Simplify cloud security with Red Hat and Microsoft

Operate consistently across open hybrid cloud environments

Red Hat Enterprise Linux includes many optimizations to ensure reliable, security-focused performance on Microsoft Azure. 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.

Security in hybrid cloud environments 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—the global average cost of a data breach in 2024 was US$4.44M[2] and 23% of all breaches involved data in the public cloud.[2]

Consistency is at the core of security and compliance best practices in any environment. To protect your business-critical operations, you need the same level of security policy and access controls in your hybrid cloud environments that you have in your on-site datacenter. Standardizing on an operating foundation that provides consistent security controls across datacenter and cloud environments can help you improve security and compliance across your organization. Using Red Hat® Enterprise Linux® as your operating foundation across your on-site and Microsoft Azure environments helps you create the consistency necessary to maintain security and compliance. This overview describes key features and capabilities for adopting a consistent security approach across your datacenter and Microsoft Azure environments.

Red Hat Enterprise Linux for Microsoft Azure delivers consistent security capabilities

Red Hat and Microsoft build advanced security features into Red Hat Enterprise Linux and Microsoft Azure to make it simpler to maintain security and compliance across hybrid cloud environments. Our security response teams work together and in collaboration with customers, partners, and the global open source community to identify and resolve vulnerabilities.

Microsoft Azure includes multilayered security across physical datacenters, infrastructure, and operations, while built-in operating security features like kernel live patching, regular updates, security profiles, and a trusted software supply chain help you meet high security and compliance expectations. Default settings, based on best practices, are used to configure your systems for increased security from the start. Minimized package sets for prebuilt cloud images reduce your cybersecurity threat attack surface.

With Red Hat Enterprise Linux and Microsoft Azure, you can mitigate security risks, implement and maintain layered security, and streamline compliance across open hybrid cloud environments.

Detect and remediate vulnerabilities at scale with Red Hat Lightspeed

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 risks before they interrupt business operations or result in a breach.

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

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

2 *IBM Security. "Cost of a Data Breach Report 2025," 2025.*

Speed security and compliance operations

Red Hat Lightspeed helps you accelerate security and compliance operations:[3]

- **79%** less hands-on time to detect and remediate CVEs
- **28%** less hands-on time to detect and remediate compliance issues

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

- Resolving issues with Red Hat Lightspeed demo (requires log in)
- Using OpenSCAP for security compliance and vulnerability scanning demo (requires log in)

Red Hat Lightspeed boosts your Red Hat Enterprise Linux subscription with AI-powered management and advanced security capabilities. Get a clearer look into business, operations, and security risks to proactively identify and mitigate issues across your infrastructure— before they affect your bottom line. Red Hat Lightspeed (Formerly Red Hat Insights) works across on-site and cloud environments, letting you manage your Red Hat Enterprise Linux systems from a single interface. Link your Red Hat account to your Microsoft Azure account to connect your cloud-based systems and workloads to Red Hat Lightspeed automatically 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 using a single interface. And the malware service helps you identify on-site and cloud-based systems that contain active malware signatures quickly to prevent long-term exposure.

Within Microsoft Azure, you can turn on security management and threat protection for Red Hat Enterprise Linux as a default. These settings deliver built-in behavioral analytics and use machine learning to identify attacks and zero-day exploits. Additionally, Microsoft Azure monitors Red Hat virtual machine-related networks and cloud services for known attack patterns and post-breach activity.

Ensure compliance with built-in scanning and remediation

Both Red Hat Enterprise Linux and Microsoft Azure are certified to key government and industry standards, allowing you to use them confidently in highly regulated environments. For example, Microsoft Azure carries more than 100 compliance certifications.

Red Hat Lightspeed includes user-friendly services that help you 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. And the compliance service lets you 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:

- 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).

Microsoft Azure Policy allows you to create, assign, and manage policy definitions for control and governance. It scans your cloud resources and enforces policy-based rules and actions to ensure compliance with corporate standards and service-level agreements (SLAs).

3 *Principled Technologies, sponsored by Red Hat. "Save administrator time with the automated remediation capabilities of Red Hat Lightspeed." November 2025.*

Deploy hardened images across environments with the image builder service

70% 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 service helps you create, manage, and deploy Red Hat Enterprise Linux operating system images across hybrid cloud environments more efficiently and in less time. To simplify provisioning, you can build customized, security-hardened images, save them as templates, and push them to your Microsoft Azure inventory. As a result, you can be sure that your systems are configured consistently across your datacenter and Microsoft Azure environments.

Verify system integrity across environments with remote attestation

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

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

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 advanced encryption capabilities

Your data is a key asset for your business, and protecting it in the cloud is critical. Using industry-standard encryption protocols, Microsoft Azure safeguards your data as it travels to, from, and within Microsoft datacenters, as well as when it is at rest in Azure Storage. Red Hat Enterprise Linux also 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 with built-in identity and access management

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

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.

Red Hat Enterprise Linux and Microsoft Azure offer a variety of mechanisms to control access to your data and applications using the principle of least privileges. Enabled by default, the Security-Enhanced Linux (SELinux) mandatory access control (MAC) architecture in Red Hat Enterprise Linux enforces separation of information based on confidentiality and integrity requirements.

Red Hat Identity Management—included with Red Hat Enterprise Linux—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 full datacenter. Red Hat Identity Management integrates with Azure Active Directory (AAD), 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.

Multifactor authentication (MFA) in Microsoft Azure also simplifies and strengthens security with two-step, sign-in verification. Authentication via multiple methods—phone call, text message, or mobile application—helps protect data and applications and reduces the likelihood of access for a compromised credential.

Streamline security configuration and management with system roles

As the size and complexity of your infrastructure grows, it becomes more challenging to manage manually. Automation can help you configure and manage your systems, more efficiently, 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 each system with a single command or workflow.

Learn more

A consistent approach to security and compliance across hybrid cloud environments can help you better protect your organization. Together, Red Hat Enterprise Linux and Microsoft Azure give you a security-focused foundation for running applications in your datacenter and in the cloud.

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

redhat.com
#3134750_1225