IDC LINK
Real-time IDC Research® opinion on industry news, trends and events

Con il suo Digital Sovereignty Pledge, AWS ha tutte le carte in regola per offrire ai suoi clienti la sovranità digitale: ora deve metterla alla prova nel mondo reale

08 dicembre 2022

Di: Rahiel Nasir, Archana Venkatraman, Giovanni Cervellati, Rick Villars

Riepilogo di IDC

Una vera sovranità digitale è difficile da implementare, ma le organizzazioni di tutto sono alla ricerca di soluzioni che soddisfino le dichiarazioni e aspettative di sovranità in rapida evoluzione. AWS vuole essere all'avanguardia in questo campo, rinnovando il suo impegno a espandere le proprie soluzioni per la sovranità nel cloud, senza compromettere funzionalità, disponibilità o agilità. La sfida per l'azienda ora è trasformare gli impegni presi in realtà.

Il Digital Sovereignty Pledge di AWS

Con il suo Digital Sovereignty Pledge annunciato di recente, AWS si impegna ad ampliare la sua attuale gamma di funzionalità di protezione dei dati per offrire ai clienti l'insieme di controlli sulla sovranità digitale disponibili nel cloud che sono oggi ritenuti i più avanzati.

L'azienda prevede di investire in ciò che descrive come un ambizioso piano d'azione in cui si impegna a espandere le funzionalità "sovereign-by-design" del cloud di AWS, concentrandosi sulle funzionalità per la residenza dei dati, la restrizione granulare degli accessi, la crittografia e la resilienza. Si propone di fare tutto questo senza compromettere le funzionalità, le prestazioni, l'innovazione e la scalabilità che il cloud può offrire.

AWS ha individuato quattro aree chiave nel suo piano d'azione.

In primo luogo, l'azienda afferma che fornirà ai clienti controlli più capillari e trasparenza sulla residenza dei loro dati, nell'ambito di un'offerta di maggior controllo sulla posizione fisica degli stessi, e un ulteriore rinforzo delle barriere di sicurezza per dati operativi che contengono informazioni su identità e fatturazione. AWS ha già aggiunto i controlli di residenza dei dati ad AWS Control Tower con l'obiettivo di offrire ai clienti un maggiore controllo sulla posizione fisica in cui i loro dati vengono archiviati ed elaborati.

In secondo luogo, AWS ha migliorato le funzionalità di Confidential Computing di Nitro, una raccolta componenti di sicurezza aggiuntive che sono alla base dei servizi di elaborazione Elastic Compute Cloud (EC2). AWS afferma che Nitro utilizza hardware e software specializzati per proteggere i dati dall'accesso esterno durante l'elaborazione, in modo che nessuno, nemmeno il personale AWS, possa accedere ai carichi di lavoro del cliente se non autorizzato. L'azienda inoltre afferma di essere trasparente sul modo in cui i suoi servizi elaborano e trasferiscono i dati e che continuerà a contestare le richieste di dati del cliente da parte di forze dell'ordine e agenzie governative.

In terzo luogo, AWS si è impegnata a investire in funzionalità che consentiranno ai clienti di crittografare tutti i loro dati ovunque si trovino, che siano in transito, a riposo o in memoria, utilizzando chiavi gestite all'interno o all'esterno di AWS Cloud. Tutto ciò sarà supportato dalla disponibilità di AWS Key Management Service o XKS, annunciata di recente.

Infine, l'azienda si impegna a potenziare le proprie opzioni per la resilienza, che consentono agli utenti di mantenere l'operatività anche durante interruzioni o disconnessioni. AWS Cloud attualmente copre 99 zone di disponibilità (AZ) all'interno di 31 regioni in tutto il mondo. Secondo l'azienda, le diverse zone di disponibilità all'interno delle regioni sono partizioni dell'infrastruttura completamente isolate e afferma che i clienti che desiderano isolare meglio i problemi e ottenere un'elevata disponibilità, possono progettare le loro applicazioni in modo da eseguirle in diverse zone di disponibilità della stessa regione.

Il punto di vista di IDC

La ricerca di IDC mostra che i disordini geopolitici ed economici che stanno attualmente influenzando le organizzazioni di tutto il mondo hanno rafforzato l'interesse globale nelle soluzioni di sovranità digitale.

Inoltre, riteniamo che l'interesse per la sovranità digitale si stia espandendo al di là dei tradizionali settori regolamentati in cui le organizzazioni sono motivate principalmente da esigenze di conformità. Man mano che l'utilizzo del cloud cresce in tutti i settori e le organizzazioni gestiscono una quantità maggiore di dati sensibili nei cloud pubblici, molte di loro cercano soluzioni di sovranità per contribuire ad alleviare i problemi relativi a sicurezza dei dati, privacy e controllo sull'accesso ai dati.

Grazie al suo impegno sul tema residenza dei dati e offrendo ai clienti un maggiore controllo sulla loro posizione fisica, AWS parte da basi solide. L'azienda sottolinea che i dati dei clienti non sono vincolati a rimanere sul proprio cloud e questo è un punto su cui vale la pena porre molta enfasi: visti i suoi progetti di investimento nelle funzionalità di portabilità dei dati, l'azienda potrebbe puntare su questo aspetto per rafforzare la fiducia dei clienti. AWS ritiene che la trasparenza nel modo in cui i suoi servizi elaborano e trasferiscono i dati sia fondamentale per ottenere tale fiducia, ma i timori relativi alla dipendenza da un unico fornitore, esacerbati dalla mancanza di portabilità dei dati e dalle limitazioni imposte ai clienti che avessero necessità di affidarsi a più provider, possono indebolire il rapporto di fiducia che è stato costruito.

Nell'opinione di IDC, il controllo sull'accesso ai dati a opera degli amministratori di un fornitore di servizi cloud è la priorità per le organizzazioni di tutto il mondo quando si tratta di lavorare con partner che offrono soluzioni sovrane (fonte: *Future Enterprise Resilience and Spending Survey*, Wave 4, maggio 2022). Ancora una volta, AWS centra il punto, impegnandosi a espandere i suoi controlli sull'accesso ai dati da parte del proprio personale, come amministratori e personale di supporto. Tuttavia, è necessario chiarire il modo in cui identità e gestione degli accessi funzioneranno effettivamente nel mondo reale quando si ha a che fare con un'organizzazione con sede negli Stati Uniti (quindi al di fuori della giurisdizione degli utenti cloud in altre parti del mondo).

La sovranità digitale riguarda in ultima analisi il rischio e la resilienza, come mostrato in IDC Sovereignty Stack Infatti, la continuità aziendale è una delle due priorità per le organizzazioni che intendono investire in partner per la sovranità digitale. In questo caso, AWS si impegna ad aumentare la resilienza delle diverse zone di disponibilità che compongono ciascuna delle sue regioni cloud, consentendo ai clienti di supportare l'operatività in caso di interruzioni o disconnessioni. L'azienda aggiunge che, per isolare meglio i problemi e ottenere disponibilità elevata, gli utenti possono suddividere le applicazioni in più zone di disponibilità nella stessa regione AWS. Si tratta sicuramente di una promessa gradita e degna di nota, ma non è chiaro quanto controllo AWS o dei suoi clienti abbiano sui livelli tecnici e operativi dello stack sovrano, come le reti che collegano tutti i centri dati in una zona di disponibilità e i centri dati stessi.

Ora che le organizzazioni sono già alle prese con cloud multipli e strutture IT ibride, l'aggiunta di sovranità alla strategia cloud introduce ulteriori complessità. AWS ne prende atto ed è inoltre consapevole del fatto che le esigenze di sovranità variano a seconda dei settori e dei paesi e di pari passo con l'evoluzione delle norme e dei regolamenti. Le partnership sono essenziali in questo caso, non solo tra fornitori e clienti, ma anche tra fornitori e partner. AWS afferma che non si aspetta né desidera che i suoi clienti "se la sbrighino da soli" e che collaborerà con partner di fiducia nei singoli mercati per supportarli.

Si tratta di un buon approccio, in quanto il successo della sovranità dipende dalla collaborazione all'interno di un ecosistema. Tuttavia, la sfida per i fornitori è garantire ai clienti che non solo offriranno credenziali sovrane garantite, ma che anche i loro partner lo faranno; questo vale anche per i partner dei partner e così via. Inoltre, si tratta di un processo continuo e di una responsabilità condivisa, in quanto tutte le parti coinvolte dovranno garantire costantemente la sovranità in tutte le operazioni pertinenti. Ciò richiede un investimento in competenze e strumenti di gestione e monitoraggio che possano essere utilizzati da tutti gli attori coinvolti e nel lungo periodo.

Un possibile effetto collaterale dell'implementazione di un cloud sovrano che, per sua stessa natura, tende a essere un cloud con funzionalità limitate, è la creazione di ostacoli all'innovazione digitale. Su questo tema, AWS si impegnerà a innovare funzionalità, controlli e garanzie di sovranità all'interno del suo cloud globale. L'azienda riconosce che è complesso soddisfare requisiti di sovranità in continua evoluzione e in continua espansione, mantenendo al contempo la sua ricca offerta di funzionalità. Ritiene che i clienti non dovrebbero scegliere tra la "piena potenza" di AWS e una soluzione cloud sovrano con funzionalità limitate che potrebbe ostacolare la loro capacità di innovare, trasformare e crescere. Resta da vedere come AWS riuscirà a raggiungere questo obiettivo. Nel frattempo, tuttavia, una delle principali preoccupazioni dell'azienda in merito alla fornitura di funzionalità per il cloud sovrano tramite partnership regionali è quella di preservare la sua "formula segreta" per il cloud pubblico.

E, naturalmente, c'è la questione del prezzo. Un cloud sovrano è, per sua stessa natura, un cloud limitato a causa di tutte le restrizioni che vi sono applicate in termini di dati, infrastruttura, operazioni e così via. Molte organizzazioni troverebbero pertanto difficile giustificare un costo più elevato per avere meno servizi. Ad esempio, molti utenti cloud in Europa, una regione che probabilmente godrà dei maggiori benefici derivanti dall'impegno preso da AWS, affermano di non essere disposti a pagare un surplus di oltre il 20% del proprio budget cloud per una soluzione di cloud sovrano (fonte: IDC EMEA, Multicloud Survey 2022, settembre, agosto 2022).

AWS parla in ultima analisi di espandere le proprie capacità di "sovereignty by design", ma resta da vedere come prevede di farlo a livello pratico come parte delle sue offerte cloud standard. Tuttavia, IDC ritiene che il mercato dovrebbe effettuare una transizione alla "sovranità di default" e, come per la sicurezza, non ci si dovrebbe nemmeno più chiedere se sia necessaria come extra opzionale e a pagamento.

Tuttavia, se AWS riuscisse a mettere in atto i suoi ambiziosi piani, non solo potrebbe stare al passo con i concorrenti, ma anche contribuire a fornire un modello di come l'intero stack di componenti digitali della sovranità possa passare dall'essere solo un'idea a un modello operativo pratico e reale.

Letture di approfondimento: T-Systems, AWS Launch Data Protection as a Managed Service to Help Cloud Adopters Adhere to EU Data Regulations While Accelerating Cloud Journeys (IDC #EUR149070722, maggio 2022)

Sottoscrizioni coperte:

Digital Sovereignty, Whole Cloud Strategies