OVERVIEW

BOOST CLOUD WORKLOAD SECURITY WITH RED HAT AND AWS

37%

of enterprises cite cloud as a top priority for technology investment in 2019.[1]

Red Hat and AWS provide hybrid environment solutions that deliver increased security for your cloud deployments.

CONNECTED ENVIRONMENTS INCREASE SECURITY RISKS

Businesses worldwide continue to add highly connected public cloud resources to their IT environments, with 37% citing cloud as a top priority for technology investment in 2019.[1] Cloud adoption has many benefits, including improved resilience, reduced cost of ownership, and greater infrastructure and business agility.

Even so, many organizations remain concerned about providing adequate security and privacy for applications and data in cloud environments. The Cloud Security Alliance (CSA) identified some of the top security threats to cloud computing as:[2]

- Data breaches.
- Misconfiguration and inadequate change control.
- Lack of cloud security architecture and strategy
- Insufficient identity, credential, and access management.
- Insecure interfaces and application programming interfaces (APIs).
- Limited cloud use visibility

Application and data protection in cloud environments depends on the underlying hardware and software. Choosing the right cloud infrastructure can alleviate security threats and help protect your applications and data. Together, Red Hat and Amazon Web Services (AWS) deliver hybrid environment solutions that effectively addresses these security concerns.

INCREASE CLOUD SECURITY WITH RED HAT AND AWS

Red Hat® Enterprise Linux® and AWS form powerful, adaptable platform for modern, cloud-based applications. With built-in security and management technologies, Red Hat Enterprise Linux offers a consistent, open source foundation across bare-metal, virtualized, container, and public and private cloud resources. As the most-deployed commercial Linux distribution in public cloud environments, it delivers performance and stability to cloud workloads.[3]

[1] Altimeter, *"The State of Digital Transformation: 2018-2019 edition,"* 2018.

[2] Cloud Security Alliance, *"Top Threats to Cloud Computing: The Egregious 11," August 2019.* cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven/.

[3] Red Hat, *"The state of Linux in the public cloud for enterprises," February 2018.* redhat.com/en/resources/state-of-linux-in-public-cloud-for-enterprises.

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

facebook.com/amazonwebservices
@awscloud
linkedin.com/company/amazon-web-services

redhat.com
aws.amazon.com

Through a globally distributed network of datacenters, AWS delivers cloud-based, security-focused, resizable compute capacity for workloads and applications. Each AWS subscription also includes advanced security features and more than 50 compliance certifications and accreditations.

Red Hat and AWS help your protect your cloud environment and manage threats. Comprehensive and effective best practices minimize the presence and limit the impact of vulnerabilities. A rich set of security-related features hardens and shields your most sensitive applications and data. Red Hat's integrated software stack allows you to implement a continuous security approach to safeguard your business and infrastructure from operating system to application. AWS policies, architecture, and operational processes are built to the stringent requirements of the most security-sensitive AWS customers. Red Hat and AWS also provide security advisories for current issues and can work with you to resolve security problems when needed.

This technology overview will detail how the combination of Red Hat Enterprise Linux and AWS alleviate top cloud security threats faced by enterprises today.

DATA BREACHES

Data breaches – the unauthorized or unlawful loss, alteration, destruction, disclosure, or acquisition of sensitive, protected, personal or confidential information – may be the result of a targeted attack, human error, application vulnerabilities, or poor security practices. If a data breach occurs, advanced encryption technologies in Red Hat Enterprise Linux and AWS help keep your data safe, both at rest and in motion, across your on-premise and cloud resources.

Red Hat Enterprise Linux includes a Federal Information Processing Standards (FIPS)-certified implementation of the Linux Unified Key Setup (LUKS) specification for full-disk encryption. This solution increases protection for cloud data at rest. The Network-Bound Disk Encryption (NBDE) feature decrypts LUKs encrypted boot or root volumes without manual intervention.

The Amazon S3 cloud storage platform allows you to apply access, log, and audit policies at the account and object level. S3 provides automatic server-side encryption, encryption with keys managed by the AWS Key Management Service (KMS), and encryption with keys that you manage. S3 encrypts data in transit when replicating across regions and lets you use separate accounts for source and destination regions to safeguard against malicious insider deletions.

Amazon Macie uses machine learning to automatically discover, classify, and protect sensitive data in AWS. It recognizes sensitive data like personally identifiable information (PII) and intellectual property and uses dashboards and alerts to provide visibility into how this data is accessed and moved. This fully managed service continuously monitors data access activity for anomalies and generates detailed alerts when it detects risk of unauthorized access or inadvertent data leaks.

MISCONFIGURATION AND INADEQUATE CHANGE CONTROL

Misconfiguration occurs when computing assets are set up incorrectly, often leaving them vulnerable to malicious activity. Some common examples include unsecured data storage elements or containers; excessive permissions; default credentials and configuration settings left unchanged; standard security controls disabled; unpatched systems with logging or monitoring disabled; and unrestricted access to ports and services. Misconfiguration of cloud resources is a leading cause of data breaches, may allow resources to be deleted or modified, and result in service interruption. Red Hat and AWS give you advanced configuration and change control tools to help you protect your data and business.

Red Hat Insights proactively scans and identifies threats to security, performance, availability, and stability. It also provides prioritized reports and remediation guidance for any issues found. Red Hat Insights is included with all active Red Hat Enterprise Linux 6.4 and higher subscriptions, including those running on AWS.

Red Hat Smart Management – comprised of Red Hat Satellite and cloud management services for Red Hat Enterprise Linux – helps you manage Red Hat systems to keep them running efficiently and provides visibility into the status of your security and compliance. You can choose to use an online, hosted interface, a traditional, on-premise tool, or both. Centralized consoles provide a consolidated location for accessing reports and for provisioning, configuring, and updating systems. Task automation streamlines operations, increases efficiency, and speeds response times.

Red Hat Ansible® Automation Platform allows you to simply create your systems for security. Human-readable syntax allows you to define security settings for any part of your system, including setting firewall rules, locking down users and groups, or applying custom security policies.

All three tools are integrated for better interoperability and efficiency. AWS configuration and management tools – including AWS Control Tower and Amazon GuardDuty – can also connect to Red Hat tools through APIs to provide configuration and compliance control across the software stack.

LACK OF CLOUD SECURITY ARCHITECTURE AND STRATEGY

Implementing a robust, consistent security architecture is critical when migrating to a cloud environment. However, this requires a shift away from traditional, on-premise strategies and a clear understanding of your cloud provider's shared security responsibility model. Red Hat and AWS provide detailed guidance for building security-focused hybrid cloud environments.

Red Hat Consulting offers expert assessment, planning, and deployment services for cloud environments. Red Hat Training delivers hands-on courses for your staff to learn about cloud security, best practices, and management skills. Additionally, the AWS Well-Architected Framework provides in-depth knowledge for reviewing and improving your cloud-based architectures and better understanding the business impact of your design decisions. It addresses general design principles and specific best practices and guidance in five conceptual areas, including security, operational excellence, reliability, performance efficiency, and cost optimization.

INSUFFICIENT IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT

Identity, credential, and access management – using techniques such as multi-factor authentication, strong passwords, and automated key, password, and certificate rotation – is the first line of defense in preventing data breaches and cyber attacks. Red Hat Enterprise Linux and AWS offer a variety of mechanisms to control access to your data and applications.

Enabled by default, Security-Enhanced Linux (SELinux) is a core component of Red Hat Enterprise Linux. The SELinux mandatory access control (MAC) architecture enforces separation of information based on confidentiality and integrity requirements. With the identity management feature set in Red Hat Enterprise Linux, you can centrally define, administer, and audit access control and single sign-on policies and privileges for users, machines, and services. Role-based access controls (RBAC) – provided in both Red Hat Enterprise Linux and AWS – assign specific permissions to users, groups, and applications to establish least privileges and maintain separation of duties between users with different roles.

Included in your AWS account, AWS Identity and Access Management (IAM) lets you manage access to AWS services and resources more securely. IAM lets you create and manage AWS users and groups and use permissions to allow and deny their access to AWS resources. You can also add specific conditions like time of day, originating IP address, SSL status, and multi-factor authentication to adjust how a user can use AWS. Finally, Amazon Cognito provides user sign-up, sign-in, and access control for your web and mobile applications.

INSECURE INTERFACES

In public cloud environments, customers manage and interact with cloud resources through software user interfaces (UIs) and APIs. Bad actors can potentially exploit these interfaces to circumvent cloud security policies. Red Hat and AWS design, build, and test UIs and APIs to defend against both accidental and malicious attempts to bypass security measures.

Red Hat Enterprise Linux implements open APIs that adhere to industry standards. Working with the open source community, Red Hat builds security features into the operating system core. Furthermore, every release of Red Hat Enterprise Linux undergoes extensive quality assurance testing to help prevent potential vulnerabilities.

AWS CloudTrail allows you to track and log use by API and user to ensure policies enforcement. Amazon GuardDuty also lets you audit API requests to prevent misuse. And AWS credential signatures are region-specific, blocking users from accessing resource APIs outside their region.

LIMITED CLOUD USE VISIBILITY

Limited visibility into how your users access cloud resources can lead to unsanctioned use and misuse of resources and applications. The ability to discern between valid and invalid users is essential. Red Hat and AWS help you track use to prevent and identify resource misuse.

Amazon GuardDuty continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads. The service uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats. You can easily turn on GuardDuty through the AWS Management Console and there is no software or hardware to deploy or maintain. AWS also helps you accurately predict your monthly bill amount, according to your use plans and setup, to help you identify unauthorized use.

Red Hat | aws

LEARN MORE

As organizations move critical applications and sensitive data to public cloud infrastructure, security concerns persist – and can even increase. Together, Red Hat and AWS mitigate threats to cloud workloads. Dedicated security teams, extensive testing, and well-established processes and best practices identify and remediate vulnerabilities. Modern, advanced security features and tools deter threats and safeguard applications and data. To discover how you can improve cloud-based application security, contact your Red Hat or AWS sales representative.

Read more about Red Hat and AWS solutions and security approaches:

- redhat.com/en/topics/security/cloud-security
- aws.amazon.com/security
- access.redhat.com/articles/2918071

ABOUT AMAZON WEB SERVICES

For almost 13 years, Amazon Web Services has been the world's most comprehensive and broadly adopted cloud platform. AWS offers over 165 fully featured services for compute, storage, databases, networking, analytics, robotics, machine learning and artificial intelligence (AI), Internet of Things (IoT), mobile, security, hybrid, virtual and augmented reality (VR and AR), media, and application development, deployment, and management from 61 Availability Zones (AZs) within 20 geographic regions, spanning the U.S., Australia, Brazil, Canada, China, France, Germany, India, Ireland, Japan, Korea, Singapore, Sweden, and the UK. Millions of customers including the fastest-growing startups, largest enterprises, and leading government agencies–trust AWS to power their infrastructure, become more agile, and lower costs.

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 integrate new and existing IT applications, develop cloud-native applications, standardize on our industry-leading operating system, and automate, secure, and manage complex environments. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500. As a strategic partner to cloud providers, system integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future.

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

facebook.com/amazonwebservices
@awscloud
linkedin.com/company/
amazon-web-services

redhat.com
aws.amazon.com