

## IBM presenta la tecnologia open per accelerare la risposta ai cyber attacchi in Cloud

Prima soluzione del settore capace di intercettare possibili minacce nei diversi cloud attraverso strumenti di sicurezza senza dover spostare i dati dalla fonte originale

**ARMONK NY - 20 nov 2019:** IBM ha annunciato oggi Cloud Pak for Security, dotato delle prime innovazioni nel settore in grado di collegarsi con qualsiasi strumento di sicurezza, cloud o sistema *on-premise*, senza dover spostare i dati dalla fonte originale. Disponibile oggi, la piattaforma include la tecnologia *open-source* capace di intercettare le minacce, di velocizzare la risposta ai *cyberattack*, grazie a sistemi di automazione, e di funzionare in qualsiasi ambiente.

Cloud Pak for Security è la prima piattaforma che sfrutta la nuova tecnologia *open-source* di IBM, in grado di ricercare e trasformare i dati di sicurezza da una varietà di fonti, mettendo insieme *insight* critici provenienti dall'ambiente IT multicloud di qualunque azienda. La piattaforma è estensibile, in modo da poter essere arricchita nel tempo con strumenti e applicazioni aggiuntive.

Mentre le aziende si spostano sempre più verso un cloud più maturo, le applicazioni e i dati sono distribuiti su più cloud privati e pubblici o *on-premise*. I tentativi di proteggere questo ambiente IT frammentato richiedono che i *team* di sicurezza effettuino integrazioni complesse e passino continuamente tra diversi schermi e prodotti. Più della metà di essi afferma di avere difficoltà ad integrare i dati con strumenti analitici e di sicurezza differenti e a combinare i dati nei loro ambienti cloud per individuare le minacce più avanzate ([SANS Institute survey](#)).

Le prime tre capacità includono:

- **Ottenere informazioni sulla sicurezza senza spostare i dati**. Il trasferimento dei dati da analizzare aggiunge complessità. IBM Cloud Pak for Security è in grado di collegare tutte le fonti dati di un'azienda per scoprire le minacce nascoste e aiutarla a prendere decisioni basate sul rischio, lasciando i dati dove si trovano. Tramite l'applicazione Cloud Pak for Security Data Explorer, gli analisti possono ottimizzare la ricerca di minacce attraverso qualsiasi strumento di sicurezza o cloud. Senza questa capacità, i *team* dedicati alla sicurezza sono costretti a cercare manualmente gli stessi indicatori di minaccia (come un *malware* o un indirizzo IP dannoso) all'interno di ogni singolo ambiente.
- **Rispondere più velocemente agli incidenti di sicurezza grazie all'automazione**. IBM Cloud Pak for Security collega i flussi di lavoro sulla sicurezza con un'interfaccia unificata e i *playbook* di automazione in modo che i *team* possano rispondere più rapidamente agli incidenti di sicurezza. La piattaforma consente alle aziende di orchestrare la loro risposta a centinaia di scenari di sicurezza, guidando gli utenti attraverso il processo e fornendo un accesso rapido ai giusti dati e agli strumenti di sicurezza. La capacità di IBM Security Orchestration, Automation and Response si integra con Red Hat Ansible per ulteriori *playbook* di automazione. Formalizzando i processi e le attività di sicurezza in tutta l'azienda, è possibile reagire più velocemente e in modo più efficiente, mentre ci si dota delle informazioni necessarie per essere conformi alle normative.
- **Vai ovunque. Collega la sicurezza in modalità open**. IBM Cloud Pak for Security si installa facilmente in qualsiasi ambiente - *on premises*, su cloud privato o pubblico. Fornisce un'interfaccia unificata per semplificare le operazioni, composta da *software* containerizzato pre-integrato con Red Hat OpenShift, una piattaforma Kubernetes che permette un modello di distribuzione multicloud mobile.

*"Mentre le aziende spostano i carichi di lavoro mission-critical in ambienti ibridi multicloud, i dati di sicurezza sono distribuiti su diversi strumenti, cloud e infrastrutture IT. Ciò crea lacune che permettono alle minacce di nascondersi, richiedendo agli specialisti di sicurezza di costruire e mantenere costose e complesse integrazioni e piani di risposta manuale", ha dichiarato Mary O'Brien, General Manager, IBM Security. "Con Cloud Pak*

*for Security, stiamo gettando le basi per un ecosistema di sicurezza più connesso progettato per il mondo ibrido e multicloud".*

IBM ha collaborato con decine di clienti e fornitori di servizi durante il processo di progettazione, sviluppando una soluzione per affrontare le sfide critiche di interoperabilità che permeano il settore della sicurezza. Il lancio di Cloud Pak for Security include connettori per l'integrazione pre-costituita con i più diffusi strumenti di sicurezza di IBM, Carbon Black, Tenable, Elastic, BigFix, Splunk, così come con i fornitori di cloud pubblici, tra cui IBM Cloud, Amazon Web Services e Microsoft Azure\*. La soluzione è costruita su *standard* aperti in modo che possa collegare ulteriori strumenti di sicurezza e dati da tutta l'infrastruttura aziendale.

*"Le organizzazioni hanno rapidamente adottato nuove tecnologie di sicurezza per stare al passo con le minacce più recenti, ma ora stanno lavorando con decine di strumenti scollegati che non sempre funzionano bene insieme", ha dichiarato **Jon Oltsik, Enterprise Strategy Group**. "L'industria deve risolvere questo problema passando a tecnologie più aperte e piattaforme unificate che possono fungere da collante tra gli strumenti per la sicurezza. L'approccio di IBM si allinea con questo requisito e ha il potenziale per riunire ogni livello dello stack di sicurezza in un'unica interfaccia semplificata".*

Nell'accelerare la migrazione del settore verso la sicurezza *open*, IBM si pone all'avanguardia anche nei progetti *open-source* per permettere ai tool di sicurezza di lavorare insieme nativamente nell'intero ecosistema della *security*. Come membro fondatore [dell'Open Cybersecurity Alliance](#), IBM insieme a più di 20 altre organizzazioni stanno lavorando insieme su *standard* aperti e tecnologie *open-source* che consentono l'interoperabilità dei prodotti e riducono il *vendor lock-in*.

### **Progettato per il mondo ibrido e multicloud**

Il 76% delle organizzazioni riferisce di utilizzare già tra 2 e 15 cloud ibridi, e il 98% prevede di utilizzare più *hybrid cloud* entro i prossimi tre anni ([IBM Institute for Business Value, 2018](#)). Il Cloud Pak for Security di IBM è costruito su tecnologie *open source* che sono fondamentali per l'ambiente cloud delle aziende - tra cui Red Hat OpenShift e Kubernetes.

La creazione di Cloud Pak per la sicurezza su questi *building blocks* aperti e flessibili consente una facile distribuzione "containerizzata" su qualsiasi cloud o *on-premise*. Mentre le aziende continuano ad aggiungere nuove implementazioni e migrazioni in cloud, Cloud Pak for Security può facilmente adattarsi e scalare questi nuovi ambienti, consentendo alle imprese di portare nel cloud anche i carichi di lavoro sensibili e *mission-critical*, mantenendo la visibilità e il controllo all'interno di una piattaforma di sicurezza centralizzata.

Cloud Pak for Security fornisce anche un modello per i Managed Security Services Providers (MSSP) per operare in modo efficiente in scala, collegare i silos di sicurezza e ottimizzare i loro processi di security. Le organizzazioni possono inoltre beneficiare di un'ampia gamma di servizi di sicurezza realizzati da IBM, come la consulenza *on-demand*, lo sviluppo personalizzato e la risposta agli incidenti.

IBM Cloud Pak for Security è ora disponibile ovunque - <https://www.ibm.com/products/cloud-pak-for-security> per maggiori informazioni.

### IBM Security

IBM Security offre uno dei portafogli più avanzati e integrati di prodotti e servizi di sicurezza aziendale. Il portafoglio, supportato da una ricerca IBM X-Force® di fama mondiale, consente alle organizzazioni di gestire efficacemente i rischi e difendersi dalle minacce emergenti. IBM gestisce una delle organizzazioni di ricerca e sviluppo di sicurezza più ampie al mondo, controlla 70 miliardi di eventi di sicurezza al giorno in più di 130 Paesi e ha ottenuto più di 10.000 brevetti di sicurezza in tutto il mondo. Per ulteriori informazioni, visitare il

sito [www.ibm.com/security](http://www.ibm.com/security), seguire @IBMSecurity su Twitter o visitare il blog IBM Security Intelligence.

---

\* Disponibile nel Q4 2019

### **Contatti**

#### **Paola Piacentini**

External Relations +39 3351270646

[paola\\_piacentini@it.ibm.com](mailto:paola_piacentini@it.ibm.com)

#### **Alessandro Ferrari**

External Relations Leader +39 3484554535

[alessandro\\_ferrari@it.ibm.com](mailto:alessandro_ferrari@it.ibm.com)

---