Semplifica la sicurezza del cloud con Red Hat e Microsoft

Red Hat Enterprise Linux on Microsoft Azure offre funzionalità di sicurezza uniformi

Lavora in modo coerente negli ambienti di cloud ibrido e aperto

Red Hat Enterprise Linux offre numerose ottimizzazioni concepite per garantire prestazioni affidabili e orientate alla sicurezza su Microsoft Azure. Costituisce una base operativa coerente per ambienti ibridi e multicloud che permette di eseguire le applicazioni ovunque si ritenga opportuno.

Scopri di più sui vantaggi di Red Hat Enterprise Linux nel cloud.

La sicurezza nel cloud è una priorità

Con la crescente diffusione delle soluzioni cloud, la sicurezza rimane un elemento cruciale per le aziende di ogni dimensione. In effetti, il 79% delle imprese colloca la sicurezza tra le principali sfide poste dal cloud.[1] Queste preoccupazioni sono giustificate: nel 2022, il 45% delle violazioni ha riguardato ambienti cloud.[2]

L'uniformità è al centro delle procedure consigliate in materia di conformità e sicurezza in ogni ambiente. Per proteggere la tua azienda, i controlli degli accessi e i criteri di sicurezza del cloud devono essere alla pari con quelli del datacenter on site. Puoi migliorare la sicurezza e la conformità dell'azienda tramite la standardizzazione della base operativa, che consente di effettuare controlli uniformi nei datacenter e negli ambienti cloud. L'uso di Red Hat® Enterprise Linux® come base operativa negli ambienti Microsoft Azure e on site ti aiuta a creare l'uniformità necessaria a mantenere conformità e sicurezza.

Adotta una base uniforme per la sicurezza e la conformità in tutti gli ambienti

Red Hat e Microsoft integrano funzionalità di sicurezza avanzate in Red Hat Enterprise Linux e Microsoft Azure per aiutarti a mantenere un ambiente di cloud ibrido conforme e incentrato sulla sicurezza. I nostri team di risposta agli incidenti lavorano insieme e in collaborazione con i clienti, i partner e la community open source globale per identificare e risolvere le vulnerabilità.

Microsoft Azure offre funzionalità di sicurezza multilivello per proteggere le operazioni, l'infrastruttura e i datacenter fisici. Le funzioni di sicurezza operativa integrate, invece, come patching live del kernel, aggiornamenti regolari, profili di sicurezza e una catena di distribuzione del software fidata, aiutano a soddisfare i più recenti requisiti di sicurezza e conformità. I parametri predefiniti, che si basano sulle procedure consigliate, garantiscono fin da subito un livello di sicurezza elevato. I set di pacchetti ridotti per le immagini cloud predefinite riducono la superficie di attacco delle minacce alla sicurezza informatica.

Red Hat Enterprise Linux e Microsoft Azure ti permettono di ridurre i rischi, implementare e gestire un sistema di sicurezza su più livelli e semplificare la soddisfazione dei requisiti di conformità negli ambienti di cloud ibrido e aperto. Questa panoramica descrive le principali funzionalità e caratteristiche che consentono l'adozione di una strategia di sicurezza uniforme negli ambienti Microsoft Azure e nei datacenter.

Rileva e correggi le vulnerabilità su larga scala con Red Hat Insights

Nel 2022, il tempo medio per identificare e contenere una violazione dei dati è stato di 277 giorni.[2] Riuscire a ridurre questo intervallo a 200 giorni, o anche meno, può portare a un taglio medio delle spese del 24%.[2] Un monitoraggio quotidiano e uniforme può contribuire a identificare i rischi e prevenire così la violazione dei dati o l'interruzione delle attività aziendali.

1 Flexera, "Flexera 2022 State of the Cloud Report", marzo 2022.
2 IBM Security. "Cost of a Data Breach Report 2022," 2022.

Esegui più rapidamente le attività legate a sicurezza e conformità

Red Hat Insights consente di velocizzare le attività legate a sicurezza e conformità:

- **91%** di tempo in meno per rilevare vulnerabilità di sicurezza[3]
- **69%** di tempo in meno per rilevare violazioni delle policy[3]

Scopri di più su come gestire sicurezza e conformità con Red Hat Enterprise Linux:

- Sintesi sulla gestione dei rischi per la sicurezza con Red Hat Insights
- Demo sulla risoluzione dei problemi con Red Hat Insights
- Demo live sull'utilizzo di OpenSCAP per la conformità alle norme di sicurezza e la scansione delle vulnerabilità

La sottoscrizione a Red Hat Enterprise Linux include l'accesso a Red Hat Insights, una suite di servizi gestiti su Hybrid Cloud Console che esegue un'analisi continua delle piattaforme e delle applicazioni in modo da assicurare e ottimizzare la gestione degli ambienti cloud ibridi. Red Hat Insights sfrutta l'analisi predittiva e una competenza settoriale approfondita per identificare e valutare diversi rischi operativi, a partire dalle minacce alla sicurezza e alla conformità, e suggerire così le correzioni appropriate. È possibile inoltre assegnare una priorità alle attività di correzione in base a gravità, tipo di rischio ed effetti della modifica. Red Hat Insights funziona in ambienti cloud e on site, consentendoti di gestire tutti i tuoi sistemi Red Hat Enterprise Linux da una singola interfaccia. Puoi collegare il tuo account Red Hat a quello di Microsoft Azure e scegliere di connettere automaticamente i sistemi e i carichi di lavoro basati sul cloud a Red Hat Insights e ad altri servizi Red Hat al momento del provisioning.

Red Hat Insights include servizi che consentono di proteggere ambienti di cloud ibrido. Il servizio anti-vulnerabilità consente di scansionare i sistemi per individuare le Common Vulnerabilities and Exposures (CVE), raccogliere i dati dell'analisi e accedere alle istruzioni per la risoluzione dei problemi, il tutto da un'unica interfaccia. Inoltre, il servizio anti-malware permette di identificare rapidamente i sistemi on site e basati su cloud che contengono firme malware attive per prevenire un'esposizione a lungo termine agli attacchi informatici.

All'interno di Microsoft Azure, puoi attivare la gestione della sicurezza e la protezione contro le minacce per Red Hat Enterprise Linux come impostazione predefinita. Queste impostazioni offrono funzionalità integrate di analisi comportamentale e utilizzano tecnologie di apprendimento automatico per identificare attacchi ed exploit zero day. Inoltre, Microsoft Azure monitora le reti collegate alle macchine virtuali e i servizi cloud di Red Hat per individuare modelli di attacco noti e attività successive a una violazione.

Garantisci la conformità alle normative con la scansione e la correzione integrate

Oltre alle violazioni della sicurezza, i problemi di conformità possono determinare sanzioni, danni all'azienda e la perdita di certificazioni. Per le aziende con gravi problemi di conformità, il costo medio di una violazione dei dati è stato di 5,57 milioni di dollari nel 2022,[2] con un incremento di 258.293 dollari rispetto agli ultimi dati disponibili.[2]

Red Hat Enterprise Linux e Microsoft Azure sono prodotti certificati in base a standard governativi e di settore e possono quindi essere utilizzati con sicurezza in ambienti altamente regolamentati. Ad esempio, Microsoft Azure è dotato di oltre cento certificazioni di conformità.

Red Hat Insights include servizi che agevolano la gestione della conformità alle normative in ambienti di cloud ibrido. Con il servizio di policy puoi definire i criteri personalizzati di sicurezza, monitorare i sistemi e, se non risultano conformi, avvisare i team. Inoltre, il servizio di conformità permette di verificare la conformità ai criteri OpenSCAP, correggere i sistemi in caso di mancanze e generare report per la conformità normativa e gli audit di sicurezza. Puoi anche personalizzare le policy predefinite per adattarle al tuo ambiente e ai tuoi processi, in modo da ottenere risultare più accurati. Le principali baseline integrate per le policy comprendono:

- Standard PCI-DSS (Payment Card Industry Data Security Standard).
- Enhanced Operating System Protection Profile (Common Criteria).
- Australian Cyber Security Centre (ACSC) Essential Eight.
- Benchmark del Center for Internet Security (CIS).
- Legislazione HIPAA (Health Insurance Portability and Accountability Act).
- Defense Information Systems Agency Secure Technical Implementation Guidelines (DISA STIG).

3 Principled Technologies, studio sponsorizzato da Red Hat. "Save administrator time and effort by activating Red Hat Insights to automate monitoring", settembre 2020.

Infine, Microsoft Azure Policy ti permette di creare, assegnare e gestire le definizioni delle policy per il controllo e la governance. Esegue la scansione delle risorse cloud e applica regole e azioni basate su policy per garantire la conformità con gli standard aziendali e gli accordi sui livelli di servizio (SLA).

Distribuisci immagini uniformi e affidabili in più ambienti con il generatore di immagini

Oggi il 72% delle aziende implementa una strategia di cloud ibrido[1], che consente di scegliere l'infrastruttura adatta per ogni carico di lavoro. Il rovescio della medaglia, però, è che una più ampia possibilità di scelta significa un incremento della complessità e del rischio di incoerenze, che possono causare problemi in materia di sicurezza e conformità.

Il servizio di generazione di immagini di Red Hat Insights consente di creare, gestire e distribuire le immagini del sistema operativo Red Hat Enterprise Linux negli ambienti di cloud ibrido in modo più semplice e rapido. Puoi realizzare immagini personalizzate e sicure, salvarle come template ed eseguirne il push all'inventario di Microsoft Azure per semplificare il provisioning. In questo modo puoi avere la certezza che la configurazione dei tuoi sistemi sia uniforme negli ambienti Microsoft Azure e nei datacenter.

Verifica l'integrità dei sistemi in più ambienti con l'attestazione remota

Negli ambienti su larga scala altamente distribuiti è fondamentale garantire l'integrità dei sistemi. Eventuali problemi di inaffidabilità e compromissione rendono le aziende vulnerabili agli attacchi di utenti malintenzionati.

Red Hat Enterprise Linux include funzionalità di attestazione remota che verificano lo stato dei sistemi al momento dell'avvio e monitorano costantemente l'integrità dei sistemi remoti. L'attestazione remota, basata sul progetto open source Keylime, si serve del chip hardware integrato Trusted Platform Module (TPM) e del kernel Linux Integrity Measurement Architecture (IMA) per monitorare sistemi su larga scala. Puoi anche inviare file crittografati ai sistemi monitorati e, se non superano il test di integrità, puoi indicare quali azioni automatiche vanno eseguite in risposta.

Proteggi i dati nel cloud con le funzionalità di crittografia avanzate

I dati aziendali sono una risorsa fondamentale che deve essere protetta anche nel cloud.

Utilizzando protocolli di crittografia standard del settore, Microsoft Azure protegge i dati durante il trasferimento verso, da e all'interno dei datacenter Microsoft, così come durante i periodi di inattività in Azure Storage. Red Hat Enterprise Linux include anche il supporto per Network Bound Disk Encryption (NBDE) che semplifica la protezione dei dati inattivi. NBDE sblocca automaticamente i volumi di storage tramite la connessione a uno o più server di rete. In questo modo non devi gestire manualmente le chiavi crittografiche per decrittografare i volumi, che risultano disponibili solo quando sono protetti. Red Hat Enterprise Linux supporta anche NBDE con TPM per garantire l'integrità dei sistemi prima di sbloccare i volumi crittografati.

Implementa le architetture zero trust con più facilità grazie all'identità integrata e alla gestione degli accessi

I nuovi ambienti ampiamente distribuiti e basati su cloud non possono essere protetti con efficacia dalle strategie di sicurezza perimetrali tradizionali. Al contrario, le architetture zero trust sono in grado di applicare misure di sicurezza a ciascuna risorsa, invece di limitarsi a proteggere il perimetro della rete. Non a caso, l'implementazione dell'approccio zero trust riduce del 20,5%, in media, i costi delle violazioni dei dati.[2] La gestione delle identità e degli accessi è il cuore pulsante delle architetture zero trust.

Con Red Hat Enterprise Linux e Microsoft Azure puoi controllare gli accessi ai dati e alle applicazioni grazie a una vasta gamma di meccanismi che sfruttano il principio dei privilegi minimi. Attiva per impostazione predefinita, l'architettura SELinux (Security-Enhanced Linux) per il controllo degli accessi vincolato (MAC, mandatory access control) di Red Hat Enterprise Linux applica la separazione delle informazioni secondo criteri di riservatezza e integrità.

Crea le basi per l'approccio zero trust negli ambienti Linux

Un'architettura zero trust può aumentare il livello di protezione dell'ambiente IT e della tua azienda.

- Scopri di più su come implementare l'approccio zero trust con Red Hat Enterprise Linux.
- Guarda una demo live della gestione degli utenti in Red Hat Enterprise Linux

Velocizza la gestione della sicurezza su più rilasci

L'automazione ti consente di ridurre gli errori manuali e gestire più rapidamente i sistemi.

Guarda una demo live dei ruoli di sistema in Red Hat Enterprise Linux

Red Hat Identity Management, incluso con Red Hat Enterprise Linux, consente di centralizzare la gestione delle identità, nonché di applicare i controlli e gli standard di sicurezza nell'intero ambiente. Offre le funzionalità necessarie per implementare le procedure consigliate per il modello zero trust e semplifica l'infrastruttura di gestione delle identità. È possibile autenticare gli utenti e implementare gli accessi basati sui ruoli (RBAC) o sulle policy tramite un'unica interfaccia scalabile per tutto il datacenter. Red Hat Identity Management può essere integrato con Azure Active Directory (AAD), il protocollo LDAP (lightweight directory access protocol) e altre soluzioni di terze parti attraverso interfacce standard. Red Hat Identity Management supporta anche le tecniche di autenticazione e autorizzazione basate su certificati.

Inoltre, l'autenticazione a più fattori (MFA) di Microsoft Azure semplifica e rafforza la sicurezza con la verifica dell'accesso in due passaggi. I vari metodi di autenticazione (telefonata, SMS o app) contribuiscono a proteggere i dati e le applicazioni, oltre a ridurre la possibilità di accedere con credenziali compromesse.

Semplifica la configurazione e la gestione della sicurezza con i ruoli di sistema

A mano a mano che le dimensioni e la complessità dell'infrastruttura aumentano, diventa più difficile gestirla manualmente. Nel 2022, gli errori di configurazione del cloud sono stati all'origine del 15% degli episodi di violazione dei dati, ciascuno dei quali è costato in media 4,14 milioni di dollari.[2] L'automazione consente di configurare e gestire i sistemi in maniera più rapida, facile e uniforme.

I ruoli di sistema di Red Hat Enterprise Linux, che si basano su Red Hat Ansible® Automation Platform, sfruttano l'automazione per aiutare gli utenti a installare e gestire i parametri di sicurezza su larga scala con un notevole risparmio di tempo. I ruoli di sistema sono compatibili con diversi rilasci di Red Hat Enterprise Linux in più ambienti dell'infrastruttura. Questo ti consente di configurare nuove impostazioni di sicurezza e gestirle su tutti i sistemi con un unico comando o flusso di lavoro.

Scopri di più

Un approccio uniforme alla sicurezza e alla conformità su più ambienti di cloud ibrido aumenta il livello di protezione della tua azienda. La combinazione di Red Hat Enterprise Linux e Microsoft Azure offre una base orientata alla sicurezza per eseguire le applicazioni nel datacenter e nel cloud.

Scopri l'approccio di Red Hat alla sicurezza del cloud ibrido.

Informazioni su Red Hat

Red Hat è leader mondiale nella fornitura di soluzioni software enterprise open source. Con un approccio basato sul concetto di community, distribuisce tecnologie come Kubernetes, container, Linux e cloud ibrido caratterizzate da affidabilità e prestazioni elevate. Red Hat consente di sviluppare applicazioni cloud native, integrare applicazioni IT nuove ed esistenti, e automatizzare e gestire ambienti complessi. Considerata un partner affidabile dalle aziende della classifica Fortune 500, Red Hat fornisce pluripremiati servizi di consulenza, formazione e assistenza, che portano i vantaggi dell'innovazione open source in qualsiasi settore. Red Hat è l'elemento catalizzatore in una rete globale di aziende, partner e community, e permette alle organizzazioni di crescere, evolversi e prepararsi a un futuro digitale.

ITALIA
it.redhat.com
italy@redhat.com

EUROPA, MEDIO ORIENTE, E AFRICA (EMEA)
00800 7334 2835
it.redhat.com
europe@redhat.com

facebook.com/RedHatItaly
twitter.com/RedHatItaly
linkedin.com/company/red-hat

it.redhat.com
295070_0423_KVM