SOPHOS
Cybersecurity delivered.

Implementazione Di Una Protezione Multicloud Completa Su Ambienti, Workload Ed Identità Diversi

L'integrazione di strumenti di cybersecurity in workload e ambienti cloud diversi, unita alla gestione degli entitlement, garantisce alle organizzazioni visibilità, sicurezza e risultati di conformità superiori negli ambienti Amazon Web Services, Microsoft Azure e Google Cloud Platform.

Briefing Sulla Soluzione Sophos. Luglio 2022

Maggiore Visibilità Sui Sistemi Da Proteggere

Con la sempre più diffusa adozione di tecnologie cloud come host, container, servizi di archiviazione e Infrastructure as Code, è ormai diventato indispensabile poter contare su una maggiore visibilità, per proteggere i sistemi da eventuali errori di configurazione, malware, ransomware, violazioni e molto di più.

Il Potere Dell'Abbreviazione Dei Tempi Di Rilevamento E Risposta

Sophos Cloud Native Security è una soluzione unificata e integrata, che impedisce che malware, exploit, errori di configurazione e comportamenti anomali compromettano la sicurezza del cloud. Grazie alle sue potenti capacità di rilevamento e risposta estesi (XDR), i team di sicurezza possono facilmente rilevare e individuare proattivamente le minacce in ambienti multicloud; inoltre, possono ricevere informazioni sui rilevamenti di eventuali incidenti in ordine di priorità e usufruire della correlazione automatica degli eventi di sicurezza per ottimizzare le indagini e i tempi di risposta alle minacce.

Massimo Ritorno Sul Tuo Investimento Nella Cybersecurity

Ottimizza i controlli e ottieni di più dal tuo budget di cybersecurity, con opzioni di protezione dei workload del cloud e gestione della configurazione e degli entitlement del cloud, tutto in un'unica soluzione.

- Visibilità su tutti i tuoi sistemi, grazie agli inventari su richiesta delle risorse e alle visualizzazioni della topologia della rete.
- Prevenzione e correzione dei rischi di configurazione su host, container, Kubernetes, ambienti serverless, servizi di archiviazione e di database, nonché gruppi di sicurezza di rete.
- Applica il principio di assegnazione di meno privilegi possibili, identificando rapidamente i ruoli IAM con privilegi eccessivi, i comportamenti degli utenti ad alto rischio ed eventuali indicatori di furto di credenziali, prima che possa verificarsi una violazione di sicurezza.
- Adotta un approccio "shift left", tenendoti un passo avanti rispetto agli hacker, con controlli di cybersecurity integrati in tutti gli stadi della pipeline di sviluppo, per individuare vulnerabilità dei sistemi operativi, errori di configurazione e l'eventuale incorporazione di segreti, password e chiavi nel codice.
- Identifica anche gli incidenti di sicurezza più sofisticati su host e container 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.
- Monitora in maniera ininterrotta i sistemi per mantenere la sicurezza e rispettare gli standard di conformità, grazie a criteri automaticamente mappati al tuo ambiente.
- Monitora e ottimizza i costi per il cloud su più servizi AWS e Azure da un'unica schermata.

[1] Bernard Marr, "The 5 Biggest Cloud Computing Trends In 2022." Forbes, 25 ott. 2021

L'uso del cloud pubblico continua a crescere

Le aziende affronteranno costi combinati pari a

482 miliardi di $

sui servizi cloud nel 2022, con un aumento rispetto ai 313 miliardi di $ del 2020[1].

Una Cybersecurity Che Si Adatta Al Tuo Mondo

Aumenta l'agilità dei sistemi della tua organizzazione, con l'integrazione di avvisi sul profilo di integrità dell'ambiente cloud nei più comuni strumenti per collaborazione, flusso di lavoro e SIEM. Potrai continuare a utilizzare i tuoi strumenti attuali.

I team SOC possono incrementare la propria efficienza grazie alle integrazioni con Splunk, Azure Sentinel e PagerDuty, che permettono di ricevere notifiche immediate sugli eventi di sicurezza e conformità che influiscono sul profilo di sicurezza.

Le integrazioni con Slack, Microsoft Teams e l'Amazon Simple Notification Service (SNS) permettono a team di organizzazioni diverse di collaborare in maniera efficace per correggere gli incidenti di sicurezza e conformità. Crea ticket di JIRA e ServiceNow direttamente dalla console Sophos per incorporare in maniera semplicissima la risoluzione degli incidenti di sicurezza e conformità nelle normali procedure quotidiane.

Un Approccio Flessibile Alla Cloud Security

Il nostro approccio flessibile ti permette di controllare come viene implementata e gestita Sophos Cloud Native Security nei tuoi ambienti cloud. Puoi dirigere il tuo team di sicurezza interno oppure affidarti al servizio Sophos Managed Threat Response per il monitoraggio 24/7 dei tuoi ambienti, che include la risposta a potenziali minacce, la ricerca di indicatori di compromissione e il blocco delle minacce più sofisticate, in modo che non possano colpire i tuoi dati e sistemi.

Comincia Subito Con Sophos

Puoi utilizzare gli strumenti di cloud security e correzione di Sophos in maniera autonoma (con l'assistenza di un Partner Sophos), oppure puoi affidarti al servizio Sophos MTR per una risposta ottimale ai più recenti incidenti di sicurezza attualmente riscontrati.

Scopri le soluzioni Sophos visitando

Sophos.it/cloud

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

2022-07-08 SB-IT (DD)

SOPHOS