Red Hat Enterprise Linux

Simplify security in the cloud

Red Hat Enterprise Linux delivers consistent security capabilities across environments

Operate consistently across cloud environments

Red Hat Enterprise Linux includes many optimizations to ensure reliable, security-focused performance in the cloud. It provides a consistent operating foundation for hybrid and multicloud environments, so you can run applications where it makes the most sense.

Learn more about the value of Red Hat Enterprise Linux in the cloud.

Security in the cloud is a top concern

As cloud adoption grows, security continues to be a leading concern for organizations of all sizes. In fact, 85% of organizations cite security as a top cloud challenge.[1] This concern is with good reason — 45% of breaches in 2022 occurred in the cloud.[2]

Consistency is at the core of security and compliance best practices in any environment. To protect your business, you need the same level of security policy and access controls in the cloud that you have on-site in your datacenter. Standardizing on an operating system that provides consistent security controls across all infrastructure footprints can help you improve security and compliance across your organization. Using Red Hat® Enterprise Linux® as your operating foundation across environments helps you create the consistency needed to maintain security and compliance in the cloud.

Adopt a consistent foundation for security and compliance across environments

Red Hat Enterprise Linux makes it simpler to maintain security and compliance across on-site, cloud, and edge environments. Security is a key part of the Red Hat Enterprise Linux architecture and life cycle. Built-in security features and compliance with industry and government regulations protect your systems in the cloud. Best practice-based default settings configure your systems for increased security from the start. Minimized package sets for prebuilt cloud images reduce your cybersecurity threat attack surface. Security upgrades and live patches are also provided as part of your Red Hat Enterprise Linux subscription.

With Red Hat Enterprise Linux, you can mitigate security risks, implement and maintain layered security, and streamline compliance across hybrid and multicloud environments. This overview describes key features and capabilities for adopting a consistent security approach across hybrid and multicloud environments.

Detect and remediate vulnerabilities at scale with Red Hat Insights

The average time to identify and contain a data breach in 2022 was 277 days.[2] Finding and stopping a breach in 200 days or less can reduce its resulting cost by an average of 24%.[2] Consistent, daily monitoring can help you identify vulnerability and compliance risks before they interrupt business operations or result in a breach.

1 Flexera. "Flexera 2022 State of the Cloud Report," March 2022.

2 IBM Security. "Cost of a Data Breach Report 2022," 2022.

Speed security and compliance operations

Red Hat Insights helps you accelerate security and compliance operations:

- ▶ **91%** less time to detect security vulnerabilities[3]

- ▶ **69%** less time to detect policy violations[3]

Learn more about managing security and compliance with Red Hat Enterprise Linux:

- ▶ Manage security risks with Red Hat Insights brief

- ▶ Resolving issues with Red Hat Insights demo

- ▶ Using OpenSCAP for security compliance and vulnerability scanning live demo

Included with Red Hat Enterprise Linux, Red Hat Insights is a suite of hosted services on the Hybrid Cloud Console that continuously analyze platforms and applications to help you better manage and optimize your hybrid cloud environments. Red Hat Insights uses predictive analytics and deep domain expertise to identify, assess, and recommend remediation for security and compliance risks, as well as other operational risks. It also helps you prioritize remediation actions based on the severity, type of risk, and impact of the change. Red Hat Insights works across on-site and cloud environments, allowing you to manage all of your Red Hat Enterprise Linux systems from a single interface. You can even link your Red Hat account to your cloud provider account to automatically connect your cloud-based systems and workloads to Red Hat Insights and other Red Hat services when you provision them.

Red Hat Insights includes services that help you protect hybrid and multicloud environments.

- ▶ **Vulnerability service:** Scan your systems for Common Vulnerabilities and Exposures (CVEs), collect scan information, and access remediation guidance using a single interface.

- ▶ **Malware service:** Identify systems that contain active malware signatures quickly to prevent long-term exposure.

Ensure compliance with built-in scanning and remediation

Noncompliance can result in fines, damage to your business, and loss of certification, in addition to security breaches. The average cost of a data breach for organizations with high levels of compliance failures was US$5.57 million in 2022.[2] High levels of compliance failures increased the cost of a data breach by US$258,293 on average in 2022.[2]

Red Hat Enterprise Linux is certified to key government and industry standards, allowing you to use it confidently in highly regulated environments. Red Hat Insights includes services that help you more easily maintain compliance in hybrid and multicloud environments.

- ▶ **Compliance service:** Audit compliance with OpenSCAP policies, remediate systems that are out of compliance, and generate reports for regulatory compliance and security audits. You can also tailor the default policies to your environment and operations to generate more accurate results. Key built-in baselines include:

  - ▶ Payment Card Industry Data Security Standard (PCI-DSS).

  - ▶ Enhanced Operating System Protection Profile (Common Criteria).

  - ▶ Australian Cyber Security Centre (ACSC) Essential Eight.

  - ▶ Center for Internet Security (CIS) Benchmark.

  - ▶ Health Insurance Portability and Accountability Act (HIPAA).

  - ▶ Defense Information Systems Agency Secure Technical Implementation Guidelines (DISA STIG).

- ▶ **Policies service:** Define custom security policies, monitor systems for compliance, and alert teams when a system is out of compliance.

---

3 Principled Technologies, sponsored by Red Hat. "Save administrator time and effort by activating Red Hat Insights to automate monitoring," September 2020.

Deploy consistent, hardened images across clouds with the image builder service

89% of organizations have a multicloud strategy in place today.[1] While a multicloud approach lets you choose the right cloud for each workload, it also creates complexity and increases your risk of inconsistencies that can lead to security and compliance issues.

The Red Hat Insights image builder service helps you create, manage, and deploy Red Hat Enterprise Linux operating system images across hybrid cloud environments more quickly and easily. You can build customized, security-hardened images, save them as templates, and push them to multiple cloud provider inventories to simplify provisioning. As a result, you can be sure that your systems are configured consistently across multiple clouds.

Verify system integrity across environments with remote attestation

Ensuring system integrity is essential in large-scale, highly distributed environments. Untrusted and compromised systems can leave your organization vulnerable to attack by malicious actors.

Red Hat Enterprise Linux includes remote attestation capabilities for verifying the state of systems at boot and continuously monitoring the integrity of remote systems. Based on the Keylime open source project, remote attestation uses embedded Trusted Platform Module (TPM) hardware and the Linux kernel Integrity Measurement Architecture (IMA) to monitor systems at scale. You can also send encrypted files to the monitored systems, and specify automated actions that are performed whenever a monitored system fails the integrity test.

Protect your data in the cloud with network bound disk encryption

Your data is a key asset for your business, and protecting it in the cloud is critical.

Red Hat Enterprise Linux includes support for network-bound disk encryption (NBDE) to simplify the protection of data at rest. NBDE automatically unlocks storage volumes via connections to one or more network servers. This allows you to decrypt volumes without manually managing encryption keys and ensures that volumes are only available when they are secured. Red Hat Enterprise Linux also supports NBDE via TPMs to ensure system integrity before unlocking encrypted volumes.

Implement zero trust architectures more easily with built-in identity and access management

Traditional perimeter-based security approaches cannot effectively protect new, widely distributed, cloud-based environments. Zero trust architectures can help by applying security to each asset, rather than exclusively at a network perimeter. In fact, implementing zero trust reduces the cost of data breaches by 20.5% on average.[2] Identity and access management is at the core of zero trust architectures.

Included with Red Hat Enterprise Linux, Red Hat Identity Management can help you centralize identity management, enforce security controls, and comply with security standards across your entire environment. It delivers the capabilities needed to implement zero trust best practices while simplifying your identity management infrastructure. Authenticate users and implement policy-based or role-based access controls (RBAC) via a single, scalable interface that spans your entire datacenter. Red Hat Identity Management integrates with Microsoft Active Directory, lightweight directory access protocol (LDAP), and other third-party solutions through standard interfaces. Red Hat Identity Management also supports certificate-based authentication and authorization techniques.

Build a foundation for zero trust in Linux environments

A zero trust architecture can help you better protect your IT environment and organization.

▶ Learn more about implementing zero trust with Red Hat Enterprise Linux.

▶ See a live demo of user management in Red Hat Enterprise Linux

Overview   Simplify security in the cloud

Manage security across releases in less time

Automation can help you reduce manual errors and manage your systems faster.

See a live demo of system roles in Red Hat Enterprise Linux

Streamline security configuration and management with system roles

As the size and complexity of your infrastructure grows, it becomes harder to manage manually. Cloud misconfigurations were the initial attack vector for 15% of data breaches, resulting in an average cost per breach of US$4.14 million in 2022.[2] Automation can help you configure and manage your systems faster, more consistently, and with less effort.

Red Hat Enterprise Linux system roles—powered by Red Hat Ansible® Automation Platform—use automation to help you install and manage security settings at scale in less time. System roles work with multiple Red Hat Enterprise Linux releases across infrastructure footprints, so you can configure new security settings and maintain them on all your systems with a single command or workflow.

Learn more

A consistent approach to security and compliance across hybrid and multicloud environments can help you better protect your organization. Red Hat Enterprise Linux gives you a security-focused foundation for running applications on any infrastructure footprint, in your datacenter, in the cloud, or at the edge.

Learn more about Red Hat's approach to hybrid cloud security.

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
@RedHat
linkedin.com/company/red-hat

redhat.com
275099_0323_KVM