Ottimizza la sicurezza di Linux con Red Hat

Il valore aziendale di Red Hat Enterprise Linux

IDC ha rilevato che le organizzazioni che hanno adottato Red Hat Enterprise Linux per la standardizzazione hanno ottenuto notevoli vantaggi in termini di sicurezza, tra cui:[1]

- Team di sicurezza più efficienti del 33%.
- Aggiornamenti di sicurezza più rapidi del 46%.
- Tempi di risposta alle vulnerabilità di sicurezza ridotti del 47%.

Non tutte le distribuzioni Linux affrontano la sicurezza allo stesso modo

Nel mondo della sicurezza dell'infrastruttura IT, emergono ogni giorno nuove minacce e normative di conformità. La standardizzazione su una base incentrata sulla sicurezza è essenziale per proteggere applicazioni, processi e carichi di lavoro. Sebbene tutte le distribuzioni Linux® siano basate sull'open source, ognuna adotta un approccio diverso alla sicurezza.

Quando si sceglie una distribuzione Linux su cui eseguire la standardizzazione, è importante considerare quanto si è preparati a mitigare i nuovi rischi e soddisfare i requisiti più recenti. Come vengono sviluppate le funzionalità di sicurezza della distribuzione? Con quale efficienza vengono applicate le protezioni della distribuzione agli ambienti? In che modo la distribuzione supporta e migliora il livello di sicurezza oltre il punto vendita, per proteggere l'infrastruttura dalle minacce attuali e future?

Red Hat® Enterprise Linux è un sistema operativo rafforzato basato su oltre 30 anni di esperienza in Linux, offerto da un leader tecnologico a cui si affida oltre il 90% delle organizzazioni Fortune 500.[2] Questa soluzione estende una strategia di difesa *approfondita* allo sviluppo di soluzioni, configurazione, gestione e supporto. Questa panoramica illustra in che modo ognuno di questi elementi contribuisce a un solido profilo di sicurezza e collabora per formare un sistema operativo affidabile e incentrato sulla sicurezza.

Red Hat Enterprise Linux è progettato per un'affidabilità e una sicurezza di importanza strategica

Red Hat è fondato su una base open source di una community globale, decentralizzata e trasparente costituita da ingegneri di tutto il mondo che mettono la sicurezza al primo posto nella tecnologia. Red Hat Enterprise Linux integra un approccio orientato alla sicurezza fin dall'inizio, semplifica l'applicazione delle funzionalità di sicurezza in fase di sviluppo e supporta gli utenti attraverso la vigilanza continua e la correzione delle minacce emergenti.

Un ciclo di vita dello sviluppo software orientato alla sicurezza

Quando si seleziona una distribuzione Linux, è importante considerare gli standard seguiti durante la fase di sviluppo.

Red Hat dà priorità alla sicurezza durante il ciclo di vita dello sviluppo, in linea con gli standard SSDF (Secure Software Development Framework) del National Institute of Standards and Technology (NIST), OWASP (Open Worldwide Application Security Project) e ISO (International Organization for Standardization).

Red Hat Product Security promuove il miglioramento continuo della sicurezza nelle pipeline di produzione di Red Hat, supportando al contempo i sistemi e i team che lavorano per garantire la riservatezza, la disponibilità e l'integrità dei prodotti e dei servizi Red Hat. Per i molti clienti Red Hat che lavorano in settori altamente regolamentati, la sicurezza della catena di distribuzione del software è un requisito prima del deployment.

1 White paper di IDC, sponsorizzato da Red Hat, "The Business Value of Standardizing on Red Hat Enterprise Linux", documento n. US52594324, settembre 2024.

2 Dati sui clienti Red Hat ed elenco della classifica Fortune 500, giugno 2024.

Sicurezza integrata nell'ambiente di produzione

La migliore piattaforma Linux per la tua organizzazione è una distribuzione che consente al tuo team di applicare in modo efficiente le protezioni basate sulle procedure di sicurezza ottimali. Red Hat integra diversi livelli di meccanismi di sicurezza all'interno della sua piattaforma Linux, tra cui configurazioni sicure per impostazione predefinita, controlli degli accessi con privilegi minimi e automazione.

Una delle funzionalità che gli utenti di Red Hat Enterprise Linux possono utilizzare per integrare la sicurezza nelle immagini fin dall'inizio sono i vari profili di sicurezza che offrono configurazioni predefinite. Queste baseline di sicurezza si basano sulle procedure consigliate e consentono agli amministratori di applicare la configurazione in fase di creazione, assicurandosi che il deployment soddisfi i requisiti di conformità e dei criteri di sicurezza aziendali. Ciò non solo riduce i rischi, ma mitiga anche l'errore umano durante quelle che altrimenti sarebbero attività manuali dopo la creazione.

Una roadmap per affrontare le minacce future

Avere un solido livello di sicurezza significa essere preparati alle minacce future ed essere in grado di soddisfare i requisiti emergenti. Alcune distribuzioni Linux potrebbero richiedere agli utenti di affrontare questa preparazione in modo indipendente, lasciando loro il compito di cercare soluzioni della community.

Red Hat Enterprise Linux è supportato da un team di sviluppo e prodotto che osserva attivamente le nuove minacce e sviluppa approcci per prepararsi a fronteggiarle. Questi esperti Red Hat sono membri attivi della community di sicurezza e molti sono coinvolti nel progetto OpenSCAP, un framework open source per il monitoraggio della sicurezza e della conformità dei sistemi Linux.

Aderenza alle richieste globali di conformità regionale

Un altro aspetto importante da considerare quando si sceglie una distribuzione Linux è se sarà in grado di supportare i vari requisiti di conformità richiesti da team e clienti. Supporta una serie di convalide e certificazioni di sicurezza informatica comuni o il tuo team dovrà scoprirlo in seguito?

Nel corso degli anni, Red Hat ha investito in modo significativo per assicurarsi che Red Hat Enterprise Linux fosse in grado di aiutare le organizzazioni a soddisfare i severi requisiti di sicurezza globali della loro regione e per consentire loro di sfruttare le best practice di sicurezza nel modo più efficiente possibile. Con oltre 100 uffici in più di 40 Paesi, il team di Red Hat è consapevole dell'esistenza di numerose normative di conformità che variano da Paese a Paese.

Per soddisfare i requisiti di conformità regionali, Red Hat ha ottenuto un'ampia gamma di convalide e certificazioni per i suoi prodotti e soluzioni, tra cui Red Hat Enterprise Linux.

Metodi di deployment efficienti

Soddisfare i requisiti di sicurezza e seguire le procedure consigliate necessarie può rappresentare un onere per i team di sicurezza. La scansione, la convalida e l'attestazione possono richiedere molto tempo e l'impegno di più team.

La modalità immagine, un metodo di deployment per Red Hat Enterprise Linux, offre un approccio container native per creare, distribuire e gestire il sistema operativo. Ciò significa che i team di sicurezza possono applicare gli strumenti di sicurezza dei container, dalla scansione e convalida alla crittografia e all'attestazione, agli elementi di base del sistema operativo, rendendo le operazioni molto meno complesse. Questo approccio non solo riduce i rischi, ma aumenta anche l'efficienza.

Red Hat Enterprise Linux aiuta i clienti a raggiungere gli obiettivi di sicurezza

Quando l'Università del Sussex aveva bisogno di eseguire la migrazione dei server di importanza strategica verso un sistema operativo completamente supportato, ha collaborato con la società di consulenza IT WM Promus per adottare Red Hat Enterprise Linux, riducendo il rischio di attacchi informatici e ottenendo una certificazione governativa significativa per aver dimostrato una elevato livello di sicurezza operativa.

"L'università dispone di un enorme patrimonio IT. Il passaggio a Red Hat Enterprise Linux ha ridotto al minimo le interruzioni e ha consentito al team di ridurre rapidamente i rischi".[3]

Eileen O'Mahony,
General Manager,
WM Promus

3 Caso cliente Red Hat, "WM Promus helps university boost efficiency and security", 23 ottobre 2024.

Gestione proattiva dei rischi

Il sistema operativo deve consentire ai team di mantenere la consapevolezza costante delle potenziali minacce e dei problemi relativi alla sicurezza in modo semplice ed efficiente.

Red Hat Lightspeed, una soluzione end to end per la gestione dei sistemi integrata in Red Hat Enterprise Linux, aiuta gli utenti a identificare e segnalare i problemi, ad assegnare la priorità ai rischi in base agli effetti potenziali per l'azienda e persino ad avviare l'azione successiva in una toolchain di automazione. Red Hat Lightspeed è in grado effettuare scansioni alla ricerca di Common Vulnerabilities and Exposures (CVE) e di assegnare priorità alle azioni di correzione in base al tipo, alla gravità e all'effetto del rischio.

Può aiutare i tuoi team a essere proattivi verificando la conformità normativa ai criteri OpenSCAP, correggere i sistemi in caso di mancanze e generare report pertinenti. Puoi anche usare Red Hat Lightspeed per identificare rapidamente i sistemi che contengono firme malware attive all'interno dell'ambiente cloud ibrido.

Supporto continuo per la sicurezza

La scelta della piattaforma Linux su cui standardizzare influisce sulla tua azienda per molti anni. Pertanto, è essenziale valutare il tipo di supporto previsto dopo il deployment, anche in futuro.

Gli utenti di Red Hat Enterprise Linux possono operare in tutta sicurezza, sapendo di avere a disposizione 10 anni di aggiornamenti e supporto per le versioni principali, e l'accesso al Red Hat Customer Portal, che fornisce informazioni sulle vulnerabilità di sicurezza in corso e sui passaggi critici che i team possono adottare per mitigare il loro effetto. Il Product Security Incident Response Team (PSIRT) di Red Hat aiuta gli utenti a comprendere i rischi e gli effetti delle CVE emergenti e fornisce indicazioni per la correzione.

Partnership affidabili e una lunga storia di collaborazione

Red Hat collabora con numerosi programmi di divulgazione responsabile coordinati. Con una lunga e documentata partecipazione a organizzazioni di sicurezza come Forum of Incident Response and Security Teams (FIRST), Open Source Security Foundation (OpenSSF), Oasis e altre, Red Hat rimane un partner globale nella collaborazione in materia di sicurezza.

Red Hat è una delle 6 organizzazioni a livello globale a ricoprire un ruolo speciale come partecipante Root con l'organizzazione CVE. Red Hat collabora con CVE.org nella sua missione di identificare, definire e catalogare le vulnerabilità della sicurezza informatica divulgate pubblicamente. Oltre al ruolo Root, Red Hat è anche una CVE Numbering Authority (CNA), che consente a Red Hat di assegnare ID CVE alle vulnerabilità e pubblicare registri CVE. Ciò significa che nel momento in cui a un utente di Red Hat Enterprise Linux viene notificata la presenza di una nuova CVE, un team di esperti di sicurezza che hanno familiarità con la piattaforma è già stato attivamente coinvolto nella ricerca, nella valutazione e nell'indagine sulle eventuali correzioni necessarie.

Condivisione nella community

Anche gli utenti di altre distribuzioni Linux trarranno vantaggio dalle procedure di sicurezza di Red Hat. In linea con l'etica open source, Red Hat crede nella collaborazione della community quando si tratta di risposte rapide, applicazione di patch e strategie di mitigazione delle vulnerabilità che influiscono sul sistema Linux, al fine di mantenere la reputazione di Linux come sistema operativo altamente incentrato sulla sicurezza.

Red Hat collabora con team di tutto il mondo allo sviluppo di procedure di sicurezza open source. Alcuni esempi sono la creazione di OpenSCAP, l'appartenenza a OpenSSF e i contributi a OSV.dev.

Questa collaborazione si estende anche al codice Red Hat: i membri della community possono ispezionarlo, verificarlo e apportare contributi.

Ottimizza la sicurezza di Linux con Red Hat

La standardizzazione su Red Hat Enterprise Linux è supportata da un'azienda che crede nella sicurezza fin dalla progettazione. Scopri in che modo Red Hat può aiutare la tua organizzazione a operare su una piattaforma Linux incentrata sulla sicurezza.

Informazioni su Red Hat

Red Hat è leader mondiale nella fornitura di soluzioni software 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, nonché 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