory use to maximize hardware performance for superior application, workload, and user experiences.

Using process scheduling technologies, operating systems optimize CPU and memory use, balance workloads across resources, and maintain system responsiveness. For example, process scheduling algorithms and load balancing mechanisms ensure efficient use and fair distribution of CPU time. Scheduling algorithms also allow multiple processes to make progress simultaneously by rapidly switching CPUs between several processes.

By prioritizing interactive processes, operating systems can create responsive experiences in which users perceive minimal to no delays. And with real-time process scheduling capabilities, processes with strict timing requirements—like embedded or industrial control systems—can meet specific deadlines and respond promptly to external events.

Linux also includes memory management capabilities to help ensure sufficient memory for applications, avoid potential conflicts, and optimize system performance. Dynamic memory allocation and deallocation provides processes with the memory needed for maximum performance. When a process is done using memory, the operating system makes it available for other processes to use.

Optimize workload performance

Look for a Linux distribution that includes tools and interfaces for tuning, monitoring, and managing system performance characteristics by application, workload, or use case. For example, some vendors offer tools and services that allow you to identify performance issues, profile application performance, and analyze data to help resolve issues rapidly or even avoid them altogether.

Operating systems also enhance memory performance through caching and buffering mechanisms that store frequently accessed data in faster, more expensive caches and other data in larger, slower random-access memory (RAM) and storage devices. And by swapping data between memory and hard disks, virtual memory lets operating systems give processes a larger address space than is actually physically available. Virtual memory increases multitasking efficiency and allows larger applications to be run on systems with smaller memory footprints.

7 Operating systems improve resource use with virtual machines.

As a key part of virtual machine technologies, operating systems optimize resource use, isolate workloads, and increase scalability across environments.

Virtual machines are isolated environments running their own guest operating systems that users and applications experience as separate hardware resources, even though they may share the actual physical resources with other virtual machines. Hypervisors are specialized software that create and manage virtual machines on a single physical server. Operating systems and hypervisors perform many of the same functions. As a result, they can share many components, including process schedulers, memory managers, device drivers, security functions, and network stacks.

Expand your virtualization

The **Kernel-based Virtual Machine (KVM)** in Linux lets you use Linux as a hypervisor. Choose a commercial Linux distribution that expands the capabilities of KVM for more efficient management.

Hypervisors perform many functions to support IT operations:

- **Resource allocation.** Hypervisors allocate resources like CPU time and memory to virtual machines, allowing multiple virtual machines to run on the same physical hardware with a guaranteed quality of service. They also present physical hardware like network adapters, storage controllers, and graphics cards to guest operating systems as virtual devices to let multiple virtual machines use the same resources without conflict.
- **Snapshots and cloning.** Many hypervisors include virtual machine snapshot and cloning capabilities to enhance the flexibility, scalability, and efficiency. Snapshots capture virtual machine state and data at specific points in time. These can be used to recover or rollback to known configurations. Cloning capabilities duplicate existing virtual machines to speed deployment of new instances.
- **Live migration and recovery.** Live migration and high availability features help balance workloads, optimize resource use, and improve virtual machine uptime. Live migration moves running virtual machines between physical hosts without service interruption. Virtual machines remain powered on, network connections remain active, and applications continue to run. If virtual machines are interrupted due to a host failure, the hypervisor automatically restarts them, within seconds and without human intervention.
- **Security and isolation.** Hypervisors enforce strict boundaries that prevent virtual machines from accessing the memory or resources allocated to other virtual machines. These boundaries help to enhance security and contain the effects of potential vulnerabilities and cyberattacks.

8 Operating systems support modern, cloud-native applications.

Linux operating systems support container technologies for deploying and managing modern, cloud-native applications with greater agility, scalability, and consistency.

52% of enterprises consider "containerizing workloads" to be a key part of application modernization efforts.[5] **Containers** are technologies that package IT components—like applications, runtimes, libraries, and dependencies—into lightweight, portable, isolated environments. Container technologies effectively virtualize the operating system, allowing multiple containers to share a single operating system kernel that manages hardware resources and interactions with the physical host system.

Linux operating systems partition kernel resources related to process spaces, file systems, and network access to give each container its own unique set of resources. As with traditional virtualization, this isolates each container to prevent conflicts and interference between containers and allows multiple containers—each with unique user spaces and runtime environments—to execute on the same host. To allocate resources fairly and appropriately, operating systems manage and limit resource use—including CPU, memory, and disk input/output (I/O)—on a per-container basis.

By managing network interfaces and configurations in container environments, operating systems ensure that containers can communicate with each other and external systems as needed while still maintaining network isolation. They also provide containers with isolated file systems that can access shared data and persistent storage via container storage drivers.

Finally, operating systems provide mandatory access controls (MAC) to enforce strict and predefined resource access policies. Containers can only interact with specified system resources to increase isolation and protect against widespread security threats and vulnerabilities.

Extend your IT environment and skills with containers

You can get started with containers with just your Linux operating system. Look for a Linux distribution that includes container tools like **Podman**, **Skopeo**, and **Buildah** to help you develop, build, run, and manage containers on your Linux systems. Choosing a Linux vendor that also provides a container orchestration platform will give you the option to expand and scale your use of containers over time.

*5 Red Hat e-book. "**How enterprises approach legacy application modernization**," 6 Feb. 2023.*

Take advantage of open source software

Open source communities create and maintain many popular operating systems—including Linux—as well as related tools and software.

Within these communities, developers propose, contribute, and test new operating system capabilities and features. Releases are made available via free community and paid enterprise distributions.

Enterprise—or commercial—distributions are often offered via subscriptions and provide additional features, services, and support tailored to business needs and concerns. For example, enterprise operating system subscriptions frequently include 24x7, production-grade technical support to speed troubleshooting and reduce downtime. They may also include training and tutorials that help users efficiently administer, optimize, and troubleshoot issues in the operating system.

Long supported life cycles increase stability across IT environments. Commercial vendors typically follow predictable release cycles, allowing organizations to plan and prepare for updates, upgrades, and new features. In-place upgrade tools and professional services can make moving to new releases smooth and efficient.

Enterprise vendors generally have security teams that assess, monitor, and respond to emerging threats to increase operating system security. Some commercial distributions include services that monitor operating systems and provide guidance for remediating security issues, noncompliant settings, unpatched systems, and configuration drift. Vendors may also certify their operating systems to industry security standards to help maintain compliance and protection.

Finally, many commercial vendors foster certified partner ecosystems for their operating systems to promote stable, reliable operations. These ecosystems may include hardware vendors, software vendors, public cloud providers, and services organizations.

Commercial open source operating system benefits

Compared to organizations that use non-paid alternatives, commercial operating system users experience:

23%
lower 3-year on-site infrastructure costs.[6]

72%
less unplanned downtime.[6]

$US17.3M
average higher net revenue per year per organization.[6]

6 *IDC White Paper, sponsored by Red Hat, "The Business Value of Red Hat Solutions vs Non-Paid Open-Source Alternatives," Document #US50423523. March 2023.*

Simplify system management

Operating system management tools can help you more effectively configure, monitor, and optimize your IT environments.

Performance management

Gain insights into system performance to identify bottlenecks, monitor utilization, and troubleshoot performance issues.

IT automation

Automate routine tasks to reduce manual intervention, minimize errors, and ensure consistent system configurations.

Security and access management

Assess, manage, and remediate security vulnerabilities to protect critical applications and data. Enforce access controls, manage permissions, and ensure that users have appropriate privileges based on their roles.

Configuration management

Apply updates and upgrades to ensure that operating systems stay current with the latest security patches and feature enhancements. Maintain consistent configurations across multiple systems to reduce configuration drift across IT environments.

Auditing and monitoring

Log and audit system events to simplify troubleshooting, compliance, and security analysis. Streamline auditing activities to ensure compliance with security and operational standards. Monitor and optimize virtual resources to ensure efficient, cost-effective use.

Backup and recovery

Create and manage backups, and implement recovery processes to safeguard data in the event of system failures or loss.

Modern IT starts with Red Hat Enterprise Linux

Your operating system plays a critical role in your IT infrastructure. Red Hat Enterprise Linux delivers more value for your organization.

No matter where you are headed in your IT journey, Red Hat Enterprise Linux can help you build an efficient, security-focused foundation for innovation across hybrid and multicloud environments. This cloud-ready operating system provides a consistent, tailored experience across footprints—including physical, virtualized, hybrid cloud, multicloud, and even edge infrastructure. Standardizing on Red Hat Enterprise Linux for both on-site datacenter and cloud environments can help you improve productivity, security, and operations as you move to the cloud and adapt to a more digital world.


Consistency across footprints


Predictive analytics and remediation tools


Advanced security capabilities


Trusted software supply chain


Built-in automation and management


Performance optimization tools


Large certified partner ecosystem


Variants for multiple architectures


Built-in container technologies

Learn more about Red Hat Enterprise Linux.

1051224_0324_KVM

Red Hat