

# Sophos Cloud Security

Accelera il tuo business e agevola una transizione verso il cloud incentrata sulla sicurezza con Sophos. Proteggi workload in cloud, dati, app e accessi dalle più recenti minacce informatiche e da altri tipi di vulnerabilità, grazie alla migliore piattaforma cloud in assoluto per la gestione della cybersecurity: Sophos Central.



## Cloud Threat Detection e Response 24/7

Potenzia l'efficacia del tuo team di sicurezza con una vista di gestione unificata, che connette tutte le soluzioni CSPM (gestione del profilo di sicurezza sul cloud), i firewall e la protezione dei workload nei tuoi ambienti cloud pubblici e ibridi. Tutto questo con il supporto di un team selezionato di esperti di sicurezza operativo 24/7, che vigila sui tuoi ambienti e ti garantisce protezione, monitoraggio e risposta alle minacce.

## La Soluzione Di Protezione Del Cloud Ibrido A Cui Si Affidano Milioni Di Persone

Milioni di utenti si affidano a Sophos per ottenere soluzioni di sicurezza potenti ed efficaci, progettate per essere accessibili e facili da gestire per qualsiasi tipo di organizzazione. Disponibili in una singola console di gestione unificata, Sophos Central e le soluzioni Sophos per la protezione, il monitoraggio e la risposta alle minacce sono garanzia di sicurezza contro minacce e vulnerabilità in ambienti on-premise e cloud.

## Protezione Nativa Del Cloud

Accelera la crescita del tuo business e salvaguarda la sicurezza dei tuoi investimenti nel cloud con la protezione Sophos nativa del cloud, che protegge Amazon Web Services, Microsoft Azure, Google Cloud Platform, Oracle Cloud Infrastructure, cluster Kubernetes, registri dei container e ambienti Infrastructure as Code. Sophos difende tutti questi sistemi dalle minacce e dalle vulnerabilità più recenti, ottimizzando allo stesso tempo la spesa per le risorse cloud.

## Una Partnership Che Estende Il Tuo Team

Gestisci la protezione a modo tuo: puoi dirigere il tuo team di sicurezza interno con l'aiuto di un Partner Sophos, oppure puoi affidarti al servizio Sophos Managed Threat Response (MTR), per usufruire delle capacità di monitoraggio e risposta 24/7 agli attacchi più sofisticati.

Sophos MTR è ideale per completare la protezione cloud di Sophos. Questo servizio di risposta gestita alle minacce interagisce con i tuoi team, monitora il tuo ambiente 24/7, risponde alle potenziali minacce, individua eventuali indicatori di compromissione e fornisce analisi dettagliate degli eventi, incluse informazioni su come, quando, dove e perché hanno avuto luogo gli attacchi, per impedire anche alle minacce più sofisticate di compromettere i tuoi dati e sistemi.

*"Siamo consci del fatto che i cybercriminali sono all'opera 24h su 24 e che cercheranno di attaccare nei momenti meno opportuni. Ad aiutarci c'è Sophos, che ci protegge 24/7, anche quando il mio team non è disponibile"*

sostiene Dinesh Adithan, Director of Software Engineering presso Celayix.

## Caratteristiche Principali

- ▶ Protezione per workload nel cloud, dati, app e accessi
- ▶ Automazione della protezione contro le minacce negli ambienti cloud pubblici
- ▶ Prevenzione proattiva degli errori di configurazione e delle vulnerabilità di sicurezza
- ▶ Risposta gestita alle minacce operativa 24/7, per monitorare, analizzare e valutare costantemente gli eventi di sicurezza
- ▶ Disponibile su AWS e Azure Marketplace
- ▶ Viene considerata come parte dei piani di utilizzo dei provider di servizi cloud concordati, inclusi nel budget di sicurezza

**SOPHOS**

## Protezione Multicloud Completa

### Automazione Della Sicurezza Per Le DevOps

Includi la cybersecurity nelle prime fasi del processo di sviluppo, imposta pipeline di CI/CD automatizzate e integra strumenti di sicurezza nel processo in assoluta semplicità, grazie al nostro generatore visivo con trascinarsi della selezione: Sophos Factory. Questa interfaccia visiva di progettazione con utilizzo minimo di codice permette sia ai team di sviluppo che a quelli operativi di compilare, strutturare pacchetti e condividere una valutazione automatica della conformità per tutte le build; inoltre, consente di automatizzare le distribuzioni di tipo Infrastructure as Code, di svolgere analisi SAST/DAST/SCA del codice prima della distribuzione e molto di più.

### Visibilità, Governance e Conformità

Riduci la superficie di attacco con una visibilità superiore sugli ambienti multicloud, per rilevare e correggere i rischi di sicurezza, nel pieno rispetto della conformità.

- Gestione del profilo di sicurezza nel cloud su ambienti AWS, Azure, GCP, Kubernetes, Infrastructure as Code e Docker Hub.
- Massima visibilità su tutto. Inventari delle risorse, visualizzazioni della rete, spesa per il cloud e rischi di configurazione.
- Automatizza le valutazioni del rispetto della conformità, per risparmiarti diverse settimane di tempo e fatica, grazie a report appositamente configurati per i controlli.
- Limita il rischio senza rallentare le DevOps, con la protezione degli ambienti Infrastructure-as-Code e delle immagini dei container.
- Assicurati la massima tranquillità, nella certezza che le tue risorse vengono gestite in ordine di priorità, con avvisi che presentano la valutazione del rischio con indicatori di colori diversi.

### Sicurezza della rete e delle applicazioni

Proteggi la rete e le applicazioni con Sophos Firewall per il cloud edge. Questa soluzione integrata offre in un'unica piattaforma la combinazione ottimale di diverse tecnologie di sicurezza leader

di settore, inclusi IPS, ATP, filtro degli URL e WAF. Integra anche opzioni di disponibilità elevata e connettività SD-WAN e VPN flessibile, per connettere qualsiasi utente, da qualsiasi luogo. Per l'auto scaling, Sophos UTM Firewall offre un'ulteriore soluzione per questi ambienti dinamici.

### Gestione Degli Entitlement

Assicurati che tutte le identità siano autorizzate a eseguire solo ed esclusivamente le azioni necessarie per svolgere le operazioni di loro competenza, grazie alla gestione degli entitlement delle infrastrutture cloud in ambienti multicloud.

- Visualizza i ruoli IAM con stretti rapporti di connessione reciproca, per segnalare e bloccare i ruoli IAM con privilegi eccessivi.
- Identifica pattern e luoghi di accesso utente insoliti, per individuare eventuali casi di furto o utilizzo improprio delle credenziali.
- Utilizza SophosAI per mettere in correlazione anche le anomalie ad alto rischio più eterogenee nei comportamenti degli utenti, per prevenire la compromissione dei sistemi di sicurezza.

### Protezione Dei Workload Nel Cloud

Proteggi gli host e i workload dei container con la protezione Linux e Windows a impatto minimo, disponibile tramite agent o API per Linux.

- Identifica anche gli incidenti di sicurezza più sofisticati su Linux a livello di runtime, senza distribuire un modulo kernel.
- Proteggi i tuoi host Windows e i dipendenti in smart working contro ransomware, exploit e minacce mai osservate prima.
- Controlla applicazioni, configurazioni di lockdown e modifiche ai sistemi di monitoraggio nei file di sistema Windows più importanti.
- Snellisci i processi di indagine e risposta alle minacce con XDR, per attribuire la giusta priorità agli eventi e metterli in correlazione.
- Estendi la protezione con le API Intelix dei SophosLabs, che offrono ricerche automatiche delle minacce nei propri database, più scansioni antimalware in ambienti serverless.

### Modernizza Il Processo Di Acquisizione Della Cybersecurity

La protezione Sophos per il cloud è disponibile su [AWS Marketplace](#) e [Azure Marketplace](#), per aiutare i clienti a semplificare l'acquisizione della cybersecurity, con soluzioni che vengono considerate come parte dei piani di utilizzo di già concordati.

Scopri di più o parla con un esperto

[sophos.it/cloud](https://sophos.it/cloud)

Vendite per Italia:  
Tel: [+39] 02 94 75 98 00  
E-mail: [sales@sophos.it](mailto:sales@sophos.it)