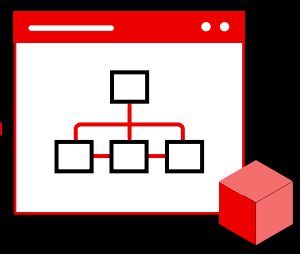
Red Hat
OpenShift
Platform Plus

Realizzare una software factory a supporto delle iniziative DevSecOps

Una guida dettagliata per avviare il tuo percorso di adozione di DevSecOps

Contenuti



1 Proteggi il tuo business adottando DevSecOps

2 L'importanza di persone, processi e tecnologia

3 Un approccio produttivo alla distribuzione del software

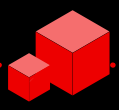
- **3.1** Come è fatta una software factory?
- **3.2** Crea la tua software factory
- **3.3** Crea, distribuisci, esegui

4 L'aiuto degli esperti per l'adozione di DevSecOps

- **4.1** Una piattaforma per la riuscita delle iniziative DevSecOps
- **4.2** Crea la tua software factory con Red Hat OpenShift Platform Plus

5 Scelte di successo

Proteggi il tuo business adottando DevSecOps



Un numero crescente di organizzazioni punta all'innovazione e alla **trasformazione digitale** adottando tecnologie **cloud native**, **container** e **microservizi**. Come parte di questa trasformazione, viene utilizzato Kubernetes per l'orchestrazione dei container, a supporto delle attività cloud native. Poiché i **cluster Kubernetes** possono gestire gli host su ambienti locali e cloud, Kubernetes rappresenta la piattaforma ideale per ospitare applicazioni cloud native che richiedono attività resilienti e rapidamente scalabili.

Questo approccio fa emergere nuove sfide, in particolare rispetto alla sicurezza e alla gestibilità su larga scala. Di fatto, il 50% dei leader IT senior di grandi aziende indica la sicurezza informatica tra le tre priorità per le iniziative tecnologiche.[1]

L'adozione di approcci e metodi DevSecOps contribuisce a integrare la sicurezza in applicazioni, processi e piattaforme, per proteggere al meglio la tua azienda.

Gli approcci e le considerazioni offerti in questo ebook ti consentiranno di adottare le pratiche DevSecOps più adatte alla tua organizzazione, con il supporto di Red Hat® OpenShift® e di altre tecnologie Red Hat.

Cosa sono le applicazioni cloud native?

Le **applicazioni cloud native** sono una raccolta di microservizi indipendenti e a basso accoppiamento.

Cosa sono DevOps e DevSecOps?

DevOps è un approccio alla cultura, all'automazione e alla progettazione di piattaforme incentrato su un'offerta di livelli superiori di valore e reattività attraverso un'erogazione dei servizi efficiente e rapida.**DevSecOps** estende la cultura collaborativa di DevOps, consentendo di incorporare la sicurezza in tutti i cicli di vita dell'applicazione. Per una più ampia diffusione della sicurezza negli ambienti distribuiti, deve includere persone, processi e tecnologia.

Tramite DevSecOps, la sicurezza diventa una responsabilità condivisa e applicata dai vari team, invece che un insieme di attività di proprietà di un team applicato al termine del processo di sviluppo e deployment. Gli sviluppatori, i team operativi e quelli dedicati alla sicurezza collaborano condividendo informazioni e feedback e mettendo a frutto le nozioni apprese e le informazioni importanti acquisite. Questo approccio aumenta la protezione e riduce i rischi, poiché la sicurezza è integrata sin dall'inizio dello sviluppo applicativo e del deployment dell'infrastruttura.

88%

delle organizzazioni intervistate utilizza Kubernetes come agente di orchestrazione dei container; il 74% lo utilizza in produzione.[2]

74%

delle organizzazioni intervistate ha in corso un'iniziativa DevSecOps.[2]

1 Flexera, "2021 Flexera State of Tech Spend Report", gennaio 2021.

2 Red Hat, "Report 2021 sullo stato della sicurezza di Kubernetes".

Obiettivi di DevSecOps

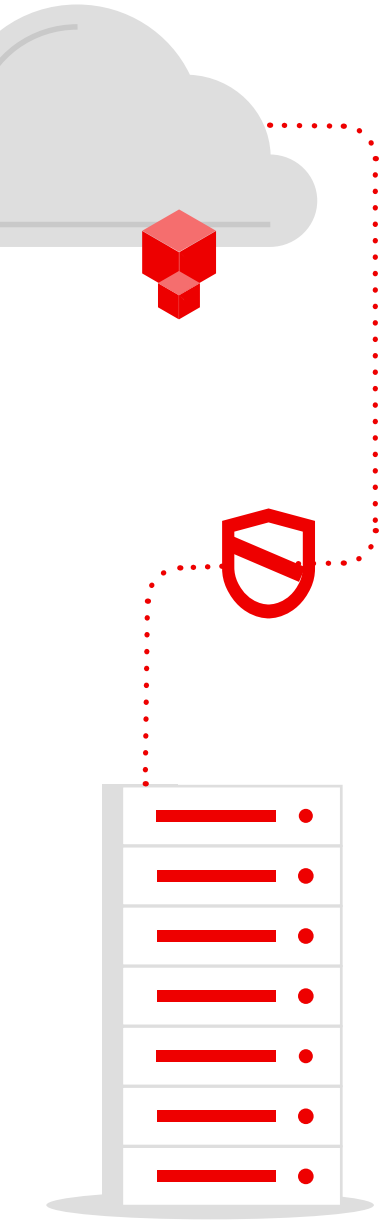
DevSecOps punta a velocizzare la distribuzione e il deployment su larga scala di applicazioni, servizi e funzionalità incentrati sulla sicurezza.

Scalabilità

Velocità

Sicurezza

Stabilità



Le sfide all'adozione di DevSecOps

Processi manuali

Quando sono necessari interventi umani, le attività correlate allo sviluppo, al test e alla sicurezza possono diventare lunghe, ripetitive e ad alta probabilità di errore.

Collaborazione limitata tra i team

Spesso i team addetti allo sviluppo, alla sicurezza e alle operazioni si limitano a operare nel proprio dominio; ciò determina processi frammentari, passaggi di consegne manuali, conoscenza e comprensione limitate dei problemi e delle esigenze degli altri team.

Applicazione tardiva dei processi di sicurezza

Nell'approccio convenzionale allo sviluppo e al rilascio delle applicazioni le procedure e i controlli di sicurezza vengono applicati solo al termine del processo, prima della distribuzione in produzione.

Complessità degli ambienti applicativi

Non è sempre facile comprendere le connessioni e le implicazioni di sicurezza dei diversi componenti (container, microservizi e servizi cloud) che costituiscono gli ambienti di sviluppo, test e produzione delle applicazioni, spesso complicati e di grandi dimensioni.

Dipendenze esterne

Quasi sempre lo sviluppo applicativo cloud native si affida a dipendenze esterne, ovvero sezioni di codice open source, librerie e servizi, anch'essi componenti che devono essere protetti.

Panorama della sicurezza in evoluzione

I continui e repentini cambiamenti delle minacce alla sicurezza e delle normative in merito (inclusi i requisiti aziendali, tecnici e geografici) complicano l'aggiornamento continuo e il rispetto della conformità.

L'importanza di persone, processi e tecnologia

DevSecOps non è un team né un solo processo, ma una capacità che coinvolge l'azienda nel suo complesso e che richiede cambiamento e allineamento in tre aree: persone, processi e tecnologie.

Persone

Qualsiasi iniziativa che coinvolga l'intera enterprise ruota intorno alle persone, e DevSecOps non è differente. Affinché sia adottato a livello globale, tutti i team – sicurezza, operazioni e sviluppo – devono essere coinvolti, partecipare e avere fiducia gli uni negli altri.

Processi

Grazie ai processi i progetti progrediscono da una fase a quella successiva, dall'inizio alla fine. Per un'adozione su vasta scala di DevSecOps sono indispensabili processi trasparenti di creazione, deployment, gestione e adeguamento delle applicazioni e dell'infrastruttura, che prevedano l'integrazione della sicurezza nei rispettivi cicli di vita.

Tecnologie

La piattaforma applicativa eroga le funzionalità di creazione, deployment ed esecuzione di applicazioni e infrastruttura. Una piattaforma unificata che supporti i team di sviluppo, sicurezza e operativi costituisce la base per la creazione e l'adeguamento delle procedure DevSecOps.

Adottare DevSecOps in modo ottimale

Nessuna organizzazione può dar vita a un'iniziativa DevSecOps completa da un giorno all'altro. L'adozione di DevSecOps è un percorso di apprendimento iterativo e graduale, che richiede tempo e una strategia logica e sostenibile.

Incoraggiare la collaborazione tra i team.

Promuovere la collaborazione in tutta l'organizzazione con strumenti di incentivazione e processi di progettazione. Il coordinamento consente ai team di creare flussi DevSecOps completi che garantiscono un maggior valore. Lavorare in sinergia aiuta a coltivare la proprietà e la responsabilità condivise dello sviluppo, della sicurezza e delle operazioni.

Documentare la situazione attuale.

Documentare in dettaglio i processi di sviluppo, gestione delle modifiche e governance già esistenti, usando framework dinamici come **GitOps**. L'analisi del punto di partenza e delle sfide da superare aiuta a capire il percorso da intraprendere. Mano a mano che i processi vengono adeguati, occorre documentare le novità e le ragioni che hanno portato alle modifiche apportate.

Valutare i processi.

Identificare e adeguare i processi che non supportano gli obiettivi DevSecOps dell'azienda. Può trattarsi di configurazioni e infrastrutture di integrazione e distribuzione continue (CI/CD) diverse o non efficienti, processi troppo centralizzati o che richiedono interventi manuali frequenti.

Definire e misurare i risultati.

Determinare gli obiettivi DevSecOps da raggiungere nell'organizzazione e identificare metriche misurabili o indicatori chiave delle prestazioni (KPI) per tenere traccia dei progressi. Sono metriche utili i tempi di creazione e distribuzione delle applicazioni, la frequenza di modifiche ed errori, i tempi di risoluzione dei problemi o la disponibilità delle applicazioni.

Condividere le conoscenze e le procedure ottimali.

Creare un team principale di interlocutori, possiamo chiamarla una community per lo sviluppo delle procedure o un centro d'eccellenza, che condividono pratiche comuni, esperienza e risultati raggiunti grazie a DevSecOps. Il team dovrebbe inoltre supportare gli altri team già pronti ad adottare DevSecOps ad avviare l'iniziativa.

Coinvolgere l'intera organizzazione.

Garantire l'intera organizzazione sia coinvolta nell'adozione di DevSecOps. I team devono essere aiutati a comprendere le motivazioni di ogni cambiamento, sottolineando l'impatto positivo che avrà sui rispettivi ruoli. Il supporto della dirigenza e incentivi basati su metriche possono aiutare i team a progredire.

Avviare l'iniziativa DevSecOps

Dopo aver definito la strategia DevSecOps, è tempo di muovere i primi passi del percorso. Non tutti i team di sviluppo saranno pronti ad adottare immediatamente DevSecOps. Si può avviare l'iniziativa con i team che hanno già ottenuto successi misurabili nell'adozione di nuovi processi e piattaforme. In genere, chi appartiene a questi team è un valido candidato anche per i team di riferimento.

Scegliendo un approccio graduale, puoi dimostrare i vantaggi effettivi di un piccolo passaggio, espanderlo ad altre aree e processi e ripetere. Ciò ti permetterà di ottenere risultati incrementali in brevi periodi di tempi. Usando le metriche definite in precedenza, monitora i progressi e analizza i progetti o i processi che hanno registrato intoppi. Per ogni successo ottenuto, promuovi il valore di DevSecOps e condividi l'esperienza in tutta l'organizzazione. Gli altri potranno consolidare queste fondamenta aggiungendo le loro esperienze per ottenere vantaggi ancora maggiori.

Un approccio produttivo alla distribuzione del software

Una moderna distribuzione del software esige velocità, coerenza e qualità. Un approccio di tipo software factory contribuisce ad abilitare, velocizzare e applicare quei cambiamenti e comportamenti indispensabili per adottare in azienda la cultura DevSecOps. Consente infatti di sviluppare e distribuire in tempi rapidi applicazioni di alta qualità mediante una **catena di distribuzione software attendibile** e un insieme coerente di processi agili, come quelli dello sviluppo basato sui test.

Vantaggi della software factory

Un approccio che prevede la software factory offre vantaggi misurabili:

Minore tempo richiesto per le modifiche

Frequenza di deployment più alta

Tempo ridotto per il ripristino di servizi non funzionanti

Minore frequenza di errore delle modifiche

Metriche di prestazione della distribuzione software quantificabili[3]

Metriche di prestazione della distribuzione software	Con una software factory	Senza una software factory
Tempo richiesto per le modifiche	< 1 ora	1-6 mesi
Frequenza di deployment	Su richiesta (>1 al giorno)	Una volta ogni 1-6 mesi
Tempo di ripristino dei servizi	< 1 ora	Da 1 giorno a 1 settimana
Frequenza di errore delle modifiche	0%-15%	16%-30%

*3 Google Cloud: "***Accelerate State of DevOps 2021***", settembre 2021.*

Come è fatta una software factory?

Una software factory ti consente di passare da processi manuali non coerenti a operazioni automatizzate e omogenee.

Senza una software factory

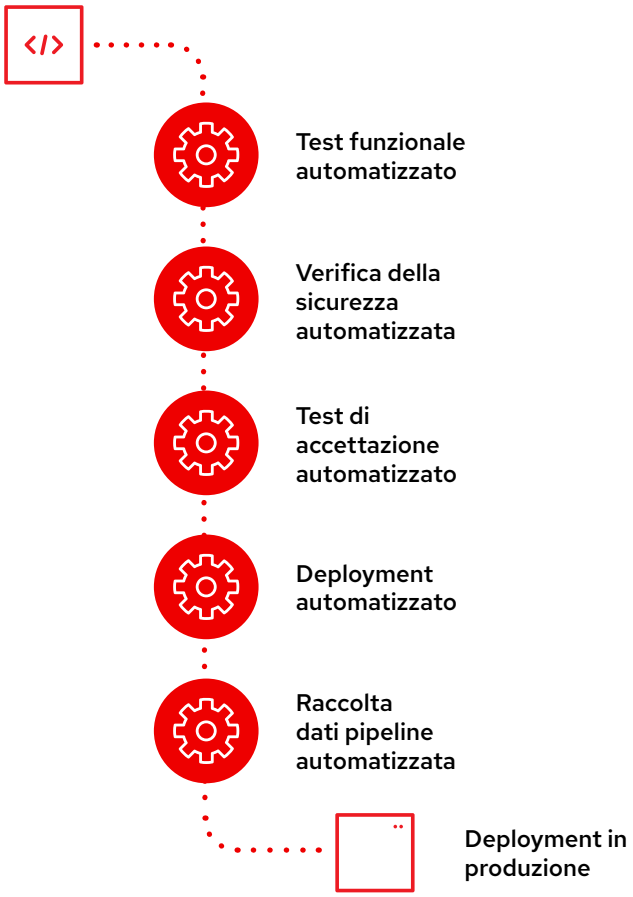
I processi e le approvazioni manuali rallentano lo sviluppo e la distribuzione, offrono aspettative poco chiare e applicazioni la sicurezza in modo non coerente. Poiché anche le modifiche di minore entità richiedono giorni o settimane, i team spesso tentano di inserire numerose modifiche in un'unica distribuzione, aumentando il rischio di applicare modifiche errate e problemi di sicurezza.

Spesso, quando l'intero processo manca di trasparenza anche la fiducia tra i team è labile. Se le misure di sicurezza e conformità vengono applicate al processo in modo manuale e tardivo, alcuni problemi possono passare inosservati durante lo sviluppo. Di conseguenza, le applicazioni vengono rinviate agli sviluppatori per risolvere problemi imprevisti di sicurezza e conformità, il che, in una fase di per sé già stressante, può aumentare frustrazione e sfiducia.

Con una software factory

Processi definiti e automatizzati velocizzano lo sviluppo e la distribuzione, consentono di integrare la sicurezza in modo coerente e creano aspettative chiare per tutti i team coinvolti. Le piccole modifiche, rese effettive in pochi minuti, possono essere distribuite dai team rapidamente e ogni giorno, riducendo il rischio complessivo.

Trasparenza e visibilità sono aspetti chiave delle software factory e gettano le basi per creare la fiducia nei team di sviluppo, operazioni e sicurezza. Le misure di sicurezza e conformità vengono applicate automaticamente durante lo sviluppo, in modo che i problemi vengano individuati e definiti nelle fasi iniziali del processo. Processi e criteri ben documentati consentono ai team di comprendere i risultati previsti da tutto il processo ed evitano sorprese al momento di distribuire le applicazioni in produzione.



Crea la tua software factory

L'approccio alla software factory si incentra sull'**automazione**, che è fondamentale per operare negli ambienti cloud native e per adottare le procedure DevSecOps. L'automazione consente la scalabilità controllata delle attività di sviluppo, distribuzione, deployment e infrastruttura, oltre al provisioning e al ritiro dinamico di risorse, ambienti e applicazioni. Tutti questi aspetti contribuiscono a velocizzare la risposta ai cambiamenti.

L'automazione può essere applicata a tutti gli aspetti del flusso di lavoro DevSecOps, inclusi i processi di sviluppo, test, controllo della qualità del codice, convalida della compliance, rilevamento delle vulnerabilità e correzione. L'utilizzo delle pipeline CI/CD consente di automatizzare sia lo sviluppo che le migliorie alle applicazioni, nonché il deployment e la gestione dell'infrastruttura. Infine, è bene definire e documentare i criteri di sicurezza e rischio e automatizzare controlli e verifiche di conformità di criteri per tutti i cicli di vita del software.

L'automazione dichiarativa e orientata agli obiettivi garantisce scalabilità e adattabilità rapide e semplici.

L'automazione dichiarativa consente di definire la configurazione target di un'applicazione o infrastruttura, invece di fornire un set di istruzioni per configurare le risorse. Vale a dire che viene definito l'obiettivo finale e non i metodi da applicare per raggiungerlo. Sarà quindi la piattaforma applicativa a provvedere al provisioning e alla configurazione delle risorse necessarie per raggiungere la condizione target, e ad applicare le correzioni che garantiranno la permanenza nel tempo delle configurazioni stabilite. Inoltre, questo approccio è preparatorio per **GitOps**, un insieme di procedure per la gestione delle configurazioni di infrastruttura e applicazione tramite il sistema di controllo della versione Git.

Decidere cosa automatizzare e quando

Così come con l'intero approccio DevSecOps, anche il deployment dell'automazione è un percorso e va pianificato. I passaggi per introdurre l'automazione sono i seguenti:

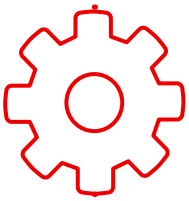
1. Documentare dettagliatamente i processi.
2. Per ogni passaggio manuale, registrare le decisioni e il processo che le ha prodotte. Il processo decisionale può prevedere la lettura di determinati materiali, la considerazione di specifici fattori, la consulenza con vari esperti e altre azioni.
3. Identificare tutti i passaggi manuali che è possibile automatizzare con facilità e valutare il livello di modifica da automatizzare. Ad esempio, è possibile automatizzare modifiche di lieve entità ma richiedere l'approvazione di determinati team per modifiche più importanti.
4. Per i passaggi manuali che non è possibile automatizzare con facilità, valutare cosa sia necessario per automatizzarli e creare un piano per adottare l'automazione.

Avviare l'automazione immediatamente, senza attendere di aver identificato tutte le aree in cui è possibile procedere. L'automazione iterativa dei processi è già di per sé un processo DevOps. Rendendo automatici, adeguando e perfezionando i processi si acquisiscono competenze ed esperienze di valore, utili a supportare le procedure DevSecOps nella loro interezza.

Focus sulle attività strategiche

L'automazione non è destinata a sostituire il personale, ma punta a garantire più produttività, coerenza ed efficienza. È il paradosso dell'automazione: adottandola l'intervento umano acquista più importanza, ma è una necessità che si presenta in modo più sporadico.

Alcuni considerano l'automazione come uno strumento per eliminare posti di lavoro, ma in realtà essa consente al personale IT più esperto di dedicarsi alla risoluzione di problemi più significativi, invece che ad attività ordinarie, ripetitive e quotidiane.



Scopri come adottare l'automazione in tutta l'azienda

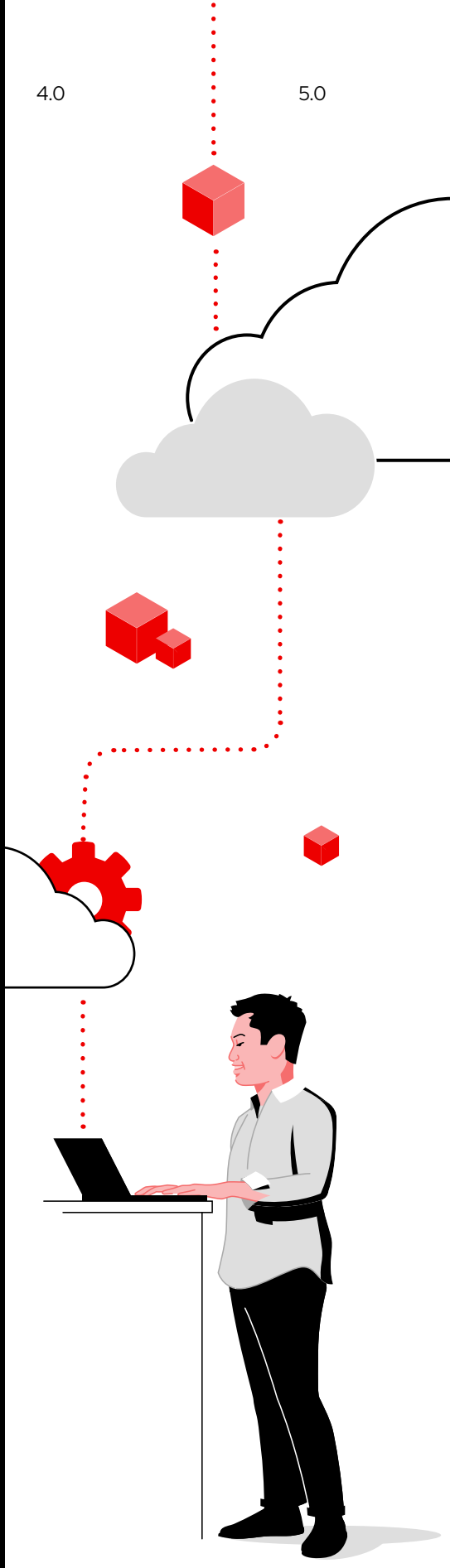
Con l'automazione persone, processi e tecnologie possono operare in sinergia per incrementare agilità, innovazione e valore dell'azienda.

Leggi **l'ebook sull'azienda automatizzata** per sapere di più su come estendere l'automazione all'intera azienda.

Strumenti per la software factory

Gli strumenti sono un aspetto importante della software factory. Red Hat consiglia di utilizzare e di automatizzare le categorie di strumenti indicati di seguito. Per ogni tipo di strumento vengono forniti degli esempi, ma è possibile utilizzarne altri.

Categoria di strumenti	Esempi
Gestione dei progetti	▸ Confluence con Jira ▸ Trello
Gestione codice sorgente	▸ Github ▸ Gitlab
Ambienti di sviluppo integrato (IDE)	▸ VS.code ▸ **Red Hat OpenShift Dev Spaces**
Repository di artefatti	▸ Nexus ▸ Artifactory
CI/CD	▸ **Red Hat OpenShift Pipelines** ▸ **Jenkins**
Runtime	▸ **Red Hat Runtimes** ▸ Golang
Compilazione	▸ Maven ▸ Dotnet build
Test dell'unità	▸ JUnit ▸ NUnit
Analisi del codice sorgente	▸ Sonarqube ▸ Fortify
Test SAST (Static Application Security Testing)	▸ CheckMarx ▸ **Red Hat Advanced Cluster Security for Kubernetes**
Test di accettabilità utente	▸ Cucumber ▸ Cyprus
Strumenti DAST (Dynamic Application Security Testing)	▸ Veracode ▸ Synopsys
Telemetria, metriche e registrazione	▸ **Prometheus** ▸ **Grafana** ▸ **Elasticsearch, Fluentd e Kibana (EFK)** ▸ Splunk
Service mesh	▸ Linkerd ▸ **Red Hat OpenShift Service Mesh**



Crea, distribuisci, esegui

Spesso sono gli architetti delle piattaforme o gli ingegneri DevOps a configurare le software factory per conto degli sviluppatori. In questa fase vanno messe in atto le migliori prassi di sicurezza in tre aree fondamentali: creazione, distribuzione, esecuzione.

Compilazione

Controlla la sicurezza e la conformità dell'applicazione.

Nel deployment cloud native è fondamentale integrare la sicurezza direttamente nelle applicazioni.

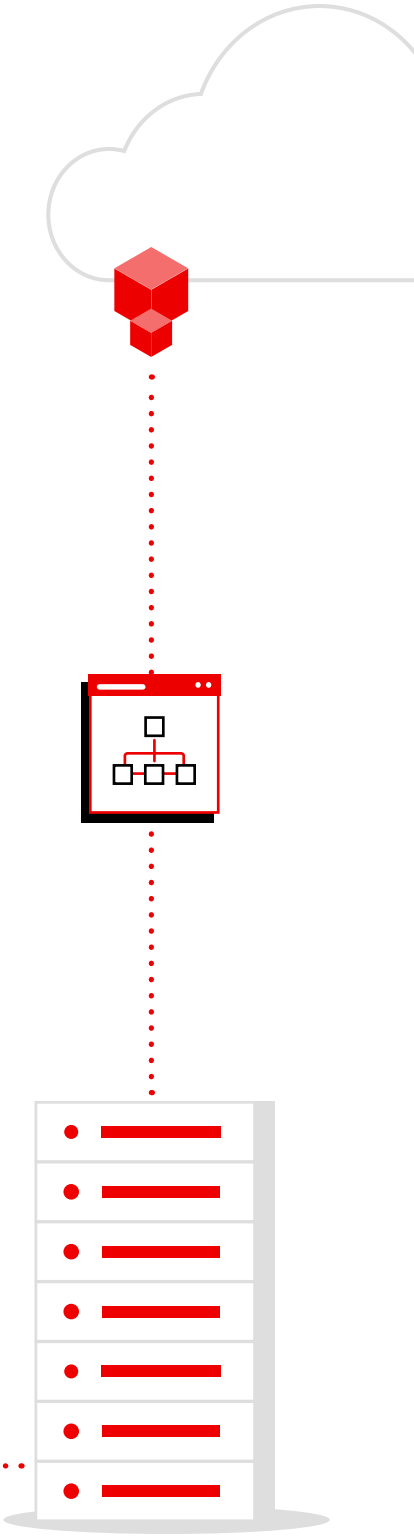
- Utilizzare sorgenti attendibili per i container esterni e il contenuto delle applicazioni, inclusi i runtime.
- Adottare un registro dei container privato e attendibile per la gestione delle immagini.
- Automatizzare le pipeline di sviluppo e distribuzione.
- Utilizzare procedure agili, come TDD, per implementare nel codice i requisiti non funzionali.
- Integrare la sicurezza nelle pipeline applicative, con analisi della qualità del codice, della vulnerabilità dell'immagine e della distribuzione Kubernetes.
- Automatizzare la distribuzione e il posizionamento delle applicazioni.

Distribuzione

Proteggi la tua piattaforma.

La protezione della piattaforma Kubernetes e l'automazione delle policy di distribuzione sono requisiti fondamentali per una sicurezza efficiente.

- Ridurre la superficie d'attacco utilizzando un sistema operativo ottimizzato per container.
- Automatizzare la gestione delle configurazioni e l'applicazione delle policy nei cluster.
- Adottare l'accesso con privilegi minimi e il controllo granulare degli accessi basato sui ruoli.
- Crittografare i dati della piattaforma e delle applicazioni in transito e in sosta.
- Utilizzare soluzioni automatizzate per la conformità, la valutazione del rischio e le correzioni.
- Ridurre i rischi della fase di distribuzione con policy di controllo dell'ammissione dei pod Kubernetes.



Esegui

Metti al sicuro i runtime dei container.

È fondamentale garantire la sicurezza dell'applicazione durante il runtime.

- Isolare le applicazioni in esecuzione con Security-Enhanced Linux® (SELinux), Security Context Constraints (SCC), spazi dei nomi Kubernetes, controllo degli accessi basato sui ruoli e policy di rete.
- Utilizzare le quote per prevenire i conflitti tra risorse e i problemi di prestazioni che ne derivano.
- Gestire l'accesso alle applicazioni e proteggere i dati applicativi con gestione degli utenti con single sign-on, gestione della sicurezza del traffico in entrata e in uscita, traffico crittografato da pod a pod e gestione dell'interfaccia di programmazione delle applicazioni (API).
- Verificare e monitorare l'attività di piattaforma e applicazioni.
- Automatizzare il rilevamento e la risposta alle minacce indirizzate ai pod da comportamenti anomali, eventi di escalation dei privilegi e processi a rischio come il mining delle criptovalute.
- Utilizzare i controller di ammissione per prevenire il deployment di container che non rispettano le policy di sicurezza.
- Creare reti zero-trust avvalendosi di service mesh e policy di rete.

Suggerimento per la sicurezza

Leggi **Un approccio multilivello alla sicurezza di Kubernetes e dei container** per saperne di più su come proteggere le applicazioni containerizzate gestite con Kubernetes.

Compilazione	Distribuzione	Esegui
Ciclo di vita dell'applicazione	**Gestione della configurazione del parco risorse**	**Osservabilità e avvisi delle risorse**
Analisi della vulnerabilità	Controller di ammissione delle policy	Analisi comportamentale dei runtime
Analisi della configurazione delle applicazioni	Valutazione della conformità	Raccomandazioni sulle policy di rete
API per l'integrazione di CI/CD	Definizione dei profili di rischio	Rilevamento e risposta alle minacce
Contenuto attendibile	Ciclo di vita della piattaforma Kubernetes	Isolamento dei container
Registro dei container	Gestione delle identità e degli accessi	Isolamento della rete
Gestione delle build	Dati della piattaforma	Accesso alle applicazioni e dati applicativi
Pipeline CI/CD	Policy di deployment	Osservabilità

DevSecOps

L'aiuto degli esperti per l'adozione di DevSecOps

Red Hat mette a tua disposizione un ecosistema di partner certificati, esperienza completa e piattaforme innovative per creare, proteggere e distribuire applicazioni in ambienti di cloud ibrido. Abbiamo maturato anni di esperienza nel supportare organizzazioni di livello enterprise, aiutandole a superare le sfide tecnologiche e di business adottando le migliori prassi e tecnologie open source.

Con una catena di distribuzione del contenuto attendibile, il supporto di un team della sicurezza dedicato e backport con funzionalità di sicurezza, le piattaforme Red Hat costituiscono la base ideale per le soluzioni DevSecOps. Offriamo anche **percorsi di formazione e certificazione**, **laboratori interattivi**, **attività di consulenza** e **offerte gestite** con le quali individuare più rapidamente l'approccio DevSecOps più adatto alla tua organizzazione.

Red Hat può aiutarti in qualunque fase del tuo percorso DevSecOps.

Le nostre affidabili piattaforme open source e i servizi offerti dai nostri esperti ti consentono di installare quanto oggi necessario, adeguarlo alle esigenze future e apprendere metodi e approcci indispensabili per adottare DevSecOps in modo efficiente ed efficace.

Scopri di più su perché scegliere Red Hat per DevSecOps.

Sfrutta al meglio l'investimento in DevSecOps

Red Hat Services può fornirti le risorse necessarie per avviare, velocizzare e ampliare le procedure DevSecOps.

- **Red Hat Open Innovation Labs**
  Un servizio di consulenza full immersion in cui clienti ed esperti Red Hat collaborano per apprendere nuove modalità di lavoro, come DevSecOps, puntando a raggiungere gli obiettivi aziendali
- **Red Hat Services Solution: DevSecOps**
  Esperti al tuo servizio per aiutarti ad adottare una software factory mediante un approccio modulare
- **Red Hat Services Journey: Container Adoption**
  Un servizio di consulenza incentrato sull'adozione dei container nei flussi di lavoro principali
- **Red Hat Services Journey: Automation Adoption**
  Un servizio di consulenza che propone un framework per l'adozione e la gestione dell'automazione nell'intera azienda

Una piattaforma per la riuscita delle iniziative DevSecOps

Red Hat OpenShift Platform Plus è la base tecnologica e il framework riconosciuto per DevSecOps. una piattaforma applicativa all'avanguardia, scalabile e funzionale in modo coerente in locale e nell'infrastruttura locale e cloud, Red Hat OpenShift Platform Plus combina una piattaforma Kubernetes enterprise leader di settore con metodi coerenti per costruire, distribuire, eseguire, proteggere e gestire le applicazioni nell'ambiente in uso. Gli strumenti di gestione multicluster forniscono visibilità e controlli completi dei cluster Kubernetes. La sicurezza Kubernetes native e le funzionalità DevSecOps proteggono la catena di distribuzione software, l'infrastruttura e i carichi di lavoro. Infine, un registro scalabile e distribuito a livello globale e funzioni di gestione dei dati del cluster proteggono l'ambiente e le informazioni.

La sinergia tra le interfacce di integrazione open source e **l'ecosistema di partner certificati** di Red Hat consente di utilizzare strumenti di sviluppo, test, operazioni e sicurezza nuovi ed esistenti insieme a Red Hat OpenShift Platform Plus. Molti fornitori offrono **operatori certificati per Red Hat OpenShift** o **container software certificati** che semplificano l'installazione e la gestione dei propri software sulle piattaforme Red Hat. Numerosi prodotti software sono acquistabili e distribuibili direttamente dal **Red Hat Marketplace**. Infine, Red Hat collabora con i principali provider di cloud per fornire **servizi cloud per ambienti Red Hat OpenShift** completamente gestiti, che semplificano il deployment e le operazioni, risparmiando sui costi di creazione interna.

Componenti di Red Hat OpenShift Platform Plus

Red Hat OpenShift

Red Hat OpenShift è una piattaforma applicativa basata su Kubernetes enterprise-ready, che consente di automatizzare le operazioni nell'intero stack per gestire deployment di cloud ibrido, multicloud e all'edge. Include funzionalità specifiche per gli sviluppatori per incrementare produttività e velocità.

Red Hat Advanced Cluster Management for Kubernetes

Red Hat Advanced Cluster Management for Kubernetes è una console che garantisce visibilità all'intero dominio Kubernetes con capacità integrate per la governance e la gestione del ciclo di vita delle applicazioni.

Red Hat Advanced Cluster Security for Kubernetes

Red Hat Advanced Cluster Security for Kubernetes è una soluzione che fornisce funzioni di sicurezza Kubernetes native per migliorare la protezione dell'infrastruttura e dei carichi di lavoro e la visibilità per tutto il ciclo di vita delle applicazioni.

Red Hat Quay

Red Hat Quay, registro di immagini container open source, oltre a offrire capacità di storage, consente di creare, distribuire ed eseguire il deployment di container nei datacenter e negli ambienti cloud.

Red Hat OpenShift Data Foundation

Red Hat OpenShift Data Foundation è una base scalabile per servizi di storage e dati che garantisce efficienza, resilienza e sicurezza dei dati per ambienti Red Hat OpenShift.

Red Hat OpenShift Platform Plus è in grado di offrirti supporto in qualunque fase del tuo percorso di adozione di DevSecOps. Soddisfa le tue esigenze odierne e ti offre una base per progredire assecondando il tuo ritmo.

Funzionalità di sicurezza integrate

Verifica che non ci siano problemi e minacce relativi alla sicurezza nei carichi di lavoro in esecuzione raccogliendo e analizzando i dati a livello di sistema e adottando oltre 60 criteri di sicurezza integrati durante tutto il ciclo di vita dell'applicazione.

Operazioni coerenti

Applica criteri operativi coerenti a sicurezza, configurazione, conformità e governance ai cluster di Red Hat OpenShift, sia su infrastrutture cloud sia nei datacenter locali.

Strumenti per sviluppatori

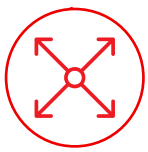
Crea, esegui e distribuisci applicazioni più rapidamente con la libreria inclusa di strumenti, linguaggi, pipeline e framework di creazione supportati. Il framework operatore offre integrazioni per i più recenti strumenti di sviluppo testati e verificati per l'uso con Red Hat OpenShift.

Gestione end to end

Gestisci in modo coerente l'ambiente Red Hat OpenShift con un'interfaccia uniforme, sia per gli amministratori che per gli sviluppatori, che funziona negli ambienti locali, cloud e all'edge, compresi quelli basati su distribuzioni Kubernetes differenti.

Supporto per DevSecOps

Integra la sicurezza dichiarativa negli strumenti e nei flussi di lavoro degli sviluppatori. Sfrutta controlli Kubernetes native per attenuare le minacce, applica criteri di sicurezza e riduci al minimo il rischio operativo.



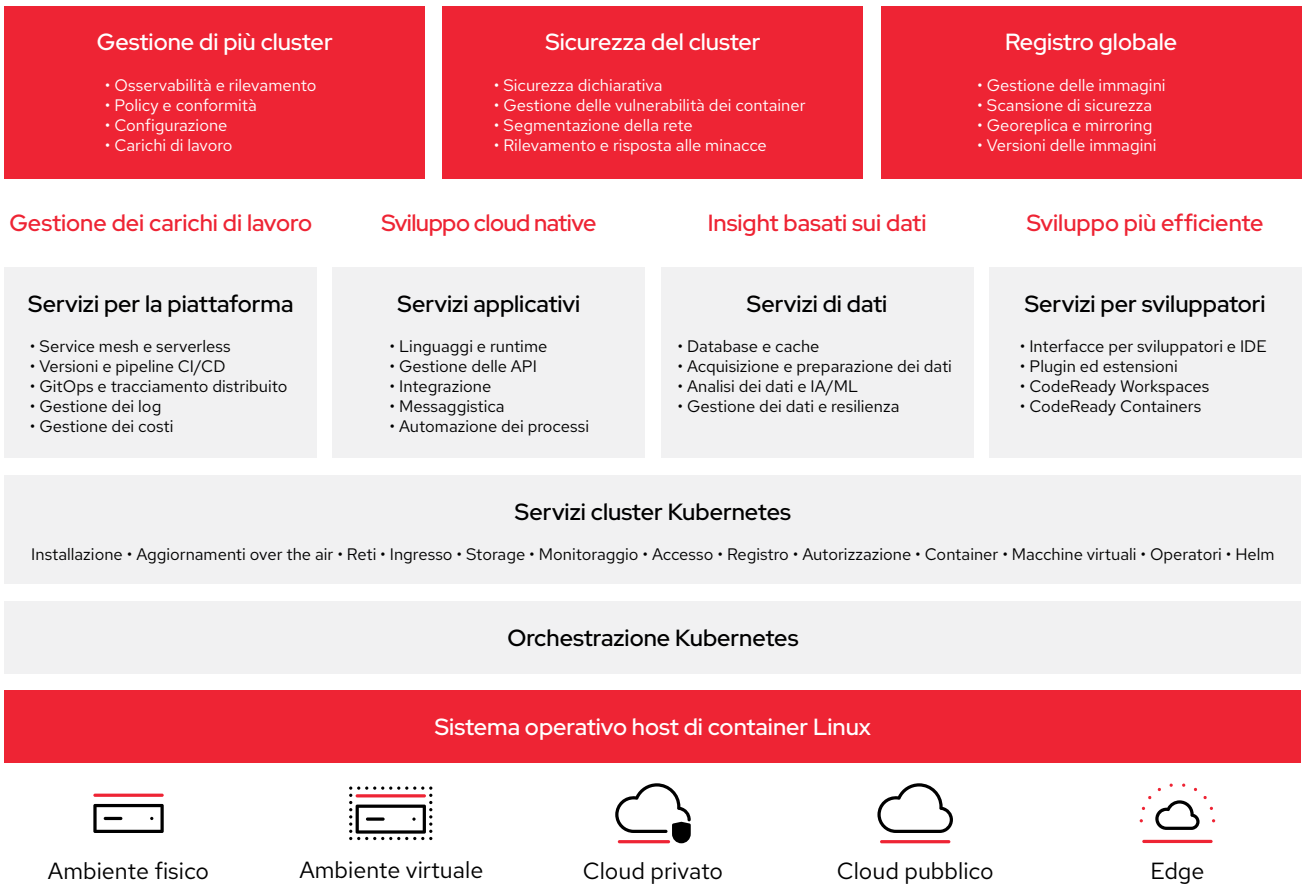
Servizi di dati scalabili

Ottimizza la gestione dei dati nei cluster. Supportando i protocolli per file, blocchi e oggetti, Red Hat OpenShift Data Foundation garantisce storage permanente e resiliente per applicazioni stateful e servizi cluster.

Funzionalità per reti zero-trust

L'implementazione di **reti zero-trust** fornisce comunicazioni resilienti, sicure e osservabili tra applicazioni e servizi. Integrata e inclusa in Red Hat OpenShift, **Red Hat OpenShift Service Mesh** contribuisce a semplificare la protezione delle comunicazioni.

Red Hat OpenShift Platform Plus fornisce le tecnologie e le capacità necessarie per un'adozione DevSecOps efficiente. Leggi la **guida alla sicurezza di Red Hat OpenShift** per scoprire come viene garantita la sicurezza nell'intero stack di tecnologie.



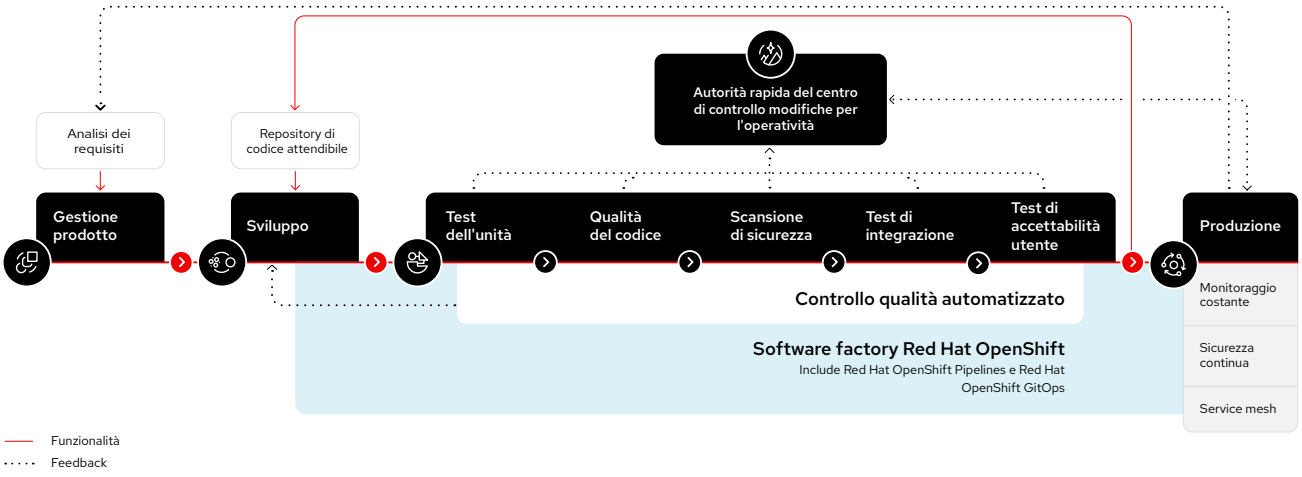
Muovi i primi passi con i servizi cloud Red Hat OpenShift

I servizi cloud Red Hat OpenShift sono disponibili su **AWS**, **Google Cloud**, **IBM Cloud** e **Microsoft Azure**: puoi scegliere l'opzione più adatta alle esigenze della tua organizzazione. Ogni servizio mette a disposizione ambienti completi con tutti i servizi e le tecnologie necessarie, semplici opzioni self service e un supporto esperto sempre disponibile con SLA rigidi.

Leggi la sintesi **Ottieni risultati migliori con i servizi gestiti di Red Hat OpenShift** per saperne di più.

Getta le basi della tua software factory con Red Hat OpenShift Platform Plus

Red Hat OpenShift Platform Plus è una base solida, adattabile e modulare per la tua software factory. Ti consente di incorporare i controlli di sicurezza nelle pipeline CI/CD per fornire agli sviluppatori protezioni automatizzate all'interno dei flussi di lavoro esistenti, per tutelare i carichi di lavoro e l'infrastruttura Kubernetes da configurazioni errate e non conformità e per implementare il rilevamento e la risposta alle minacce nel runtime.



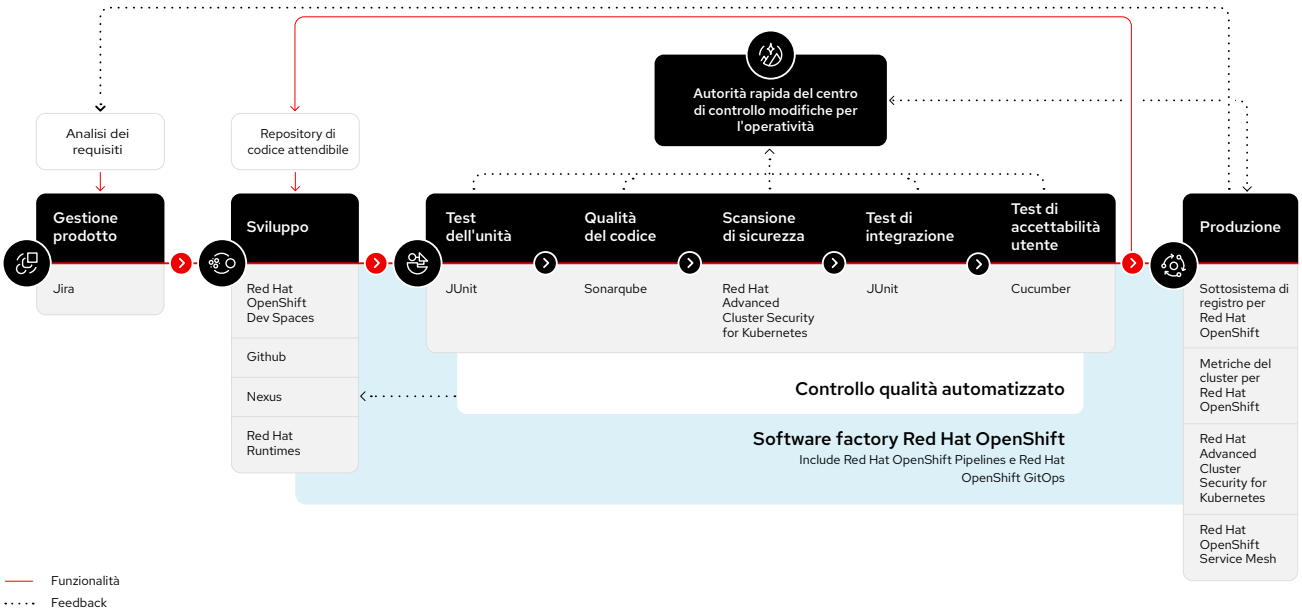
Componi software factory complete con un ecosistema di strumenti di terze parti

Ogni scenario di utilizzo richiede strumenti diversi nell'ambito della software factory. A partire da Red Hat OpenShift Platform Plus, puoi comporre ogni elemento della software factory utilizzando i prodotti e le tecnologie di terze parti che preferisci, tra cui:

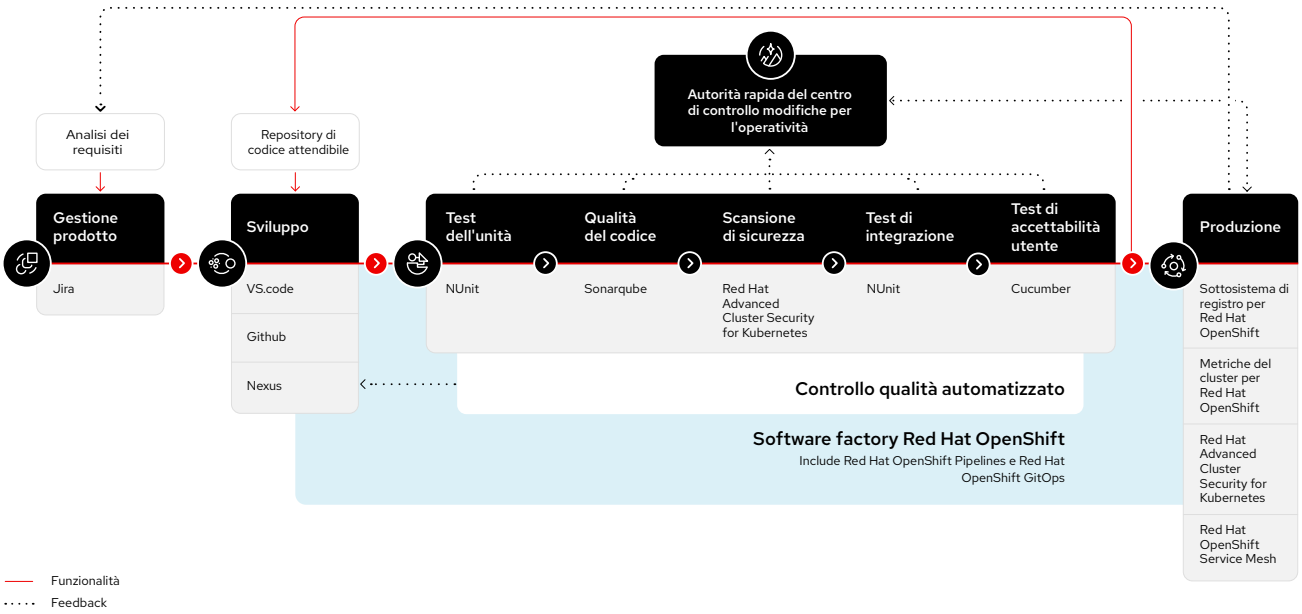
- Strumenti di gestione degli accessi privilegiati.
- Autorità di certificazione esterne.
- Vault esterni e soluzioni di gestione delle chiavi.
- Scanner di contenuti dei container e strumenti per la gestione delle vulnerabilità.
- Strumenti di analisi del runtime dei container.
- Sistemi di sicurezza informatica e gestione eventi (SIEM).
- Strumenti di gestione del controllo della sorgente.
- Repository di artefatti.
- Strumenti di test del software.

Ad esempio, una software factory per lo sviluppo cloud native di applicazioni Spring Boot utilizzerebbe strumenti di runtime, creazione e test diversi da quelli utilizzati da una software factory per applicazioni .Net Core. Alcune delle possibili composizioni per queste due software factory sono illustrate di seguito, e mostrano la flessibilità ottenuta da una software factory fondata su Red Hat.

Software factory per lo sviluppo cloud native di applicazioni Spring Boot basate su microservizi



Software factory per lo sviluppo cloud native di applicazioni .Net Core basate su microservizi



Scelte di successo

Snam, una delle principali reti mondiali per la distribuzione del gas naturale, ha scelto e adottato le tecnologie e i servizi Red Hat, incluso Red Hat OpenShift, Red Hat Quay e Microsoft Azure Red Hat OpenShift per sostenere la trasformazione digitale dell'azienda. Oggi l'azienda distribuisce automaticamente le applicazioni in circa 30 minuti e ha migliorato di 10 volte il tempo di distribuzione dei nuovi prodotti software. Snam ha ottenuto anche una maggiore scalabilità dei carichi di lavoro e delle applicazioni in qualsiasi cloud pubblico o privato, per soddisfare le future esigenze aziendali e ridurre i potenziali rischi di vincoli dei provider cloud.

> Red Hat OpenShift è la chiave di volta del nostro progetto di trasformazione; ci ha consentito di creare una piattaforma IT efficiente, ad alte prestazioni e affidabile, grazie alla quale abbiamo semplificato la gestione di sistemi e applicazioni complessi.

Roberto Calandrini
Head of architecture, Digital and AI Services, Snam

Scopri di più

VodafoneZiggo, una delle maggiori aziende per la fornitura di servizi di intrattenimento e comunicazioni dei Paesi Bassi, ha eseguito il deployment di una piattaforma di cloud ibrido basata su Red Hat OpenShift per unificare l'infrastruttura applicativa dell'organizzazione. L'azienda ha inoltre coinvolto Red Hat Consulting per ottenere aiuto nell'adozione di DevSecOps e per passare a una cultura improntata all'apertura e alla collaborazione. VodafoneZiggo intende garantire una scalabilità più rapida ed efficiente su più cloud e verso l'edge, per adattarsi agilmente alle necessità aziendali e ai cambiamenti del mercato.

> Per noi, Red Hat OpenShift è una base coerente per servizi e applicazioni cloud native con i quali incrementare la produttività ed erogare innovazione continua.

André Beijen
Director, Mobile Network, VodafoneZiggo

Scopri di più

Muovi i primi passi con DevSecOps

Velocità, scalabilità e sicurezza sono fondamentali in un mondo cloud native.

Una software factory basata su Red Hat OpenShift Platform Plus può aiutare a creare procedure DevSecOps ottimali e in grado di accelerare lo sviluppo, semplificare le operazioni e proteggere la tua azienda.

Prova gratis Red Hat OpenShift

cloud.redhat.com/try

Scopri di più su Red Hat OpenShift Platform Plus:

red.ht/openshift-platform-plus

F31657_0522_KVM

Red Hat