Boost hybrid cloud security

Protect your business with cloud-native security approaches

By Lucy Huh Kerner, Senior Principal Security Global Technical Evangelist and Strategist, Red Hat

See what's inside

Deploy a security-focused hybrid cloud

Today, 94% of organizations use some type of cloud, and 58% of enterprises have a hybrid cloud strategy.[1] Hybrid cloud is an IT architecture that incorporates some degree of workload portability, orchestration, and management across two or more connected but separate environments, including bare metal, virtualized, private cloud, and public cloud. With a hybrid cloud architecture, you can run workloads in any of the connected environments, move them between environments, and use resources from those environments interchangeably.

Organizations adopt hybrid cloud environments to:

- Connect infrastructure, platforms, applications, and tools from different vendors.
- Increase efficiency and scalability.
- Reduce costs.
- Increase agility.
- Optimize data placement.

No matter where you are in your hybrid cloud journey, security is a big concern. In fact, 81% of enterprises cite cloud security as a challenge.[1] Hybrid cloud security vulnerabilities typically take the form of loss of resource oversight and control, including unsanctioned public cloud use, lack of visibility into resources, inadequate change control, poor configuration management, and ineffective access controls. Unauthorized users can take advantage of these gaps to gain access to sensitive data and internal resources.

Security breaches can be costly. The average cost of a data breach is US$3.92 million, with lost business accounting for 36.2% of this cost.[2] And threats are growing. The likelihood of experiencing a breach within two years is 29.6%.[2] Both the average number of data records and the time to identify and contain breaches increased in 2019.[2]

Even faced with these challenges, you can deploy a **security-focused hybrid cloud** by adapting your methods to account for the differences between on-premise and cloud architecture. This e-book discusses new approaches and considerations for protecting your business in the hybrid cloud.

Impacts of ineffective security

Security breaches are costly and threats are growing.

US$3.92 million
average cost of a data breach in 2019.[2]

279 days
average time to identify and contain a data breach in 2019.[2]

US$1.22 million
savings in costs if a breach can be identified and contained in
200 days
or less.[2]

29.6%
likelihood of experiencing a breach within two years.[2]

[1] Flexera, *"RightScale 2019 State of the Cloud Report from Flexera,"* February 2019. info.flexerasoftware.com/SLO-WP-State-of-the-Cloud-2019.

[2] IBM Security, *"2019 Cost of a Data Breach Report,"* 2019. ibm.com/security/data-breach.

Security is a process, not a product

Effective security requires a holistic approach that incorporates people, processes, and technology. Simply deploying security-focused products and tools is not enough to protect your infrastructure, cloud, or business. You must also implement security strategies and processes to use your products' capabilities to effectively mitigate security risks. And these strategies and processes must be adapted over time as technologies, threats, and needs evolve.

Hybrid cloud environments require you to shift your security approaches. Because they do not have a defined perimeter, traditional, perimeter-based security approaches are not effective. Centralized identity management and access control is key for cloud-centric security approaches. Effective centralized identity management and access control uses the principle of least privilege to provide users with only the access they actually need. This approach requires auditing the current access rights for each user, then reassessing each user to determine the right level of access.

Hybrid cloud security also requires a layered, defense-in-depth security strategy that uses the capabilities of each layer in your environment, including operating systems, container platforms, automation tools, Software-as-a-Service (SaaS) assets, and cloud services.

Operating system

Look for built-in tools that help you ensure security compliance, implement physical security, improve network security, control user access, isolate processes, and increase data security. Examples include OpenSCAP, USBGuard, firewalls, Security-Enhanced Linux® (SELinux), identity management, and Network Bound Disk Encryption.

Container platform

Use built-in capabilities within your platform and Kubernetes to increase container security. Examples include pod security policies, network traffic controls, cluster ingress and egress controls, role-based access controls (RBACs), integrated certificate management, and network microsegmentation.

Automation tools

Choose an automation language that everyone across your organization – including development, operations, security, and compliance teams – can easily learn and use. Look for access control, logging, and auditing capabilities. See page 4 for more information about automation.

Finally, you should revisit your existing security processes and tools. Ensure you are using all available features and determine if any settings can be modified or reconfigured to provide better protection, or if new processes and tools are needed.

1. Create an inventory of your current IT assets and tools.
2. Document your existing security and network architectures, cybersecurity policies, work processes, and skills and talent gaps.
3. Establish a threat model and determine your risk tolerance and mitigation strategies for cybersecurity breaches.
4. Assess your architectures, policies, and processes to identify areas for change.
5. Assess your current tools and assets to determine if they can support your updated strategies and processes. Document and plan how to address any security gaps.

The following sections discuss key considerations for hybrid cloud security and provide tips for improving your protection.

SECURITY CONSIDERATION

Collaboration

Why is it important?

Compartmentalized security approaches often result in security gaps and duplicated efforts, as security becomes an afterthought in application development and infrastructure deployment. As development speed and deployment flexibility increases, it becomes increasingly important to consider security earlier in the process. Applying effective security only at the end of development cycles takes considerably more time, which can result in delivery delays and encourage teams to skimp on security.

Recommendations and best practices

Unify security across your organization using a **DevSecOps** approach. DevSecOps is a collaborative framework in which security becomes a shared responsibility that is integrated from beginning to end. It extends security across teams, rather than having a single, disconnected team responsible for setting security policy. Staff from security, development, and operations teams work together, sharing visibility, feedback, lessons learned, and insights. This approach allows security to be built at the start of application development and infrastructure deployment, increasing protection.

Formal training programs help everyone understand the importance of security and how they can help safeguard your organization. These programs should address topics like:

- Maintaining application and resource compliance with security policies and regulations.
- Establishing different approaches to security for traditional, containerized, and hybrid cloud environments.
- Creating a patching strategy that helps you stay current with new and existing security vulnerabilities.

Executive endorsement is also important. Executives should encourage collaboration and be open to feedback from teams across their organization.

Tactical steps

Try these actions to increase collaboration within your organization.

Start small and grow.

Choose a single project to begin. Encourage experimentation and iterative, continuous improvement to tune and optimize your process. Celebrate successes and showcase proven value to others within your organization.

Set clear, agreed-upon goals and timelines.

Transparency is key for DevSecOps. Ensure that everyone involved understands and agrees with the goals and timelines for the project.

Cross-train your staff.

Establish learning paths about security, infrastructure, and development that are regularly updated and readily available for all team members.

Create a security workgroup.

Build an integrated, cross-discipline team to define security use cases and strategies.

Learn from others.

Take advantage of findings from other organizations like the United States **Internal Revenue Service** and **Department of Homeland Security**.

SECURITY CONSIDERATION

Automation

Why is it important?

Misconfigurations and inadequate change control are a top threat to security.[3] Misconfigurations can leave systems vulnerable to attack. Change control is critical for understanding who modified configurations, when, and what was changed throughout system life cycles. Automation can help you streamline daily operations as well as integrate security into processes, applications, and infrastructure from the start. In fact, fully deploying security automation can reduce the average cost of a breach by 95%, but only 16% of organizations have done so.[4]

Recommendations and best practices

Implement a unified automation strategy to reduce the risk of misconfigurations and manual errors across your organization. Automation streamlines and increases the consistency of infrastructure management, application development, and security operations to improve protection, compliance, and change control.

- Consistently configure resources according to pre-approved policies and proactively maintain them in a repeatable fashion over their life cycle.
- Rapidly identify systems that require patches or reconfiguration.
- More easily apply patches or change system settings according to defined baselines – in a consistent manner across a large number of systems.
- Ease auditing and troubleshooting with automatically recorded action logs.

Implementing identity management and access controls for your automation platform and processes helps to ensure that only authorized staff can execute automation tasks.

Choose an automation platform that everyone in your organization can use. A platform that implements a common, easy-to-learn automation language can improve:

- **Visibility.** Everyone can understand what each automated task does.
- **Repeatability.** An accessible platform and language allows all approved staff to use automation effectively and efficiently.
- **Collaboration.** Automation tasks can be shared across your organization, allowing other teams to take advantage of work done and avoid duplicate efforts.
- **Auditing.** Multiple staff can verify automation tasks and view logs for auditing.

Tactical steps

Try these actions to get started with security automation.

Start with a single project.

Don't try to automate everything at once. Choose a single project or limited set of tasks to start.

Choose repetitive tasks.

Automate tasks that are performed repetitively, including configuration management, software package and patch management, security vulnerability identification and remediation, and policy enforcement.

Measure, adapt, and repeat.

Work iteratively to deploy automation, measure results, and adapt accordingly.

Plan for expansion.

Ensure that all automation is verifiable, auditable, and shareable so that others within your organization can take advantage of gains.

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

[4] *IBM Security, "2019 Cost of a Data Breach Report," 2019.* ibm.com/security/data-breach.

SECURITY CONSIDERATION

Updates and patches

Why is it important?

Unpatched and out-of-date systems can be a source of compliance issues and security vulnerabilities. In fact, most vulnerabilities exploited are ones already known by security and IT teams when a breach occurs.

Recommendations and best practices

Patch often and test your patches to ensure they are applied correctly. Scan systems daily for compliance issues and security vulnerabilities that require patching. Prioritize actions to correct items found according to your threat model, as well as risk, performance, and time considerations. Patch all applicable systems on a regular basis to keep pace with important issues. Apply patches for critical issues and known vulnerabilities as soon as possible. Test patched systems for functionality before placing them back into production.

You should also update your patching strategy to account for cloud and containerized resources, which are deployed from base images. Ensure that base images are compliant with your organization's security baselines. As with physical and virtualized systems, scan and patch your base images regularly. When you patch a base image, rebuild and redeploy all containers and cloud resources based on that image.

Finally, apply automation to streamline patching operations. Create an automation workflow for patching to speed operations, reduce the risk of errors, and improve consistency across systems. For example, you can use a Jenkins-based continuous integration/continuous deployment (CI/CD) pipeline for both applications and infrastructure to automate life-cycle processes like patching.

Tactical steps

Follow these steps to create a stronger patching and update strategy.

1. Identify systems that need patching.
2. Prioritize actions based on your threat model, anticipated risk, performance impacts, and available patching windows.
3. Automate patch application to improve consistency and repeatability for both traditional and hybrid cloud infrastructure.
4. Periodically reassess and adapt your patching strategy to keep pace with evolving capabilities, technologies, and threats.

SECURITY CONSIDERATION

Open source technologies

Why is it important?

Open source technologies are integral to cloud and container operations, but they can be a source of security vulnerabilities if your organization uses unsigned software or deploys these technologies in an insecure manner. Using unvetted open source software directly from upstream communities can leave you open to security vulnerabilities and supply chain attacks, which exploit weaknesses in third-party services and software to compromise a final target. These attacks take many forms, including hijacking software updates and injecting malicious code into legitimate software. And supply chain attacks increased by 78% in 2018.[5]

Recommendations and best practices

Be sure you understand who distributes the open source technologies you use and deploy those technologies in a secure manner. First, take an inventory of the open source technologies currently used in your organization. Stop using any that are not obtained from known, trusted sources. Define processes and policies to bring the remaining technologies back under the control of IT and security teams.

You should also create a strategy for security-focused use of open source technologies. Your strategy should include measures to ensure that your open source technologies come from reliable sources, are continuously patched in an automated fashion, and configured with security in mind. Additionally, you should encourage the use of enterprise-grade open source offerings that include enterprise support throughout their entire life cycle.

⚠ **78%** more supply chain attacks occurred in 2018 than the previous year.[5]

Tactical steps

Try these actions to improve the security of the open source technologies you use.

Switch to commercially available versions.

Migrate open source software that you use directly from upstream open source projects to trusted, **commercially available versions**. These versions are tested and validated to reduce the risk of bugs and security vulnerabilities. They may also include enterprise support that can quickly deliver security patches and provide guidance on configuring your software for security.

Read more about securing open source technologies in **this article**.

Deploy open source software based on templates.

Check your management and platform tools to see if they offer self-service provisioning based on predefined, vetted templates. You can use templates to ensure that only trusted, up-to-date open source technologies are deployed. Fast, automated deployment also encourages users to employ authorized IT resources, rather than deploying resources outside the control of the IT and security teams.

[5] *Symantec, "Internet Security Threat Report, Volume 24," February 2019.*

Ready to get started?

Hybrid cloud security is an important concern for all organizations. No matter where you are in your hybrid cloud journey, Red Hat can help you deploy a security-focused hybrid cloud. With integrated, built-in security capabilities, Red Hat's portfolio of production-grade open source software gives you the tools and platforms to overcome current and future security and compliance challenges. Red Hat also delivers enterprise-grade support, hands-on training, and expert services to help you build and operate your hybrid cloud environment more efficiently and securely.

Read these resources to learn more about Red Hat's approach to security and compliance.

- **Overview of hybrid cloud security**
- **Why choose Red Hat for continuous IT security**
- **Why automate security and compliance**
- **Red Hat® Services: Automate System Security and Compliance**

Schedule a complimentary discovery session:
redhat.com/consulting

About Lucy Huh Kerner, Senior Principal Security Global Technical Evangelist and Strategist, Red Hat

Lucy Huh Kerner helps develop security thought leadership and leads the technical and go-to-market strategy for security across the entire Red Hat portfolio globally. In addition, she helps create and deliver security-related technical content to the field, customers, partners, analysts, and press and has spoken at numerous events. Prior to this role, she was a Senior Cloud Solutions Architect for the North America Public Sector team at Red Hat. With her domain expertise in cloud technologies, she supported the Red Hat cloud sales efforts by designing and presenting Red Hat cloud solutions for a wide range of North America Public Sector customers. Lucy has more than 15 years of professional experience as both a software and hardware development engineer and a presales solutions architect, where she worked on various aspects of cybersecurity.