Garantisci alla tua azienda sicurezza e conformità

Linux: riduci i rischi con una piattaforma open source affidabile

Red Hat

Contenuti

Pagina 1
Linux: una base solida per il futuro della tua azienda

Pagina 2
Un approccio efficace alla gestione dei rischi per sicurezza e conformità

Pagina 3
Identificazione ed eliminazione delle vulnerabilità negli ambienti Linux

Pagina 4
Gestione della conformità negli ambienti Linux

Pagina 5
Procedure ottimali

Pagina 6
Strumenti consigliati

Pagina 7
Ottimizza i livelli di sicurezza e conformità con Red Hat

Pagina 8
Sfrutta gli strumenti di gestione integrati

Pagina 9
Caso cliente in evidenza:
Metalloinvest

Pagina 10
Scopri come garantire sicurezza e conformità

Linux: una base solida per il futuro della tua azienda

Linux® è uno dei sistemi operativi più utilizzati al mondo, in tutti i settori e con gran parte delle tecnologie emergenti.[1] Solitamente viene utilizzato per i carichi di lavoro critici che richiedono alti livelli di affidabilità e disponibilità, nei datacenter e negli ambienti cloud, e supporta una vasta gamma di scenari di utilizzo, sistemi target e dispositivi. Nei marketplace di tutti i provider di cloud pubblico puoi trovare varie distribuzioni di Linux.

Tuttavia, è bene ricordare che la distribuzione di Linux e gli strumenti di gestione che scegli di utilizzare possono influire notevolmente sull'efficienza, sulla sicurezza e sull'interoperabilità del tuo ambiente IT. In questo ebook troverai descritti alcuni aspetti chiave delle vulnerabilità di sicurezza, i rischi per la conformità più comuni negli ambienti Linux, e i nostri consigli su come gestirli.

L'importanza cruciale di sicurezza e conformità per l'ambiente IT

I rischi in ambito di sicurezza e conformità dell'ambiente IT sono motivo di preoccupazione per tutte le organizzazioni. Per il 33% dei CEO gli attacchi informatici costituiscono uno dei principali pericoli che minacciano le prospettive di crescita dell'azienda,[2] e le violazioni della sicurezza possono costare molto care. Una violazione dei dati costa in media 3,86 milioni di dollari.[3]

Come se non bastasse, le normative statali e settoriali continuano a cambiare. Tenere il passo può essere complicato, ma i problemi di conformità possono aumentare del 6% circa il costo di una violazione dei dati.[3]

Conseguenze di una sicurezza inefficace

La velocità costituisce un elemento essenziale per limitare il rischio di violazione e ridurre gli effetti.

3,86 milioni di dollari
Costo medio di una violazione dei dati nel 2020[3]

280 giorni
Tempo medio necessario per identificare e contenere una violazione dei dati nel 2020[3]

1,12 milioni di dollari
Risparmio sui costi ottenibile riuscendo a identificare e contenere una violazione entro 200 giorni[3]

Problematiche comuni di sicurezza e conformità

La gestione della conformità e delle vulnerabilità di sicurezza è ostacolata da molti fattori.

Cambiamento del panorama di sicurezza e conformità

Le minacce alla sicurezza e le norme di conformità si evolvono rapidamente ed esigono una reazione altrettanto veloce.

Ambienti di cloud ibrido e multicloud distribuiti

La distribuzione geografica e la logica di distribuzione possono impedirti di ottenere un quadro completo dell'ambiente IT.

Ambienti ampi e complessi

Nelle infrastrutture di grandi dimensioni vengono spesso utilizzati strumenti diversi per garantire sicurezza e conformità, ma questo complica la gestione dei rischi.

Personale limitato e direttive sul lavoro remoto

La maggior parte delle aziende non dispone di tutto il personale necessario per gestire manualmente le attività di conformità e sicurezza.

1 *Linux Foundation.* "**Linux è il progetto open source di maggior successo della storia**", *accesso effettuato il 24 settembre 2020.*

2 *PWC.* "**23rd Annual Global CEO Survey: Navigating the rising tide of uncertainty**", *2020.*

3 *IBM Security.* "**Cost of a Data Breach Report 2020**," *2020.*

Un approccio efficace alla gestione dei rischi per sicurezza e conformità

Per gestire le vulnerabilità di sicurezza e la conformità è necessario monitorare e valutare i sistemi, allo scopo di verificare che rispettino le policy di legge e sicurezza. L'approccio ideale alla gestione delle vulnerabilità di sicurezza e della conformità dovrebbe consentire lo sviluppo di processi coerenti e ripetibili nell'intero ambiente per:

Valutazione
Identifica i sistemi non conformi o vulnerabili. È necessario valutare agevolmente il livello di sicurezza dell'ambiente, dall'infrastruttura al carico di lavoro, per identificare gli avvisi di sicurezza effettivamente applicabili al tuo ambiente e ai tuoi sistemi.

Definizione delle priorità
Organizza le attività di correzione in base all'impegno richiesto, all'impatto e alla gravità del problema. Utilizza le tecniche di gestione dei rischi per identificare i rischi aziendali effettivamente associati a ciascun problema e pianifica le misure correttive di conseguenza. Per valutare il rischio è necessario determinare la probabilità che un problema dia origine a una violazione, la gravità potenziale di tale violazione e le implicazioni della risoluzione del problema. Potrebbe non avere senso risolvere un determinato problema nei sistemi di sviluppo e test, ma quello stesso problema potrebbe costituire una priorità nei sistemi di produzione.

Correzione
Occorre applicare le patch e riconfigurare in modo semplice e rapido i sistemi che richiedono un intervento. Automatizza i processi di configurazione e gestione delle patch, per accelerare la correzione, garantire coerenza fra i sistemi e ridurre il rischio di errore umano. Se utilizzati efficacemente, gli strumenti automatizzati consentono di raggiungere uno stato in cui è possibile risolvere i problemi velocemente, migliorando la sicurezza dell'ambiente e dell'intera azienda.

Analisi
Verifica che le modifiche siano state applicate e automatizza la generazione dei report sulle correzioni, per semplificare le attività di audit. Un'attività di reporting efficace ti permette di fornire informazioni complete dei dettagli necessari al fine di consentire a dirigenti di alto livello, auditor e team tecnici di comprendere le esposizioni e i rischi attuali per la sicurezza.

Questo approccio consente inoltre di preparare l'azienda ad adottare tecniche di sviluppo e gestione moderne e in rapida evoluzione, come **DevSecOps**. Secondo il 38% delle aziende, la valutazione delle vulnerabilità costituisce l'aspetto della sicurezza più critico per i flussi di lavoro DevOps.[4]

Nelle sezioni successive vengono illustrate le considerazioni e le misure più importanti per gestire più efficacemente i rischi per sicurezza e conformità.

4 451 Research (S&P Global Market Intelligence) - Voice of the Enterprise, DevOps, secondo semestre 2019.

Identificazione ed eliminazione delle vulnerabilità negli ambienti Linux

Per identificare ed eliminare le vulnerabilità è necessario valutare l'infrastruttura allo scopo di trovare e correggere i sistemi che risultano vulnerabili agli attacchi. Tali vulnerabilità possono essere dovute a nuove minacce, patch obsolete o mancanti, o ad errori di configurazione dei sistemi. Gli interventi correttivi includono solitamente l'applicazione delle patch, l'aggiornamento e la riconfigurazione dei sistemi, al fine di eliminare le vulnerabilità.

Perché è importante?

Le vulnerabilità della sicurezza possono causare costose violazioni, con il rischio di compromettere la fiducia dei clienti, la reputazione dell'azienda e i profitti. Infatti, il 39,4% del costo medio di una violazione dei dati è imputabile alla perdita di opportunità commerciali.[5]

Ostacoli che impediscono di identificare ed eliminare efficacemente le vulnerabilità

Nella maggior parte delle aziende manca una strategia di sicurezza coerente per le operazioni su vasta scala.

- Lo scarso personale disponibile è sovraccarico di lavoro e potrebbe non disporre delle competenze necessarie per sviluppare ed eseguire una strategia di sicurezza completa.
- Gli strumenti di scansione della sicurezza generici producono interminabili elenchi di vulnerabilità potenziali, ma non tutte sono applicabili al tuo ambiente e il personale è costretto a dedicare moltissimo tempo alla ricerca delle vulnerabilità e alle azioni correttive.
- L'utilizzo di strumenti manuali per l'identificazione, la correzione e i processi di tracciamento rallentano le operazioni, e le vulnerabilità note rimangono spesso prive di patch.
- I metodi di correzione ad hoc determinano un'applicazione incoerente delle patch e incrementano i potenziali rischi per la sicurezza.

Funzionalità principali degli strumenti di gestione della sicurezza

Per garantire una sicurezza efficace occorre essere in grado di identificare e correggere rapidamente le vulnerabilità dei sistemi prima che si verifichi una violazione. Cerca strumenti unificati di gestione della sicurezza che:

Analizza i sistemi per identificare i rischi, sia a livello di sistema operativo che di carico di lavoro, nei sistemi e nelle istanze di tutto l'ambiente.

Automatizza la correzione dei rischi identificati, per migliorare la velocità, la precisione e l'efficienza dei team IT e di sicurezza.

Sfrutta l'esperienza del fornitore allo scopo di fornire indicazioni sulla correzione per i relativi prodotti, ad esempio tramite semplici misure che consentono di ridurre il rischio.

Accedi regolarmente ai dati più recenti sulle vulnerabilità note e sui rischi per la sicurezza forniti dal sistema operativo e dai fornitori delle applicazioni.

Genera i report relativi a rischi potenziali, azioni correttive e audit, con il livello di dettaglio più appropriato ai diversi tipi di destinatari.

5 *IBM Security. "Cost of a Data Breach Report 2020", 2020.*

Gestione della conformità negli ambienti Linux

La gestione delle conformità ha lo scopo di verificare la conformità dei sistemi alle policy aziendali, agli standard settoriali e alle normative applicabili in un determinato momento. Valuta l'infrastruttura per individuare i sistemi che risultano non conformi a causa delle modifiche apportate a normative, policy o standard, a causa di configurazioni errate o per altri motivi.

Perché è importante?

Oltre alle violazioni della sicurezza, i problemi di conformità possono determinare sanzioni, danni all'azienda e la perdita di certificazioni. I problemi di conformità possono aumentare il costo medio delle violazioni.[6]

Ostacoli a una gestione efficace della conformità

Per gestire la conformità molte aziende utilizzano operazioni manuali e script personalizzati, ma questi processi sono troppo lenti e hanno un impatto limitato rispetto ai moderni ambienti operativi e di sviluppo in rapida evoluzione.

- A causa dei numerosissimi dati di riferimento e standard generici, è difficile comprenderne la rilevanza e l'impatto sull'ambiente.
- I processi manuali rallentano il monitoraggio della conformità, la correzione e le operazioni di audit, determinando un uso inefficiente del tempo a disposizione del personale, un'applicazione incoerente delle policy e un rischio superiore di introdurre problemi di conformità.
- Molte aziende usano diversi strumenti per gestire sicurezza e conformità, ma questo riduce l'efficienza operativa e ostacola la configurazione di policy personalizzate coerenti.

Funzionalità principali degli strumenti di gestione della conformità

Per massimizzare l'efficacia, occorre poter definire e applicare policy contestuali, garantire la conformità dei sistemi con tali policy, oltre a generare e gestire velocemente i report di conformità per gli audit. Cerca strumenti unificati di gestione della conformità che:

Utilizzano l'analisi allo scopo di identificare i rischi per la conformità in modo coerente, senza sprecare tempo.

Correggono automaticamente i sistemi non conformi.

Forniscono un quadro completo del livello di conformità nell'intero ambiente.

Generano automaticamente i report sulla conformità, in base ai tuoi requisiti di auditing e alle esigenze dei destinatari.

Forniscono consigli specialistici e indicazioni contestuali per correggere i sistemi non conformi nell'intero ambiente.

6 *IBM Security. "Cost of a Data Breach Report 2020", 2020.*

Procedure ottimali

Analizza regolarmente i sistemi

Il monitoraggio quotidiano può aiutarti a identificare le vulnerabilità e i rischi per la conformità prima che interrompano le operazioni aziendali e determinino una violazione. Assicurati di utilizzare i dati più recenti sulla sicurezza forniti dal sistema operativo e dai fornitori delle applicazioni per migliorare la precisione delle analisi e configura policy di sicurezza adatte al tuo ambiente e ai tuoi processi, per generare risultati di conformità più accurati.

Identificando e bloccando una violazione in un massimo di **200 giorni** è possibile ridurre notevolmente i costi associati.[7]

Applica e testa le patch di frequente

L'aggiornamento regolare dei sistemi consente di migliorarne i livelli di sicurezza, l'affidabilità, le prestazioni e la conformità. Applica le patch regolarmente e tieniti informato sui problemi importanti in generale. Applica tempestivamente le patch per i bug e i difetti critici. Esegui un test dei sistemi a cui sono state applicate le patch prima del passaggio in produzione.

Uno strumento efficace per la gestione delle patch può accelerare fino all' **88,9%** l'applicazione delle patch ai sistemi.[8]

Adotta soluzioni di automazione

A mano a mano che le dimensioni e la complessità dell'infrastruttura aumentano, diventa più difficile gestirla manualmente. L'automazione consente di semplificare il monitoraggio, accelerare la correzione, migliorare la coerenza e garantire un'attività di reporting regolare.

L'automazione della sicurezza consente di ridurre del **93%** il costo medio di una violazione.[7]

Connetti gli strumenti e allinea i processi

Spesso, negli ambienti distribuiti vengono utilizzati strumenti di gestione diversi a seconda della piattaforma. Integra tali strumenti utilizzando le interfacce di programmazione delle applicazioni (API) e usa le tue interfacce preferite per eseguire attività in altri strumenti. Riduci il numero delle interfacce in uso, per semplificare le operazioni e aumentare la visibilità sulle condizioni di sicurezza e conformità di tutti i sistemi dell'ambiente. Infine, allinea i processi fra i diversi ambienti per aumentare i livelli di coerenza e affidabilità.

Il **52%** delle aziende sta ottimizzando i processi e l'infrastruttura IT per migliorare la sicurezza.[9]

Adotta una strategia di sicurezza continua e coerente

Per ottenere una sicurezza efficace occorre adottare un approccio olistico, che tiene conto di persone, processi e tecnologie. Una strategia di sicurezza continua richiede feedback e adattamento, per supportare le moderne tecniche di sviluppo DevSecOps e le esigenze delle aziende digitali. Adotta un approccio alla sicurezza analitico e stratificato, per sfruttare al meglio le funzionalità di ogni livello del tuo ambiente, inclusi sistemi operativi, piattaforme container, strumenti di automazione, soluzioni Software as a Service (SaaS) e servizi cloud.

L'adozione di un approccio DevSecOps può ridurre del **5%** il costo medio di una violazione dei dati.[7]

7 *IBM Security. "Cost of a Data Breach Report 2020", 2020.*

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

9 *Qualtrics e Red Hat. Studio sull'ottimizzazione dell'IT, febbraio 2020.*

Strumenti consigliati

Gli strumenti ideali per sicurezza e conformità devono fornire numerose funzioni e capacità essenziali.

Analisi proattiva

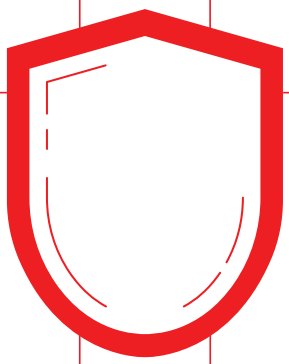
Per migliorare il livello di sicurezza e conformità, occorre innanzitutto conoscerlo. Gli strumenti che eseguono un'analisi automatizzata possono garantire il monitoraggio regolare dei sistemi e l'invio di notifiche in caso di problemi, riducendo il tempo e l'impegno richiesto da parte del personale.

Correzioni prioritarie

Gli strumenti che forniscono istruzioni prescrittive per le correzioni eliminano la necessità di ricercare misure da adottare a posteriori, permettendoti di risparmiare tempo e ridurre il rischio di errore. Attribuendo le priorità agli interventi in base all'impatto potenziale e ai sistemi interessati, è possibile ottimizzare i tempi di correzione.

Risultati personalizzabili

Su alcuni sistemi non è possibile eseguire determinati controlli di vulnerabilità e conformità, a causa di configurazioni, utilizzi e carichi di lavoro specifici. È consigliabile utilizzare strumenti che consentono di definire il contesto aziendale per ridurre i falsi positivi, gestire i rischi e fornire una visuale più realistica delle condizioni di sicurezza e conformità.



Report intuitivi

Utilizzando strumenti che generano report chiari e intuitivi al fine di mostrare quali sistemi sono dotati di patch, quali necessitano di interventi e quali sistemi non sono conformi con le policy di sicurezza, è possibile semplificare le attività di audit e comprendere meglio le condizioni dell'ambiente.

Interfaccia unificata

Utilizzando strumenti che non si limitano alla gestione di un singolo componente o livello dell'ambiente è possibile semplificare le operazioni di sicurezza e migliorare la comprensione dei livelli di sicurezza e conformità. Gli strumenti unificati possono inoltre fornire ulteriore contesto per le scansioni e indicazioni per la correzione.

Un piano d'azione attuabile

Gli strumenti che forniscono informazioni su misura per l'ambiente possono aiutarti a identificare più rapidamente i potenziali problemi di conformità e vulnerabilità di sicurezza, i sistemi interessati e una previsione dell'impatto. Tali strumenti consentono anche di pianificare le azioni correttive e definirne le priorità.

Ottimizza i livelli di sicurezza e conformità con Red Hat

Red Hat adotta un approccio olistico alla gestione dei rischi per la sicurezza e la conformità, che migliora i livelli di velocità, scalabilità e stabilità nell'intero ambiente IT, dai server bare metal a quelli virtualizzati, fino all'infrastruttura di cloud privato, pubblico e ibrido. Integrando persone, processi e tecnologia, le piattaforme Red Hat® aiutano a migliorare l'efficienza operativa, promuovere l'innovazione e aumentare la soddisfazione dei dipendenti.

L'elemento centrale della strategia è costituito da **Red Hat Enterprise Linux**, una piattaforma operativa coerente e intelligente che fornisce una base per i moderni deployment IT e di cloud ibrido, massimizzando i vantaggi per l'azienda. Un'infrastruttura coerente permette di distribuire applicazioni, carichi di lavoro e servizi ovunque utilizzando gli stessi strumenti.

La sicurezza costituisce un elemento fondamentale dell'architettura e del ciclo di vita di Red Hat Enterprise Linux. Per prevenire le violazioni alla sicurezza con un approccio stratificato, sono necessari controlli automatizzati e ripetibili, che consentano di limitare il rischio di esposizione alle vulnerabilità. Gli aggiornamenti critici per la sicurezza e le patch live, forniti nell'ambito della sottoscrizione Red Hat Enterprise Linux, garantiscono un ambiente aggiornato aumentandone la sicurezza.

Gli strumenti di gestione Red Hat si integrano con Red Hat Enterprise Linux allo scopo di offrire le funzionalità necessarie per gestire efficacemente i rischi associati alle vulnerabilità di sicurezza e la conformità.

- Le baseline e gli strumenti configurabili riducono i falsi positivi e forniscono una visione accurata dello stato dell'infrastruttura.
- Le funzionalità di automazione migliorano la configurazione, consentono di gestire le patch in modo più preciso e riducono il rischio di errore umano.
- Le viste personalizzabili consentono di ottenere rapidamente le informazioni giuste al momento giusto.
- La correzione automatizzata e proattiva consente di risolvere i problemi più velocemente, senza richiedere l'intervento del supporto tecnico.
- Una libreria di risorse esaustiva offre un accesso continuo a informazioni dettagliate e specifiche.
- Le opzioni di deployment in loco e Software as a Service (SaaS) consentono di installare gli strumenti nel modo desiderato,

"Per la nostra organizzazione IT è fondamentale implementare server ottimizzati, pronti all'uso e più sicuri fin dal primo giorno. Red Hat Enterprise Linux e Red Hat Insights ci offrono questa possibilità, permettendoci di eseguire il deployment di server che possono essere utilizzati immediatamente, rispondendo alle nostre esigenze specifiche al momento del "go live"."[10]

Steve Short
Platforms Manager, Unix, Kingfisher PLC

10 *Comunicato stampa Red Hat. "**Red Hat Delivers Force Multiplier for Enterprise IT with Enhanced Intelligent Monitoring, Unveils Latest Version of Red Hat Enterprise Linux 8**", 21 aprile 2020.*

Sfrutta gli strumenti di gestione integrati

Gli strumenti di gestione Red Hat sono basati su anni di esperienza in materia di sviluppo e supporto di Linux. Operano in sinergia per semplificare l'amministrazione IT, permettere al tuo team di risparmiare tempo e fatica, oltre a migliorare i livelli di sicurezza, ottimizzazione e affidabilità dell'ambiente.

Red Hat Insights

Analisi predittiva dei rischi IT

Red Hat Insights, incluso in tutte le sottoscrizioni Red Hat Enterprise Linux attive, consente ai team IT di identificare e correggere in modo proattivo una vasta gamma di minacce per evitare interruzioni di servizio, tempi di inattività non pianificati e rischi per sicurezza e conformità.

- Analizza a fondo i sistemi per rilevare proattivamente vulnerabilità di sicurezza, problemi di conformità e violazioni delle policy.
- Indica le azioni correttive prescrittive, con le relative priorità, e genera i playbook Red Hat Ansible® Automation Platform per semplificare la correzione.
- Confronta i sistemi con baseline, cronologie e altri sistemi.
- Semplifica il deployment in ambienti locali e cloud.

96%
Accelerazione del rilevamento dei problemi specifici delle app.[11]

91%
Accelerazione dell'identificazione delle vulnerabilità di sicurezza.[11]

89%
Accelerazione del rilevamento delle divergenze di configurazione.[11]

Scopri di più

Red Hat Smart Management

Gestione e correzione efficaci ed efficienti

Red Hat Smart Management unisce le avanzate funzionalità infrastrutturali di Red Hat Satellite con la semplicità di gestione del cloud, per migliorare e integrare le capacità di Red Hat Insights.

- Consente di applicare patch, eseguire il provisioning e controllare gli host Red Hat Enterprise Linux, oltre che di generare report dettagliati utilizzando Red Hat Satellite.
- Identifica e corregge i problemi tramite cloud.redhat.com e Red Hat Insights.
- Consente di correggere i problemi identificati da Red Hat Insights con la semplice pressione di un pulsante, tramite Cloud Connector.

56%
Aumento dell'efficienza di applicazione delle patch ai sistemi.[12]

14%
Incremento dell'efficienza dei team di sicurezza IT[12]

23%
Incremento della produttività in termini di conformità.[12]

Scopri di più

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

*12 White paper IDC sponsorizzato da Red Hat. "**Red Hat Satellite Helps Enterprise Organizations Optimize Infrastructure with Automation Tools**", marzo 2020. Documento n. US46109220.*

Caso cliente in evidenza

Metalloinvest

Assicurare le prestazioni dei sistemi critici utilizzando informazioni dettagliate sui dati e l'analisi predittiva dei rischi

Sfida

Metalloinvest è un importante produttore e fornitore globale di ferro agglomerato a caldo (HBI, Hot-Briquetted Iron) e prodotti a base di minerali ferrosi, oltre che un produttore locale di acciaio di alta qualità. Dopo decenni di attività Metalloinvest ha dovuto affrontare la nuova sfida di Industry 4.0, la transizione del settore manifatturiero verso le operazioni automatizzate incentrate sui dati. L'azienda desidera gestire e utilizzare le risorse in modo più efficiente, automatizzando e digitalizzando la produzione, puntando a diventare la società mineraria più importante e produttiva del mondo. Allo scopo di gettare una base per Industry 4.0, l'azienda desiderava integrare e ottimizzare il suo complesso ambiente SAP®.

Soluzione

Con l'aiuto di JSA-Group, il suo provider di servizi gestiti, Metalloinvest ha adottato Red Hat Enterprise Linux for SAP Solutions allo scopo di creare una solida base enterprise per il suo ambiente SAP S/4HANA®. Red Hat Enterprise Linux for SAP Solutions, che è stato progettato congiuntamente da **Red Hat e SAP**, include Red Hat Insights, per l'analisi predittiva dei dati, e Red Hat Smart Management, per semplificare la gestione degli ambienti Red Hat Enterprise Linux tramite Red Hat Satellite e servizi cloud gestiti. Questa singola sottoscrizione combina le caratteristiche di affidabilità, scalabilità e alte prestazioni di Linux con una tecnologia in grado di soddisfare le esigenze specifiche delle applicazioni SAP.

Oggi Metalloinvest esegue tutto il suo ambiente di produzione SAP S/4HANA sulle soluzioni Red Hat Enterprise Linux for SAP. L'azienda può sfruttare le informazioni esaustive sui dati e l'analisi predittiva dei rischi allo scopo di garantire prestazioni stabili e affidabili per i suoi sistemi critici, in vista della digitalizzazione del suo ambiente di produzione.

"Red Hat ci offre tutti gli strumenti necessari per aumentare la produttività di operazioni e personale."

Konstantin Zelenkov
Chief Technology Officer, JSA Group

Livelli di affidabilità e prestazioni superiori per i sistemi operativi critici.

Informazioni esaustive sui dati, grazie all'integrazione più efficace di SAP

Rischi inferiori, grazie alla gestione della sicurezza e al supporto completo

Leggi la storia di successo

Scopri come garantire sicurezza e conformità

Le applicazioni e l'infrastruttura IT sono fondamentali per la tua azienda. Adottando approcci e strumenti efficaci alla gestione delle vulnerabilità di sicurezza e dei rischi per la conformità, è possibile migliorare la protezione dell'azienda. Red Hat fornisce la piattaforma Linux e gli strumenti di gestione integrati necessari per le operazioni e l'innovazione incentrate sulla sicurezza.

Aiuta il tuo team a partire nel modo giusto con Red Hat Insights:

redhat.com/insights

Scopri come accelerare i flussi di lavoro IT con Red Hat Insights:

red.ht/insights_savetime

Leggi la sintesi sulla gestione dei rischi per la sicurezza con Red Hat Insights:

red.ht/insights-security-brief

Guarda la demo sulla gestione dei rischi con Red Hat Insights:

red.ht/insights-security-demo

F26049_1120_KVM

Red Hat