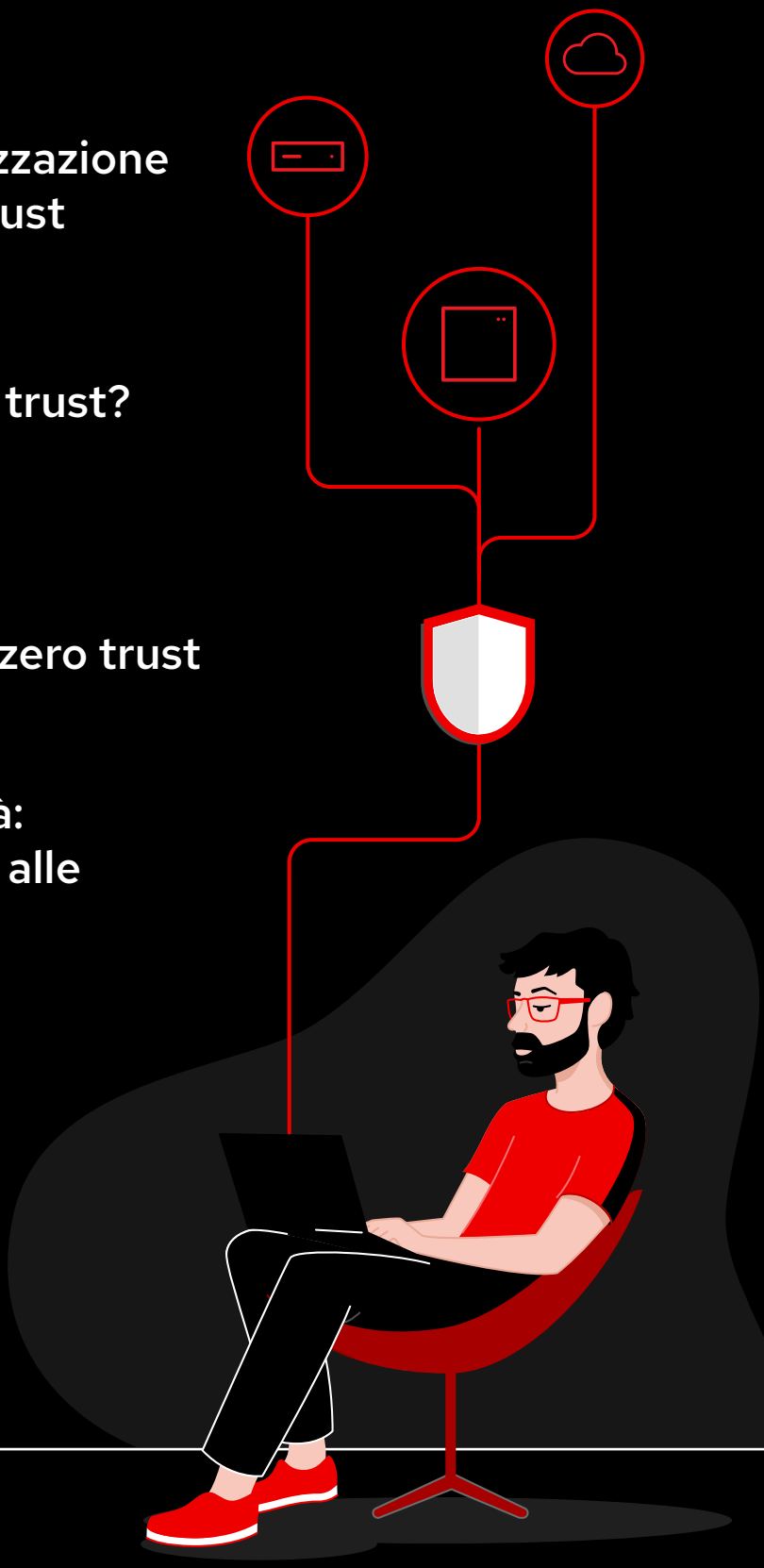
Red Hat
Enterprise Linux

Principali funzionalità di Red Hat Enterprise Linux per la realizzazione di architetture zero trust

Contenuti



Proteggi la tua organizzazione con l'approccio zero trust

Di pari passo al maggior utilizzo dei cloud pubblici, dei dispositivi mobili e del lavoro a distanza, i tradizionali perimetri delle reti aziendali si disgregano, generando nuove problematiche di sicurezza degli ambienti IT.

Sempre più spesso, le organizzazioni devono far fronte a utenti malintenzionati che sfruttano le vulnerabilità dei sistemi, in genere causate da paradigmi di sicurezza datati. Alcuni esempi sono l'autenticazione a un fattore, l'attendibilità implicita, le architetture perimetrali e il tracciamento inefficiente del comportamento di eventi e utenti. L'aumento incessante delle minacce alla sicurezza e dell'impatto delle violazioni impone alle organizzazioni la necessità di una strategia di sicurezza più robusta e proattiva. Di fatto, oltre il 50% dei professionisti della sicurezza informatica considera prioritario il miglioramento della gestione delle identità e degli accessi e l'accesso sicuro alle applicazioni.[1]

L'approccio zero trust trasforma sostanzialmente il modo in cui viene percepita e definita l'attendibilità di una rete, rifiutando il presupposto che tutto ciò che si trova al suo interno sia sicuro e tutto ciò che si trova al suo esterno non lo sia. Il modello tradizionale viene perciò messo in discussione in quanto nessun utente o risorsa può essere considerato implicitamente attendibile, che sia dentro o fuori dal perimetro di rete. Utenti e risorse devono quindi essere costantemente autenticati e autorizzati, a prescindere dalla loro posizione o dal tipo di accesso alla rete.

Le considerazioni offerte in questo ebook ti aiutano a definire le architetture zero trust per gli ambienti Linux®, illustrando come Red Hat® Enterprise Linux può favorire la protezione degli ambienti IT e dell'intera organizzazione.

I costi in un panorama delle minacce in continua evoluzione

4,45 milioni di dollari
Costo medio di una violazione dei dati in diversi settori e regioni nel 2023[2]

180.358 dollari
Riduzione media del costo delle violazioni con l'adozione della gestione delle identità e degli accessi[2]

82%
Percentuale di violazioni che ha coinvolto dati archiviati in ambienti cloud o in più ambienti.[2]

51%
Percentuale di organizzazioni che progetta di aumentare gli investimenti in sicurezza dopo una violazione[2]

1 Report di Cybersecurity Insiders, sponsorizzato da Fortra, "2023 Zero Trust Security Report", 2023.

2 IBM Security, "Cost of a Data Breach Report 2023", luglio 2023.

Cos'è l'approccio zero trust?

Zero trust è un modello architetturale che gestisce la sicurezza a livello di ciascuna risorsa invece che applicarla solo al perimetro di rete o tramite una soluzione centralizzata. Il principio base del modello zero trust è che nessun attore, sistema, rete o sistema che opera dentro o fuori dal perimetro di sicurezza è considerato implicitamente affidabile. Per consentire la connessione tra due risorse, la fiducia viene stabilita in modo esplicito solo quando la sessione viene autenticata e autorizzata.

Come funziona il modello zero trust?

La gestione degli accessi e delle identità è al centro delle architetture zero trust. La loro particolarità è che negano l'accesso alle risorse per impostazione predefinita. Ogni soggetto che vuole interagire con una risorsa deve richiedere l'accesso esplicito per quella specifica interazione. I rischi ad essa collegati vengono valutati prima che l'accesso venga autorizzato. La comprensione dell'identità e degli attributi del soggetto è indispensabile ai fini di questa valutazione. È necessario stabilire chi inoltra la richiesta di accesso, quali sono le risorse coinvolte, qual è lo scopo della transazione e in che modo l'accesso deve essere limitato in base al tempo, al metodo e alla funzione.

Dopo aver preso le decisioni necessarie riguardo all'accesso, bisogna archiviare, gestire, selezionare e aggiornare le identità e i rispettivi attributi in modo sicuro e uniforme. Per gestire queste informazioni, la maggior parte delle aziende impiega uno o più sistemi di server delle directory e di gestione delle identità e delle credenziali. Inoltre, è necessario riesaminare continuamente le decisioni che riguardano gli accessi per garantire che siano ancora valide con il passare del tempo.

Se fondata su questi principi, un'architettura zero trust può aumentare il livello di protezione dell'ambiente IT e della tua azienda.

1. Mai fidarsi implicitamente degli utenti.
2. Utilizzare una strategia di accesso con privilegi minimi.
3. Dare per scontato che le reti e il traffico di rete siano automaticamente compromessi.

Questi principi guidano Red Hat nell'adozione del metodo zero trust nell'intera offerta Red Hat, inclusi Red Hat Enterprise Linux, Red Hat Insights e Red Hat Identity Management.

Cos'è un limite di trust?

Definiamo "limite di trust" qualsiasi separazione logica tra componenti in cui i soggetti che partecipano all'interazione cambiano il proprio stato di attendibilità, alternando in genere tra *attendibile* e *non attendibile*. In genere, la transizione dallo stato *non attendibile* allo stato *attendibile* richiede sia l'autenticazione dell'identità del soggetto sia l'autorizzazione del diritto e dell'esigenza del soggetto ad accedere a una risorsa specifica.

Sistemi operativi: la base dell'approccio zero trust

Il sistema operativo è l'elemento chiave dell'ambiente IT e dell'architettura zero trust, in quanto fornisce le funzionalità di sicurezza essenziali, controlla l'accesso degli utenti e delle applicazioni, crittografa le informazioni sensibili e protegge i segreti, per creare e mantenere l'ambiente di elaborazione focalizzato sulla sicurezza.

In questo capitolo vengono esaminate le funzionalità indispensabili in un sistema operativo per l'adozione del modello zero trust.

Catena di distribuzione affidabile del sistema operativo

I modelli zero trust richiedono un sistema operativo che offra il massimo livello di sicurezza possibile. Per ridurre il rischio di vulnerabilità della sicurezza nel sistema operativo, Red Hat Enterprise Linux viene distribuito tramite una catena di distribuzione del software affidabile. L'analisi statica del codice dell'intero sistema operativo garantisce la conformità con le pratiche consigliate in materia di coding e identifica gli errori a livello di stile di programmazione, metodi di riferimento della memoria e convalida del flusso di input. I test completi di quality engineering (QE) riducono al minimo le falle nella sicurezza prima del rilascio. I processi di patching eseguono regolarmente correzioni delle vulnerabilità note. Le distinte base dei materiali software (SBOM) pubblicate aiutano a verificare e valutare i componenti già selezionati e testati, inclusi codice sorgente, software e librerie open source, middleware e framework di sviluppo che fanno parte di Red Hat Enterprise Linux.

Controllo degli accessi obbligatorio

Per poter adottare un'architettura zero trust, il sistema operativo deve essere in grado di isolare e controllare l'accesso alle risorse su base individuale. Red Hat Enterprise Linux integra in Security-Enhanced Linux (SELinux) i controlli degli accessi obbligatori (MAC), una tecnologia che gestisce gli accessi tramite policy di sicurezza centralizzate, e garantisce il controllo personalizzabile e granulare di file, processi, utenti e applicazioni, per ridurre al minimo il rischio di escalation inappropriate dei privilegi. Al contempo, offre isolamento dei processi e separazione dei container per contenere gli attacchi con escalation dei privilegi. Permette inoltre di negare ogni accesso per impostazione predefinita, applicando i principi zero trust e dei privilegi minimi.

Sperimenta come generare profili di sicurezza SELinux personalizzati per applicazioni containerizzate.

Accedi ai **laboratori interattivi**.

Elenchi di applicazioni consentite

Un elenco di applicazioni consentite è un indice di applicazioni o file eseguibili approvati che possono essere eseguiti su un sistema da un utente specifico. Questa pratica completa i controlli dell'accesso obbligatori, che monitorano il comportamento delle applicazioni ma non sono in grado di valutarne l'affidabilità. Red Hat Enterprise Linux fornisce funzionalità integrate per creare elenchi di applicazioni consentite, come File Access Policy Daemon (fapolicyd), in modo da rilevare e prevenire l'esecuzione di applicazioni non autorizzate su reti o sistemi. Le policy per creare elenchi di applicazioni consentite, predefinite e personalizzabili, garantiscono agli amministratori di sistema maggior controllo sulle applicazioni eseguite su server e reti.

Scopri come approvare le applicazioni con fapolicyd.

Accedi ai **laboratori interattivi**.

Crittografia moderna, scalabile e basata sulle policy

La crittografia del traffico dei dati e della rete aumenta la protezione dell'ambiente IT e dell'intera azienda. Molti standard di settore, inclusi il National Institute of Standards Technology (NIST) e il Federal Information Processing Standard (FIPS) 140, richiedono impostazioni di crittografia estese a tutti i sistemi. I controlli di crittografia basati sulle policy inclusi in Red Hat Enterprise Linux garantiscono l'applicazione uniforme delle configurazioni a tutti i sistemi, facilitando il rispetto dei requisiti aziendali. La conformità è semplificata anche grazie ai profili predefiniti per gli standard di sicurezza comuni, mentre l'applicazione e l'esecuzione automatizzate delle policy permettono di snellire la gestione, ridurre gli errori e controllare la decrittografia di file e volumi software.

Scopri come utilizzare le policy di crittografia a livello di sistema.

Accedi ai **laboratori interattivi sulla configurazione**.

Accedi ai **laboratori interattivi sulla personalizzazione**.

Protezione dei dati in ogni fase

I modelli zero trust richiedono la protezione dei dati attivi, inattivi e in transito. Red Hat Enterprise Linux supporta tecnologie e funzionalità adeguate a garantire la protezione ininterrotta dei dati. I carichi di lavoro e i dati in uso sono protetti da funzionalità Trusted Execution Environment (TEE) e dal supporto Secure Encrypted Virtualization (SEV) per AMD e Software Guard Extensions (SGX) per Intel. La sicurezza dei dati in transito è maggiore con la creazione e la gestione centralizzata e automatizzata di connessioni Transport Layer Security (TLS) crittografate. Infine, Linux Unified Key Setup (LUKS) e Network Bound Disk Encryption (NBDE) garantiscono una protezione dei dati coerente negli ambienti di cloud ibrido.

Radice di attendibilità hardware

Tecnologie come le radici di attendibilità hardware, le attestazioni remote e la misurazione dei componenti dei processi di avvio consentono di verificare che i sistemi siano integri, non modificati né manomessi. Red Hat Enterprise Linux offre funzionalità che supportano queste tecnologie.

- Sposta i segreti crittografati fuori dal software e su dispositivi hardware sicuri come smart card, moduli di protezione hardware (HSM) e tecnologia Trusted Platform Module (TPM).
- Utilizza le funzionalità TPM e di misurazione dei componenti di avvio per elaborare e archiviare con la crittografia le misurazioni con hash dei processi di avvio protetti e dei fine binari di runtime.
- Verifica le misurazioni dei componenti di avvio con agenti di attestazione remota per controllare l'eventuale compromissione dei sistemi prima di avviare le azioni di correzione appropriate.

Scansioni di conformità

La mancata conformità alle norme e agli standard aziendali e di settore può portare la tua impresa a incorrere in costi e rischi indesiderati. Red Hat Enterprise Linux include strumenti di analisi della conformità e delle vulnerabilità, come Open Security Content Automation Protocol (OpenSCAP) che aiutano ad automatizzare e semplificare gli audit, a individuare e correggere i sistemi con configurazioni errate e a gestire la conformità con meno difficoltà. Tra le funzionalità incluse:

- Profili di conformità predefiniti e personalizzabili.
- Funzionalità di generazione di report e baseline.
- Integrazione con Red Hat Satellite e Red Hat Insights per gestire la conformità in modo scalabile.
- Baseline di sicurezza integrate per Payment Card Industry Data Security Standard (PCI-DSS), Enhanced Operating System Protection Profile (OSPP), Australian Cyber Security Centre (ACSC) Essential Eight, Center for Internet Security (CIS) Benchmark, Health Insurance Portability and Accountability Act (HIPAA), Defense Information Systems Agency Security Technical Implementation Guides (DISA STIG).

Prova OpenSCAP per la conformità alle norme di sicurezza e la scansione delle vulnerabilità.

Accedi ai **laboratori interattivi**.

Scopri come correggere le vulnerabilità con Red Hat Insights.

Accedi ai **laboratori interattivi**.

Gestione automatizzata della configurazione

Per mantenere la coerenza tra le configurazioni di sicurezza e garantire sicurezza e conformità in modo scalabile, l'automazione è imprescindibile. I ruoli di sistema di Red Hat Enterprise Linux facilitano l'automazione delle attività di gestione e configurazione della sicurezza negli ambienti di cloud ibrido, semplificando l'implementazione dell'architettura zero trust anche ai meno esperti. I contenuti di automazione predefiniti di Red Hat Ansible® Automation Platform semplificano la configurazione di funzionalità di sicurezza come SELinux, NBDE, Secure Shell (SSH), e della gestione delle policy di crittografia, identità e certificati.

Prova i ruoli di sistema di Red Hat Enterprise Linux

Accedi ai **laboratori interattivi**.

Gestione delle identità: controllo degli accessi alle risorse IT

Le soluzioni di gestione delle identità (IdM) garantiscono l'accesso alle risorse necessarie esclusivamente agli utenti autorizzati. Fornendo policy e tecnologie valide per l'intera organizzazione, queste soluzioni gestiscono l'identificazione, l'autenticazione e l'autorizzazione degli accessi alle risorse tramite identità, attributi, credenziali e certificati.

In questo capitolo vengono esaminate le funzionalità di gestione delle identità per l'adozione del modello zero trust.

Archivio di identità

Un controller di dominio consente di gestire identità, accesso e policy per gli utenti, i servizi e gli host. Incluso in Red Hat Enterprise Linux, Red Hat Identity Management è costituito da un archivio di identità e da un controller di dominio centralizzati, che consentono di ridurre il lavoro amministrativo, semplificare la gestione della sicurezza e garantire un ambiente uniforme. La soluzione permette l'archiviazione di tutte le identità in un'unica posizione, la riduzione del numero di operazioni e l'applicazione uniforme delle policy a risorse e ambienti. La registrazione dei domini semplificata consente di creare un confine di sicurezza affidabile, mentre l'autenticazione ottimizzata migliora l'esperienza complessiva degli utenti.

Single sign-on

Nelle architetture zero trust, ogni servizio, dispositivo e server richiede un'autenticazione di accesso separata. I sistemi single sign-on (SSO) semplificano l'accesso tramite un servizio di identità centrale per consentire ai server di controllare gli utenti verificati. Red Hat Enterprise Linux supporta OAuth 2.0 e Red Hat Identity Management, permettendo agli utenti di accedere a più servizi autenticandosi una volta sola, per un'esperienza ottimizzata. Grazie all'integrazione con diversi servizi, tra cui la tecnologia single sign-on di Red Hat, Microsoft AzureAD e GitHub, potrai continuare a utilizzare i servizi di identità già esistenti e ottenere più flessibilità per le scelte future.

Integrazione con altri sistemi di gestione delle identità

La maggior parte delle organizzazioni utilizza già uno o più sistemi di gestione delle identità per gli ambienti Linux e Windows. L'integrazione di questi sistemi in un'unica soluzione generale contribuisce a centralizzare le operazioni, a garantire l'uniformità a livello aziendale e a migliorare l'efficienza gestionale. L'integrazione nativa tra Red Hat Identity Management e Microsoft Active Directory facilita la gestione delle identità negli ambienti misti e l'applicazione delle policy di controllo degli accessi direttamente al tuo dominio Red Hat Enterprise Linux.

Gestione delle policy

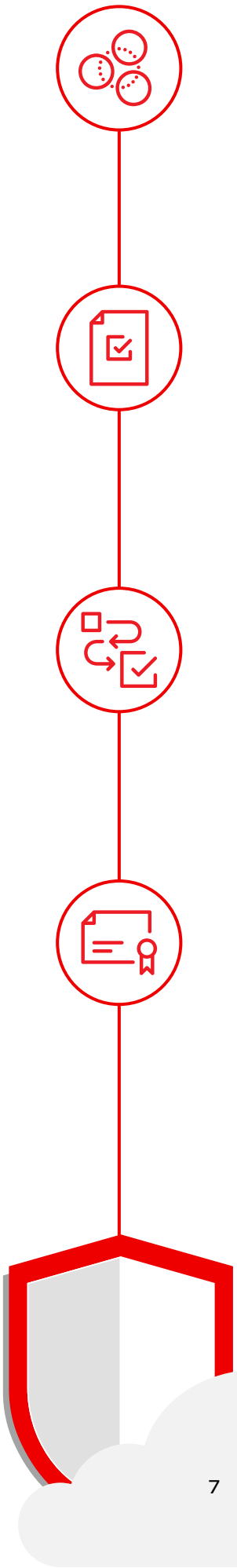
Un approccio alla gestione delle identità basato sulle policy può migliorare l'uniformità, l'efficienza e la sicurezza. Con Red Hat Identity Management puoi impostare e applicare controlli basati sulle policy da un'interfaccia centralizzata per garantire la configurazione corretta di identità, accessi e risorse. Le policy di identità e accesso personalizzabili aiutano a limitare la possibilità di escalation dei privilegi negli ambienti. Il controllo degli accessi basato sui ruoli (RBAC) permette di delegare l'amministrazione delle attività dei server delle identità, tra cui la gestione delle autenticazioni e delle autorizzazioni, la registrazione delle sessioni, gli audit e le registrazioni.

Autenticazione a più fattori

L'autenticazione a più fattori (MFA) aggiunge un livello di sicurezza supplementare che prevede la verifica con più metodi di autenticazione prima di poter accedere al sistema. Red Hat Identity Management supporta l'autenticazione MFA tramite dispositivi di crittografia, come i token hardware e le smart card. Puoi anche selezionare e configurare diverse tipologie di autenticazione, tra cui password, certificati, Remote Authentication Dial-In User Service (RADIUS), password temporanee (OTP), e Public Key Cryptography for Initial Authentication (PKINIT), oltre a impostare metodi di autenticazione predefiniti per tutti gli utenti.

Gestione dei certificati

I certificati digitali contengono le informazioni necessarie per autenticare l'identità di utenti, applicazioni, siti web e altri soggetti. Devono essere creati, monitorati, rinnovati ed eliminati a seconda del principio del privilegio minimo. Red Hat Identity Management supporta la gestione del ciclo di vita completo per i certificati di utenti, host e servizi. Puoi inoltre distribuire Red Hat Certificate System, un'autorità di certificazione che supporta attività di gestione avanzate come il provisioning delle smart card, i certificati personalizzati e lo storage segreto protetto. Il supporto per i protocolli e gli standard più diffusi, inclusi X.509, Automatic Certificate Management Environment (ACME), Simple Certificate Enrollment Protocol (SCEP), Secure Sockets Layer (SSL) e TLS permette di creare certificati per l'intero ecosistema IT. Il tracciamento automatico delle date di scadenza dei certificati garantisce la tempestività dei rinnovi, mentre l'autenticazione PKI verifica l'attendibilità delle identità.

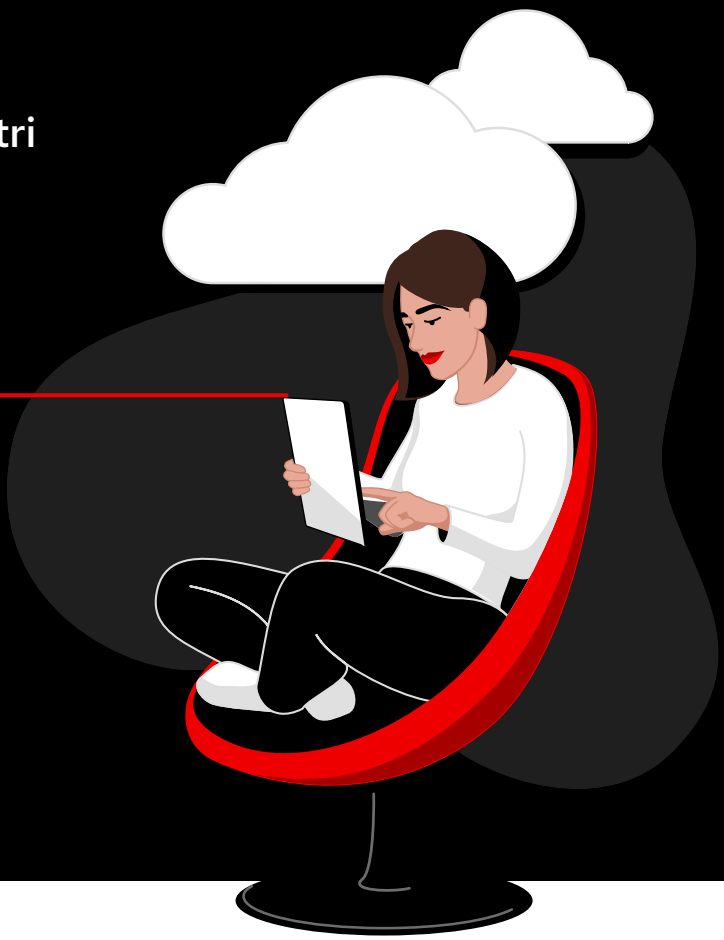


Adotta l'approccio zero trust

L'adozione di un'architettura zero trust ti aiuta a proteggere gli ambienti IT e le risorse aziendali in un panorama in continua evoluzione.

Red Hat ti offre una base affidabile, integrata e incentrata sulla sicurezza per le tue architetture zero trust. È probabile che la tua azienda stia già utilizzando molti dei componenti necessari per adottare un modello zero trust. Red Hat Enterprise Linux offre tecnologie di sicurezza, controlli, certificazioni e supporto per la progettazione, la realizzazione e la gestione di architetture basate sull'approccio zero trust. Red Hat Identity Management consente di centralizzare la gestione delle identità e applicare i controlli e gli standard di sicurezza nell'intero ambiente.

Provalo subito con i nostri **laboratori interattivi gratuiti e su web**.



568051_0124_KVM

Red Hat