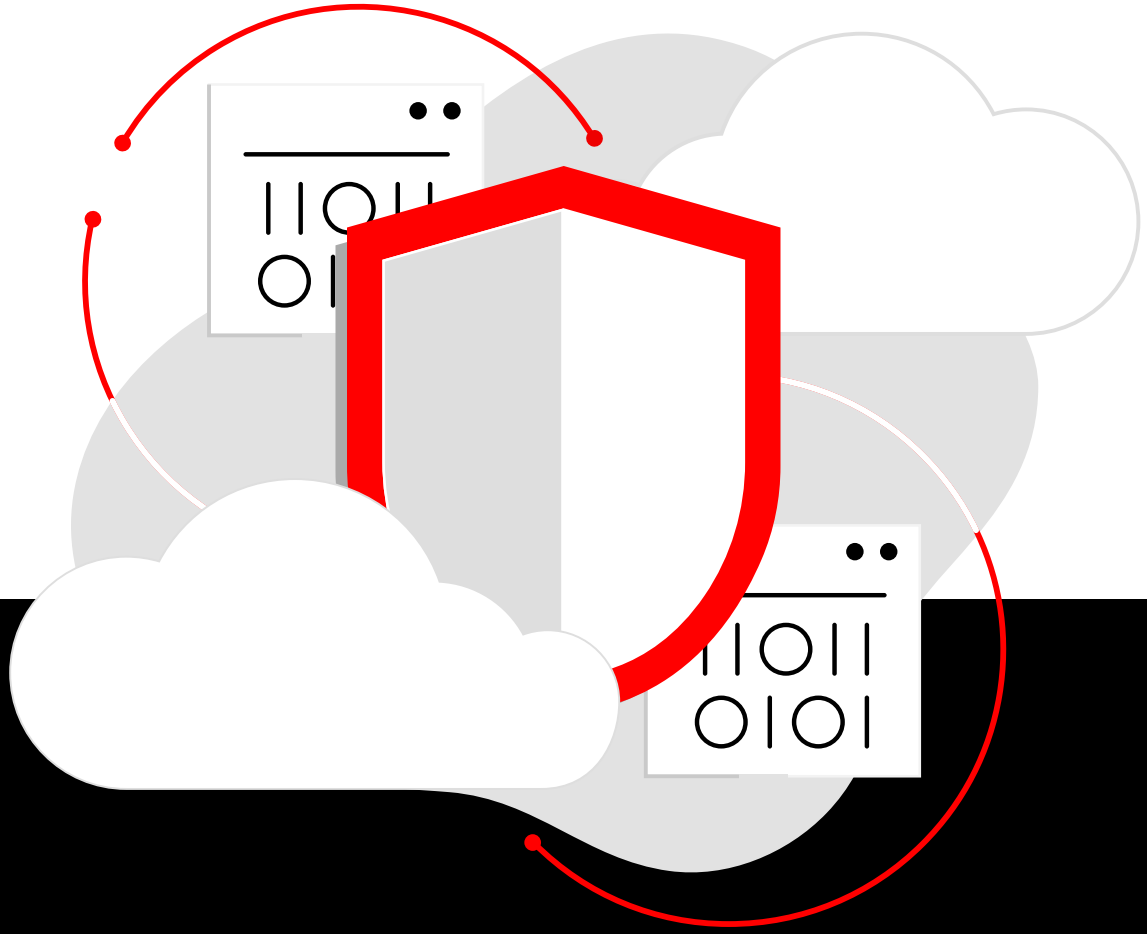
Red Hat



Modernizza e metti in sicurezza il ciclo di vita delle applicazioni con DevSecOps

Contenuti

Introduzione

L'importanza della sicurezza delle applicazioni nel mondo digitale

Mentre le aziende adottano sempre più di frequente le tecnologie basate su cloud, container e microservizi per restare competitive nel mondo digitale, la priorità assoluta resta una: la sicurezza. Di fatto, il 50% dei leader IT senior di grandi aziende indica la sicurezza informatica tra le tre priorità per le iniziative tecnologiche.[1] Allo stesso tempo, l'86% prevede un'accelerazione nel processo di trasformazione digitale della propria azienda nel 2021.[1]

Queste nuove tecnologie richiedono un approccio differente alla sicurezza, poiché le strategie tradizionali con rete perimetrale non sono efficaci negli ambienti distribuiti. Inoltre, le metodologie cloud native e DevOps sono caratterizzate da processi di sviluppo più rapidi e deployment più flessibili, che rendono fondamentale pianificare le misure di sicurezza fin da subito. Adottarle solo alla fine dei cicli di sviluppo, infatti, può generare ritardi nella distribuzione e abbassare il livello di protezione.

L'adozione di approcci e metodi **DevSecOps** contribuisce a proteggere la tua azienda e l'ambiente applicativo in cui operi.

Cos'è la metodologia DevSecOps?

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 tecnologie.

Tramite DevSecOps, la sicurezza diventa una responsabilità condivisa dai vari team, anziché un insieme di attività svolte da un unico team specifico da applicare al termine del processo di sviluppo e deployment. Gli sviluppatori, i team operativi e quelli dedicati alla sicurezza collaborano condividendo informazioni, feedback e approfondimenti e mettendo a disposizione i risultati ottenuti da esperienze pratiche. 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.

I vantaggi dell'approccio DevSecOps

Più sicurezza, meno rischi

Risolvi i problemi legati alla sicurezza nella fase di sviluppo, anziché durante la produzione, per tutelare al meglio le applicazioni e ridurre i ritardi o le interruzioni nel deployment a causa dei mancati controlli delle policy.

Risoluzione più rapida dei problemi di sicurezza

Adotta strumenti e prassi di sicurezza all'avanguardia che agevolino la collaborazione e integrino l'automazione per accelerare i cicli di rilascio, ridurre le tempistiche di risoluzione dei problemi legati alla sicurezza durante la produzione e risparmiare tempo e denaro.

Conformità e visibilità maggiori

Adotta strumenti e processi automatizzati che riducano la possibilità che si verifichino errori manuali e aumentino la prevedibilità e la ripetibilità, al fine di aumentare la conformità e semplificare i processi di audit.

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

Le sfide legate all'adozione delle procedure DevSecOps

Nonostante i numerosi vantaggi, l'integrazione dell'approccio DevSecOps può risultare complicata a causa di alcuni fattori.

- **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 costante.
- **Complessità degli ambienti applicativi.** Non è sempre facile comprendere le connessioni e le implicazioni di sicurezza delle diverse tecnologie (container, microservizi e servizi cloud) che costituiscono gli ambienti applicativi, spesso complessi e di grandi dimensioni.
- **Processi e strumenti in uso poco efficienti.** Molti team adottano le iniziative DevSecOps applicandole inizialmente ai processi e agli strumenti in uso, per poi scoprire che, nel tempo, questo approccio non li aiuta a raggiungere gli obiettivi.
- **Strumenti di sicurezza molteplici.** Selezionare, testare, integrare e gestire gli strumenti di sicurezza più adatti all'azienda richiede tempo, studio e impegno costante.

Cultura, processi e tecnologie sono alla base di un approccio DevSecOps efficace

La messa in sicurezza del ciclo di vita delle applicazioni con la metodologia DevSecOps richiede cambiamenti e coerenza in tre aree: cultura, processi e tecnologie.

Cultura

Promuovi la collaborazione e gli obiettivi condivisi tra i team dedicati allo sviluppo, alle operazioni e alla sicurezza. Aiutali a comprendere perché è importante integrare la sicurezza nel ciclo di vita delle applicazioni e come è possibile farlo.

Processi

Standardizza, documenta e automatizza i processi e i flussi di lavoro per migliorare l'efficienza e la sicurezza del ciclo di vita delle applicazioni.

Tecnologie

Integra le piattaforme, gli strumenti e i processi utilizzati per lo sviluppo, il deployment e l'esecuzione delle applicazioni in un singolo sistema compatto.

Scopri di più sui concetti base dell'approccio DevSecOps

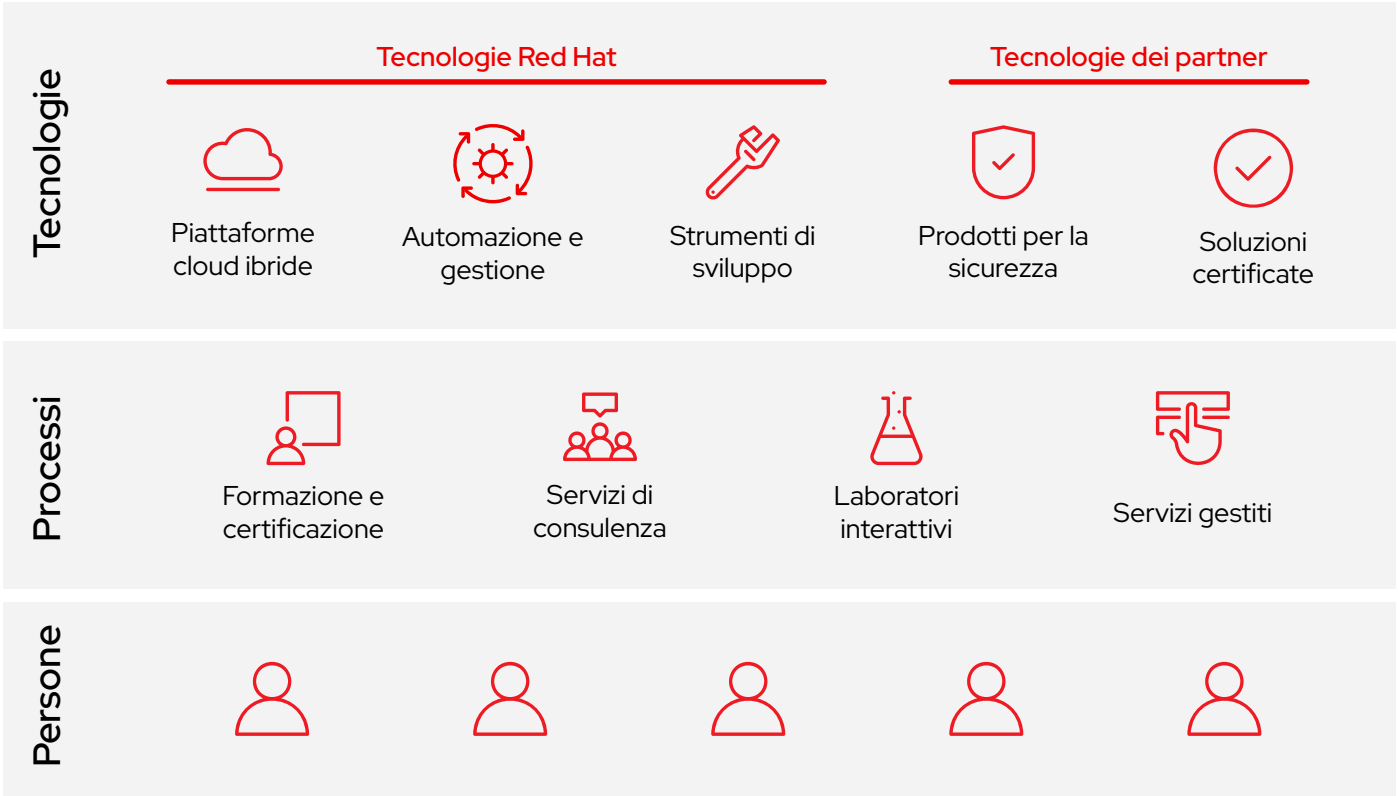
Leggi l'articolo del blog **Why your DevSecOps practice may be falling short** per conoscere le modifiche che è necessario apportare per integrare con efficacia la metodologia DevSecOps. Leggi l'ebook **Incrementa la sicurezza del cloud ibrido** per scoprire come proteggere la tua azienda adottando approcci alla sicurezza cloud native.

La strategia DevSecOps di Red Hat

Red Hat mette a tua disposizione un ecosistema di partner certificati, esperienza e competenze esaustive e piattaforme innovative per creare, proteggere e distribuire applicazioni in ambienti di cloud ibrido. Insieme, questi elementi ti consentono di adottare soluzioni DevSecOps complete per aumentare la sicurezza delle applicazioni, ridurre i rischi, migliorare le prestazioni e massimizzare gli investimenti.

Con una catena di distribuzione dei contenuti 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. Grazie agli innovativi prodotti integrati dei nostri partner puoi ampliare e potenziare questa base per incorporare la sicurezza e l'automazione nel ciclo di vita delle applicazioni. Infine, mettiamo a disposizione **percorsi di formazione e certificazione**, **laboratori interattivi**, **attività di consulenza** e **offerte gestite** con le quali puoi integrare con efficacia l'approccio DevSecOps.

Possiamo aiutarti in qualunque fase del tuo percorso DevSecOps. Le nostre soluzioni modulari espandibili e i servizi offerti dai nostri esperti ti permettono di installare quanto oggi necessario, adeguarlo alle esigenze future e apprendere metodi e approcci indispensabili per adottare DevSecOps in modo efficiente ed efficace.



Crea una base DevSecOps open source con i prodotti Red Hat

Red Hat OpenShift

Red Hat OpenShift® è una piattaforma di cloud ibrido, enterprise ready e incentrata sulla sicurezza, che include strumenti DevOps integrati e funzionalità di sicurezza attive per impostazione predefinita. È pensata per essere utilizzata con tecnologie e strumenti di sicurezza forniti da partner e terze parti per aumentare la sicurezza e integrare strategie DevSecOps resilienti. Leggi la **guida alla sicurezza di Red Hat OpenShift** per scoprire come garantire la sicurezza nell'intero stack di tecnologie.

Provalo gratuitamente

Funzionalità di sicurezza principali

- Security-Enhanced Linux (SELinux)
- Vincoli del contesto di sicurezza (SCC)
- Gestione delle identità e degli accessi
- Crittografia dei dati
- Modalità Federal Information Processing Standard (FIPS)

Red Hat Ansible Automation Platform

Red Hat Ansible® Automation Platform è una piattaforma efficiente e flessibile che consente di automatizzare e integrare le soluzioni di sicurezza, oltre a fornire ai relativi strumenti un linguaggio comune. Scopri gli **scenari di utilizzo dell'automazione**.

Red Hat Enterprise Linux CoreOS

Red Hat Enterprise Linux® CoreOS è un sistema operativo leggero e immutabile, ottimizzato per i container, fondato sulla base incentrata sulla sicurezza di Red Hat Enterprise Linux e utilizzato con Red Hat OpenShift.

Red Hat Quay

Red Hat Quay è un registro di immagini di container distribuito e ad alta disponibilità con cui è possibile creare, distribuire e adottare container.

Red Hat CodeReady Workspaces

Red Hat CodeReady Workspaces è uno strumento che gli sviluppatori utilizzano per programmare, creare e testare nei container in esecuzione su Red Hat OpenShift.

Red Hat Advanced Cluster Security for Kubernetes

Red Hat Advanced Cluster Security for Kubernetes consiste in un'architettura cloud native per la sicurezza dei container che protegge le applicazioni dalla creazione al runtime.

Red Hat Advanced Cluster Management for Kubernetes

Red Hat Advanced Cluster Management for Kubernetes permette di controllare cluster e applicazioni da una singola console, applicando i criteri di sicurezza integrati.

Ottieni flessibilità e affidabilità con un ecosistema di partner certificati per la sicurezza

Un solo fornitore non può offrire tutte le funzionalità necessarie ad adottare in modo efficace e completo l'approccio DevSecOps. Inoltre, ogni organizzazione è un caso a sé e richiede una combinazione ad hoc di prodotti e tecnologie.

Red Hat collabora con **partner all'avanguardia leader nel settore della sicurezza** per offrire soluzioni complete basate su integrazioni certificate, immagini dei container e **operatori Red Hat OpenShift**. Alle aziende è offerta la flessibilità di scegliere i partner, i prodotti e le tecnologie più confacenti alle loro esigenze, con la garanzia che funzioneranno perfettamente insieme. Le soluzioni sono abbinate alla formazione, al supporto e ai servizi degli esperti per assicurare che l'adozione della cultura, dei processi e degli strumenti DevSecOps avvenga con successo.

I vantaggi dei partner di sicurezza di Red Hat

Libertà di scelta

Scegli i prodotti e i fornitori che meglio si addicono alla tua situazione.

Certificazione

Realizza una soluzione personalizzata in tutta sicurezza con la garanzia che i componenti si integreranno perfettamente poiché certificati.

Competenza

Coniuga le competenze e l'esperienza DevSecOps di Red Hat con quelle dei suoi partner per ottenere il massimo beneficio.

Servizi

Integra la cultura, i processi e gli strumenti DevSecOps con il supporto di Red Hat e dei suoi partner.

Formazione

Apprendi le procedure consigliate e acquisisci le competenze necessarie per adottare gli approcci DevSecOps.

Red Hat Vulnerability Scanner Certification

Red Hat Vulnerability Scanner Certification riduce le discrepanze tra i risultati delle scansioni della vulnerabilità. Red Hat collabora con partner di sicurezza certificati per elaborare risultati accurati e affidabili delle scansioni della vulnerabilità dei container per le immagini pubblicate e i pacchetti Red Hat.

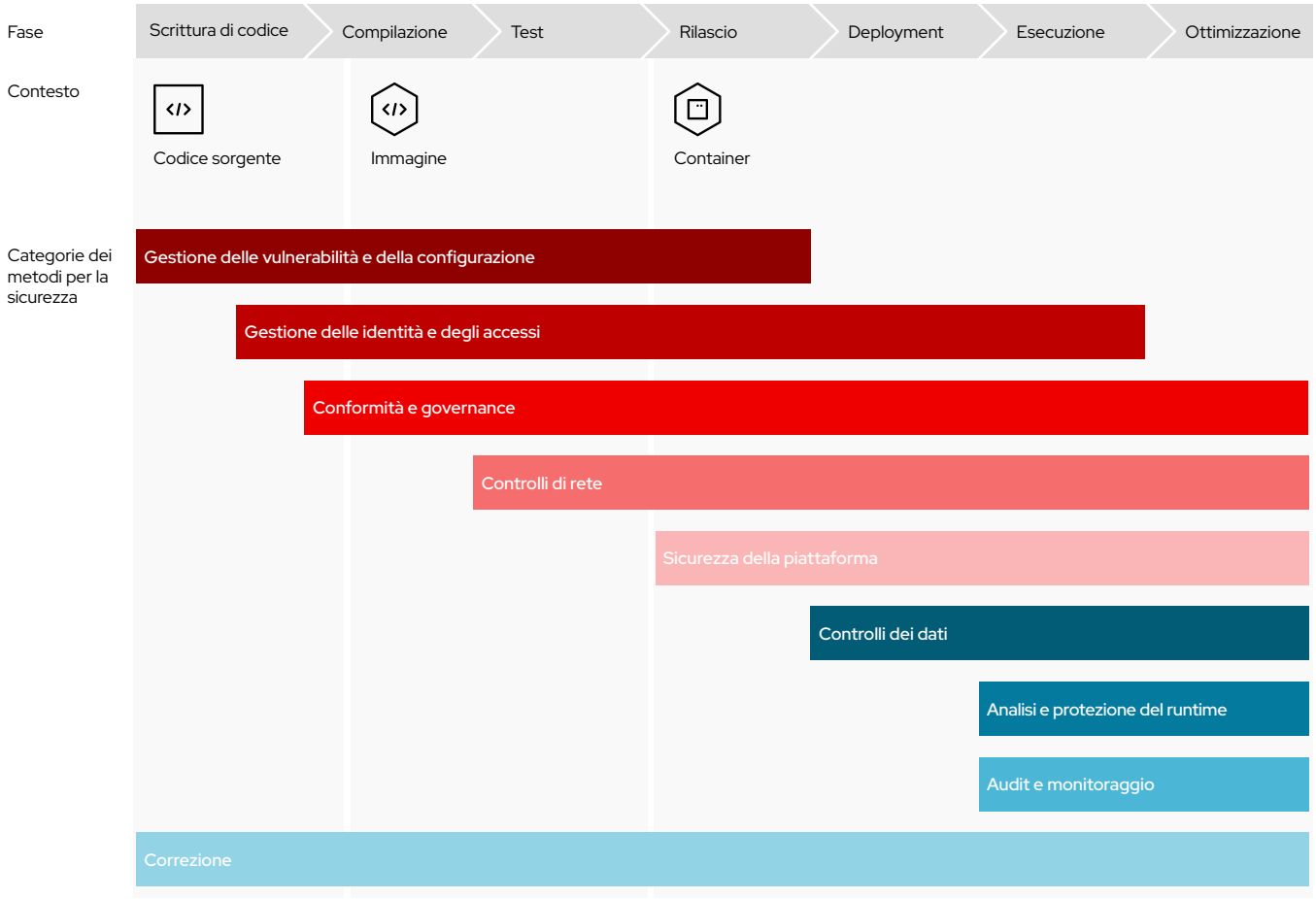
- Riduci al minimo i falsi positivi e altre discrepanze.
- Svincola tempo e budget da dedicare a iniziative e progetti strategici.
- Raggiungi livelli di sicurezza più elevati.
- Migliora la precisione con i dati centralizzati per le immagini pubblicate di Red Hat.
- Semplifica la gestione delle vulnerabilità.

Trova i prodotti certificati

Realizza soluzioni DevSecOps complete

Red Hat offre un framework per la creazione di soluzioni DevSecOps complete e scalabili che soddisfano i requisiti di sicurezza durante l'intero ciclo di vita delle applicazioni. Creato in collaborazione con i nostri partner di sicurezza, il framework agevola l'integrazione DevSecOps in base alle esigenze presenti e future dell'azienda.

Il framework DevSecOps di Red Hat associa un set completo di metodi e strumenti di sicurezza, suddivisi per funzione, all'intero processo di sviluppo delle applicazioni.



Leggi la panoramica

Scegli i prodotti e i metodi per la sicurezza più adatti alle tue esigenze

Il framework DevSecOps di Red Hat suddivide 34 metodi per la sicurezza fondamentali in 9 categorie. Le tecnologie di Red Hat e dei partner certificati sono in linea con uno o più metodi per aiutarti a creare una soluzione DevSecOps completa e flessibile che risponda alle esigenze della tua azienda preparandola al futuro.

Gestione delle vulnerabilità e della configurazione

- Test SAST (Static Application Security Testing)
- Analisi statica del codice (SCA)
- Strumenti IAST (Interactive Application Security Testing)
- Strumenti DAST (Dynamic Application Security Testing)
- Gestione della configurazione
- Rischio immagine

Gestione delle identità e degli accessi

- Autenticazione
- Autorizzazione
- Archivio protetto di segreti
- Moduli di sicurezza hardware (HSM)
- Provenienza

Conformità e governance

- Audit della conformità normativa
- Controlli della conformità e correzione

Controlli di rete

- Plugin CNI (Container Network Interface)
- Criteri di rete
- Controllo del traffico
- Service mesh
- Visualizzazione
- Analisi dei pacchetti
- Gestione dell'interfaccia di programmazione delle applicazioni (API)

Sicurezza della piattaforma

- Host protetto
- Piattaforma container
- Spazio dei nomi
- Isolamento
- Kubernetes e potenziamento dei container

Controlli dei dati

- Protezione e crittografia dei dati

Analisi e protezione del runtime

- Controller di ammissione
- Analisi del comportamento delle applicazioni
- Difesa dalle minacce

Audit e monitoraggio

- Monitoraggio dei cluster
- Sicurezza informatica e gestione eventi (SIEM)
- Diagnostica

Correzione

- Piattaforme SOAR (Security Orchestration, Automation and Response)
- Risoluzione automatica

Trova i partner certificati

Partner in evidenza

Sysdig

Sysdig permette alle organizzazioni di eseguire con facilità i carichi di lavoro nel cloud grazie a tecnologie DevOps incentrate sulla sicurezza. I suoi prodotti per il monitoraggio e la messa in sicurezza di applicazioni, carichi di lavoro e container consentono a centinaia di imprese di distribuire le applicazioni cloud native più velocemente.

Red Hat e Sysdig aiutano le aziende ad adottare rapidamente approcci cloud native. **Sysdig Secure DevOps Platform**, **Sysdig Secure** e **Sysdig Monitor** si integrano con Red Hat OpenShift e **Red Hat Advanced Cluster Management for Kubernetes** per fornire sicurezza, conformità e monitoraggio unificati per ambienti privati, ibridi e multicloud. Grazie a queste soluzioni puoi proteggere le pipeline di creazione, rilevare le minacce e porvi rimedio, verificare costantemente l'integrità e la conformità del cloud, nonché monitorare le prestazioni. Basate su un insieme di tecnologie open source, le funzionalità cloud native di monitoraggio, sicurezza e diagnostica offerte da Sysdig consentono di avere le informazioni e il controllo necessari a passare al cloud in modo più sicuro.

2020
Rising Star Partner of the Year di Red Hat per il settore pubblico[2]

Le soluzioni di Red Hat e Sysdig ti permettono di:

- Effettuare la scansione delle immagini direttamente nelle pipeline di integrazione e deployment continui (CI/CD).
- Monitorare le prestazioni e la disponibilità in più ambienti cloud.
- Mantenere la conformità continua e la sicurezza del runtime.
- Convalidare le configurazioni dell'infrastruttura di Red Hat OpenShift.
- Individuare e risolvere i problemi più facilmente.

Gestione dei rischi per la sicurezza

Individua e correggi le vulnerabilità nelle pipeline. Rileva e blocca le minacce durante il runtime con policy e controlli automatizzati. Risolvi gli imprevisti e analizza le cause anche quando i container non sono più disponibili.

Prestazioni e disponibilità aumentate

Analizza e conserva milioni di metriche. Monitora l'integrità e le prestazioni dell'intero ambiente per rilevare e correggere le vulnerabilità in modo proattivo. Risolvi più facilmente i problemi all'interno di cluster, pod e container.

Verifica della conformità del cloud

Verifica la conformità dell'ambiente Red Hat OpenShift con gli standard comuni. Esamina cluster, nodi e container con report dettagliati sull'attività. Incorpora il monitoraggio dell'integrità dei file nel ciclo di vita dei container.

Accedi alle integrazioni

2 Blog Red Hat, "**Red Hat awards North American partners for commitment to open source innovation**", 23 aprile 2020.

Partner in evidenza

Synopsys

Synopsys offre soluzioni di analisi statica, dinamica e SCA (Software Composition Analysis) per la creazione rapida di software sicuri. Coniugando esperienza, servizi e strumenti leader di settore, Synopsys permette alle organizzazioni di integrare l'approccio DevSecOps per ottimizzare la sicurezza e la qualità nell'intero processo di sviluppo dei software.

Red Hat e Synopsys ti aiutano a creare codice di alta qualità e incentrato sulla sicurezza per ridurre al minimo i rischi e massimizzare la velocità e la produttività. **L'analisi SCA offerta da Black Duck di Synopsys** si integra con Red Hat OpenShift per migliorare la visibilità e il controllo delle vulnerabilità di sicurezza e delle violazioni delle policy nel codice open source all'interno dei container. **Black Duck for OpenShift** rileva, scansiona, monitora e ispeziona automaticamente tutte le immagini dei container nei cluster Red Hat OpenShift per identificare i rischi per la conformità e per la sicurezza open source in qualsiasi fase della realizzazione dei container. Il software assicura anche che i container vulnerabili non arrivino alla fase di produzione, poiché consente di rispondere rapidamente a nuove vulnerabilità che intaccano i container in esecuzione.

La soluzione Black Duck for OpenShift:

- Offre un elenco completo del codice open source di terze parti in ciascuna immagine dei container e annota i pod con metadati su vulnerabilità e policy.
- Segnala immediatamente le nuove vulnerabilità, identificando le immagini e i container interessati.
- Analizza i fork e le backport open source e, all'occorrenza, segnala le vulnerabilità a cui sono state applicate patch, riducendo quelle da investigare.
- **Si integra** con Red Hat Advanced Cluster Management for Kubernetes per assicurare il deployment coerente in tutti i cluster.

Scansione automatica delle immagini dei container

Monitoraggio costante del codice open source

Individuazione delle vulnerabilità di sicurezza

"Synopsys e Red Hat hanno una visione comune sul futuro dello sviluppo e del deployment sicuri delle applicazioni. Insieme intendiamo rafforzare la fiducia delle organizzazioni nelle applicazioni containerizzate."

Vatsal Sonecha
VP of Business Development, Synopsys

Accedi alle integrazioni

Partner in evidenza

Palo Alto Networks

Palo Alto Networks offre prodotti all'avanguardia che supportano la trasformazione digitale in tutta sicurezza, anche quando i cambiamenti avvengono a ritmo sostenuto. Nel portafoglio dell'azienda figurano soluzioni di sicurezza che consentono a oltre 60.000 clienti in tutto il mondo di tutelare la propria attività.

Red Hat e Palo Alto Networks ti aiutano a proteggere il tuo ambiente con sicurezza e conformità cloud native durante l'intero ciclo di vita dello sviluppo. Prisma Cloud di Palo Alto Networks viene utilizzato con Red Hat OpenShift per fornire una gestione completa della situazione della sicurezza del cloud (CSPM) e una protezione del carico di lavoro del cloud (CWP) per i tuoi deployment. La soluzione protegge host, container e architetture serverless durante l'intero ciclo di vita, ma fornisce anche visibilità e governance sul livello di sicurezza dell'azienda.

Partner Red Hat dal

2017

Caratteristiche e vantaggi chiave

Gestione delle vulnerabilità

Incorpora la sicurezza in tutte le fasi del ciclo di vita delle applicazioni, dallo sviluppo alla produzione, con il rilevamento, l'analisi e la prevenzione delle vulnerabilità.

Conformità

Integra e garantisci con facilità la conformità ai benchmark del Center for Internet Security (CIS), ai regimi di compliance esterni e ai requisiti personalizzati.

Sicurezza CI/CD

Incorpora la sicurezza direttamente nei processi di integrazione continua (CI) per individuare e risolvere i problemi prima che intacchino la fase di produzione.

Protezione del runtime

Adotta la sicurezza su larga scala utilizzando il machine learning per creare automaticamente modelli di runtime basati sul principio del privilegio minimo e sui componenti consentiti per tutte le versioni delle applicazioni.

Sicurezza dell'interfaccia e delle applicazioni web

Proteggi il tuo business dalle 10 minacce principali individuate dall'Open Web Application Security Project (OWASP), nonché da quelle di livello 7, negli ambienti cloud pubblici e privati.

Accesso ai controlli

Definisci e monitora i controlli degli accessi per i carichi di lavoro e le applicazioni, integrandoli con gli strumenti di gestione dell'identità, degli accessi e dei segreti già in uso.

Accedi alle integrazioni

Partner in evidenza

CyberArk

CyberArk propone un particolare approccio incentrato sulla sicurezza per il controllo degli accessi privilegiati in base all'identità. L'azienda offre soluzioni complete per la protezione delle credenziali e dei segreti utilizzati da utenti, applicazioni, script e sistemi all'interno di aziende, cloud e ambienti DevOps.

Red Hat e CyberArk ti aiutano a migliorare la sicurezza dei tuoi ambienti container e degli script di automazione. I criteri di sicurezza dell'accesso privilegiato a livello aziendale forniscono visibilità, controllo, applicazione e gestione dei segreti per mitigare i rischi aziendali. I prodotti DevSecOps di CyberArk, inclusi **Conjur Secrets Manager** e **Credential Providers**, si integrano con Red Hat OpenShift e Red Hat Ansible Automation Platform per proteggere, ruotare, monitorare e gestire credenziali privilegiate per utenti, applicazioni, script e altre identità non umane utilizzando una piattaforma centralizzata. Con un solo punto di controllo in tutta l'organizzazione puoi unificare la gestione della sicurezza, ridurre le vulnerabilità, limitare le superfici di attacco e semplificare le operazioni.

L'architettura modulare consente di distribuire ciascun componente in modo indipendente per personalizzare la protezione tra ambienti di cloud ibrido, multicloud, containerizzati e DevOps. L'autenticazione affidabile del runtime e i controlli degli accessi basati sui ruoli fanno sì che solo i pod e i container autorizzati ricevano i segreti. L'integrazione con Red Hat Ansible Automation Platform consente ai playbook di accedere ai segreti gestiti e di eliminare la necessità di inserirli e ruotarli manualmente. Ciò permette anche di automatizzare le attività di correzione in risposta agli imprevisti legati alla sicurezza.

Sicurezza unificata

Centralizza la gestione e la messa in sicurezza dei segreti e delle credenziali di accesso privilegiato all'interno dell'infrastruttura, secondo le tue policy.

Semplificazione delle operazioni

Consenti agli sviluppatori e ai tecnici dell'automazione di mettere in sicurezza, gestire e ruotare i segreti e le credenziali che utilizzano in base alle tue policy.

Più coerenza

Proteggi in modo coerente le credenziali e i segreti utilizzati da applicazioni, script e utenti che accedono alle console di gestione.

Guarda il webinar

Partner in evidenza

Tigera

Tigera trasforma le pratiche di messa in sicurezza e osservazione della rete e dei microservizi Kubernetes da parte delle aziende, nonché la risoluzione dei relativi problemi.

Red Hat e Tigera aiutano le aziende a integrare la sicurezza negli ambienti Kubernetes con il monitoraggio, l'analisi e la gestione del traffico di rete. Certificato con Red Hat OpenShift, **Tigera Calico Enterprise** consente di rendere operative, ottimizzare e proteggere con efficacia le applicazioni containerizzate fondamentali tra più ambienti cloud. L'architettura Kubernetes native integra la soluzione nell'ambiente applicativo, fornendo controlli di sicurezza dettagliati e una maggiore visibilità tra i livelli della rete e dei microservizi. Questa soluzione si combina anche con gli strumenti, gli ambienti e i centri operativi per la sicurezza (SOC) in uso per fornire più controlli e funzionalità per i carichi di lavoro moderni. Migliora la sicurezza delle applicazioni tra gli ambienti di sviluppo, test e produzione con le reti zero trust, i controlli di accesso in uscita, la visibilità del traffico, la protezione e la difesa dalle minacce e i report automatizzati di verifica della conformità.

Funzionalità di sicurezza ampliate

Proteggi le applicazioni con i firewall in uso, la sicurezza basata sul principio dei privilegi minimi e la crittografia del traffico tra pod.

Maggiore visibilità di rete

Accedi ai flussi di rete per eseguire il debug della connettività e della ricerca delle minacce, nonché automatizzare i report sulla conformità.

Conformità garantita

Monitora la conformità delle applicazioni e invia segnalazioni in tempo reale sui carichi di lavoro non conformi.

Accedi all'operatore

Partner in evidenza

Aqua Security

Aqua Security aiuta i clienti a innovare e gestire l'azienda nel modo più agile possibile. Questa azienda offre soluzioni automatizzate di prevenzione, rilevamento e risoluzione delle minacce durante il ciclo di vita delle applicazioni per migliorare la sicurezza nell'intero ambiente.

Red Hat e Aqua Security ti aiutano a gestire e sfruttare la scalabilità dei carichi di lavoro cloud native in maniera più sicura nelle infrastrutture ibride, cloud e in loco. Aqua Cloud Native Security Platform si integra con Red Hat OpenShift per offrire una gestione delle vulnerabilità basata sul rischio, una protezione avanzata del runtime, nonché sicurezza e conformità complete dell'infrastruttura. La soluzione consente ai team dedicati allo sviluppo, alla sicurezza e alle operazioni di distribuire le applicazioni in modo più sicuro, di proteggersi dalle minacce durante il runtime e di valutare e correggere le configurazioni dell'infrastruttura in base ai controlli delle policy.

Caratteristiche e vantaggi chiave

Approcci DevSecOps supportati

- Analizza il codice, le configurazioni e i permessi per le immagini di registro di Red Hat OpenShift su larga scala.
- Dai priorità alle vulnerabilità a seconda del rischio.
- Automatizza i processi di creazione mediante l'integrazione con le pipeline CI/CD.

Applicazioni protette durante il runtime

- Individua e mitiga automaticamente l'attività non autorizzata dei container senza interrompere il funzionamento delle applicazioni.
- Garantisci l'immutabilità dei container con l'individuazione e la prevenzione di variazioni non autorizzate dalle immagini standard.

Catena di distribuzione del software più sicura

- Esegui e convalida le immagini in ambienti di test di preproduzione protetti.
- Individua i malware avanzati che potrebbero non essere rilevati dalle scansioni statiche prima del deployment.

Conformità dell'infrastruttura garantita

- Scansiona e convalida centinaia di policy di controllo e configurazione per la conformità alle pratiche consigliate e ai benchmark del Center for Internet Security (CIS).
- Applica i controlli degli accessi basati sui ruoli (RBAC) mediante policy di sicurezza dichiarativa basate sull'Open Policy Agent (OPA).

Accedi alle integrazioni

Avvia il tuo percorso di adozione dell'approccio DevSecOps

La sicurezza delle applicazioni è un requisito fondamentale per le aziende digitali. L'adozione di approcci DevSecOps contribuisce a proteggere la tua azienda e l'ambiente applicativo in cui operi.

Red Hat coniuga una base tecnologica innovativa, un ecosistema DevSecOps completo e un'ampia competenza per aiutarti a integrare con successo le operazioni DevSecOps in tutta l'organizzazione.

- Scegli i prodotti più adatti alle tue esigenze tra le tecnologie e gli strumenti innovativi e certificati da Red Hat.
- Scopri le procedure consigliate e sviluppa nuove competenze DevSecOps grazie alle risorse di formazione create dagli esperti Red Hat.
- Accelera i deployment grazie alle risorse e ai servizi di consulenza specializzati.

Scopri di più sull'adozione dell'approccio DevSecOps con Red Hat: **redhat.com/it/partners/devsecops**

F29623_0721_KVM

Red Hat