Boost hybrid cloud security

Protect your business with essential cloud-native security considerations

/Keep your options open

Red Hat

By Lucy Huh Kerner, Director, Security Global Strategy and Evangelism, Red Hat

See what's inside

Chapter 1

Deploy a security-focused hybrid cloud

Cloud adoption continues to grow in use and popularity. Today, 65% of organizations say they are heavy cloud users, and 72% 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 2 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 connected environment, moving and using resources from those environments interchangeably.

Organizations adopt hybrid cloud environments to:

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

[1] Flexera, "2023 State of the Cloud Report," March 2023.

Security is a primary concern no matter where you are in your hybrid cloud journey, with 79% of enterprises citing cloud security as a challenge.[1] Hybrid cloud security vulnerabilities typically result from loss of resource oversight and control, including unsanctioned public cloud use, lack of visibility into resources, inadequate change control, poor configuration management, ineffective access controls, human error, and more. Unauthorized users can take advantage of these gaps to gain access to sensitive data and internal resources, which can be costly.

The average global cost of a data breach reached a new high of US **$4.45 million** in 2023, with lost business accounting for **29.2%** of this cost.[2]

51%

of companies say they plan to increase security investments as a result of a breach.[2]

[1] Flexera, "2023 State of the Cloud Report," March 2023.
[2] IBM Security, "Cost of a Data Breach Report 2023," 2023.

Both the average cost per record involved in a data breach and the time required to contain breaches increased in 2023.[2] By adapting your methods to account for the differences between on-premise and cloud architecture, you can deploy a security-focused hybrid cloud to help overcome these mounting challenges. This e-book discusses new approaches and considerations for hybrid cloud security.

277 days

average time to identify and contain a data breach in 2023.[2]

US $1.02 million

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

[2] IBM Security, "Cost of a Data Breach Report 2023," 2023.

Chapter 2

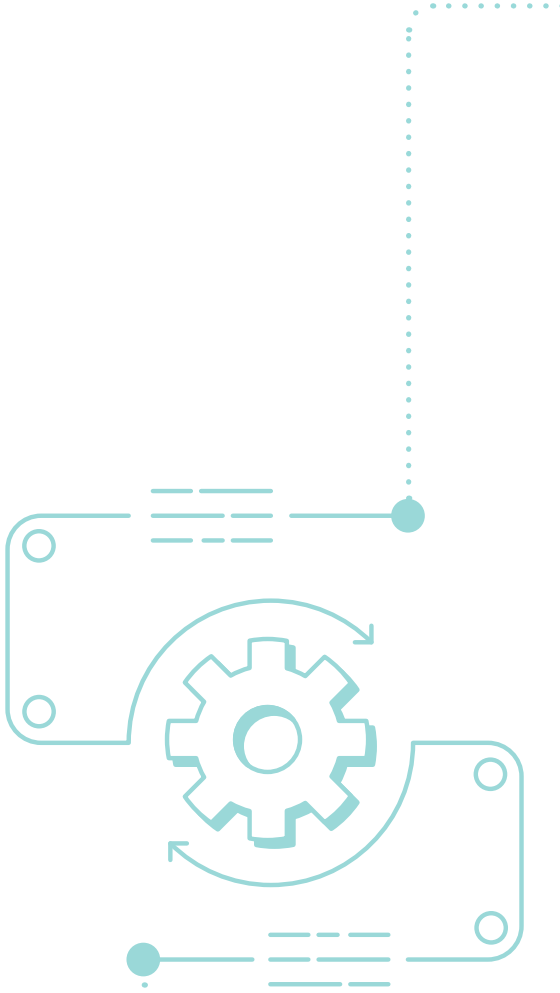
Security is a process, not a product

Effective security requires a holistic approach incorporating people, processes, and technology. Simply deploying security-focused products and tools is not enough to protect your infrastructure, cloud, or business. You should also consider security strategies and processes to maximize the capabilities of your products and mitigate risks.

These strategies and processes can be adapted over time as technologies, threats, and needs evolve. Hybrid cloud environments require you to shift your security approaches, and because they do not have a defined perimeter, traditional security approaches are ineffective.

Centralized identity management and access control is key for cloud-centric security approaches. It uses the principle of least privilege to provide users with only the access they need. This approach requires auditing the current access rights for each user, and then reassessing them to determine the appropriate 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, and automation tools.



Operating system

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

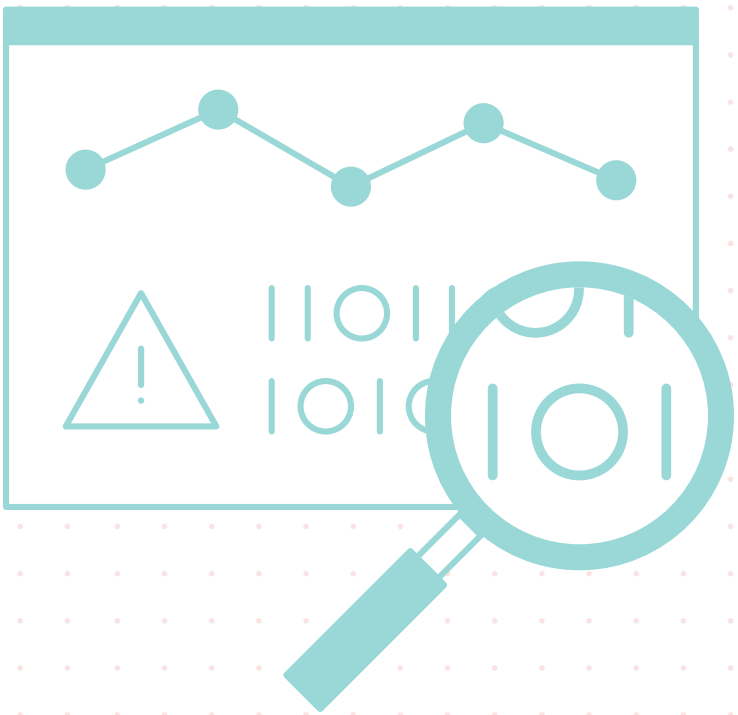
Container platform

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 and platform that everyone across your organization—including development, IT operations, security, and compliance teams—can easily learn and use. Look for access control, logging, and auditing capabilities.

It is also important to 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.

Chapter 3

Security consideration 1

Start with a strong foundation

Why is it important?

When your workloads are spread across multiple environments or when unvetted open source technologies are used in your environment, it can be challenging to identify where vulnerabilities are located. In addition, it will be hard to reduce risk with multilayered security without a strong security foundation. Using open source software directly from upstream communities can leave you open to security risks and supply chain attacks, which exploit weaknesses in 3rd-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–there has been a 742% average annual increase in software supply chain attacks over the past 3 years.[3] This is why building on a unified, stable, security-focused foundation is critical for protecting your business.

Recommendations and best practices

Reduce software supply chain security risks by using open source software from a trusted enterprise open source vendor that provides enterprise support throughout the entire life cycle of their software, such as Red Hat. An enterprise open source vendor develops their software with a robust software supply chain security process that includes curating open source software on behalf of their customers. This ensures that the open source software that customers use is trustworthy, resilient, and safe for consumption.

In addition, it's important to run critical applications on top of a platform with built-in security capabilities. This will provide the foundational security from which customers can reliably run critical applications, include multilayered security capabilities to reduce risk, and implement security and compliance automation.

Prioritize a security-focused foundation for applications and processes by adopting a resilient, trusted operating system hardened for stability and security such as Red Hat® Enterprise Linux®. This provides a stable foundation from which you can reliably scale critical applications, maintain security compliance, and roll out emerging technologies consistently across bare-metal, virtual, container, and all types of cloud environments.

[3] Sonatype. "9th Annual State of the Software Supply Chain," 2023.

Red Hat Enterprise Linux is the foundation for much of the Red Hat portfolio and is the trusted operating system for many enterprises due to the built-in security capabilities it delivers.

With Red Hat Enterprise Linux, you can:

Mitigate the risk of exposing data or systems with built-in security capabilities such as live kernel patching. This allows applying security patches without the need to reboot or interrupt runtime. In addition, other built-in security capabilities include application allowlisting, which is the practice of specifying an index of approved applications or executable files that are permitted to run on a system by a specific user, SELinux to apply fine-grained level of control over files, processes, users, apps, and more.

Automate data protection at scale and maintain them over time with built-in security capabilities such as Network Bound Disk Encryption, which allows you to automate the unlocking of encrypted systems without managing encryption keys. In addition, with system-wide cryptography policies, you can focus on keeping data secure and address compliance with system-wide consistent and customizable cryptography settings to meet your site-specific policy requirements, and more.

Meet compliance requirements and streamline audits. Red Hat Enterprise Linux has built-in compliance scanning and remediation with OpenSCAP to perform configuration and vulnerability scans on a local system to validate compliance to a wide variety of industry security standards.

With the foundational security approach provided by Red Hat Enterprise Linux, the layered products that run on top, such as **Red Hat OpenShift**, offer defense in depth for containers and Kubernetes. Red Hat extends security capabilities up the stack to Kubernetes components. Similarly, with its built-in security capabilities, **Red Hat Ansible Automation Platform** allows enterprises to implement security and compliance automation at scale.

Tactical steps

Take these actions when getting started with hybrid cloud security:

Switch to commercially available versions

Migrate your open source software 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. By adopting open source software from a trusted enterprise open source vendor, you can ensure that their software is developed with a robust software supply chain security process and enterprise support is provided throughout the entire life cycle of their software. All of this allows enterprises to consume open source software while minimizing security risks.

Choose a platform with built-in security features

It's important to choose a platform (such as an OS, container application platform, and automation platform) with built-in security capabilities. This will provide the foundational security from which customers can reliably run critical applications, include multilayered security capabilities to reduce risk, and implement security and compliance automation at scale.

Implement security throughout your technology stack

Once you've established a foundational base for security, ensure that the layered technologies running on top of that foundation inherit the security benefits and work in tandem for multilayer security.

Chapter 4

Security consideration 2

Implement a trusted software supply chain with DevSecOps

Why is it important?

In 2023, 12% of data breaches originated from a software supply chain attack.[2] Using unvetted open source software directly from upstream communities can leave you open to security vulnerabilities and supply chain attacks, which exploit weaknesses in 3rd-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.

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 increase, it becomes more important to consider security throughout the entire process.

Recommendations and best practices

In order to adopt a security-focused approach to your software supply chain, the initial step is developing a DevSecOps mindset. A DevSecOps mindset sees Application Developers, IT Operations, and Security teams all working collaboratively to implement software supply chain security across the software development life cycle (SDLC) and infrastructure life cycle, built over an enterprise-hardened open source foundation across a hybrid cloud.

[2] IBM Security, "Cost of a Data Breach Report 2023," 2023.

DevSecOps automates the integration of security at every phase of the software development life cycle, from initial design through integration, testing, deployment, and software delivery.

Benefits of adopting a DevSecOps process include:

- Helping IT and security teams tackle challenges across people, processes, and technologies.
- Allowing for improved efficiency, consistency, repeatability, and collaboration.
- Reducing human error, which ultimately reduces risk.

With DevSecOps, security becomes a shared responsibility that is integrated from beginning to end. Rather than having a single, disconnected team be solely 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 processes to be built at the start of application development and infrastructure deployment, increasing protection.

Enterprise application developers who build new software capabilities for their organizations need to dramatically increase their security posture as well as reduce their cognitive load. Security needs to be implemented across the SDLC, at code time through integrated application security checks to catch issues early in the SDLC and reduce prolonged downtimes, at build time by safeguarding build systems using security-focused continuous integration and continuous delivery (CI/CD) workflows, and at deployment time and run time with golden path templates, vulnerability analysis, artifact signatures, attestations, provenance, policy enforcement points and software bill of materials (SBOMs).

It's also necessary to create a strategy to ensure that the open source technologies being used by your teams come from reliable sources, are continuously patched in an automated fashion, and are configured with security in mind. Additionally, you should encourage using enterprise-grade open source offerings that include enterprise support throughout their entire life cycle.

By using enterprise-grade open source offerings, such as those offered by Red Hat, you can take advantage of the over 30 years of experience Red Hat has in securing the open source software supply chain of their products. In addition, enterprises need solutions to help them deploy, manage, and secure their fleet of Kubernetes clusters and a unified way to build, modernize, and deploy applications securely at scale.

Red Hat OpenShift Platform Plus is a unified platform that includes Red Hat OpenShift, Red Hat Advanced Cluster Security for Kubernetes, Red Hat Advanced Cluster Management for Kubernetes, Red Hat Quay, and Red Hat OpenShift Data Foundation. This platform helps enterprises build, modernize, and deploy containerized applications in Kubernetes securely and at scale. Multicluster security, compliance, application and data management are provided for consistency throughout the software supply chain.

Tactical steps

Try these actions when implementing DevSecOps and software supply chain security improvements:

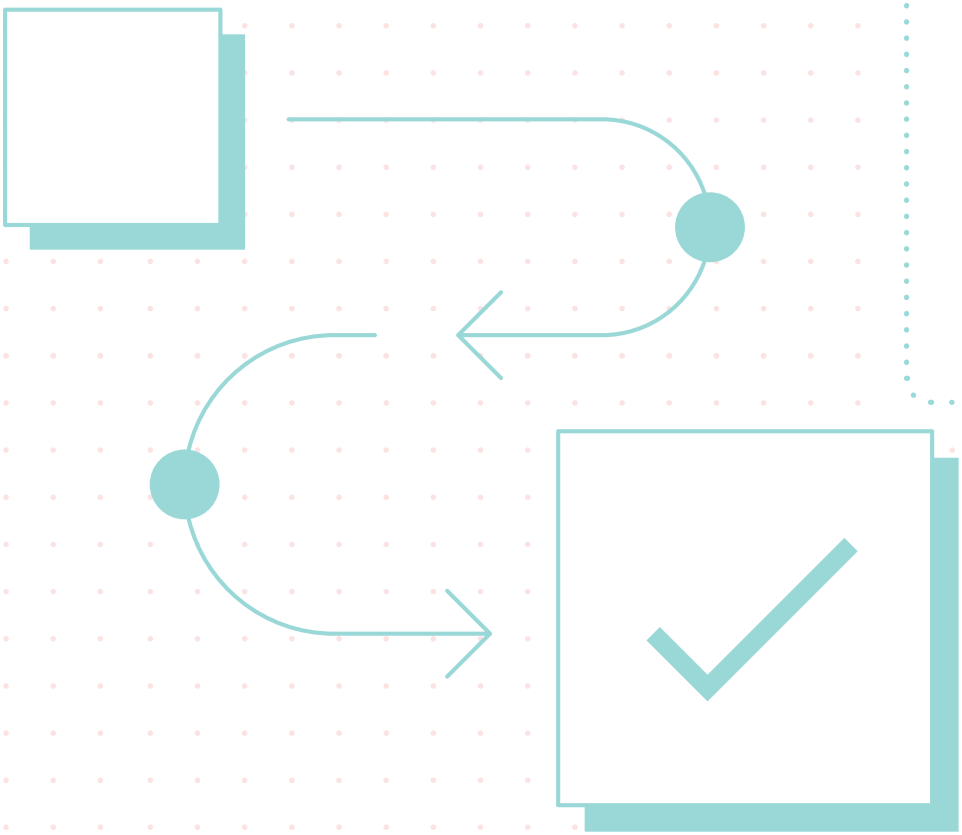
Start small and expand.
Choose a single project to begin. Encourage experimentation and iterative, continuous improvement to fine-tune and optimize your process. Celebrate successes and showcase proven value to others within your organization.

Set clear, agreed-upon goals and timelines.
Transparency is key. 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 to all team members.

Create a security work group.
Build an integrated, cross-discipline team to define security use cases and strategies. Learn from others. Take advantage of findings from other organizations.

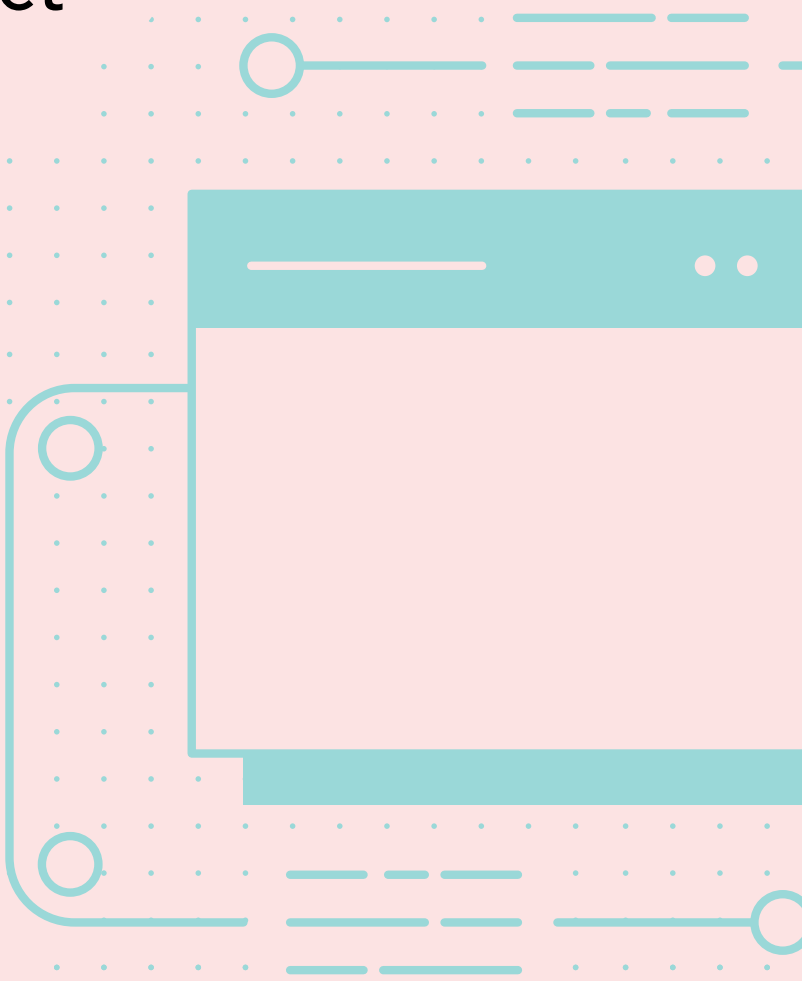
Implement security across the SDLC with a unified application platform.
Security needs to be implemented across the SDLC, at code time through integrated application security checks to catch issues early in the SDLC and reduce prolonged downtimes, at build time by safeguarding build systems using security-focused continuous integration and continuous delivery (CI/CD) workflows, and at deployment time and run time with golden path templates, vulnerability analysis, artifact signatures, attestations, provenance, policy enforcement points and software bill of materials (SBOMs).



Chapter 5

Security consideration 3

Use automation and management to protect your hybrid cloud



Why is it important?

Misconfigurations and inadequate change control are top threats to security.[4] 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, management, and AI can help you streamline daily operations as well as integrate security into processes, applications, and infrastructure from the start. Having an automation and management strategy across your organization can help reduce human error and provide speed, consistency, repeatability, and the ability to verify and audit. In addition, a centralized automation and management strategy helps improve security and compliance by helping enterprises to integrate security into application development and IT operations from the start and throughout the life cycle. This allows them to implement DevSecOps successfully. In fact, incorporating extensive automation, management, and AI into security processes can reduce the average cost of a breach by an average of 39.3%, but only 28% of organizations have done so.[2]

[2] IBM Security, "Cost of a Data Breach Report 2023," 2023.

[4] Cloud Security Alliance, "Top Threats to Cloud Computing: Pandemic 11 Deep Dive," October 2023.

Recommendations and best practices

Implement an enterprise-wide automation and management strategy to keep pace with dynamic security, risk, and compliance requirements. By adopting a consistent automation and management strategy for your hybrid cloud, you can gain increased agility, repeatability, consistency, and simplified auditing.

A unified automation and management strategy reduces the risk of misconfigurations and manual errors across your organization. Automation and management streamlines and increases the consistency of infrastructure management, application development, and security operations to improve protection, compliance, and change control. This allows you to:

Consistently configure resources according to preapproved policies and proactively maintain them in a repeatable fashion over their life cycle.

Rapidly identify systems that require patches or reconfiguration.

Streamline patching or change system settings according to defined baselines, and in a consistent manner across a large number of systems.

Ease auditing and troubleshooting with automatically recorded action logs.

With identity management and access controls for your automation platform and processes, you can ensure that only authorized staff can execute automation tasks. Choose an automation platform that everyone in your organization can use. Choosing 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 completed work and avoid duplicate efforts.

Auditing. Multiple staff can verify automation tasks and view logs for auditing.

Enterprises rely on IT automation to manage security across increasingly complex operating environments, applications, security operations, and hybrid cloud environments. **Red Hat Ansible Automation Platform** is an end-to-end automation platform that provides a consistent enterprise framework to build and operate IT automation at scale, while prioritizing security every step of the way. It helps improve efficiency, increases productivity, helps to control risk and expenses, allows teams to automate security and compliance consistency across the enterprise in a repeatable way, and provides certified automation content to respond to threats in a coordinated manner with around-the-clock enterprise support from Red Hat.

Red Hat Ansible Automation Platform helps organizations manage automated security processes to stay ahead of malicious attacks– providing everything from automated configuration management to automated patching and remediation. Additionally, Red Hat Ansible Automation Platform can serve as an integration point for security solutions by using content from certified partners like CyberArk, IBM, and Palo Alto Networks, allowing users to automate the management and integration of a wide range of external security technologies.

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 limited set of tasks to start with.

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 by using an end-to-end enterprise automation platform to scale.
Ensure that all automation is verifiable, auditable, and shareable so that others within your organization can take advantage of gains and use an end-to-end enterprise automation platform to scale.

Chapter 6

Ready to get started?

Hybrid cloud security is a shared responsibility 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-ready support, hands-on training, and expert services to help you build and operate your hybrid cloud environment more efficiently and safely.

Discover Red Hat's approach to hybrid cloud security

Consult these resources to learn more about Red Hat's approach to security and compliance across a hybrid cloud.

- Overview of hybrid cloud security
- Hybrid cloud security assessment
- Security approaches for hybrid cloud environments
- Elevate your hybrid cloud security

About Lucy Huh Kerner, Director, Security Global Strategy and Evangelism, Red Hat
Lucy Huh Kerner leads security thought leadership and the technical and go-to-market strategy for security across Red Hat and Red Hat's entire portfolio globally. Additionally, she helps create and deliver security-related technical content to the field, customers, partners, analysts, and press and has spoken at numerous events, including security conferences. Lucy has more than 20 years of professional experience as both a software and hardware development engineer, solutions architect, and global security strategist, where she worked on various aspects of security.

North America
1 888 REDHAT1
www.redhat.com

Europe, Middle East, and Africa
00800 7334 2835
europe@redhat.com

Asia Pacific
+65 6490 4200
apac@redhat.com

Latin America
+54 11 4329 7300
info-latam@redhat.com

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

redhat.com