Streamline your cloud security with Red Hat for AWS

Optimize for efficiency and consistency across hybrid cloud environments

Red Hat Enterprise Linux includes many optimizations to deliver reliable, security-focused performance in the cloud. It provides a consistent operating foundation for hybrid cloud 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, 77% of organizations cite security as a top cloud challenge.[1] This concern is with good reason—40% of breaches in 2023 occurred in the cloud.[2]

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. Using Red Hat® Enterprise Linux® for AWS as your standardized operating foundation with consistent security controls across your datacenter and Amazon Web Services (AWS) cloud environments helps you create the consistency needed to maintain a focus on security and compliance.

This operating system (OS) is deeply integrated with AWS products and services, preconfigured for performance with AWS-specific profiles, and overall, built for the highest quality experience running Red Hat Enterprise Linux on AWS infrastructure.

Additionally, with a ready-to-use solution and pretuned, ready-to-run OS images, your organization can start building faster with a plug-and-play approach using customizable settings that persist across all new images to help you save time on all provisioning.

Adopt a consistent foundation for security and compliance across environments

The combination of Red Hat Enterprise Linux and AWS delivers integrated, automated security capabilities throughout your infrastructure and software stack. Security is a major part of both the Red Hat Enterprise Linux and the AWS architectures lifecycles, with key capabilities that include:

- Built-in OS security features, security profiles, and compliance with industry and government regulations to safeguard your systems wherever you deploy them.
- Best practice-based default settings to configure your systems for increased focus on security from the start.
- Minimized package sets for prebuilt cloud images and immutable system images that reduce your cybersecurity threat attack surface.
- Image attestation and top-down memory encryption provided by Secure Boot, Confidential Compute, and Confidential Hypervisor that deliver a streamlined approach to deployment and enhanced focus on security from boot to runtime.

1 Flexera. "Flexera 2025 State of the Cloud Report." March 2025.

2 IBM. "Cost of a Data Breach Report 2025."

- Security upgrades and live patches provided as part of your Red Hat Enterprise Linux subscription.
- Security profiles that have been validated by Red Hat and AWS to run as expected on AWS infrastructure.
- Advanced security features and a large number of compliance certifications and accreditations provided by AWS.
- AWS policies, architecture, and operational processes built to the stringent requirements of security-sensitive organizations.
- Security advisories for current issues and assistance with resolving security problems when needed provided by both Red Hat and AWS.

Detect and remediate vulnerabilities at scale with predictive analytics and AI-powered guidance

The average time to identify and contain a data breach in 2023 was 258 days.[2] Consistent, daily monitoring can help you identify vulnerability and compliance risks before they interrupt business operations or result in a breach.

Included with Red Hat Enterprise Linux for AWS and delivered as a ready-to-use tool, Red Hat Lightspeed (formerly Red Hat Insights), provides AI-powered management and advanced security capabilities. Red Hat Lightspeed uses predictive analytics and deep domain expertise to identify, assess, and recommend remediation for security and compliance risks, along with other operational risks. It also helps you prioritize remediation actions based on the severity, type of risk, and impact of the change. Red Hat Lightspeed works across on-premise and cloud environments, allowing you to streamline management of all of your Red Hat Enterprise Linux systems from a single, ready-to-use interface. You can even link your Red Hat account to your AWS account to automatically connect your cloud-based systems and workloads to Red Hat Lightspeed and other Red Hat services when you provision them.

Red Hat Lightspeed includes services that help you protect hybrid cloud environments. The vulnerability service lets you scan your systems for Common Vulnerabilities and Exposures (CVEs), collect scan information, and access remediation guidance that is validated with AWS, using a single, streamlined management interface. And the malware service helps you identify on-premise and cloud-based systems that contain active malware signatures more quickly to mitigate long-term exposure.

Additionally, Red Hat Enterprise Linux for AWS provides access to Red Hat's decades of Linux expertise via Red Hat Lightspeed to help you manage increasingly complex IT environments and the growing difficulty of deploying new applications, scaling infrastructure, and managing lifecycles. This gen AI-powered service lets you use natural language prompts to get the information you need to streamline your business operations, anticipate and mitigate the risk of service disruptions, fix existing problems in less time, and more.

AWS also offers innovative security services and solutions that help you prevent, detect, respond, and remediate issues to improve your organization's security posture.

Enforce compliance with standards certification and built-in scanning and remediation

Noncompliance can result in fines, damage to your business, and loss of certification, in addition to security breaches.

Bolster security and compliance operations

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

- Read: Streamline security operations with Red Hat Lightspeed
- Demo: Resolving issues with Red Hat Lightspeed
- Live demo: Using OpenSCAP for security compliance and vulnerability scanning

Both Red Hat Enterprise Linux and AWS are certified to stringent government and industry standards, letting you use them confidently in highly regulated environments. For example, AWS regularly achieves third-party validation for thousands of global compliance requirements, including Payment Card Industry Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA), FedRAMP, General Data Protection Regulation (GDPR), and Federal Information Processing Standard Publication (FIPS) 140-2.

Additionally, Red Hat Lightspeed includes services that help you readily maintain compliance in hybrid cloud environments. The policies service lets you define custom security policies, monitor systems for compliance, and alert teams when a system is out of compliance, as well as 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 policy baselines include:

- PCI-DSS.
- Enhanced Operating System Protection Profile (Common Criteria).
- Australian Cyber Security Centre (ACSC) Essential Eight.
- Center for Internet Security (CIS) Benchmark.
- HIPAA.
- Defense Information Systems Agency Secure Technical Implementation Guidelines (DISA STIG).

Deploy consistent, hardened images across environments with image builder

72% of organizations have a hybrid cloud strategy in place today.[1] While this approach lets you choose the right infrastructure for each workload, it also creates complexity and increases your risk of inconsistencies that can lead to security and compliance issues.

Red Hat Lightspeed image builder helps you create, manage, and deploy Red Hat Enterprise Linux OS images, while optimizing for efficiency and consistency, across your hybrid cloud environment. You can build customized, security-hardened images, save them as templates, and push them to your AWS inventory to streamline provisioning. As a result, you can be sure that your systems are configured consistently across your datacenter and AWS environments.

As well, because image mode for Red Hat Enterprise Linux uses container-native tooling that allows your organization to deploy Red Hat Enterprise Linux as a bootc container image, you can streamline your cloud-native application development and IT operations into a single, consolidated pipeline.

Manage system integrity across environments with an integrated management interface and 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 for AWS helps you gain better visibility and control of both your AWS and Red Hat systems by allowing you to manage AWS services using a preset list of commands on an integrated, preconfigured AWS command line interface (CLI) directly from your Red Hat Enterprise Linux host.

Red Hat Enterprise Linux also 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 advanced encryption capabilities

Your data is a key asset for your business, and protecting it in the cloud is critical. Red Hat Enterprise Linux and AWS help you maintain privacy and safeguard your data. Red Hat Enterprise Linux includes support for network-bound disk encryption (NBDE) to reduce the complexity of the protection of data at rest. NBDE automatically unlocks storage volumes via connections to 1 or more network servers or TPMs. This allows you to decrypt volumes without manually managing encryption keys and enforces that volumes are only available when they are secured.

AWS provides detailed data management capabilities, allowing you to encrypt, move, and administer your data according to your organization's requirements in addition to regional and local data privacy laws. All data flowing across the AWS global network between AWS datacenters and regions is automatically encrypted at the physical layer. AWS also provides additional layers of encryption for all virtual private cloud (VPC) cross-region peering traffic, transport-layer security (TLS) connections, and more.

Implement zero trust architectures 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. Identity and access management is at the core of zero trust architectures.

Red Hat Enterprise Linux and AWS offer identity management tools and services to help you centralize identity management, enforce security controls, and comply with security standards across your entire environment. These tools and services deliver the capabilities needed to implement zero trust best practices while reducing the complexity of your identity management infrastructure. Authenticate users and implement policy-based or role-based access controls (RBAC). These tools and services integrate with Microsoft Active Directory, lightweight directory access protocol (LDAP), and other third-party solutions through standard interfaces. They also support certificate-based authentication and authorization techniques.

Streamline security configuration and management with automation

As the size and complexity of your infrastructure grows, it becomes harder to manage manually. Cloud misconfigurations were the initial attack vector for about 12% of data breaches, resulting in an average

Build a foundation for zero trust in Linux environments

A zero trust architecture can help you better safeguard 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.

cost per breach of US$3.98 million in 2023.[2] Automation can help you configure and manage your systems faster, more consistently, and using fewer resources.

Red Hat Enterprise Linux system roles can be used to manage your infrastructure but as your environment grows, complex and highly customizable automation capabilities outside of Red Hat Enterprise Linux will be required.

Red Hat Ansible® Automation Platform is the next step in your automation tooling to help you install and manage security settings at scale and with more efficiency. Ansible Automation Platform works with multiple Red Hat Enterprise Linux releases across datacenter and AWS cloud infrastructure, so you can configure new security settings and maintain them on all your systems with a single command or workflow. AWS also lets you automate manual security tasks to improve response times and mitigate risk due to human errors.

Learn more

A consistent approach to security and compliance across hybrid cloud environments can help you better protect your organization. Red Hat Enterprise Linux for AWS gives you a security-focused foundation for running applications with optimized efficiency and consistency across your datacenter and cloud environments.

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

Explore purchasing and deployment options for Red Hat Enterprise Linux for AWS available in the AWS Marketplace.

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

Copyright © 2025 Red Hat, Inc. Red Hat, the Red Hat logo, and Ansible are trademarks or registered trademarks of Red Hat, Inc. 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.