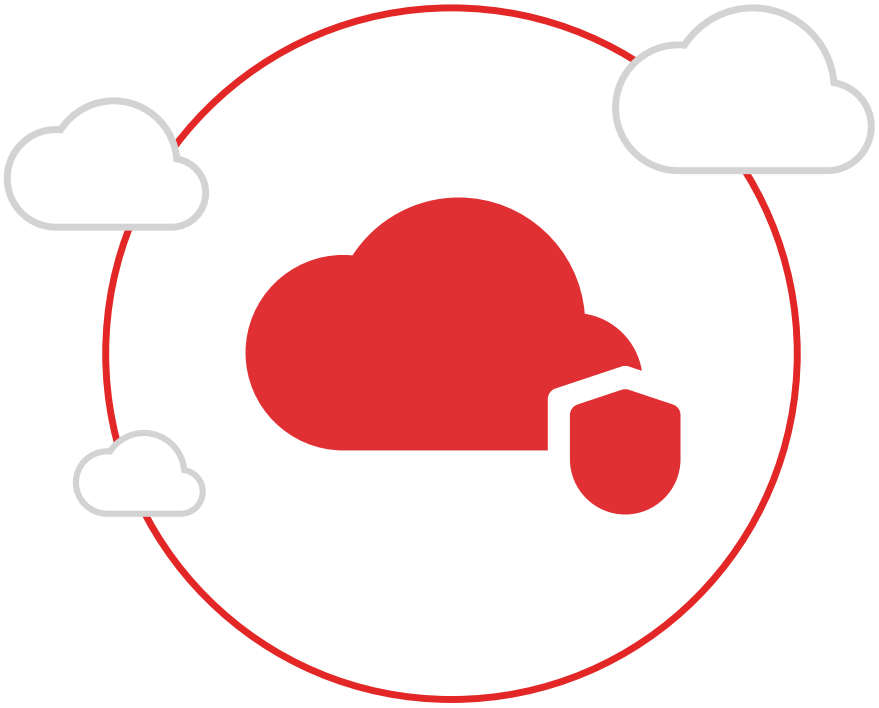
Red Hat



# Incrementa la sicurezza del cloud ibrido

## Proteggi la tua azienda adottando approcci alla sicurezza cloud native

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

# Contenuti

# Adotta una strategia di cloud ibrido che punta alla sicurezza

Il 94% delle organizzazioni ha scelto di utilizzare una tipologia di cloud, e il 58% ha in atto una strategia di cloud ibrido.[1] Il modello architetturale di cloud ibrido offre un certo livello di portabilità, di orchestrazione e di gestione dei carichi di lavoro su due o più ambienti connessi ma separati, inclusi ambienti bare metal, virtualizzati, di cloud privato e pubblico. Un'architettura di cloud ibrido ti consente di eseguire i carichi di lavoro in qualsiasi ambiente connesso, spostandoli tra i vari ambienti e attingendo alle risorse da tali ambienti in modo intercambiabile.

L'adozione di una strategia di cloud ibrido garantisce alle organizzazioni i seguenti vantaggi:

- Fruibilità di infrastrutture, piattaforme, applicazioni e strumenti di diversi fornitori grazie a una completa interconnessione.
- Efficienza e scalabilità maggiori.
- Riduzione dei costi.
- Agilità migliorata.
- Posizionamento dei dati ottimizzato.

La sicurezza è un aspetto importante da affrontare, qualsiasi sia la fase del tuo percorso di adozione del cloud ibrido. L'81% delle aziende si dice infatti preoccupato della sicurezza del cloud.[1] Le vulnerabilità della sicurezza del cloud ibrido sono spesso legate a: controlli carenti o inefficaci sulle risorse (incluso l'utilizzo di cloud pubblico non approvato), una mancanza di visibilità delle risorse, un controllo delle modifiche non adeguato, una gestione della configurazione carente e controlli degli accessi non efficaci. Queste manchevolezze possono essere sfruttate da utenti non autorizzati per accedere a dati sensibili e risorse interne.

Le violazioni alla sicurezza possono comportare perdite notevoli per un'azienda. Il costo medio di una violazione alla sicurezza si aggira intorno ai 3,92 milioni di dollari USA, con una perdita aziendale pari al 36,2% di questo costo.[2] E le minacce sono in crescita. La possibilità di essere vittime di una violazione alla sicurezza in un lasso di tempo di due anni è del 29,6%.[2] Il 2019 ha assistito a un incremento sia del numero medio delle registrazioni dei dati sia del tempo per identificare e contenere le violazioni.[2]

Trasformare la tua strategia, in modo tale che tenga conto delle differenze tra architetture cloud e on premise ti permette di ottenere il deployment di un ambiente di **cloud ibrido incentrato sulla sicurezza** e di superare questi ostacoli. Gli approcci e le considerazioni offerti in questo ebook ti aiutano a potenziare la sicurezza del tuo cloud ibrido per proteggere la tua azienda nel tempo.

## Le conseguenze di una sicurezza inefficace

Le violazioni alla sicurezza sono costose e le minacce in aumento.

**3,92 milioni di dollari USA**
costo medio di ogni violazione alla sicurezza nel 2019.[2]

**279 giorni**
tempo medio per identificare e contenere una violazione alla sicurezza nel 2019.[2]

**1,22 milioni di dollari USA**
risparmio se una violazione venisse identificata e contenuta in
**200 giorni**
o meno.[2]

**29,6%**
possibilità di essere vittime di una violazione in un periodo di due anni.[2]

1 *Flexera, "RightScale 2019 State of the Cloud Report from Flexera", febbraio 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**.

# La sicurezza è un intero processo

Per ottenere una sicurezza efficace occorre adottare un approccio olistico che tenga in considerazione persone, processi e tecnologie. Eseguire il deployment di prodotti e strumenti incentrati sulla sicurezza non basta a proteggere la tua infrastruttura, il tuo cloud o la tua azienda. Per ridurre in modo efficace i rischi legati alla sicurezza sfruttando al meglio le funzionalità dei tuoi prodotti, diventa necessario definire strategie e processi incentrati sulla sicurezza in grado di adattarsi nel tempo, di pari passo all'evolversi delle tecnologie, minacce e necessità aziendali.

Non essendo caratterizzati da confini definiti, gli ambienti di cloud ibrido richiedono nuovi approcci alla sicurezza. Quelli tradizionali basati su modelli di sicurezza perimetrale non sono efficaci. La gestione centralizzata delle identità e il controllo degli accessi sono fondamentali per gli approcci alla sicurezza basati sul cloud, in quanto entrambi sfruttano il principio dei privilegi minimi per fornire agli utenti l'accesso solo a ciò di cui hanno effettivamente bisogno. Questo approccio richiede un controllo dei diritti di accesso correnti per ogni utente, quindi la rivalutazione di ogni utente per stabilire il livello di accesso corretto.

Una strategia di sicurezza del cloud ibrido efficace deve inoltre essere caratterizzata da misure avanzate che consentano di utilizzare le funzionalità di ogni livello nel tuo ambiente, inclusi i sistemi operativi, le piattaforme per container, gli strumenti di automazione, le risorse Software-as-a-Service (SaaS) e i servizi cloud.

### Sistema operativo

Adotta strumenti integrati in grado di aiutarti a garantire la conformità della sicurezza, implementare misure protettive fisiche, migliorare la sicurezza della rete, controllare gli accessi degli utenti, isolare i processi e incrementare la sicurezza dei dati. Tra questi si annoverano OpenSCAP, USBGuard, firewall, Security-Enhanced Linux® (SELinux), gestione delle identità e Network Bound Disk Encryption.

### Piattaforma per container

Utilizza funzionalità integrate all'interno della tua piattaforma e di Kubernetes per migliorare la sicurezza dei container. Tra queste sono inclusi i criteri di sicurezza del pod, i controlli del traffico di rete, i controlli di cluster in entrata e in uscita, i controlli degli accessi basati sui ruoli (RBAC), la gestione integrata dei certificati e la microsegmentazione della rete.

### Strumenti per l'automazione

Scegli un'automazione facilmente comprensibile e fruibile da ogni membro della tua organizzazione, inclusi i team dedicati a sviluppo, operazioni, sicurezza e conformità. Implementa funzionalità di controllo degli accessi, logging e controllo. Leggi a pagina 4 per saperne di più sull'automazione.

Infine, è indispensabile rivedere i processi e gli strumenti di sicurezza esistenti. Assicurati di usare tutte le funzionalità disponibili e stabilisci se alcune impostazioni possano essere modificate o riconfigurate per fornire una protezione migliore o se siano necessari nuovi processi e strumenti.

1. Crea un inventario delle risorse IT e degli strumenti correnti.
2. Documenta le architetture di sicurezza e di rete, i criteri di sicurezza informatica, i processi lavorativi, le lacune nelle competenze e nei talenti.
3. Definisci un modello delle minacce, determinando la tolleranza al rischio, e le strategie per la riduzione delle violazioni alla sicurezza informatica.
4. Analizza le architetture, i criteri e i processi per identificare le aree di miglioramento.
5. Valuta gli strumenti e le risorse attuali per capire se siano in grado di supportare le strategie e i processi aggiornati. Documenta e pianifica come gestire qualsiasi eventuale lacuna nella sicurezza.

Le sezioni che seguono offrono alcune considerazioni chiave sulla sicurezza del cloud ibrido nonché consigli per migliorare la protezione del tuo IT.

CONSIDERAZIONI SULLA SICUREZZA

# Collaborazione

## Perché è importante?

Essendo un aspetto gestito in un secondo momento nell'ambito dello sviluppo applicativo e del deployment dell'infrastruttura, gli approcci alla sicurezza organizzati per compartimenti comportano spesso lacune alla sicurezza stessa e causano inoltre un utilizzo inefficiente delle risorse. Considerata la costante necessità di ottenere cicli di sviluppo sempre più rapidi e modelli di deployment sempre più flessibili, pensare alla sicurezza in una fase preliminare del processo diventa fondamentale. Implementare un sistema di sicurezza efficace solo al termine dei cicli di sviluppo porta a un dispendio di tempo maggiore, con conseguenti ritardi nell'erogazione dei servizi e potenziali falle alla sicurezza.

## Consigli e best practice

Adotta un approccio DevSecOps per uniformare la sicurezza in tutta l'organizzazione. DevSecOps è un framework di collaborazione in cui la sicurezza diventa una responsabilità condivisa e integrata dall'inizio alla fine. La sicurezza viene estesa a tutti i team in modo da non relegare a un singolo team disconnesso la responsabilità di impostarne i criteri. Gli sviluppatori, i team operativi e quelli dedicati alla sicurezza collaborano condividendo visibilità e feedback, e mettendo a frutto le nozioni apprese e le informazioni importanti acquisite. Questo approccio aumenta la protezione dell'intero stack IT poiché la sicurezza è definita al principio dello sviluppo applicativo e del deployment dell'infrastruttura.

I programmi di formazione mirati aiutano i componenti di ogni team a capire l'importanza della sicurezza e le azioni da seguire per salvaguardare la propria organizzazione. La formazione dovrebbe trattare argomenti come questi:

- Garantire la conformità applicativa e delle risorse grazie a criteri e regole sulla sicurezza.
- Definire diversi approcci alla sicurezza per qualsiasi tipo di ambiente: tradizionale, containerizzato e di cloud ibrido.
- Delineare una strategia di applicazione delle patch che consenta di essere sempre aggiornati sulle vulnerabilità nuove ed esistenti alla sicurezza.

Anche il sostegno dei team esecutivi è fondamentale. I dirigenti dovrebbero promuovere la collaborazione incoraggiando i team a condividere idee e suggerimenti.

## Azioni strategiche

Segui questi suggerimenti per migliorare la collaborazione all'interno della tua organizzazione.

### Scegli un approccio graduale.

Scegli un progetto singolo da cui iniziare. Incoraggia la sperimentazione e il miglioramento continuo e iterativo per perfezionare e ottimizzare i tuoi processi. Riconosci i successi di ciascun contributo evidenziandone il loro valore all'interno dell'organizzazione.

### Definisci tempistiche e obiettivi condivisi e chiari.

La trasparenza è un aspetto cardine per DevSecOps. Assicurati che ogni membro coinvolto comprenda e condivida gli obiettivi e le tempistiche del progetto.

### Forma il tuo personale in diverse aree.

Definisci percorsi formativi sulla sicurezza, sull'infrastruttura e sullo sviluppo che siano regolarmente aggiornati e sempre accessibili a tutti i membri del team.

### Crea un gruppo di lavoro dedicato alla sicurezza.

Forma un team integrato e interdisciplinare per definire gli esempi di utilizzo e le strategie nell'ambito della sicurezza.

### Sfrutta le competenze e conoscenze altrui.

Trai vantaggio dai risultati delle ricerche delle altre organizzazioni, come l'Internal Revenue Service e il Department of Homeland Security statunitensi.

CONSIDERAZIONI SULLA SICUREZZA

# Automazione

## Perché è importante?

Configurare i sistemi in maniera errata e applicare un controllo delle modifiche non adeguato significa lasciarli in balia delle minacce più gravi[3], rendendoli vulnerabili agli attacchi. Il controllo delle modifiche è fondamentale per comprendere chi abbia modificato le configurazioni, quando e quali modifiche abbia apportato nell'ambito dei cicli di vita del sistema. L'automazione può aiutarti a semplificare le operazioni quotidiane integrando — da subito — la sicurezza nei processi, nelle applicazioni e nell'infrastruttura. Ottenere un deployment della sicurezza completamente automatizzato può infatti ridurre il costo medio di una violazione del 95%, ma fin'ora solo il 16% delle organizzazioni ha implementato questo approccio.[4]

## Consigli e best practice

Implementa una strategia unificata di automazione per ridurre il rischio di configurazioni errate ed errori manuali nella tua organizzazione. L'automazione agevola la gestione dell'infrastruttura, dello sviluppo applicativo e delle operazioni rivolte alla sicurezza, rendendo ogni aspetto coerente, per incrementare la protezione, la conformità e il controllo delle modifiche.

- Configura in modo coerente le risorse in base a criteri pre-approvati e mantienili in modo proattivo e reiterativo durante l'intero ciclo di vita.
- Identifica rapidamente i sistemi che richiedono patch o una riconfigurazione.
- Applica patch più facilmente o modifica le impostazioni di sistema in conformità a baseline definite, in modo coerente e su più sistemi.
- Semplifica i processi di controllo e risoluzione dei problemi attraverso registri delle azioni automatici.

Implementare la gestione delle identità e il controllo degli accessi per la tua piattaforma e i tuoi processi di automazione ti aiuterà a garantire che solo il personale autorizzato possa eseguire le attività di automazione.

Affidati a una piattaforma di automazione facilmente fruibile da ogni team, che implementi un linguaggio di automazione comune e semplice da imparare e che consenta di migliorare:

- **Visibilità.** Chiunque deve essere in grado di capire ogni attività automatizzata.
- **Ripetibilità.** Una piattaforma e un linguaggio accessibili consentono a tutto il personale approvato di sfruttare l'automazione in modo efficace ed efficiente.
- **Collaborazione.** Le attività di automazione possono essere condivise nella tua organizzazione, consentendo agli altri team di evitare di svolgere le stesse attività più volte.
- **Controllo.** Più team possono verificare le attività di automazione e visualizzare i log ai fini dei controlli.

## Azioni strategiche

Segui questi suggerimenti per avviare il tuo processo di automazione della sicurezza.

### Inizia da un singolo progetto.

Non automatizzare tutti i processi contemporaneamente. Scegli un singolo progetto o un set limitato di attività da cui partire.

### Scegli attività ripetitive.

Automatizza attività eseguite in modo ripetitivo, tra cui la gestione della configurazione, la gestione del pacchetto software e delle patch, l'identificazione delle vulnerabilità e la relativa correzione e l'applicazione dei criteri.

### Scegli l'automazione continua.

Implementa l'automazione e misura i risultati per un'adattabilità costante.

### Adotta un piano di condivisione.

Rendendo ciascun processo di automazione controllabile e condivisibile, tutti i membri della tua organizzazione possono sfruttare al meglio i vantaggi realizzati.

3 *Cloud Security Alliance, "Top Threats to Cloud Computing: The Egregious 11", agosto 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**.

CONSIDERAZIONI SULLA SICUREZZA

# Gestione di aggiornamenti e patch

## Perché è importante?

Non disporre di sistemi con patch e aggiornamenti eseguiti con cadenza regolare può portare a problemi di compliance, causando vulnerabilità alla sicurezza. Molte delle vulnerabilità sfruttate alla base di una violazione sono infatti già note ai team IT e dedicati alla sicurezza.

## Consigli e best practice

Applica patch con regolarità e testale per garantire che vengano utilizzate correttamente. Analizza i sistemi quotidianamente per identificare eventuali problemi di conformità e vulnerabilità della sicurezza che richiedano patch. Definisci le priorità delle azioni per correggere i problemi riscontrati in base al tuo modello di risposta alle minacce, tenendo in considerazione tempistiche, prestazioni e rischi. Applica periodicamente patch a tutti i sistemi applicabili per restare al passo con le criticità più importanti. Applica patch per i problemi più critici e le vulnerabilità note il prima possibile. Testa i sistemi su cui sono state applicate le patch prima di rimetterli in produzione.

È importante inoltre aggiornare la tua strategia di applicazione delle patch, in modo che tenga conto delle risorse cloud e containerizzate, che vengono avviate a partire da immagini di base. Assicurati che le immagini di base siano conformi alle baseline relative alla sicurezza della tua organizzazione. Come con i sistemi fisici e virtualizzati, analizza e applica patch regolarmente alle tue immagini di base. Quando applichi patch a un'immagine di base, crea e implementa nuovamente tutti i container e le risorse cloud su quell'immagine.

Infine, semplifica le operazioni di applicazione delle patch rendendole automatiche. Crea un flusso di lavoro di automazione per l'applicazione delle patch per accelerare le operazioni, ridurre il rischio di errore e incrementare la coerenza tra tutti i sistemi. Ad esempio, per automatizzare i processi relativi ai cicli di vita, come l'applicazione delle patch, puoi sfruttare i flussi di integrazione e deployment continui (CI/CD) basati su Jenkins sia per le applicazioni che per l'infrastruttura.

## Azioni strategiche

Segui questi passaggi per ottenere una strategia di applicazione delle patch e degli aggiornamenti più efficiente.

1. Identifica i sistemi su cui è necessario applicare le patch.
2. Attribuisci le priorità delle azioni in base al tuo modello delle minacce, alla valutazione del rischio, all'impatto sulle prestazioni e alle finestre di applicazione delle patch disponibili.
3. Automatizza l'applicazione delle patch per migliorare la coerenza e la ripetibilità sia per le infrastrutture tradizionali che per quelle di cloud ibrido.
4. Rivaluta e adatta periodicamente la tua strategia di applicazione delle patch per tenere il passo delle funzionalità, delle tecnologie e delle minacce in continua evoluzione.

CONSIDERAZIONI SULLA SICUREZZA

# Tecnologia open source

## Perché è importante?

**Le tecnologie open source** sono una parte integrante delle operazioni cloud e relative ai container. Tuttavia, se implementate in maniera non sicura o usate con software open source non approvati e distribuiti direttamente dalle community upstream, espongono i sistemi a potenziali vulnerabilità alla sicurezza. Tali falle vengono sfruttate per attaccare la supply chain e compromettere un target finale, approfittando dei punti deboli dei servizi e dei software di terze parti. Gli attacchi alla sicurezza sono di varie tipologie e possono includere hijack degli aggiornamenti software o inserimento di un codice dannoso in programmi software legittimi. Nel 2018 gli attacchi alla supply chain sono aumentati del 78%.[5]

## Consigli e best practice

Assicurati che le tecnologie open source che utilizzi provengano da fonti affidabili e siano implementale in modo sicuro. Innanzi tutto, fai un inventario delle tecnologie open source in uso nella tua organizzazione e rimuovi quelle distribuite da fonti non note. Definisci i processi e i criteri che consentano ai team IT e dedicati alla sicurezza di gestire le le tecnologie restanti.

Delinea un approccio di adozione delle tecnologie open source che punti alla sicurezza. La tua strategia deve garantire: l'affidabilità delle fonti da cui provengono le tue tecnologie open source, l'adozione di flussi di automazione continua per l'applicazione di patch e aggiornamenti e l'integrazione della sicurezza in tutti i processi e componenti del progetto. È fondamentale inoltre incoraggiare l'utilizzo di soluzioni open source di livello enterprise che includano un supporto aziendale durante tutto il loro ciclo di vita.

**78%** di attacchi alla supply chain in più nel 2018 rispetto all'anno precedente.[5]

## Azioni strategiche

Segui questi suggerimenti per migliorare la sicurezza delle tue tecnologie open source.

### Passa a versioni disponibili in commercio.

Esegui la migrazione dei software dei progetti open source upstream a versioni affidabili e **disponibili in commercio**. Queste versioni vengono testate e convalidate per ridurre il rischio di bug e vulnerabilità alla sicurezza. Possono inoltre includere un supporto di livello enterprise in grado di erogare patch di sicurezza rapidamente e fornire linee guida su come configurare il tuo software per garantire la massima sicurezza.

Scopri di più sulla sicurezza delle tecnologie open source in **questo articolo**.

### Esegui il deployment di un software open source basato su modelli.

Verifica se i tuoi strumenti di gestione e relativi alla piattaforma offrono un provisioning self service basato su modelli preconfigurati e approvati. Questi modelli ti servono a ottenere il deployment solo di tecnologie open source affidabili e aggiornate. Un deployment rapido e automatizzato promuove inoltre l'utilizzo di risorse IT autorizzate e controllate dai team IT e dedicati alla sicurezza.

5 *Symantec, "Internet Security Threat Report, Volume 24", febbraio 2019.*

# Inizia il tuo percorso di adozione del cloud

La sicurezza del cloud ibrido è una sfida che affrontano tutte le organizzazioni. Qualsiasi sia la fase di adozione del cloud ibrido che la tua azienda si trova a gestire, Red Hat può aiutarti a ottenere il deployment di un ambiente che punta alla sicurezza. Grazie a funzionalità di sicurezza integrate, la gamma di prodotti Red Hat di software open source per la produzione ti offre gli strumenti e le piattaforme necessari a superare gli ostacoli presenti e futuri legati a sicurezza e conformità. Red Hat propone inoltre un supporto di livello enterprise, formazione pratica e servizi esperti per aiutarti a creare e gestire il tuo ambiente di cloud ibrido in modo efficiente e sicuro.

Accedi a queste risorse per scoprire di più sull'approccio di Red Hat alla sicurezza e alla conformità.

- **Panoramica sulla sicurezza del cloud ibrido**
- **Perché scegliere Red Hat per una sicurezza IT continua**
- **I vantaggi dell'automazione di sicurezza e conformità**
- **Red Hat® Services: automatizza la sicurezza e la conformità del tuo sistema**

## Prenota una discovery session gratuita:

## **redhat.com/consulting**

---

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

Responsabile della strategia di go to market e tecnica per la sicurezza dell'intero portafoglio di prodotti Red Hat, Lucy Huh Kerner aiuta a sviluppare la sicurezza a livello globale. Aiuta inoltre a realizzare e distribuire contenuti tecnici correlati alla sicurezza per esperti di settore, clienti, partner, analisti e stampa e ha partecipato a numerosi eventi offrendo il suo contributo in quanto esperta in materia. Prima di ricoprire questo ruolo, è stata Senior Cloud Solutions Architect per il team North America Public Sector di Red Hat. Grazie alla sua esperienza nelle tecnologie cloud, ha supportato le vendite cloud di Red Hat progettando e presentando le soluzioni cloud Red Hat per svariati clienti nordamericani nel settore pubblico. Lucy vanta un'esperienza comprovata di oltre 15 anni sia come ingegnere dedicato allo sviluppo di hardware e software, che come architetto dedicato alle soluzioni nella fase di pre-vendita, ruolo che le ha consentito di approfondire vari aspetti della sicurezza informatica.

---



F18867_0220_KVM

Red Hat