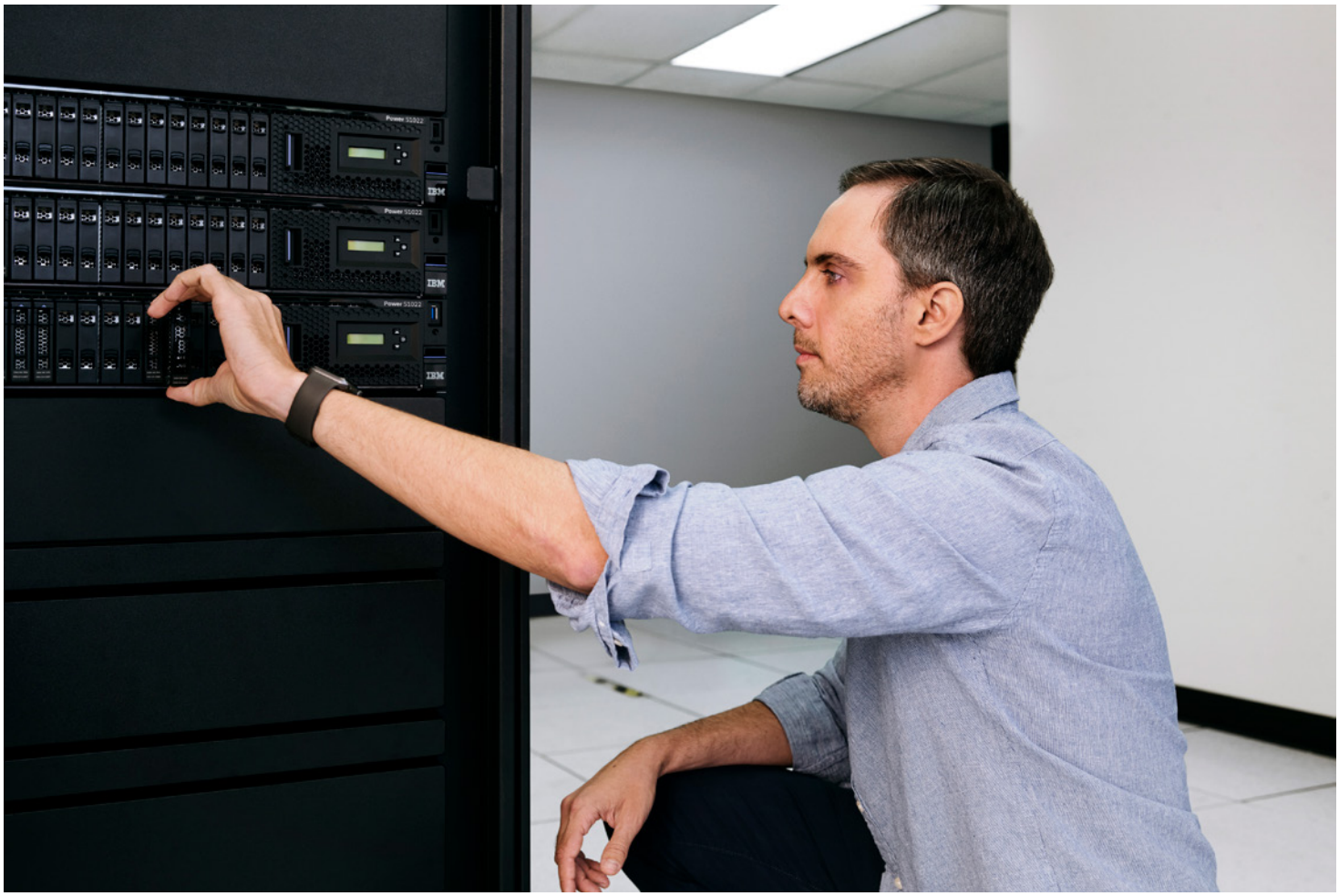
Un approccio multilivello alla sicurezza con IBM Power

Infrastruttura essenziale per un approccio Zero Trust



Sommario

L’IT aziendale nell’era degli attacchi informatici avanzati

Il panorama IT di oggi

Fin dall’inizio della pandemia di COVID-19 è stato registrato un numero impressionante di devastanti violazioni dei dati. Il costo medio di una violazione dei dati è oggi pari a 4,24 milioni di dollari, il 10% in più rispetto al dato di 3,86 milioni di dollari dello scorso anno. Rappresenta l’incremento più consistente a cui il settore abbia assistito negli ultimi sette anni[1], rendendo la sicurezza una preoccupazione primaria. Migliorare la propria strategia di sicurezza e consentire al proprio business di muoversi in modo rapido, sicuro e protetto in questo mondo che non conosce pause è oggi l’interesse primario di molti dirigenti, con un conseguente aumento del budget destinato alla sicurezza. Tuttavia, l’aumento della spesa e il cambiamento tecnologico introducono complessità e rischi inediti che continuano a minacciare la sicurezza IT. Una delle maggiori preoccupazioni dei professionisti della sicurezza è il crescente numero di vettori di attacco sofisticati che continuano a esporre più aspetti delle aziende di oggi rispetto al passato.

Le vulnerabilità a livello hardware e firmware potevano non essere motivo di grande preoccupazione in un passato non troppo lontano; ora, invece, sono diventate obiettivi primari nel panorama odierno delle minacce.

Per molti versi, le sfide di sicurezza informatica che la tua azienda deve affrontare oggi possono essere ricondotte a due verità empiriche:

- Lo stack IT si espande e gli hacker stanno ampliando i loro orizzonti.
- Le organizzazioni devono anticipare le minacce future per proteggere le proprie piattaforme con il massimo livello di sicurezza per salvaguardare l’infrastruttura di cloud ibrido.

4,24 milioni di dollari

Il costo medio di una violazione dei dati è oggi pari a **4,24 milioni di dollari**, il 10% in più rispetto al dato di 3,86 milioni di dollari dello scorso anno.

Le realtà del panorama delle minacce attuali

Un approccio olistico

Le aziende si avvalgono dei propri sistemi di sicurezza per prevenire le minacce attuali e future alla proprietà intellettuale, alle informazioni aziendali sensibili, ai dati dei clienti e alla privacy dei carichi di lavoro.

Il modo in cui i professionisti approcciano strategicamente la sicurezza IT è fondamentale per prevenire le violazioni dei dati e gli attacchi informatici. Oltre a causare tempi di inattività, le vulnerabilità della sicurezza sono costose per qualsiasi organizzazione. Gli attacchi ransomware rappresentano la minaccia maggiore e ogni attacco costa in media alle aziende 4,62 milioni di dollari[1]. L'integrità della piattaforma IBM® Power® può ridurre il rischio di ransomware implementando il rilevamento e la risposta degli endpoint (EDR, Endpoint Detection and Response) e concetti di Zero Trust come l'autenticazione a più fattori continua (MFA, Multifactor Authentication).

L'adozione di un approccio basato esclusivamente sull'attività di business, sulla conformità o sui costi non può fornire ai processi di business una protezione adeguata contro il crescente numero di rischi per i sistemi IT. Gli approcci che tengono conto di un unico fattore possono trascurare aspetti interdisciplinari fondamentali di una strategia di sicurezza efficiente e integrata. La soluzione ideale è quella che prevede una pianificazione e una valutazione per individuare i rischi nelle aree chiave correlate alla sicurezza. La tecnologia IBM Power e i sistemi basati sui processori IBM® Power10 offrono un approccio olistico, Zero Trust e multilivello per la tua strategia di sicurezza, in modo da garantire che la tua organizzazione sia protetta e conforme. Questo approccio multilivello comprende:

- Hardware
- Sistema operativo
- Firmware
- Tecnologia IBM® PowerSC 2.0
- Hypervisor

L'adozione di un approccio di sicurezza olistico può consentire alla tua organizzazione di soddisfare le esigenze derivanti dalle minacce che gravano sul panorama della sicurezza.

Gli hacker diventano sempre più sofisticati

Più un'organizzazione si sposta fuori dai limiti dei tradizionali data center on-premise ed esegue la transizione ad ambienti di cloud ibrido o multicloud e più gli aggressori hanno spazio per pensare fuori dagli schemi. L'implementazione dei privilegi minimi e l'aumento dei controlli basati sul perimetro contribuirà a gestire il crescente numero di minacce. I metodi del passato degli aggressori non sono più limitati al livello di rete, il che porta ad ampliare gli orizzonti e a rendere maggiormente efficaci gli attacchi.

Con l'aumento dell'accesso ai dati, la sicurezza assume un ruolo primario

I dati all'interno di un'organizzazione possono ora essere archiviati e consultati dai dipendenti praticamente ovunque: su server, ambienti di cloud ibrido e numerosi dispositivi mobili ed edge. Questo inestricabile incrociarsi di server e dispositivi è l'effetto collaterale della continua trasformazione e modernizzazione digitale. Di conseguenza, questa accessibilità crea una pletora di vettori di attacco pronti per essere sfruttati.

Una regolamentazione più rigorosa influisce sui profili di rischio

Anche i processi messi in atto per garantire la conformità normativa possono portare a un'esposizione involontaria dei rischi. Il regolamento generale sulla protezione dei dati (GDPR) è solo uno dei recenti sviluppi di una tendenza in crescita. Gli enti governativi prestano molta più attenzione al modo in cui le organizzazioni utilizzano i dati. Ma aggiungono anche livelli di complessità alle operazioni di business quotidiane.

I dipendenti costituiscono delle vulnerabilità in attesa di essere sfruttate

L'anno scorso le credenziali compromesse dei dipendenti sono state la causa del 20% di tutte le violazioni di dati[1]. Oltre alle informazioni di accesso, le truffe di phishing e la compromissione delle e-mail, sono altri i modi in cui i dipendenti mettono inconsapevolmente a rischio le informazioni aziendali. La tua forza lavoro rappresenterà sempre un certo livello di rischio, indipendentemente dai controlli di sicurezza messi in atto o dalla capacità di gestire le vulnerabilità. Nell'era dei crimini informatici è fondamentale istruire i dipendenti su queste minacce comuni alla sicurezza e implementare un sistema di reportistica. Il duro lavoro svolto per proteggere gli endpoint e rispettare la conformità può essere vanificato da un errore o da un ingegnoso attacco malintenzionato.

Nel frattempo, molte organizzazioni faticano a trovare e trattenere il personale competente in materia di sicurezza informatica e si ritrovano con una perenne carenza di competenze. Per contrastare tali carenze di competenze, le organizzazioni possono implementare una gestione della sicurezza semplificata che automatizza operazioni, conformità, applicazione di patch e monitoraggio. Sfrutta i vantaggi di una sicurezza end-to-end progettata per la protezione con un rilevamento degli endpoint aggiuntivo senza risorse aggiuntive.

Il volume, la varietà e la velocità dell'attuale panorama delle minacce informatiche non faranno che moltiplicarsi man mano che le architetture IT continueranno a evolversi e adattarsi alle mutevoli tendenze della tecnologia, della cultura del lavoro e della conformità. Questo significa che la tua strategia di sicurezza deve evolversi per andare oltre il livello di rete.

Una strategia di sicurezza Zero Trust è fondamentale

Un approccio olistico

L'implementazione di concetti Zero Trust può aiutare le organizzazioni a occuparsi della sicurezza in un ambiente IT spesso complesso. La visibilità e il controllo nei panorami multicloud e di cloud ibrido sono fattori che mettono in difficoltà i professionisti IT. Zero Trust gestisce i rischi grazie a un orientamento verso una strategia più completa che limita i controlli di accesso senza influire sulle prestazioni o sull'esperienza degli utenti. È possibile consolidare la sicurezza in ogni livello dello stack implementando diverse soluzioni di sicurezza di fornitori terzi. Tuttavia, tale approccio peggiora la complessità che già esiste e introduce ancora più vulnerabilità e punti di esposizione nella rete. La soluzione migliore consiste nell'adottare un approccio Zero Trust multilivello. In questo modo è possibile proteggere tutti i dati e i sistemi dell'organizzazione, riducendo al minimo la complessità. In quest'ottica, IBM® Information Security Framework aiuta a garantire che ogni aspetto della sicurezza IT possa essere affrontato in modo adeguato quando si adotta un approccio olistico alla sicurezza basata sul business.

IBM Information Security Framework si concentra su:

1. Infrastruttura - Fornisci la protezione contro gli attacchi più sofisticati grazie a insight di utenti, contenuti e applicazioni.
2. Ricerca avanzata in materia di sicurezza e minacce - Acquisisci una conoscenza delle vulnerabilità e delle metodologie di attacco e applica questo insight tramite le tecnologie di protezione.
3. Persone - Gestisci e amplia l'identità aziendale nei domini di sicurezza con un'intelligence sulle identità completa.
4. Dati - Proteggi la privacy e l'integrità degli asset più affidabili della tua organizzazione.
5. Applicazioni - Riduci il costo di sviluppo delle applicazioni più sicure.
6. Intelligence e analytics della sicurezza - Ottimizza la sicurezza con il contesto, l'automazione e l'integrazione aggiuntivi.
7. Filosofia Zero Trust - Connetti gli utenti giusti ai dati giusti, proteggendoli e al contempo salvaguardando la tua organizzazione.

Scopri di più su IBM Security Framework (PDF, 25,2 MB) e come ottenere informazioni ancora più approfondite.

In che modo la tecnologia IBM Power protegge lo stack

Esplora IBM Power

Grazie alla tecnologia IBM Power è possibile aumentare la resilienza informatica e gestire i rischi con una sicurezza end-to-end completa che si integra nell'intero stack, dal processore e dal firmware al sistema operativo e agli hypervisor, alle app e alle risorse di rete, fino alla gestione del sistema di sicurezza.

Hardware, firmware e hypervisor

Acceleratori su chip
Il chip del processore IBM Power10 è progettato per potenziare le prestazioni di mitigazione del canale laterale ed è dotato di un isolamento della CPU migliorato dai processori di servizio. Questo processore da 7 nm è progettato per fornire un aumento fino a tre volte della capacità con un conseguente incremento delle prestazioni[2].

Crittografia end-to-end
La crittografia della memoria trasparente delle soluzioni IBM Power è progettata per abilitare una sicurezza end-to-end che soddisfi gli esigenti standard di sicurezza che le aziende devono affrontare oggigiorno. Inoltre, è progettata per supportare l'accelerazione crittografica, la crittografia post quantistica e la crittografia omomofrica completa per la protezione dalle future minacce. La crittografia accelerata per il modello di sistema IBM Power più recente dispone di prestazioni crittografiche AES (Advanced Encryption Standard) 2,5 volte più veloci per core rispetto alla tecnologia IBM Power E980[3]. Le organizzazioni possono trarre vantaggio dalla crittografia della memoria trasparente senza alcuna impostazione di gestione aggiuntiva.

Software EDR
L'aumento delle minacce esterne rende la sicurezza degli endpoint fondamentale quando si tratta di proteggere i dati dei clienti e gli asset digitali. Rilevando eventuali minacce potenziali all'endpoint, le organizzazioni possono intervenire rapidamente e risolvere gli incidenti senza interrompere la business continuity. Un approccio integrato elimina le complicazioni e protegge l'organizzazione anche dagli attacchi più pericolosi.

x2,5

La crittografia accelerata per il modello di sistema IBM Power più recente dispone di prestazioni crittografiche AES (Advanced Encryption Standard) **2,5 volte più veloci per core** rispetto alla tecnologia IBM Power E980[3].

L’abilitazione di principi quali l’autenticazione a più fattori e i privilegi minimi apporta ulteriore protezione proteggendo tutte le API, gli endpoint, i dati e le risorse di cloud ibrido.

Principi Zero Trust
Le organizzazioni si stanno evolvendo verso l’adozione di principi Zero Trust per contribuire a gestire queste crescenti minacce. L’abilitazione di principi quali l’autenticazione a più fattori e i privilegi minimi apporta ulteriore protezione proteggendo tutte le API, gli endpoint, i dati e le risorse di cloud ibrido.

Il framework IBM Zero Trust dà vita a questo concetto.

- **Raccolta di insight** - Comprendi utenti, dati e risorse per creare le politiche di sicurezza necessarie per garantire una protezione completa.
- **Protezione** - Proteggi l’organizzazione convalidando il contesto e implementando politiche in modo rapido e coerente.
- **Rilevamento e risposta** - Risolvi le violazioni della sicurezza con un impatto minimo sulle operazioni di business.
- **Analisi e miglioramento** - Migliora continuamente il profilo di sicurezza modificando le politiche e le prassi per prendere decisioni più informate.

Implementando i principi Zero Trust, le aziende possono realizzare l’innovazione ed eseguire la scalabilità in tutta sicurezza.

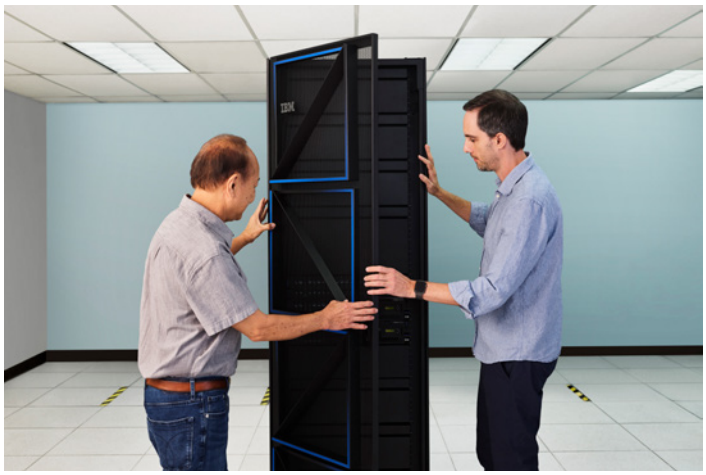
Avvio sicuro su soluzioni IBM Power10
L’avvio sicuro è progettato per proteggere l’integrità del sistema verificando e convalidando tutti i componenti firmware tramite le firme digitali. Tutto il firmware rilasciato da IBM è firmato e verificato digitalmente come parte del processo di avvio. Tutti i sistemi IBM Power sono dotati di un modulo di piattaforma affidabile che accumula le misurazioni di tutti i componenti firmware caricati su un server, consentendone l’ispezione e la verifica in remoto.

Hypervisor aziendale IBM PowerVM
Se confrontato ai principali concorrenti, l’hypervisor aziendale IBM PowerVM® vanta risultati eccellenti in materia di sicurezza, per cui è possibile proteggere con sicurezza le VM (Virtual Machine) e gli ambienti cloud.

Sistema operativo

I sistemi IBM Power offrono funzionalità di sicurezza leader del settore per una vasta gamma di sistemi operativi come IBM® AIX®, IBM i e Linux®. La tecnologia EDR per IBM Power può fornire sicurezza aggiuntiva per i carichi di lavoro di VM, garantendo una protezione completa a ogni endpoint all’interno della rete. Per i sistemi che affidano la loro sicurezza alle password, i sistemi operativi AIX e Linux utilizzano l’autenticazione a più fattori (MFA, Multifactor Authentication) di IBM PowerSC che richiede ulteriori livelli di autenticazione per tutti gli utenti, proteggendoli dal malware per la decifrazione delle password. Le funzioni variano a seconda del sistema operativo, ma tra gli esempi di queste funzionalità vi è la possibilità di:

- Assegnare funzioni amministrative normalmente riservate all’utente root senza compromettere la sicurezza
- Crittografare i dati a livello di file tramite singoli keystore
- Acquisire un maggiore controllo sui comandi e sulle funzioni a disposizione degli utenti, oltre al controllo sugli oggetti a cui possono accedere
- Registrare l’accesso a un oggetto nel journal di controllo della sicurezza utilizzando i valori di sistema e i valori di controllo oggetto per gli utenti e gli oggetti
- Eseguire la crittografia su un’intera unità, crittografando prima un oggetto e scrivendo quindi nel formato crittografato
- Misurare e verificare ogni file prima che venga aperto per l’utente richiedente



Carichi di lavoro, VM e container

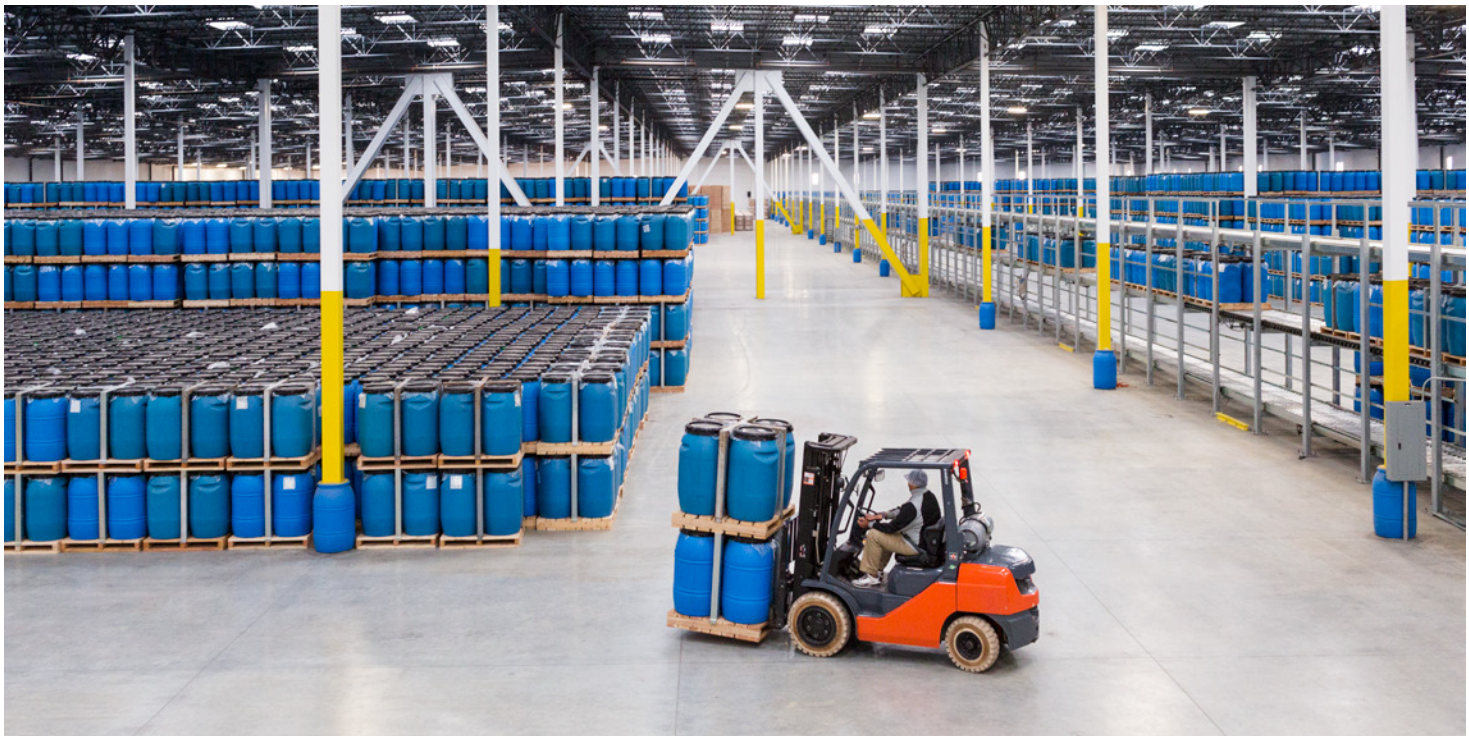
I carichi di lavoro non sono più limitati ai data center on-premise; si spostano continuamente verso ambienti di cloud ibrido e multicloud virtualizzati. Ad esempio, molte organizzazioni adottano i container per implementare applicazioni nuove ed esistenti nelle infrastrutture ibride.

Questi ambienti e carichi di lavoro sempre più dinamici richiedono funzionalità di sicurezza altrettanto versatili. Le soluzioni IBM Power possono soddisfare le esigenze di sicurezza preservando la privacy dei carichi di lavoro con l'accelerazione dell'algoritmo crittografico, l'archiviazione sicura delle chiavi e il supporto della CPU per la crittografia post quantistica e gli algoritmi crittografici FHE (Fully Homomorphic Encryption).

Inoltre, per rispondere ai requisiti di sicurezza unici delle implementazioni containerizzate, IBM ha stretto collaborazioni con ISV (Independent Software Vendor) come Aqua Security, che esegue le sue attività di sviluppo con la tecnologia IBM Power e Red Hat® OpenShift® Container Platform per proteggere ulteriormente i container durante il loro ciclo di vita.

I server IBM Power sono progettati per proteggere i dati dagli ambienti on premise al cloud con una crittografia della memoria end-to-end e prestazioni crittografiche accelerate. Le politiche integrate per i carichi di lavoro nativi del cloud, compresi le VM, i container e le funzioni serverless, sono sviluppate per supportare i clienti Red Hat OpenShift e IBM Power quando integrano i loro requisiti di sicurezza e conformità per la modernizzazione delle applicazioni.

LPM (Live Partition Mobility)
La tecnologia IBM Power consente di proteggere i dati in movimento. LPM protegge le VM tramite la crittografia quando è necessario eseguire migrazioni da un sistema all'altro. Se disponi di data center on premise virtualizzati, ambienti di cloud ibrido o entrambi, questa funzionalità è di importanza cruciale.



Prodotti di sicurezza integrati su soluzioni IBM Power

IBM® PowerSC 2.0 technology

La tecnologia IBM® PowerSC 2.0 è un'offerta del portfolio integrata per la sicurezza aziendale e la conformità in ambienti cloud e virtuali. Si trova in cima al tuo stack e fornisce un'interfaccia utente basata sul web per gestire le funzioni di sicurezza della tecnologia IBM Power che risiedono nelle soluzioni dal livello più basso in su.

Grazie alle funzionalità di semplificazione e automazione, la tecnologia IBM PowerSC 2.0 può ridurre tempi, costi e rischi semplificando il monitoraggio e l'applicazione della conformità. Questa soluzione può supportare i processi di controllo e consente ai clienti di conseguire le certificazioni di conformità in modo più efficiente. Può anche ridurre i rischi di sicurezza aumentando la visibilità in tutto lo stack.

Funzioni di IBM PowerSC 2.0 Standard Edition

Tecnologia di autenticazione a più fattori (MFA, Multifactor Authentication)
L'MFA è ora integrata nelle soluzioni IBM PowerSC 2.0. Ciò semplifica l'implementazione dei meccanismi MFA nel rispetto del principio Zero Trust "Non ti fidare mai, verifica sempre". Questo approccio supporta fattori alternativi per l'accesso degli utenti con opzioni di autenticazione basate su RSA SecurID e di autenticazione dei certificati, comprese le schede CAC (Common Access Card) e PIV (Personal Identification Verification). L'MFA IBM PowerSC aumenta i livelli di garanzia dei sistemi richiedendo fattori di autenticazione supplementari per gli utenti.

La tecnologia IBM PowerSC 2.0 può ridurre tempi, costi e rischi

Funzionalità EDR
La soluzione IBM PowerSC 2.0 introduce EDR per i carichi di lavoro Linux on IBM Power, offrendo le funzionalità standard del settore più recenti per la gestione della sicurezza degli endpoint, compresi il rilevamento e la prevenzione delle intrusioni, l'ispezione e l'analisi dei log, il rilevamento delle anomalie e la risposta agli incidenti.

Automazione della conformità
La famiglia IBM Power è dotata di profili predefiniti che supportano una miriade di standard di settore. Puoi personalizzare questi profili e unirli con le regole aziendali senza dover mettere mano a XML (Extensible Markup Language).

Conformità in tempo reale
Rileva e ti avvisa quando qualcuno apre o interagisce con i file critici per la sicurezza.

Connessione di rete affidabile
Ti avvisa quando una VM non è al livello di patch prescritto. Inoltre, ti avverte quando le correzioni diventano disponibili.

Avvio sicuro
Consente l'ispezione e la verifica in remoto dell'integrità di tutti i componenti software in esecuzione su partizioni logiche AIX.

Firewall affidabile
Protegge e instrada il traffico di rete interno tra i sistemi operativi AIX, IBM i e Linux.

Registrazione affidabile
Crea log di controllo centralizzati, di cui è facile eseguire il backup, l'archiviazione e la gestione.

Reportistica preconfigurata e sequenza temporale interattiva
IBM PowerSC Standard Edition supporta il controllo con cinque report preconfigurati. Disponi anche di una sequenza temporale interattiva per visualizzare il ciclo di vita e gli eventi di una VM.

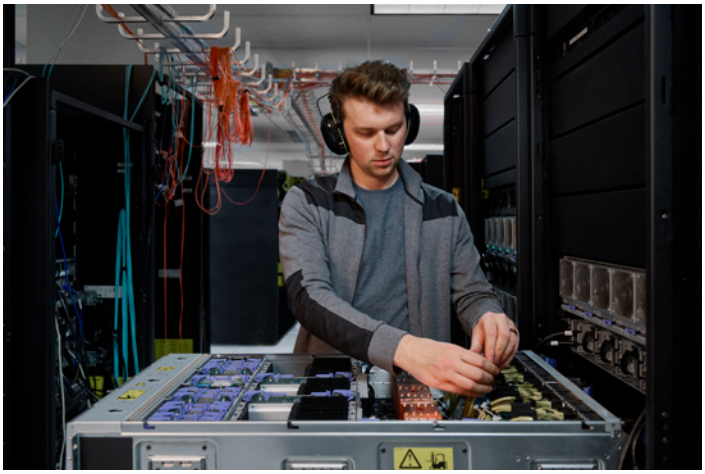
Scopri come semplificare la gestione della sicurezza IT e della conformità con IBM PowerSC in ambienti cloud e virtualizzati

L’approccio più potente alla sicurezza è un approccio perfettamente integrato

Integrazione completa

Poiché i criminali informatici continuano a rendere più sofisticati i loro metodi e l’evoluzione tecnologica introduce nuove vulnerabilità nelle aziende di oggi, è fondamentale integrare una soluzione di sicurezza Zero Trust a più livelli che non aumenti la complessità dell’organizzazione. Le soluzioni IBM Power possono proteggere ogni livello del tuo stack, dall’edge al cloud e al core, con le soluzioni approfondite e strettamente integrate di un unico fornitore. Lavorare con più fornitori introduce delle complessità che alla fine possono rivelarsi costose, in più di un senso. La tecnologia IBM Power supporta la crittografia end-to-end a livello del processore senza influire sulle prestazioni. L’integrazione della tua infrastruttura mette a fuoco ogni livello dello stack.

La sicurezza offerta da un unico fornitore può fornire dei vantaggi naturali che semplificano e consolidano la tua strategia di sicurezza. Forte di tre decenni di leadership nella sicurezza, la tecnologia IBM Power porta con sé ampie collaborazioni con altre organizzazioni interne ed esterne a IBM che approfondiscono ed estendono ulteriormente la sua competenza nel campo della sicurezza. Queste collaborazioni possono consentire alla tecnologia IBM Power di avvalersi di una comunità ancora più grande di professionisti della sicurezza e garantire che i problemi possano essere individuati rapidamente e affrontati con fiducia. Inoltre, con il supporto delle unità di business IBM Security® e IBM Research®, oltre al portfolio PowerSC 2.0, i server Power10 possono sventare molteplici minacce, compresi gli attacchi interni, dall’alto verso il basso.



Prenota una consulenza per esplorare il potenziale delle soluzioni IBM Power

Contattaci →

Note:
1. Cost of a Data Breach Report 2021, IBM Security, luglio 2021 (PDF, 3,6 MB)
2. 3. Le prestazioni triple sono basate su un'analisi ingegneristica virtuale di ambienti aziendali, a numeri interi e a virgola mobile su un server a 2 socket POWER10 con 2 moduli da 30 core rispetto all'offerta di server a 2 socket POWER9 con 2 moduli da 12 core: entrambi i moduli hanno lo stesso livello di energia.
Un miglioramento dell'inferenza dell'AI da 10 a 20 volte è basato su un'analisi ingegneristica virtuale di diversi carichi di lavoro (Linpack. Resnet-50 FP32, Resnet-50 BFloat16, e Resnet-50 INT8) su un'offerta di server a 2 socket POWER10 con 2 moduli da 30 core rispetto all'offerta di server a 2 socket POWER9 con 2 moduli da 12 core.
3. AES-256 in entrambe le modalità GCM e XTS ha un'esecuzione circa 2,5 volte più veloce per core rispetto a IBM Power10 E1080 (moduli da 15 core) e IBM POWER9 E980 (moduli a 12 core) secondo le misurazioni preliminari ottenute su RHEL Linux 8.4 e la libreria OpenSSL 1.1.1g

IBM Italia S.p.A.
Circonvallazione Idroscalo
20054 Segrate (Milano)
Italia

Prodotto negli
Stati Uniti d'America
Giugno 2022