

IBM annuncia nuovi servizi per semplificare la sicurezza degli ambienti cloud ibridi

La nuova suite di servizi può aiutare le aziende a proteggere dati, utenti, progetti e applicazioni su cloud distribuiti e sistemi on-premise

12 aprile 2021 – IBM Security annuncia nuovi servizi per aiutare le aziende a gestire la propria strategia di sicurezza, le policy e i controlli negli ambienti hybrid cloud. I servizi uniscono tecnologie cloud native, di IBM e di terze parti, insieme alle competenze ed esperienze di IBM per aiutare le organizzazioni a sviluppare un approccio alla sicurezza unificato attraverso i loro ecosistemi cloud.

Le imprese oggi si avvantaggiano di un mix di risorse cloud e on-premise per raggiungere il giusto equilibrio tra agilità, sicurezza e risparmio dei costi. Sebbene la flessibilità del cloud ibrido offra molti vantaggi, le aziende devono continuamente mantenere visibilità e gestire in modo efficace l'intera gamma dei controlli di sicurezza in un ambiente IT diffuso. Secondo il "2020 Cost of Data Breach Report^[1]", gli errori di configurazione nel cloud sono stati una delle principali cause di violazione dei dati, ovvero 1 su 5 delle violazioni analizzate.

La nuova suite IBM Security Services for Cloud è progettata per aiutare le aziende nell'adozione di una strategia di sicurezza coerente attraverso i loro ambienti di cloud ibrido, supportata dagli esperti di IBM capaci di gestire i controlli di sicurezza nativi anche per Amazon Web Services (AWS), Google Cloud, IBM Cloud e Microsoft Azure. Questi servizi possono aiutare le aziende a valutare lo stato attuale della sicurezza del cloud, nonché a definire e gestire accessi, politiche e controlli tecnici per salvaguardare le risorse cloud nuove ed esistenti. Il tutto sfruttando l'intelligenza artificiale e l'automazione per identificare e prioritizzare i rischi, rispondere a potenziali minacce negli ambienti cloud delle imprese e connettere i dati con le operazioni di sicurezza e i sistemi on-premise.

"La sicurezza del cloud può sembrare instabile, data la necessità di difendere superfici più ampie di attacco, la presenza di modelli di responsabilità condivisa e piattaforme e strumenti cloud in rapida evoluzione", ha affermato Vikram Chhabra, Global Director, Offering Management and Strategy, IBM Security Services. "Non possiamo presumere che gli approcci legacy per la sicurezza funzioneranno in questo nuovo modello operativo; crediamo però che la sicurezza debba essere modernizzata specificatamente per l'era del cloud ibrido, con una strategia basata su principi di zero trust che riuniscono contesto, collaborazione e visibilità in qualsiasi ambiente cloud".

La combinazione di tecnologia e competenza semplifica la sicurezza del cloud

[IBM Security Services for Cloud](#) offre un approccio aperto e automatizzato per semplificare la sicurezza del cloud ibrido, unendo competenze di sicurezza per tutti gli ambienti cloud, anche della concorrenza, insieme a un set integrato di soluzioni cloud, proprietarie e di terze parti. I servizi possono supportare i clienti in qualsiasi fase del loro percorso verso la sicurezza nel cloud: dalla consulenza su come spostare in modo sicuro dati, utenti e carichi di lavoro al cloud, fino al monitoraggio continuo dei rischi e la gestione delle minacce della loro architettura cloud ibrida.

I nuovi servizi includono:

- **Cloud Native Security:** nuovi servizi di consulenza e servizi di sicurezza gestiti che forniscono visibilità, gestione e monitoraggio centralizzati dei controlli di sicurezza nativi in tutti gli ambienti cloud, contribuendo a ridurre il rischio di errori di configurazione del cloud, fornendo allo stesso tempo informazioni rapide su potenziali rischi e minacce. Gli esperti di sicurezza IBM aiutano a progettare e

implementare le *best practice* per i controlli cloud nativi in base a requisiti aziendali e normativi specifici; forniscono inoltre monitoraggio e reporting continui per configurazioni ottimizzate.

- **Cloud Security Posture Management:** nuovi servizi di consulenza e sicurezza gestiti che aiutano i clienti a progettare e implementare una soluzione di *cloud security posture management* (CSPM) per garantire la governance e la conformità tra i fornitori di servizi cloud. Questi nuovi servizi offrono un'unica soluzione per la progettazione di framework di governance e compliance, l'integrazione di sistemi CSPM e servizi gestiti, fornendo consigli concreti per risolvere rapidamente problematiche legate alla conformità, effettuare attività di monitoraggio e correzione.
- **Container Security:** servizi di sicurezza end-to-end unificati per gli ambienti container, dalla consulenza e integrazione dei sistemi alla gestione delle minacce, delle vulnerabilità fino ai servizi di sicurezza gestiti per l'intero ciclo di vita del container.
 - I consulenti IBM possono valutare gli ambienti container già esistenti, analizzare i processi DevSecOps, rivedere la progettazione dell'applicazione e i requisiti della soluzione, supportando la costruzione di una roadmap per le future implementazioni.
 - [IBM Managed Security Services](#) offre visibilità centralizzata, gestione e monitoraggio dei container, grazie a immagini, registri, console per l'orchestrazione, fornitori di servizi cloud.
 - L'integrazione con la gestione delle vulnerabilità di IBM Security X-Force Red può identificare, analizzare e classificare migliaia di vulnerabilità relative ai container all'interno degli ambienti dei clienti per prioritizzare gli interventi di remediation.
- **Cloud Security Strategy:** servizi di consulenza per l'analisi della sicurezza ibrida e multi-cloud, basata su framework di settore come il CSA Cloud Controls Matrix (CCM). Le aziende possono così beneficiare delle capacità analitiche e ricevere consigli in grado di mitigare i rischi. Utilizzando tecniche proprietarie, offrono una strategia personalizzata e una roadmap avanzata per la messa in sicurezza, in linea con gli specifici requisiti aziendali e di settore.

Questi servizi si basano sulle competenze ed esperienze di IBM nel supportare le imprese nel loro percorso di cloud security. IBM X-Force Threat Management Services aiuta i clienti a gestire l'intero ciclo di vita delle minacce, attraverso il rilevamento, l'analisi e la risposta. IBM offre anche servizi di sicurezza per Cloud Access Security Broker (CASB), che indirizza le aziende verso ambienti cloud sicuri grazie a un approccio integrato nella pianificazione e implementazione di una soluzione CASB.

Per maggiori informazioni su IBM Security Services for Cloud: www.ibm.com/security/services/cloud-security-services

IBM Security

IBM Security offre uno dei portfoli più completi e integrati di prodotti e servizi per la protezione aziendale. Il portfolio, supportato dal team di ricerca di fama mondiale IBM X-Force, consente alle organizzazioni di gestire con efficacia i rischi cyber e difendersi dalle minacce emergenti. IBM gestisce una delle organizzazioni di ricerca, sviluppo e delivery di soluzione di sicurezza più grandi al mondo, monitora 150 miliardi di eventi di security al giorno in più di 130 Paesi e ha ottenuto oltre 10.000 brevetti di sicurezza. Per maggiori informazioni, visita il sito www.ibm.com/security, segui [@IBMSecurity](#) su Twitter o visita il [blog di IBM Security Intelligence](#).

[1] Studio di riferimento, condotto da Ponemon Institute e promosso da IBM su 524 aziende che hanno subito una violazione di dati

For further information: Ufficio stampa IBM Claudia Ruffini – cla@it.ibm.com – 335 6325093
