GUIDA PER PMI · L'EVOLUZIONE DI WAZUH

Cloud Posture per PMI

Di cosa sei davvero responsabile nel cloud, e come tenerlo sotto controllo ogni giorno.

> La guida pratica per capire di cosa sei davvero responsabile quando porti dati e applicazioni nel cloud, e come tenere sotto controllo la sicurezza ogni giorno invece che una volta l'anno. Scritta per chi in azienda deve decidere, non solo per chi configura i server.

IN QUESTA GUIDA

01 Il cloud non è sicuro "di default"

02 Le 5 misconfigurazioni che fanno più danni

03 CSPM in continuo: ogni giorno, non ogni anno

04 Multi-cloud, vista unica

05 Compliance senza dolore: dai controlli ai report

ArcaSafe S.r.l. · Partner Wazuh · Azienda certificata ISO/IEC 27001 e ISO 9001
SOC gestito on-prem con tecnici certificati · Cybersecurity, NIS2 & GDPR

> La maggior parte delle violazioni cloud non nasce da attacchi sofisticati: nasce da errori di configurazione che restano lì, silenziosi, per mesi. Questa guida spiega di cosa sei responsabile quando porti dati e applicazioni nel cloud, quali sono i cinque errori che fanno più danni, e come il monitoraggio continuo li trova prima che lo faccia qualcun altro.

CAPITOLO 01

Il cloud non è sicuro "di default"

C'è un equivoco che costa caro a molte PMI: pensare che spostare tutto su AWS, Azure o Google Cloud significhi "delegare la sicurezza al provider". Non è così. Il modello che regola il cloud si chiama responsabilità condivisa, ed è la prima cosa da mettere a fuoco prima di parlare di strumenti.

Responsabilità condivisa: il provider protegge il cloud, tu proteggi ciò che ci metti dentro.

La regola è semplice da enunciare e facile da dimenticare: il provider protegge il cloud, tu proteggi ciò che ci metti dentro. Amazon, Microsoft e Google si occupano dei data center, dell'hardware, della rete fisica, dell'hypervisor. Ma le configurazioni dei tuoi servizi, i permessi che assegni agli utenti, le regole di accesso ai tuoi bucket, le chiavi e le password che gestisci: quelli sono tuoi. Al cento per cento.

Il punto scomodo è che la maggior parte delle violazioni cloud non nasce da attacchi sofisticati o da exploit esotici. Nasce da errori di configurazione: uno storage lasciato pubblico "per fare in fretta", un utente amministratore creato per un test e mai rimosso, una porta aperta verso internet che nessuno ricorda. Nessun hacker geniale: solo una svista che resta lì, silenziosa, per mesi. È una buona notizia, perché gli errori di configurazione si possono trovare e correggere — ma richiede un cambio di mentalità: la sicurezza cloud non è un prodotto che si compra e si accende, è una postura che si mantiene.

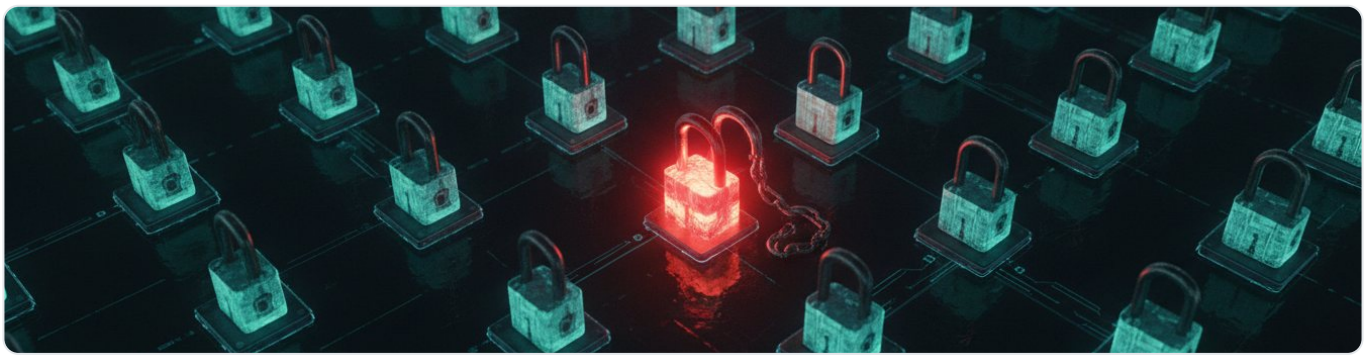
E qui entra in gioco un tema che per molte imprese italiane è diventato un obbligo, non un'opzione. NIS2 e GDPR chiedono di dimostrare che dati e sistemi siano protetti con misure adeguate e verificabili. Dire "è tutto sul cloud, ci pensa il provider" non è una risposta accettabile davanti a un'autorità di controllo. La responsabilità di ciò che metti nel cloud resta tua, e va documentata. I capitoli che seguono spiegano come.

> ✓ **La regola da ricordare**
>
> Il provider protegge il cloud; configurazioni, permessi, chiavi e accessi sono tuoi. Al cento per cento.

CAPITOLO 02

⚠ Le 5 misconfigurazioni che fanno più danni

Se la maggior parte dei problemi cloud nasce da errori di configurazione, la buona notizia è che questi errori sono quasi sempre gli stessi. Conoscerli significa sapere dove guardare. Ecco i cinque che, nella pratica, provocano più danni.



Porte esposte, privilegi eccessivi, segreti in chiaro, bucket pubblici, log spenti: gli stessi cinque errori, ovunque.

- **1. Porte esposte a internet.** Database, pannelli di amministrazione e protocolli di accesso remoto lasciati aperti verso il mondo vengono scansionati in continuazione da bot automatici. Non serve essere un bersaglio designato: basta essere raggiungibili.
- **2. Utenti sovra-privilegiati.** Il principio del minimo privilegio dice che ognuno deve avere solo i permessi che gli servono. Nella realtà si moltiplicano gli account con diritti da amministratore "perché era più comodo". Ogni utente over-privilegiato è una chiave universale: se qualcuno se ne impossessa, non apre una stanza, apre l'intero edificio.
- **3. Segreti esposti.** Password, chiavi di accesso e token salvati in chiaro dentro file di configurazione, repository di codice o variabili non protette. Un secret in chiaro è la combinazione della cassaforte scritta su un post-it attaccato allo sportello: chi trova quel file, trova le chiavi.
- **4. Bucket pubblici.** Lo storage cloud è comodissimo, e proprio per questo pericoloso: basta una spunta sbagliata e un archivio destinato a restare privato diventa consultabile da chiunque conosca l'indirizzo. Molte fughe di dati clamorose sono esattamente questo — nessuna effrazione, solo un contenitore lasciato aperto.
- **5. Log spenti.** Il più subdolo, perché non causa un danno diretto: lo abilita. Senza registrazione degli eventi un attacco può avvenire senza lasciare traccia. Non puoi accorgerti di nulla, non puoi indagare, e non puoi dimostrare a un'autorità cosa è successo e quando — un problema serio sul piano NIS2 e GDPR.

Queste cinque voci hanno un tratto in comune: sono invisibili finché non le cerchi. Nessuna genera un allarme da sola. È per questo che serve qualcosa che le vada a cercare, sistematicamente e di continuo. Ed è esattamente il compito del CSPM.

> **Invisibili finché non le cerchi**
>
> Nessuna di queste cinque genera un allarme da sola: serve qualcosa che le vada a cercare, di continuo. È il compito del CSPM.

CAPITOLO 03

CSPM in continuo: ogni giorno, non ogni anno

Per anni la sicurezza si è misurata con l'audit annuale: una volta all'anno arriva un consulente, controlla, produce un report, e per dodici mesi si vive su quella fotografia. Il problema è che il cloud non sta fermo dodici mesi. Cambia ogni giorno: si crea un nuovo utente, si apre un servizio, si modifica un permesso, si aggiunge uno storage. Ognuna di queste azioni può introdurre una delle misconfigurazioni del capitolo precedente. L'audit di gennaio non sa nulla della porta aperta a marzo.

Dalla fotografia annuale al monitoraggio continuo della postura cloud.

Il Cloud Security Posture Management ribalta l'approccio. Invece di una fotografia una volta l'anno, offre un monitoraggio continuo: valuta la tua postura di sicurezza cloud costantemente e la mantiene nel tempo. In pratica, il CSPM confronta di continuo la configurazione reale del tuo ambiente con quella che dovrebbe essere. Quando qualcuno lascia un bucket pubblico, crea un utente con troppi privilegi, espone una porta o spegne un log, il sistema se ne accorge — non a fine anno, ma vicino al momento in cui l'errore viene commesso.

La distanza tra "abbiamo sbagliato" e "ce ne siamo accorti" si accorcia da mesi a poco tempo. E in sicurezza quella distanza è tutto: è la finestra in cui un attaccante può muoversi indisturbato.

Per una PMI il valore è doppio. Da un lato, un livello di controllo enterprise-grade: il tipo di vigilanza continua che finora sembrava riservato alle grandi aziende con team di sicurezza dedicati. Dall'altro, arriva senza investimenti infrastrutturali pesanti: il monitoraggio continuo diventa un servizio, non un progetto edilizio. C'è poi la conformità: un audit annuale prova che un giorno all'anno eri a posto; il monitoraggio continuo prova

che lo sei stato ogni giorno — ed è questo che un'autorità di controllo vuole vedere. Prima, però, va risolto un altro problema pratico: quasi nessuna PMI vive su un solo cloud.

> **La finestra che conta**
>
> La distanza tra "abbiamo sbagliato" e "ce ne siamo accorti" è la finestra in cui un attaccante può muoversi indisturbato. Il CSPM la accorcia da mesi a poco tempo.

CAPITOLO 04

Multi-cloud, vista unica

La cartolina del "portiamo tutto su un unico cloud" corrisponde raramente alla realtà. La PMI tipica ha le macchine su AWS o Azure, la posta e i documenti su Microsoft 365, il codice su GitHub, magari un servizio su Google Cloud ereditato da un progetto passato. Non è disordine: è come funzionano le aziende vere, che adottano lo strumento migliore per ogni esigenza nel momento in cui serve.

AWS, Azure, GCP, Microsoft 365 e GitHub in un'unica vista, con lo stesso metro.

Il problema è che ogni piattaforma ha la sua console, il suo linguaggio, le sue impostazioni di sicurezza. Controllarle una per una significa saltare da un pannello all'altro, imparare cinque logiche diverse, e — inevitabilmente — trascurarne qualcuna. La sicurezza che dipende dalla buona volontà di aprire cinque cruscotti ogni mattina è una sicurezza che non c'è. Gli angoli ciechi non stanno dentro le singole piattaforme: stanno negli spazi tra una piattaforma e l'altra, dove nessuno guarda.

Il CSPM affronta proprio questo. Porta AWS, Azure, GCP, Microsoft 365 e GitHub dentro un'unica vista. Le stesse misconfigurazioni — porte esposte, utenti sovra-privilegiati, segreti in chiaro, storage pubblici, log spenti — vengono cercate ovunque, con lo stesso metro, e riportate in un unico posto. Su Microsoft 365 e GitHub, in particolare, questo significa anche tenere sotto osservazione i log delle azioni degli utenti: chi ha fatto cosa, quando, e se qualcosa si discosta dalla norma.

Il guadagno per una PMI è concreto e misurabile in tempo. Non serve un esperto per ogni cloud: serve un solo posto dove leggere lo stato complessivo. La domanda "siamo sicuri?" smette di richiedere cinque risposte parziali e ne ottiene una sola, coerente. E c'è un riflesso diretto sulla conformità: NIS2 e GDPR guardano ai dati e ai processi dell'azienda nel loro insieme, non cloud per cloud. Avere una vista unica è il

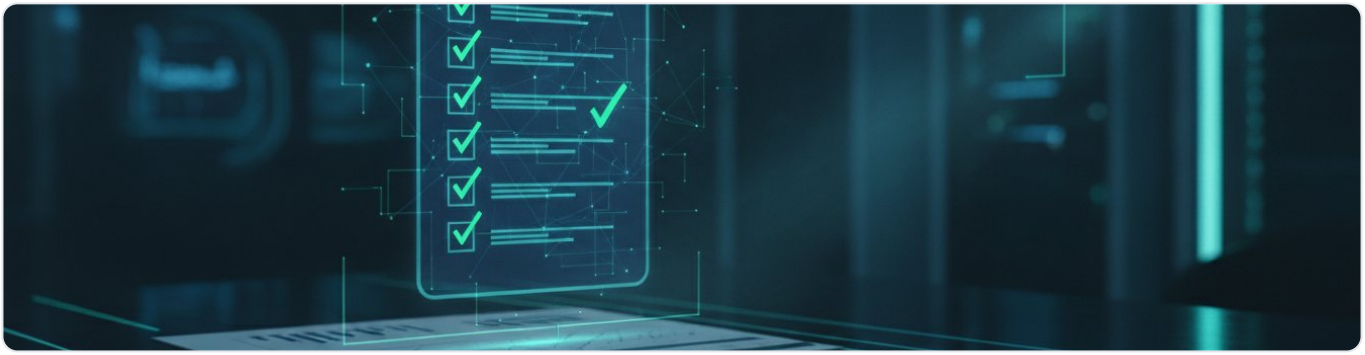
modo in cui la tua postura di sicurezza smette di essere una collezione di isole e diventa un quadro unico — l'unico che ha senso mostrare quando qualcuno chiede conto di come proteggi le tue informazioni.

> **Gli angoli ciechi stanno nel mezzo**
>
> Non dentro le singole piattaforme, ma negli spazi tra una piattaforma e l'altra, dove nessuno guarda.

CAPITOLO 05

Compliance senza dolore: dai controlli ai report

Per molte PMI la parola "conformità" evoca fatica: fascicoli da riempire, evidenze da raccogliere di corsa, notti prima dell'audit passate a cercare screenshot. Il paradosso è che quasi tutto il materiale che serve a dimostrare la conformità è lo stesso materiale che serve a essere sicuri. Il CSPM sfrutta esattamente questa sovrapposizione: i controlli che ti tengono al sicuro producono, come sottoprodotto naturale, le prove che sei in regola.



Gli stessi controlli che ti tengono al sicuro producono le prove che sei in regola.

Il meccanismo è la verifica di conformità in continuo. Gli stessi controlli che cercano porte esposte, utenti sovra-privilegiati, segreti in chiaro, bucket pubblici e log spenti sono mappati sui requisiti dei principali standard: PCI DSS per i dati di pagamento, GDPR per i dati personali, NIST 800-53 e HIPAA per i framework più strutturati. Ogni volta che il sistema valuta la tua postura, sta anche misurando quanto sei allineato a queste normative — non a fine anno, ma con continuità.

È qui che il discorso si aggancia alla NIS2. La direttiva non chiede un certificato appeso alla parete: chiede misure adeguate e la capacità di dimostrare che siano attive e mantenute nel tempo. Un controllo continuo che registra ogni giorno lo stato del tuo cloud è esattamente il tipo di evidenza che regge davanti a un'autorità. La differenza tra "ci fidiamo che sia tutto a posto" e "ecco i dati che lo provano, giorno per giorno" è la differenza tra subire un'ispezione e affrontarla con serenità.

Il passaggio finale è dai controlli ai report. I dati grezzi, da soli, non parlano il linguaggio di un revisore o di un consiglio di amministrazione. Il valore sta nel tradurli: prendere un rilievo tecnico — "questo bucket è pubblico", "questo utente ha troppi privilegi" — e trasformarlo in ciò che conta per l'azienda, cioè un requisito NIS2 o GDPR soddisfatto o da sistemare, con una priorità chiara. Ed è precisamente il punto in cui lo

strumento da solo non basta: un cruscotto pieno di rilievi tecnici, senza qualcuno che li interpreti e li ordini per rischio reale, resta rumore. La conformità "senza dolore" nasce dall'unione delle due cose: uno strumento che vede tutto in continuo, e una consulenza che traduce quel tutto in decisioni, priorità e adempimenti.

> ✓ **Il nodo NIS2**
>
> La direttiva non chiede un certificato appeso alla parete: chiede misure attive e dimostrabili nel tempo. Un controllo continuo, registrato ogni giorno, è quel tipo di evidenza.

Vuoi sapere dove sei esposto oggi?

Il cloud non ti chiede di essere un esperto di sicurezza. Ti chiede di sapere di cosa sei responsabile e di tenerlo sotto controllo con continuità. Il CSPM rende possibile la seconda parte; la prima è una scelta. In ArcaSafe uniamo lo strumento che vede tutto — AWS, Azure, GCP, Microsoft 365 e GitHub in un'unica vista, ogni giorno — alla consulenza che traduce il tecnico in adempimento NIS2 e GDPR concreto. Se vuoi capire dove sei oggi, un buon punto di partenza è un check gratuito della tua postura cloud: una fotografia onesta, senza impegno, per sapere quali porte sono aperte prima che lo scopra qualcun altro.

Richiedi il check gratuito della postura cloud →

Un click apre un'email già compilata: aggiungi i tuoi dati e invia. Oppure scrivici a commerciale@arcasafe.eu.

ArcaSafe S.r.l. · Via G. Segantini 5, 20825 Barlassina (MB) · CF e P.IVA 09546870966 · info@arcasafe.eu · PEC arcasafe@pec.it · arcasafe.eu · Partner Wazuh · ISO/IEC 27001 e ISO 9001