Cloud Security Landscape: una guida per il 2025-2026



Il panorama della sicurezza cloud ha raggiunto un punto di svolta critico: le organizzazioni si trovano a fronteggiare un **incremento del 388% negli alert di sicurezza cloud** e un **aumento del 47% negli attacchi informatici settimanali**, mentre devono al contempo confrontarsi con la realtà che il **99% dei fallimenti nella sicurezza cloud è attribuibile a errori di configurazione dei clienti**. Questa analisi approfondita evidenzia come, a fronte di un'adozione del cloud sempre più rapida, la maturità della sicurezza debba evolvere drasticamente per tenere il passo con la sofisticazione delle minacce contemporanee e la complessità degli ambienti cloud moderni.

Lo scenario attuale delle minacce evidenzia sfide senza precedenti

L'ambiente di sicurezza cloud 2024-2025 è caratterizzato da **attacchi privi di malware che costituiscono il 79% delle intrusioni cloud**, segnando un cambiamento fondamentale nelle tattiche degli avversari. I cybercriminali si sono evoluti oltre il malware tradizionale, sfruttando credenziali legittime: il **35% degli incidenti cloud coinvolge l'abuso di credenziali valide**, e si registra un impressionante **aumento del 442% delle operazioni di vishing** tra la prima e la seconda metà del 2024.

Gli **attacchi cross-domain sono diventati la norma**, con il **70% degli incidenti di sicurezza che coinvolgono tre o più superfici di attacco**, tra endpoint, reti e ambienti cloud. Il tempo più rapido registrato per l'espansione di un attacco eCrime si è ridotto a soli **51 secondi**, dimostrando la velocità

con cui le minacce possono propagarsi nelle infrastrutture cloud. Questi attacchi sono sempre più sofisticati: l'**86% degli attacchi hands-on-keyboard è condotto da attori eCrime** che mescolano attività malevole e operazioni legittime per eludere i sistemi di rilevamento.

L'emergere delle **minacce potenziate dall'intelligenza artificiale (IA)** rappresenta probabilmente l'evoluzione più significativa nello scenario delle minacce: le organizzazioni segnalano un **incremento del 67% degli attacchi basati su IA** rispetto al 2023, mentre il **61% delle imprese teme che attacchi alimentati dall'IA possano compromettere dati sensibili**. Tuttavia, solo il **25% si ritiene adeguatamente preparato** a contrastare queste minacce potenziate, creando un pericoloso divario che gli avversari stanno sfruttando attivamente.

Gli errori di configurazione continuano a rappresentare un tallone d'Achille: il **23% degli incidenti di sicurezza cloud deriva da errori di configurazione**, mentre il **27% delle aziende ha subito violazioni nelle infrastrutture cloud pubbliche**. Il problema è aggravato dal fatto che il **96% degli exploit nel 2024 ha sfruttato vulnerabilità divulgate prima di quest'anno**, segno che le organizzazioni faticano a risolvere efficacemente problemi noti.

Strategie di difesa Cloud Security: approccio defense-in-depth

Un'implementazione efficace della sicurezza cloud richiede un **approccio defense-in-depth** che copra tutti i livelli architetturali. Le *Security Guidance v5* della *Cloud Security Alliance* offrono un framework che copre **12 domini critici di sicurezza**, mentre la *Cloud Computing Security Reference Architecture* del *NIST* sottolinea l'importanza di controlli su layer fisici, virtuali, applicativi, di piattaforma e di infrastruttura.

La **gestione delle identità e degli accessi (IAM) emerge come pilastro fondamentale** della sicurezza cloud, con l'architettura *Zero Trust* che sta diventando lo standard de facto nelle implementazioni moderne. Le organizzazioni che adottano Zero Trust riportano notevoli miglioramenti nella postura di sicurezza: il **61% ha già definito iniziative Zero Trust**, mentre un ulteriore **35% prevede di implementarle a breve**. Il principio cardine del *never trust, always verify* richiede la **verifica continua e il monitoraggio costante** di tutte le richieste di accesso, indipendentemente dalla posizione o dalle credenziali dell'utente.

Le strategie di **protezione e cifratura dei dati** devono coprire l'intero ciclo di vita delle informazioni, dalla creazione alla cancellazione. È indispensabile implementare la **cifratura dei dati a riposo, in transito e sempre più spesso anche in uso**, grazie a tecnologie di confidential computing. Le **chiavi di cifratura gestite dal cliente** stanno diventando standard per la classificazione dei dati sensibili, con **politiche di rotazione automatica delle chiavi** essenziali per mantenere un'adeguata postura di sicurezza.

L'integrazione del **DevSecOps** rappresenta un cambiamento radicale nell'implementazione della sicurezza, passando da un modello a checkpoint a un'**integrazione continua della sicurezza lungo l'intero ciclo di sviluppo**. Questo include il **Static Application Security Testing (SAST)** nei pipeline CI/CD, il **Dynamic Application Security Testing (DAST)** per la protezione in runtime e la **scansione di Infrastructure as Code (IaC)** per prevenire errori di configurazione prima del rilascio.

Le **configurazioni di sicurezza di rete** devono prevedere strategie di **microsegmentazione** per isolare applicazioni, ambienti e accessi utente. Le soluzioni di **Zero Trust Network Access (ZTNA)** stanno sostituendo le tradizionali VPN, offrendo **controlli di accesso specifici per applicazione** e un **monitoraggio continuo del traffico di rete**.

Framework e standard come roadmap di conformità

Il panorama normativo della sicurezza cloud si sta facendo sempre più complesso, con il **75% della popolazione mondiale che sarà coperta da normative sulla privacy entro il 2025**. Le organizzazioni devono orientarsi tra diversi framework sovrapposti, ciascuno con requisiti e criteri di audit specifici.

Il *NIST Cybersecurity Framework* rappresenta la struttura di riferimento globale, con le cinque funzioni principali (*Identify, Protect, Detect, Respond, Recover*) che offrono un approccio completo alla gestione del rischio cibernetico. I **tier di implementazione** del framework permettono alle organizzazioni di scalare l'adozione in base alla tolleranza al rischio e alle risorse disponibili.

Lo standard **ISO 27001 costituisce la base del sistema di gestione**, mentre l'**ISO 27017 introduce 44 controlli specifici per il cloud** (37 migliorati da ISO 27002 più 7 nuovi) e l'**ISO 27018 disciplina la protezione dei dati personali (PII)** in ambienti cloud. Questi standard forniscono **framework certificabili da terze parti**, con obbligo di audit di sorveglianza annuale.

Il *Cloud Controls Matrix (CCM) v4.0* della *Cloud Security Alliance* offre **197 obiettivi di controllo su 17 domini**, con una guida dettagliata per le implementazioni di sicurezza cloud. Il CCM mappa i controlli con i principali standard come **NIST 800-53, ISO 27001, PCI DSS e HIPAA**, consentendo di soddisfare più requisiti di conformità in un'unica implementazione.

Le **normative specifiche di settore** introducono ulteriori complessità: **FedRAMP** richiede l'implementazione dei controlli NIST SP 800-53 Rev. 5 per le agenzie federali, con

monitoraggio continuo e audit annuali; **HIPAA** impone **Business Associate Agreements (BAA)** e salvaguardie tecniche per i dati sanitari; **PCI DSS 4.0** introduce requisiti rafforzati per gli ambienti cloud, con **obbligo di conformità entro marzo 2025**.

I modelli di responsabilità condivisa definiscono i confini della sicurezza

Comprendere i modelli di responsabilità condivisa dei fornitori cloud è fondamentale per un'implementazione efficace della sicurezza, soprattutto considerando che, secondo Gartner, **il 99% dei fallimenti di sicurezza nel cloud fino al 2025 sarà imputabile ai clienti**. Ogni grande provider ha sviluppato approcci distinti per definire questi confini.

Il modello **AWS "Sicurezza DEL cloud vs. sicurezza NEL cloud"** offre una chiara distinzione: AWS è responsabile di **infrastruttura fisica, sistemi operativi host e layer di virtualizzazione**, mentre i clienti devono gestire **sistemi operativi guest, applicazioni e protezione dei dati**. La suddivisione delle responsabilità varia significativamente a seconda del tipo di servizio, con **IaaS che richiede la massima responsabilità da parte del cliente** e **SaaS che la riduce al minimo**.

Microsoft Azure sottolinea le responsabilità costanti del cliente in tutti i modelli di deployment, inclusi **classificazione dei dati, gestione degli endpoint, degli account e delle identità**. L'approccio di Azure evidenzia che le **responsabilità del cliente rimangono coerenti** a prescindere dal modello di servizio, sebbene il loro ambito vari sensibilmente tra IaaS, PaaS e SaaS.

Google Cloud Platform ha superato il tradizionale modello di responsabilità condivisa, introducendo il concetto di **"Shared**

Fate”, un approccio più collaborativo che prevede **linee guida proattive sulla sicurezza, configurazioni sicure di default e programmi di protezione del rischio**. Questo modello rappresenta l’evoluzione verso partnership di sicurezza più integrate tra provider e clienti.

Le **variazioni specifiche per servizio** creano ulteriori complessità: le implementazioni **IaaS richiedono ai clienti la gestione di sistemi operativi, applicazioni e configurazioni di rete**, mentre negli ambienti **PaaS la gestione di OS e runtime** è trasferita al provider. Le implementazioni **SaaS riducono al minimo le responsabilità del cliente**, ma richiedono comunque **una scrupolosa governance dei dati e gestione degli accessi utente**.

Gli strumenti moderni consolidano le capacità di sicurezza

Il panorama degli strumenti di sicurezza cloud ha subito una profonda trasformazione, con l’emergere delle **Cloud-Native Application Protection Platforms (CNAPP)** come architettura dominante. Secondo Gartner, entro il 2029 **il 60% delle imprese prive di un CNAPP unificato non avrà visibilità sufficiente sul cloud** e non riuscirà a raggiungere gli obiettivi di zero trust.

Le **soluzioni CNAPP leader** includono **Wiz** (che ha raggiunto un **fatturato ricorrente annuale di 100 milioni di dollari in soli 18 mesi**, conquistando **il 40% delle aziende Fortune 100**), **Palo Alto Networks Prisma Cloud** (con una **quota di mercato del 26%**) e **Microsoft Defender for Cloud** (che offre **integrazione conveniente per organizzazioni con ecosistemi Microsoft**). Queste piattaforme integrano in un’unica soluzione funzionalità di **Cloud Security Posture Management (CSPM)**, **Cloud Workload Protection Platforms (CWPP)** e **Cloud Infrastructure Entitlements Management (CIEM)**.

L’**integrazione di IA e machine learning** è diventata uno standard in questi strumenti: il **63% dei professionisti della sicurezza ritiene che l’IA migliori la sicurezza**, mentre il **55% delle organizzazioni ha implementato soluzioni di IA generativa** per la protezione cloud. **Google Cloud Security Operations** è stato il **primo grande provider a offrire IA generativa in disponibilità generale per la sicurezza**, abilitando **query di sicurezza in linguaggio naturale** e **generazione automatizzata di playbook di risposta agli incidenti**.

La **sicurezza di container e Kubernetes** si è evoluta per affrontare le sfide specifiche dei workload containerizzati: **SentinelOne** offre **protezione K8s in tempo reale** e rilevamento del **configuration drift**, mentre **Aqua Security** garantisce **sicurezza completa sul ciclo di vita del container** con scanning delle vulnerabilità e gestione della conformità. Soluzioni open source come **Falco** e **Kubescape** rappresentano alternative community-driven per le organizzazioni che necessitano di personalizzazioni specifiche.

La **gestione della sicurezza multi-cloud** è ormai essenziale, dato che il **79% delle organizzazioni utilizza più provider cloud** e il **69% segnala difficoltà nella gestione delle configurazioni**. Le soluzioni leader offrono **visibilità e controllo unificati** su AWS, Azure e Google Cloud Platform, semplificando la gestione di **policy di sicurezza coerenti** in ambienti cloud eterogenei.

Le tendenze emergenti ridefiniscono le strategie di sicurezza

L’**integrazione dell’intelligenza artificiale** rappresenta la trasformazione più significativa nelle capacità di sicurezza cloud: le soluzioni di rilevamento basate su IA consentono **analisi comportamentale**, **rilevamento in tempo reale di anomalie** e **risposta automatizzata agli incidenti**. Tuttavia,

l’IA introduce anche nuovi rischi, come le **implementazioni shadow AI** che sfuggono al controllo delle organizzazioni e gli **attacchi assistiti dall’IA** sempre più sofisticati.

L’adozione dell’**architettura Zero Trust** continua ad accelerare, con il **61% delle organizzazioni che ha già definito iniziative Zero Trust** e oltre il **90% che ne riconosce l’importanza**. Le principali sfide di implementazione includono la **resistenza culturale all’adozione di misure di sicurezza più rigide**, la **complessità tecnica nell’integrazione con sistemi legacy** e gli **elevati costi di implementazione**, soprattutto in ambienti ibridi.

L’evoluzione della **sicurezza per serverless e container** affronta la **natura effimera dei workload moderni**: il mercato globale della sicurezza serverless ha raggiunto **1,82 miliardi di dollari nel 2022**, con un CAGR previsto del **29,9%**. Le soluzioni moderne offrono **sensori runtime per ambienti serverless**, **analisi comportamentale delle funzioni basata su IA** e **miglioramento delle capacità di logging e osservabilità**.

La preparazione alla **cifratura quantum-safe** è iniziata, con organizzazioni che iniziano a **implementare tecniche di crittografia post-quantistica** per prepararsi alle minacce dei computer quantistici. Questo include **crittografia basata su reticoli** per ambienti ad alta sicurezza e la preparazione ai **futuri standard quantum-safe** attesi nei prossimi anni.

Errori comuni come fonte di vulnerabilità persistenti

Nonostante la crescente consapevolezza, le organizzazioni continuano a commettere **errori critici nella sicurezza cloud**, esponendosi a rischi significativi. Le **chiavi di accesso esposte** restano la **principale causa di violazioni**, con **una rotazione inadeguata delle credenziali che incide sul 45% degli incidenti** e **account con privilegi eccessivi coinvolti**

nel 37% dei casi.

Le **errate configurazioni dei bucket di storage pubblici** rappresentano un'altra fonte di vulnerabilità: il **68,97% dei bucket Amazon S3 risulta configurato in modo errato**, con impostazioni di blocco dell'accesso pubblico disabilitate che creano rischi di esposizione dei dati. Questi errori derivano spesso da **policy dei bucket non corrette**, **mancata implementazione della cifratura** e **controlli di accesso insufficienti**.

Le **configurazioni di rete insicure** costituiscono una categoria di vulnerabilità particolarmente critica, includendo **security group configurati in modo improprio**, **porte aperte e protocolli non protetti**, oltre a **mancanza di segmentazione di rete**. A questi problemi si somma una gestione IAM carente, con **permessi di default troppo permissivi**, **assenza di autenticazione a più fattori** e **scarsa gestione dei privilegi**.

Le **lacune di competenze interessano il 98% delle organizzazioni** e compromettono in modo significativo l'efficacia delle strategie di sicurezza: il **95% ritiene che il gap di competenze abbia un impatto negativo sul business**, mentre il **53% segnala carenze problematiche di competenze in ambito cybersecurity**. Si stima che la **carenza di professionisti della sicurezza cloud superi i 3 milioni a livello globale**, creando sfide significative per una protezione efficace.

Indicazioni pratiche per un'implementazione efficace

Per implementare strategie di sicurezza cloud efficaci, le organizzazioni dovrebbero adottare un **approccio a fasi**, iniziando con i **controlli di sicurezza fondamentali** e progredendo verso una **protezione avanzata dalle minacce**. Nella **fase 1** (mesi 1-3) è essenziale definire un **framework di**

governance per la sicurezza cloud, costruire le basi della **gestione delle identità e degli accessi** e implementare le **prime capacità di logging e monitoraggio**. La **fase 2** (mesi 4-6) dovrebbe concentrarsi sull'implementazione di **controlli di sicurezza di rete**, **protezione e cifratura dei dati** e sulle pratiche di **DevSecOps**.

Il **budget** deve riflettere la centralità della sicurezza cloud: il **60% delle organizzazioni prevede un aumento del budget per la sicurezza cloud**, con una spesa globale stimata di **7 miliardi di dollari nel 2024**. È consigliabile destinare **dal 10% al 20% del budget IT alla cybersecurity**, investendo in soluzioni cloud-native che garantiscano **copertura completa** e **capacità di automazione**.

Il **monitoraggio e il miglioramento continuo** sono indispensabili: occorre effettuare **scansioni di conformità quotidiane**, monitorare le configurazioni in tempo reale e attivare **workflow di remediation automatizzati**. Gli obiettivi dovrebbero comprendere il **mantenimento di una compliance del 95% rispetto ai baseline di sicurezza** e tempi di **rilevamento inferiori a un'ora** per eventuali deviazioni di configurazione.

Raccomandazioni strategiche

La **strategia tecnologica** deve privilegiare **piattaforme unificate rispetto a soluzioni puntuali**, con l'implementazione di **CNAPP** per offrire **capacità di sicurezza integrate** su tutta l'infrastruttura cloud. Gli investimenti in **IA e automazione** devono concentrarsi su **rilevamento e risposta alle minacce**, accompagnati da un'adeguata **governance per le implementazioni IA**.

La **gestione dei talenti** richiede **programmi di formazione completi**, **collaborazioni con managed security service provider** e **percorsi di aggiornamento del personale esistente** sui principi della sicurezza cloud. È fondamentale sviluppare **strategie di retention** per i professionisti qualificati e

definire **chiari percorsi di crescita professionale** per affrontare il problema delle carenze di competenze.

La **gestione del rischio** deve adottare strategie orientate alla **prevenzione**, con pratiche di **Infrastructure as Code**, **monitoraggio continuo della compliance** e **valutazioni regolari della sicurezza**. Le organizzazioni devono prepararsi alla **crittografia quantum-safe**, pur mantenendo aggiornati gli **standard e i protocolli di sicurezza attuali**.

Il panorama della sicurezza cloud continuerà a evolversi rapidamente: l'**IA diventerà essenziale per gestire la sicurezza su larga scala**, i **framework di governance delle identità** dovranno affrontare la sfida delle identità non umane, che superano quelle umane con un rapporto di **45 a 1**, mentre le normative sulla privacy copriranno il **75% della popolazione mondiale entro il 2025**. Il successo richiede di considerare la sicurezza cloud come un **processo continuo**, anziché un'implementazione una tantum, con **revisioni, aggiornamenti e miglioramenti regolari** in base alle minacce emergenti e ai cambiamenti nei requisiti di business.

Le organizzazioni che sapranno implementare strategie di sicurezza cloud complete otterranno **vantaggi competitivi** in termini di **continuità operativa**, **riduzione dei costi legati alle violazioni** e **maggiore fiducia da parte dei clienti**. Gli investimenti in sicurezza cloud si traducono in benefici economici concreti, con **ambienti semplificati che permettono risparmi medi di 1,64 milioni di dollari** e **un'adeguata dotazione di personale che riduce i costi di violazione di circa 550.000 dollari**. La chiave è **bilanciare innovazione e gestione del rischio**, investendo in **tecnologie e risorse umane**, mantenendo al contempo un **atteggiamento proattivo** verso le minacce e le opportunità emergenti.

Fonti

Threat Intelligence e analisi delle minacce

Statistiche e dati di mercato

Framework e standard di sicurezza

Zero Trust e architetture moderne

Modelli di responsabilità condivisa

Strumenti e tecnologie di sicurezza

Compliance e normative

Trend e previsioni future

Intelligenza artificiale e sicurezza

DevSecOps e sviluppo sicuro

Strumenti open source

Formazione e certificazioni

Misconfigurazioni e vulnerabilità

Ricerca Accademica e Analisi Settoriali

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/cloud-security/