Data Security in the Hybrid Cloud

Uday Boppana
Senior Principal Product Manager

Mark Thacker
Principal Product Manager, Team Lead
Introductions

Mark Thacker
Principal Product Manager, Team Lead
mthacker@redhat.com

Uday Boppana
Senior Principal Product Manager
uboppana@redhat.com
Agenda

- Challenges
- Security across the data lifecycle and hybrid cloud
- Red Hat Solutions
Security across the data life cycle - Hybrid Cloud
Challenges

- “The cloud is just someone else’s datacenter”

  BUT

- Security is a big(ger) problem with more workflows and different cloud paradigms
  - Cannot outsource all security control to the cloud vendor
  - Lack of full control - In the hybrid cloud, every controllable constant of the traditional data center may now be a variable
  - How does this affect data at rest, in motion and in action?

- Must address CIA triad*
  - Confidentiality - who has access to the data
  - Integrity - is the data trustworthy and unmodified
  - Availability - is the data appropriately accessible when needed

#securitysymposium  
CIA Definition credit: [https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA](https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA)
DATA AT REST

Confidentiality
- Encrypted cloud block storage
  - Transparent, easy, obvious
  - Is access encrypted?
  - Who owns & where are the encryption keys?
- Encrypted cloud object storage
  - Introduces in-motion encryption requirements
- File / volume level access controls
  - Consistent with on-premise

Integrity
- File-level integrity checking
  - AIDE, Tripwire®-like tools
- Cryptographic verification
  - IMA hashes
  - Encryption verification
- Filesystem / volume integrity checks
  - Dmintegrity
  - Checksums, etc.
  - Object integrity
- Immutability / Read-only access
  - WORM

Availability
- Snapshots w/verification
- Backups
- Access controls
- RAID or HA redundancy
- Multi-region data availability
  - With storage mirroring
  - Or erasure encoding
Confidentiality

- Application level network encryption
  - TLS, SSL
  - Most common
- Encrypted tunnels
  - For legacy applications or ssh
  - Broad compatibility
- Network segmentation
  - To eliminate exposures

Integrity

- Encryption verification
  - Cryptographic hashes required to match for de-encryption to function
- Network traffic checksums
- Application-level verification
  - Database integrity checking
  - Erasure encoding for distributed data

Availability

- Redundant networking access
  - Physical network failover
  - Virtual networking duplication
- Application redundancy
  - With consistent access controls
  - Databases, object stores, etc.

#securitysymposium
DATA IN ACTION

Confidentiality
- Execution isolation
  - Resource controls
  - Security labels
  - CPU-core affinity
  - Pod / cluster affinity
- Memory encryption
  - Relatively new
  - Platform / system level
- Confidential Computing
  - Trusted Execution Environments (TEE)

Integrity
- Physical memory integrity verification
  - Checksums,
  - Error Correction Code
- Application level verification
- Cryptographic verification when memory is encrypted

Availability
- Clustering w/failover
- Containers for higher availability
- Multi-region availability
Hybrid cloud security: Layered defense in-depth
Red Hat Enterprise Linux Solutions

For Small / Medium institutions

- Use RHEL with NFS and/or Samba for file sharing
  - Uses Kerberos for authentication / authorization
  - Implements access controls use ACLs and SELinux labels
- Encrypt data at rest with LUKS and manage with NBDE
  - Provides consistent encryption on-premise or in cloud environments
  - Manage LUKS keys using Network Bound Disk Encryption
- Encrypt traffic using IPSec or TLS and leverage FIPS-validated cryptography

For Enterprises

- Increase data availability with High Availability clustering and Resilient Storage
- Authenticate and manage digital certificates with Identity Manager
- Verify data integrity using AIDE and Application Allowlisting (fapolicyd)

Red Hat Enterprise Linux Security Hardening guide

Red Hat Cloud Storage and Data Services

For Small / Medium institutions

- CephX authentication between client and storage system and users and daemons
- Defaults to separate networks for cluster and user traffic
- Uses FIPS validated cryptographic modules when running on RHEL
- Support for encryption of data on the disk using LUKS encryption of data on OSDs

For Enterprises

- Full spectrum of data at rest encryption and user authentication options
  - User provided keys, Vault and KMIP support, Server managed encryption and LDAP support
  - OpenStack encryption key management support with Barbican integration
- S3 Object lock API support for WORM capabilities
- Encryption support for of inter-cluster traffic with Ceph messenger V2
- OpenShift PV and cluster wide encryption with KMIP support in ODF

Red Hat storage data security and hardening guide:
Red Hat Hybrid Cloud Solutions

Red Hat Ceph Storage and OpenShift Data foundation

- AWS S3 compliant API for application portability
- Time based credential and data set sharing with AWS STS support with Ceph object gateway (RGW)
- Multi cloud API, security, encryption and data federation support from single access API access point with Multi Cloud Gateway (MCG - NooBaa)

Red Hat Enterprise Linux

- Separate workloads via VMs or Containers
  - Leverages SELinux labeling, cGroups & processor affinity
- Encrypt data at rest with LUKS and manage with NBDE
  - Manage cloud encryption keys from on-premise devices
- Encrypt inner-cluster traffic with TLS
- Leverage HA and Resilient storage for critical applications
Resources

Red Hat product security
secalert@redhat.com

Customer Portal
access.redhat.com/security

Red Hat Enterprise Linux hands-on lab
lab.redhat.com

Red Hat Enterprise Linux 8
redhat.com/rhel

Red Hat Ceph Storage
redhat.com/ceph
Thank you

Red Hat is the world’s leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.