E-BOOK

Come ottenere una sicurezza uniforme per i workload nel multi-cloud

Contenuti

Introduzione

Le applicazioni e i workload delle aziende migrano sul cloud pubblico a un ritmo senza precedenti per tanti buoni motivi.

La trasformazione cloud porta con sé numerosi vantaggi, che vanno dalla riduzione dei costi all'aumento dell'efficienza operativa e molto altro. Il passaggio al cloud è fondamentale per la trasformazione digitale, in quanto consente a un'organizzazione di diventare più agile, di soddisfare meglio le esigenze di clienti, fornitori e partner terzi e di migliorare l'esperienza del cliente.

Poiché un numero crescente di organizzazioni in tutti i settori persegue strategie cloud per rimanere competitiva nel suo settore, il cloud pubblico è diventato il nuovo data center aziendale. Allo stesso tempo, gli ambienti ibridi e multicloud sono diventati la norma. Una recente ricerca condotta da IDC ha previsto che entro la fine del 2025, la maggior parte delle aziende sfrutterà il cloud pubblico per piattaforme di intelligenza artificiale generativa, strumenti per sviluppatori e infrastrutture, e l'utilizzo del cloud supererà quello dei sistemi on-premise.[1]

I primi 3 fornitori di servizi cloud detengono il 67% della quota di mercato

Gartner prevede che il 51% della spesa IT per software applicativi, infrastrutture e servizi per i processi organizzativi si sposterà sul cloud pubblico entro il 2025, superando la spesa per l'IT tradizionale.[4]

Anche se la trasformazione cloud sta conoscendo un enorme aumento, con un ricavo combinato previsto per i fornitori di cloud pubblico superiori agli 800 miliardi di dollari entro la fine del 2024,[2] il mercato è dominato da soli tre attori:[3]

- Amazon Web Services (AWS), con una quota di mercato del 31%
- Microsoft Azure, con una quota di mercato del 25%
- Google Cloud, con una quota di mercato dell'11%

Questi provider di cloud pubblico offrono ai clienti nuove opportunità per ottenere maggiore velocità, agilità e flessibilità nell'utilizzo delle risorse informatiche. Tutto ciò consente agli sviluppatori di creare nuovi ambienti in pochi secondi. Queste aziende offrono centinaia di servizi diversi, sia autogestiti che gestiti dal provider.

Tuttavia, questi fattori contribuiscono anche all'emergere di nuovi rischi per la sicurezza, soprattutto per le organizzazioni che continuano ad affidarsi ad architetture di sicurezza legacy per proteggere i loro moderni ambienti cloud. La discrepanza tra gli approcci tradizionali alla protezione dei workload on-premise e quello che sarebbe necessario implementare negli attuali ambienti cloud rende spesso la protezione dei workload cloud costosa, complessa e difficile.

1. Ricerca IDC, IDC FutureScape: Worldwide Cloud 2024 Predictions, 2023.
2. Ricerca IDC, Worldwide Semiannual Public Cloud Services Tracker.
3. Statista, Cloud Infrastructure Market, 2024.
4. Gartner, Gartner Says More Than Half of Enterprise IT Spending in Key Market Segments Will Shift to the Cloud by 2025.

Le sfide della sicurezza per i workload sul cloud

Le organizzazioni che spostano i workload sul cloud senza modernizzare allo stesso tempo l'approccio alla sicurezza si trovano ad affrontare una serie di sfide comuni.

L'applicazione incoerente o inefficace delle policy espone i workload a minacce e attacchi informatici.

Affidarsi ad approcci legacy per proteggere e connettere i workload nel cloud è inevitabilmente complesso e costoso. Le architetture di sicurezza informatica basate su firewall e reti private virtuali (VPN) non sono state progettate per gli ecosistemi di cloud computing odierni.

I workload esposti possono essere facilmente compromessi. I criminali informatici possono tenere in ostaggio le aziende con attacchi ransomware devastanti. Porre rimedi a questi problemi può essere costoso e richiedere molto tempo.

I workload nel cloud richiedono comunicazioni estese con altri workload e Internet. Gli approcci di sicurezza legacy non sono all'altezza di questa connettività sempre attiva.

44%

ha subito una violazione dei dati basata sul cloud nel 2024.[5]

49%

segnala che la complessità del cloud rappresenta una sfida significativa per conformità e sicurezza.[6]

69%

ha riscontrato uno sforamento di budget relativo alla spesa per il cloud nel 2023.[7]

5. Thales Group, 2024 Cloud Security Study.
6. Ivi.
7. Gartner, 2024 Cloud Spending: IT Balances Costs with GenAI Innovation.

Le applicazioni odierne sono movimento. Lo zero trust dovrebbe spostarsi con esse.

Con l'avvento del lavoro da remoto e ibrido, le organizzazioni di tutti i settori stanno adottando il modello Zero Trust per proteggere i propri utenti. Con un approccio Zero Trust, la fiducia non viene mai concessa implicitamente. Si presume invece che ogni richiesta sia ostile o compromessa e che la richiesta di accesso a un'app venga consentita solo se:

- L'identità e il contesto della richiesta possono essere verificati
- I rischi associati a tale richiesta possono essere valutati in modo approfondito
- Le policy possono essere applicate per ogni sessione

Con il crescente numero di applicazioni e workload trasferiti sul cloud, è fondamentale che le organizzazioni estendano lo stesso livello di protezione di cui godono attualmente i propri utenti per l'accesso alle applicazioni a tutte le risorse e ai servizi cloud. Questo significa estendere la sicurezza basata sullo zero trust a tutti i workload nel cloud.

Quando le organizzazioni migrano le loro applicazioni legacy sul cloud, spesso scelgono di riorganizzarle utilizzando un approccio basato sui microservizi. Ciò consente di sfruttare funzionalità esclusive del cloud, come database cloud specializzati, funzioni serverless e architetture basate sugli eventi. Questo consente di ottenere una maggiore efficienza e ridurre i costi, ma crea anche un ambiente dinamico e altamente automatizzato. In questo ambiente, le comunicazioni tra workload avvengono costantemente.

I workload nel cloud devono spesso:

- Connettersi a Internet
- Comunicare con altri workload

In questo tipo di ambiente, il numero di comunicazioni che devono essere inviate tra workload è molto più elevato rispetto ai data center tradizionali.

Che cos'è un workload?

Un workload è l'elemento costitutivo di un'applicazione cloud moderna. Negli ambienti legacy on-premise, la maggior parte dei workload erano componenti all'interno di grandi applicazioni monolitiche. Tuttavia, questo non è il caso degli attuali ambienti nativi del cloud, in cui le applicazioni sono solitamente costituite da molti componenti modulari o microservizi. Ogni servizio esegue un'attività specifica e comunica con altri servizi per eseguire la logica organizzativa.

Alcuni esempi di workload:

- Contenitori
- Macchine virtuali (VM)
- Infrastrutture desktop virtuali (VDI)
- Funzioni serverless

La sicurezza di rete legacy non funziona per le aziende native del cloud

Troppe organizzazioni hanno intrapreso il percorso di trasformazione verso il cloud senza aggiornare di pari passo la propria strategia di sicurezza. Tuttavia, le architetture di sicurezza di rete legacy sono state concepite per i data center locali, non per il cloud. Quando le organizzazioni provano a trasferirle sul cloud, l'architettura che ne risulta è estremamente complessa e inefficace.

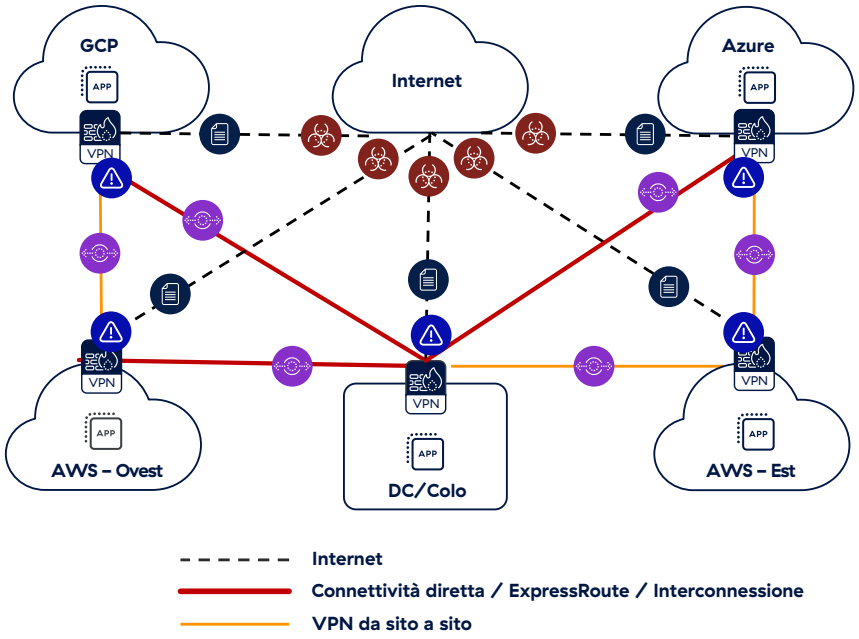
I workload nel cloud devono comunicare in modo sicuro sia tra di loro sia con Internet. L'approccio legacy per raggiungere questo obiettivo prevede la creazione di reti instradabili tra infrastrutture cloud mediante l'uso di firewall e VPN, estendendo sostanzialmente la rete WAN dell'organizzazione al cloud.

Con questo modello, le organizzazioni devono installare firewall virtuali di nuova generazione (vNGFW) ovunque risiedano i loro workload. In un mondo in cui gli ambienti ibridi e multicloud sono onnipresenti, si creano reti mesh piene, in cui ogni nodo si connette direttamente a tutti gli altri. Questa architettura è estremamente complessa e difficile da gestire.

Se le organizzazioni desiderano implementare funzionalità di sicurezza aggiuntive, come la prevenzione della perdita di dati (DLP) o l'ispezione TLS/SSL, dovranno aggiungere ulteriori dispositivi di sicurezza virtuali, aumentando ulteriormente la complessità.

Anche all'interno dell'ambiente di un singolo fornitore di servizi cloud, le organizzazioni dovranno configurare e gestire più vNGFW aggiuntivi per proteggere il traffico nord–sud ed est–ovest tra i workload cloud.

Le comunicazioni dei workload moltiplicano la complessità e le sfide per la sicurezza



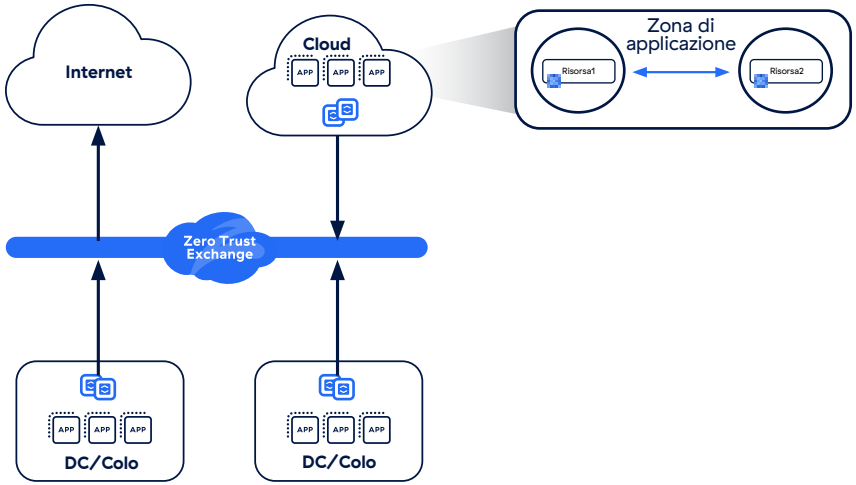
Difesa informatica inadeguata per gli ecosistemi informatici odierni

Affidarsi ad approcci legacy per proteggere e connettere i workload nel cloud comporta:

- **Una superficie di attacco estesa.** Ogni vNGFW ha una posizione di rete identificabile e quindi può essere scoperto dagli aggressori. Più firewall vengono implementati, maggiore è la superficie di attacco.
- **Compromissione dei workload.** Una volta che i malintenzionati scoprono un punto d'ingresso nell'ambiente e vi accedono, sono in grado di compromettere i workload.
- **Movimento laterale delle minacce.** Poiché tutti i workload sono connessi tramite una rete mesh, una volta che un singolo workload è compromesso, i malintenzionati possono muoversi lateralmente attraverso la rete per comprometterne altri.
- **Nessuna protezione per i dati sensibili.** Muovendosi attraverso la rete, gli aggressori saranno in grado di trovare ed esfiltrare dati sensibili come informazioni finanziarie dei clienti e segreti commerciali.

Cosa serve: un nuovo approccio alla protezione dei workload nel cloud

Per proteggere gli attuali ecosistemi informatici aziendali, che usano IaaS (Infrastructure as a Service), PaaS (Platform as a Service) e SaaS (Software as a Service) di più fornitori di servizi cloud, è necessario un approccio diverso che ponga le policy di sicurezza dell'organizzazione al centro della progettazione della sua rete. Questo significa permettere un accesso sicuro e con privilegi minimi basato sulla connettività diretta tra workload diversi e tra workload e Internet. Un simile approccio semplifica inoltre la creazione e la manutenzione di un'architettura zero trust per tutti i workload nel cloud.



Con questo nuovo approccio moderno:

- **La superficie di attacco viene eliminata.** A differenza di quanto succede con le soluzioni legacy, i workload sono effettivamente invisibili agli attori delle minacce, eliminando così l'intera superficiedi attacco.
- **I workload sono protetti.** L'ispezione completa dei contenuti inline, insieme alle capacità DLP, garantisce una sicurezza solida per dati e workload.
- **Il movimento laterale delle minacce è impedito.** Fornire una connettività diretta senza connessione a una rete rende impossibile il movimento laterale.
- **I dati sono protetti.** Aggiungere l'ispezione TLS/SSL su larga scala alle funzionalità DLP fornisce una protezione dei dati completa e generalizzata.
- **Complessità e costi sono ridotti.** Centralizzare la gestione della configurazione cloud insieme alla sicurezza e abilitare la connettività diretta rende possibile ridurre complessità e costi.

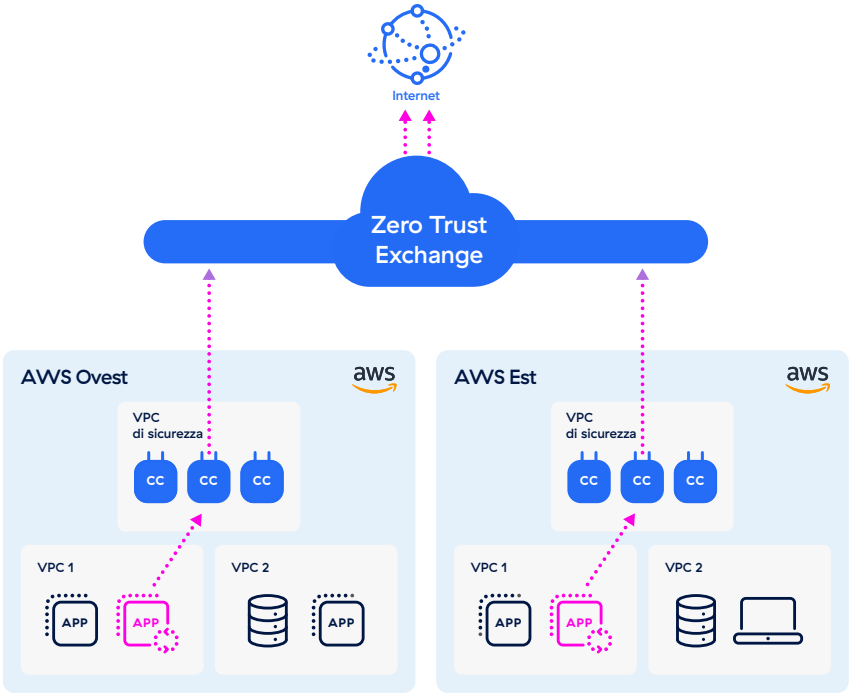
Semplificare e proteggere le comunicazioni da workload a Internet

Poiché ciascun workload nel cloud si basa su una comunicazione pressoché costante attraverso la rete Internet pubblica, una soluzione Zero Trust per i workload nel cloud deve essere in grado di proteggere tutta la connettività in uscita. All'interno di una semplice architettura diretta al cloud, la soluzione deve garantire un accesso a Internet sicuro per tutti i workload, indipendentemente dal fatto che siano ubicati in un cloud pubblico o nel data center aziendale.

Le principali funzionalità necessarie per proteggere le comunicazioni tra workload e Internet includono:

- Ispezione completa basata su proxy TLS/SSL
- Azzeramento della superficie di attacco
- Accesso consentito solo ai siti approvati
- Protezione avanzata contro i malware per bloccare le minacce 0-day

Per fare un esempio, supponiamo che la tua organizzazione disponga di app situate in AWS West e AWS East e che queste richiedano un aggiornamento. La richiesta dovrà essere inoltrata a una piattaforma centrale in cui le policy vengono applicate e gestite. Una soluzione ideale sarà in grado di applicare policy zero trust e di connettere l'origine e la destinazione in modo sicuro.



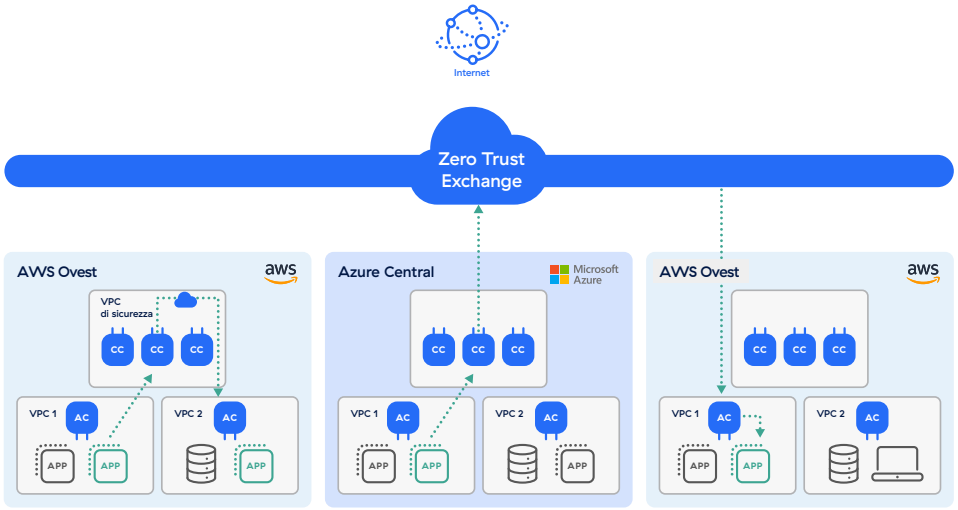
Semplificare e proteggere le comunicazioni tra workload

L'applicazione del modello zero trust per i workload nel cloud richiede anche una connettività sicura tra workload. È essenziale che i workload siano in grado di comunicare, sia tra più cloud che all'interno di un singolo cloud privato virtuale (VPC). Queste comunicazioni dovrebbero passare attraverso la piattaforma zero trust centrale, dove vengono applicate le policy di sicurezza e dove identità e contesto vengono utilizzati per verificare l'affidabilità prima di consentire la connessione.

In particolare, dovrebbe essere previsto un meccanismo per facilitare le comunicazioni all'interno del workload. Per la connettività VPC–VPC, il traffico potrebbe essere instradato da una VPC a un private service edge, da cui verrebbe quindi negoziata una connessione all'app di destinazione (ubicata in una VPC diversa). Per la connettività cloud–to–cloud, il traffico potrebbe essere inoltrato a una piattaforma zero trust centrale, dove verrebbe stabilita una connessione verso un'app di destinazione situata in un cloud diverso.

Le principali funzionalità necessarie per proteggere le comunicazioni tra workload includono:

- Protezione della connettività multicloud e multi–regione
- Garanzia di connettività sicura tra VPC/VNET
- Eliminazione della superficie di attacco della rete con accesso Zero Trust (ZTNA)
- Blocco del movimento laterale delle minacce



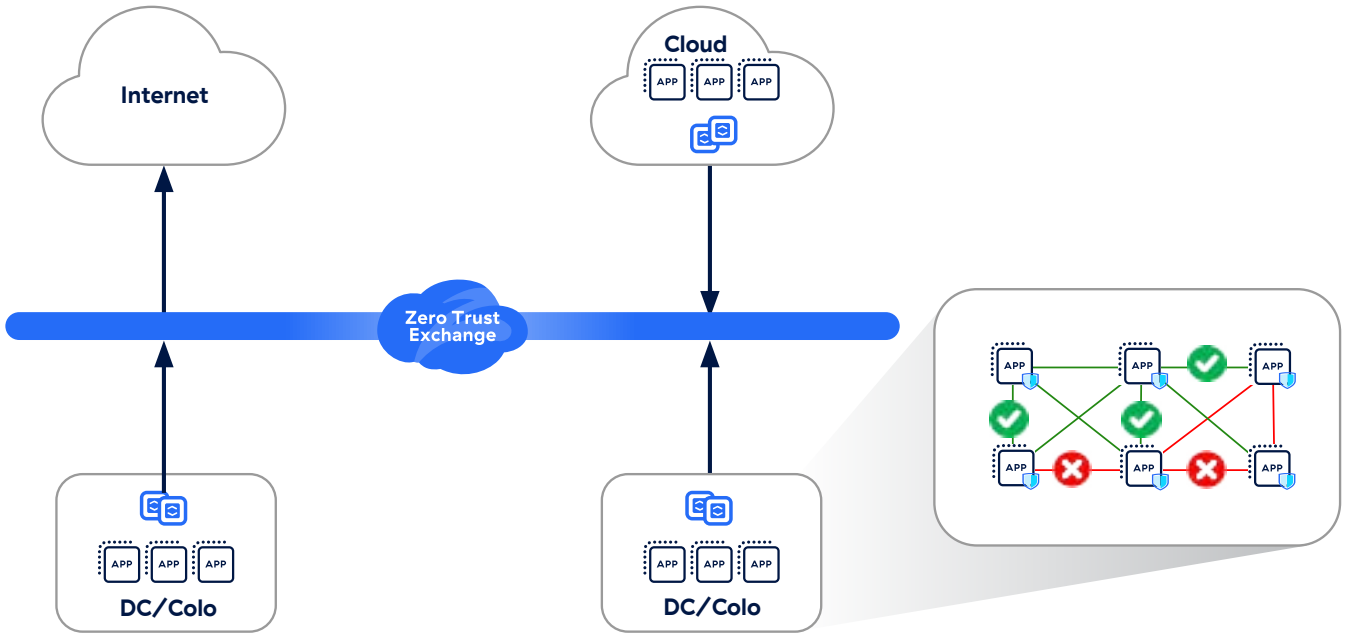
Ottieni facilmente una microsegmentazione granulare

La microsegmentazione, considerata un componente fondamentale della sicurezza zero trust, impedisce lo spostamento laterale delle minacce suddividendo gruppi di applicazioni o workload in piccoli segmenti in base ai requisiti di comunicazione delle singole applicazioni. Ai workload è consentito comunicare all'interno dei propri segmenti, ma essi non possono scambiare comunicazioni non autorizzate con workload esterni.

La microsegmentazione consente di applicare policy zero trust a livello granulare nell'intera rete interna dell'organizzazione, non solo a livello perimetrale, in modo da estendere le protezioni sia ai workload on-premise sia a quelli in esecuzione nel cloud.

Le principali funzionalità necessarie per la microsegmentazione del workload includono:

- Rilevamento delle risorse in tempo reale basata sull'intelligenza artificiale
- Segmentazione basata su host e non basata su host
- Capacità di segmentare i workload all'interno e tra VPC/VNET



Una soluzione zero trust per i workload cloud deve avere diverse caratteristiche fondamentali:

#1: La capacità di eseguire ispezioni TLS/SSL su larga scala

Molte delle minacce più pericolose di oggi si nascondono nel il traffico cifrato. Per rilevarle, è necessaria una piattaforma completa in grado di eseguire ispezioni TLS/SSL complete su larga scala, senza le limitazioni prestazionali imposte dalle applicazioni legacy.

Cerca una soluzione che possa offrire:

- **Capacità illimitata** di ispezionare il traffico TLS/SSL di tutti i tuoi utenti senza influire negativamente sulle prestazioni
- **Scalabilità elastica** in base alle richieste del traffico
- **Gestione semplificata dei certificati**
- **Controllo granulare delle policy** che semplifica la conformità escludendo il traffico utente cifrato per categorie di siti Web come assistenza sanitaria o servizi bancari

#2: Funzionalità affidabili di protezione dei dati

Un approccio di difesa avanzata alla protezione dei dati include la capacità di applicare policy di prevenzione della perdita di dati (DLP) su larga scala senza influire sulle prestazioni. In questo modo si fornisce un ulteriore livello di protezione. Nel caso in cui un workload nel cloud dovesse essere compromesso, sarà comunque possibile applicare le policy e impedire l'esfiltrazione dei dati.

Cerca una soluzione che possa offrire:

- **Una dashboard semplificata** in cui è possibile configurare e gestire le policy DLP
- **Tecniche avanzate di gestione dei dati** come Exact Data Management (EDM) e Optical Character Recognition (OCR)
- **Ispezione dei contenuti inline affidabile su larga scala**

#3: Funzionalità avanzate di protezione dalle minacce

Per bloccare le minacce più pericolose e sofisticate di oggi, una piattaforma di sicurezza dei workload cloud zero trust deve essere in grado di garantire che ogni pacchetto, proveniente da qualsiasi workload, possa essere completamente ispezionato dall'inizio alla fine. Ciò richiede un sistema integrato e sempre attivo di ispezione TLS/SSL e la possibilità di applicare policy dettagliate per tutto il traffico.

Inoltre, le principali funzionalità necessarie includono:

- **Tecnologie di deception integrate** che utilizzano esche, trappole e honeypot per proteggere i dati più preziosi con elevata affidabilità e un basso tasso di falsi positivi
- **Cloud sandbox** per mettere in quarantena e ispezionare potenziali minacce, senza permettere che si diffondano
- **Protezione da malware** in grado di bloccare ransomware, spyware e malware noti oltre a minacce nuove

#4: Segmentazione completa basata sull'host

La microsegmentazione impedisce lo spostamento laterale delle minacce per ridurre al minimo il raggio di azione degli attacchi e i danni che un incidente informatico potrebbe causare. La microsegmentazione basata sull'host utilizza agenti installati sui dispositivi endpoint per fornire controllo e visibilità molto più granulari e semplificare la gestione della segmentazione basata sull'identità. L'utilizzo di un agente consente la segmentazione in base a policy dinamiche e comprensibili per gli utenti anziché regole statiche a livello di rete.

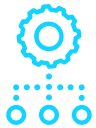
In particolare, cerca una soluzione che possa fornire:

- **Rilevamento delle risorse in tempo reale** con l'intelligenza artificiale, per offrire visibilità granulare su tutti i dispositivi, servizi e risorse all'interno del tuo ecosistema aziendale
- **Suggerimenti sulle policy zero trust** in base all'analisi del traffico
- **Integrazione con una piattaforma zero trust,** in modo da poter proteggere e segmentare il tuo ambiente in un unico posto, senza dover distribuire più prodotti singoli

I principali casi d'uso per proteggere la connettività dei workload

Una soluzione per la connettività dei workload basata sullo zero trust può aiutare le organizzazioni ad affrontare con successo diverse sfide. Ecco quattro tra le più comuni:

Protezione del traffico verso Internet
Quando le applicazioni comunicano con Internet o con le applicazioni SaaS, il traffico in uscita deve essere ispezionato per rilevare attacchi informatici e potenziali perdite di dati. Zscaler gestisce la più grande piattaforma di sicurezza cloud inline al mondo, che offre una protezione avanzata dalle minacce su scala cloud senza alcun impatto sulle prestazioni e senza compromettere il servizio.



Segmentazione dei workload
Con la giusta soluzione per la comunicazione dei workload, è possibile adottare un approccio granulare e metodico alla segmentazione di questi ultimi. In questo modo, è possibile semplificare l'applicazione delle policy per controllare la connettività dei workload su VPC, regioni, cloud pubblici e privati.

Migrazione sul cloud
Questo è spesso un processo lungo e complicato per le organizzazioni, durante il quale è necessario considerare molti fattori, tra cui la strategia di migrazione da seguire: optare per un semplice trasferimento, o ricostruire le app? La giusta soluzione per la comunicazione dei workload può rendere più semplice e sicuro il collegamento delle nuove applicazioni spostate sul cloud.

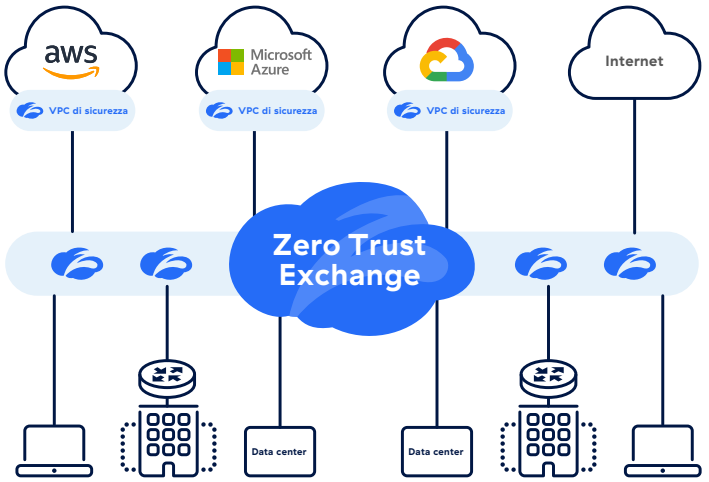
Fusioni e acquisizioni
Con una soluzione moderna per la comunicazione dei workload basata su zero trust e nativa nel cloud, è possibile garantire un accesso sicuro alle applicazioni tra reti diverse, senza la necessità di riprogettare o ristrutturare le reti.

Zscaler Workload Communications è la risposta

Cerchi una soluzione end-to-end che possa fare tutto questo e molto altro? Zscaler Zero Trust Exchange™ ha reso possibile ripensare completamente le comunicazioni tra workload all'interno di un'architettura semplice, collaudata e diretta al cloud.

Zscaler Workload Communications rappresenta un approccio completo per proteggere la connettività dei workload nel cloud e on-premise; questa soluzione combina Zscaler Internet Access™ (ZIA) per le comunicazioni tra workload e Internet, e Zscaler Private Access™ (ZPA) per le comunicazioni tra workload e le funzionalità di microsegmentazione zero trust a segmento singolo. Allo stesso tempo, è in grado di offrire prestazioni elevate, per garantire agli utenti esperienze eccellenti, e la scalabilità necessaria per tenere il passo con l'evoluzione dell'infrastruttura cloud all'aumento delle operazioni.

Zscaler Workload Communications offre una sicurezza cloud basata su zero trust altamente efficace e in grado di adattarsi alle tue esigenze. Le funzionalità di scalabilità automatica flessibile consentono di gestire con facilità l'aumento del traffico. Zero Trust Exchange opera già su larga scala, con oltre 150 data center in tutto il mondo. Zscaler gestisce automaticamente tutti gli aggiornamenti per conto tuo; l'infrastruttura è integrata in modo nativo con l'infrastruttura di sicurezza dei provider di cloud pubblici con funzionalità come gateway di transito e bilanciatori di carico.



Inoltre, Zscaler Workload Communications semplifica e centralizza la gestione delle policy. Tutte le policy possono essere create e aggiornate in un'unica console centrale facile da usare. Esse vengono poi applicate all'interno di Zero Trust Exchange, dove è possibile usare le policy ZIA o ZPA per garantire un'ispezione completa dei contenuti e un controllo delle comunicazioni dei workload basato sull'identità. Le comunicazioni possono quindi essere inoltrate verso qualsiasi destinazione, che si tratti di Internet o di altre applicazioni private all'interno di ambienti cloud. Le policy possono essere facilmente applicate su larga scala ogni volta che sia necessario distribuire workload aggiuntivi nel cloud.

Se ti interessa saperne di più sui vantaggi dell'utilizzo di Zscaler Workload Communications, contattaci oggi stesso. Puoi anche ricevere ulteriori informazioni visitando la pagina web Zscaler Zero Trust Cloud Connectivity.

zscaler™ | Experience your world, secured.™

Informazioni su Zscaler
Zscaler (NASDAQ: ZS) accelera la trasformazione digitale in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. Zscaler Zero Trust Exchange protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati grazie alla connessione sicura di utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in più di 150 data center nel mondo, Zero Trust Exchange, basata sul framework SASE, è la più grande piattaforma di cloud security inline del mondo. Scopri di più su **zscaler.com/it** o seguici su **X (precedentemente Twitter) @zscaler**.

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

zscaler. com/it