Novità: Sophos Cloud Native Security

Protezione Multicloud Completa Per Ambienti, Workload E Identità

SOPHOS
Cybersecurity delivered.

Un'Unica Soluzione Di Cloud Security Integrata

Con la sempre più diffusa adozione generale di tecnologie cloud come host, container, servizi di archiviazione e Infrastructure as Code, le organizzazioni devono a tutti i costi incrementare la propria visibilità, per poter proteggere i sistemi da eventuali errori di configurazione, malware, ransomware, violazioni e altri pericoli.

Sophos Cloud Native Security offre in un'unica soluzione la combinazione ottimale degli strumenti necessari per ottenere gli elevati livelli di visibilità di cui hai bisogno e trasformare le tue strutture cloud in ambienti robusti, difficili da compromettere e rapidi da ripristinare. Sophos Cloud Native Security è una soluzione integrata e unificata, che include Sophos Cloud Optix e Sophos Intercept X Advanced for Server XDR; è disponibile per Amazon Web Services, Microsoft Azure e Google Cloud Platform.

Grazie alla vista di gestione unificata della console di Sophos Central, avrai il potere di individuare proattivamente le minacce in ambienti multicloud. Inoltre, riceverai notifiche sui rilevamenti degli incidenti, classificati in ordine di priorità, e potrai usufruire degli eventi di sicurezza automaticamente connessi, per ottimizzare le indagini e la risposta alle minacce, tutto da un'unica dashboard.

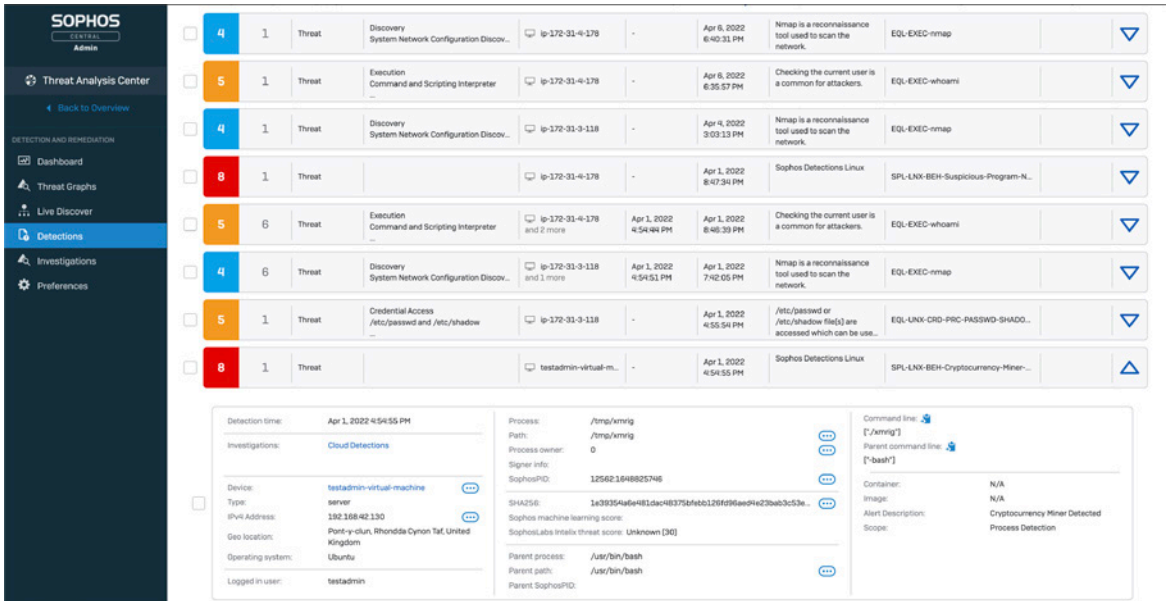
La Nuova Evoluzione Di Sophos Server Protection

Per proteggere i tuoi workload dei server nel cloud pubblico, ora l'efficacia comprovata della protezione Sophos per Windows è stata estesa e include anche le distribuzioni Linux: uno dei sistemi operativi più diffusi nel cloud.

Pochi mesi fa, per Sophos Server Protection per i workload nel cloud c'è stata un'evoluzione importante in termini di opzioni per Linux e per i container, grazie alla nuova protezione antiexploit contro le minacce in fase di runtime basata sui comportamenti: questa funzionalità è in grado di identificare in tempo reale anche i più sofisticati incidenti sui sistemi Linux.

Sophos Cloud Native Security offre le opzioni di sicurezza dei workload necessarie per proteggere i tuoi dati e la tua infrastruttura sia oggi che nelle sue evoluzioni future nel cloud.

- Proteggi tutto: cloud, data center, host, container, sistemi Windows o Linux.
- Ottieni massimi livelli di performance e tempi di attività superiori, grazie alla protezione a impatto minimo per host Linux e Windows, disponibile tramite agent o API per Linux.
- Identifica gli incidenti di sicurezza più sofisticati a livello di runtime sui container e su Linux, senza bisogno di 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 (rilevamento e risposta estesi), per attribuire la giusta priorità agli eventi e metterli in correlazione.



Esempi di rilevamenti di minacce in fase di runtime su Linux, effettuati da Sophos XDR e visualizzati nella console di Sophos Central.

Opzioni Di Distribuzione Per La Protezione Dei Workload Nel Cloud

Gestione con Sophos Central: l'agent Linux a impatto minimo offre ai team di sicurezza tutte le risorse di cui hanno bisogno per svolgere le indagini e rispondere a comportamenti anomali, tentativi di exploit e minacce malware su Windows e Linux. Poiché monitora l'host, questa opzione di distribuzione consente di gestire le soluzioni Sophos da un'unica area di lavoro, per passare liberamente dalle attività di threat hunting a quelle di correzione e gestione, e viceversa, con la massima semplicità.

Integrazione tramite API: Sophos Linux Sensor è un'opzione estremamente flessibile e ottimizzata per garantire massimi livelli di performance. Il sensore utilizza API per integrare negli strumenti di risposta alle minacce che già usi i rilevamenti dettagliati in fase di runtime ottenuti da ambienti host o container. Avrai così maggiore controllo sulla creazione di set di regole personalizzate, e potrai specificare regole contenenti solo i rilevamenti dei comportamenti in esecuzione di cui hai bisogno per identificare un caso di utilizzo specifico.

Oltre all'agent Sophos Linux, Sophos Linux Sensor offre:

- Più opzioni di rilevamento: accesso a rilevamenti aggiuntivi per i tentativi di exploit di applicazioni e sistema
- Configurazione e ottimizzazione: opzioni di modifica degli elenchi di autorizzazione e di blocco per i rilevamenti predefiniti
- Migliore distribuzione delle risorse: opzioni di configurazione che aiutano a ottimizzare l'uso delle risorse

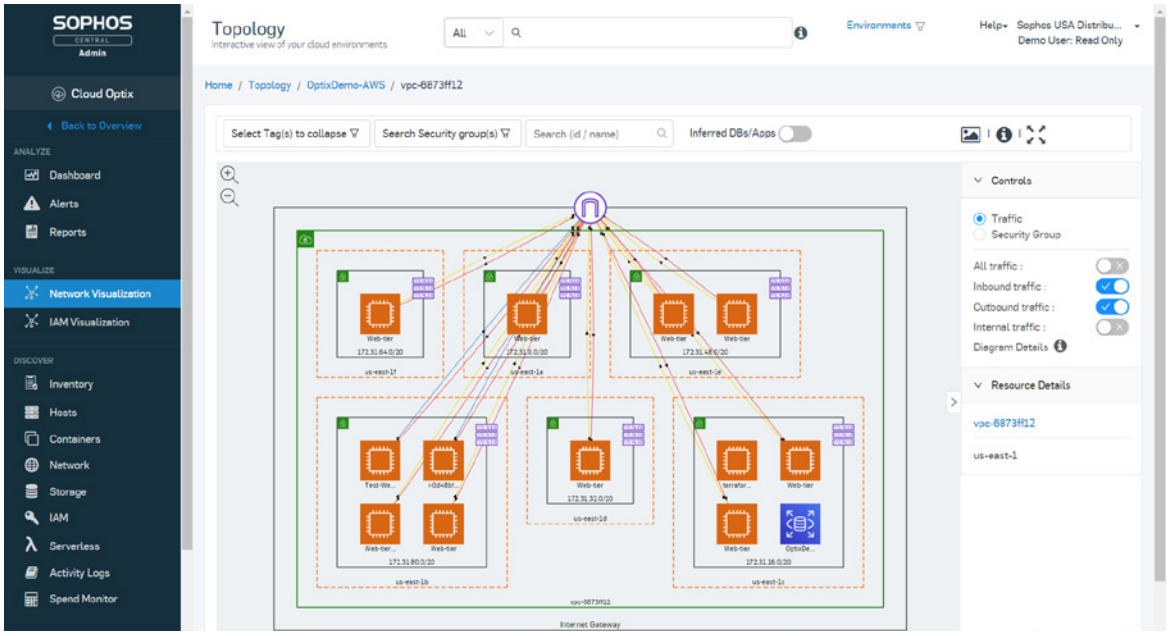
Maggiore Visibilità Sui Sistemi Da Proteggere

Ridurre la superficie di attacco dei tuoi ambienti AWS, Azure e GCP significa molto di più della semplice protezione e del rilevamento delle minacce per i workload nel cloud. Ed è per questo motivo che Sophos Cloud Native Security sostituisce tutte le opzioni del tuo toolkit di sicurezza con un unico strumento, che include funzionalità di gestione del profilo di sicurezza nel cloud per Kubernetes, protezione degli ambienti Infrastructure as Code, gestione degli entitlement per le infrastrutture cloud e monitoraggio della spesa per il cloud.

Visibilità, Governance e Conformità In Ambienti Multicloud

Incrementa l'efficienza grazie a una visibilità senza agent e a strumenti di correzione per ambienti AWS, Azure, GCP, Kubernetes, Infrastructure as Code e Docker Hub, tutto da un'unica console.

- Ottieni il quadro completo delle tue strutture, con inventari delle risorse su richiesta e visualizzazioni della topologia della rete esportabili.
- Integra servizi di sicurezza per il cloud in un'unica vista, inclusi: Azure Advisor, Azure Sentinel, AWS Security Hub, Amazon GuardDuty, AWS CloudTrail, AWS IAM Access Analyzer, Amazon Detective, Amazon Inspector, AWS Systems Manager e AWS Trusted Advisor.
- Blocca lo shadow IT con l'individuazione automatica delle risorse, le visualizzazioni degli agent di protezione Sophos per i workload e le distribuzioni dei firewall.
- Previeni e correggi gli elementi di configurazione rischiosi su host, container, Kubernetes, ambienti serverless, servizi di archiviazione e di database, nonché gruppi di sicurezza di rete.
- Monitora in maniera ininterrotta i sistemi per mantenere la sicurezza e rispettare gli standard di conformità, grazie a criteri automaticamente mappati al tuo ambiente e a report appositamente configurati per i controlli, che ti risparmiano diverse settimane di tempo e fatica. I criteri disponibili includono CIS Foundations Benchmark, ISO 27001, EBU R 143, FEDRAMP FIEC, GDPR, HIPAA, PCI DSS, SOC2 e le best practice di Sophos.
- Tieni traccia dei costi di servizi multipli su AWS e Azure, grazie a un confronto diretto in un'unica schermata, per migliorare la visibilità. Ricevi consigli su come ottimizzare la spesa per il cloud da Sophos, oppure tramite l'integrazione dei servizi AWS Trusted Advisor o Azure Advisor.
- Riduci il sovraccarico di avvisi e individua in maniera efficace sia i problemi facili da risolvere che quelli di importanza critica, grazie ad avvisi che presentano la valutazione del rischio con indicatori di colori diversi, definendo una procedura dettagliata di correzione.

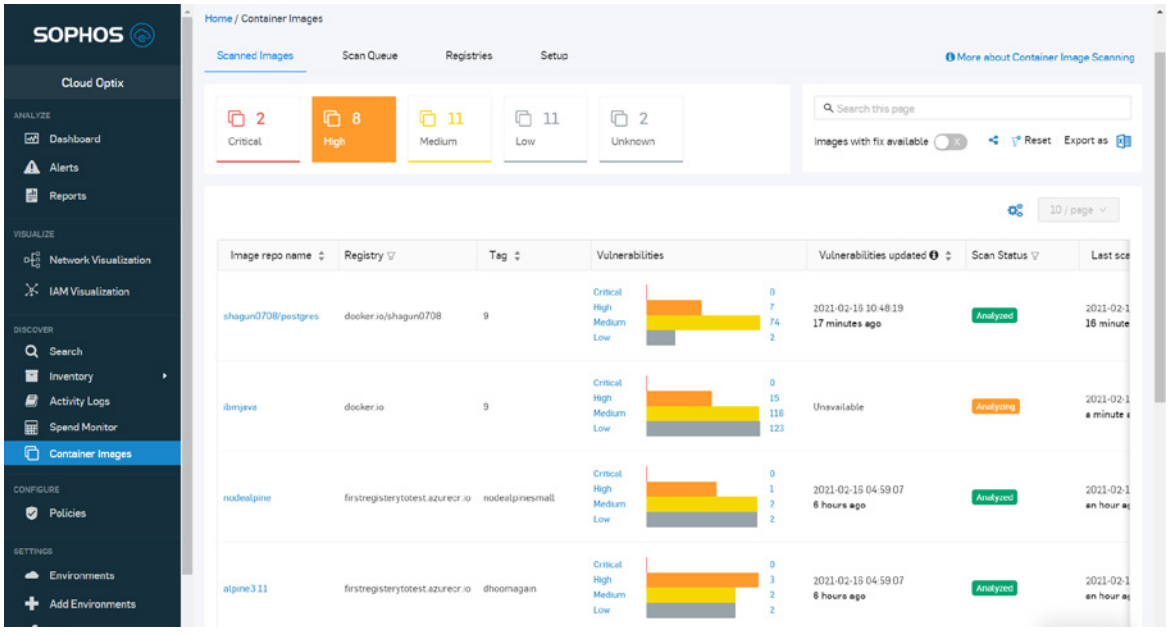


Esempio della visualizzazioni della topologia della rete Sophos per AWS con l'analisi dei gruppi di sicurezza.

Riduci Il Rischio, Senza Compromessi Sulla Rapidità Delle DevOps

Permetti ai tuoi team di sviluppare software in maniera rapida e sicura, con controlli di sicurezza integrati che valutano la conformità e la configurazione in tutte le fasi della pipeline di sviluppo.

- Rileva automaticamente eventuali configurazioni errate, nonché segreti, password e chiavi incorporati nei file dei modelli per Terraform, AWS CloudFormation, Ansible, Kubernetes e Azure Resource Manager.
- Impedisci la distribuzione di container con vulnerabilità del sistema operativo e identifica i fix disponibili, grazie al supporto di Amazon ECR, ACR, registri Docker Hub, ambienti Infrastructure as Code e immagini nelle pipeline di compilazione.
- Approfitta dell'integrazione perfetta con GitHub e Bitbucket, per ricevere i risultati delle scansioni su richiesta in Sophos Central oppure per utilizzare la REST API e analizzare i modelli Infrastructure-as-Code e le immagini dei container in qualsiasi stadio di sviluppo.

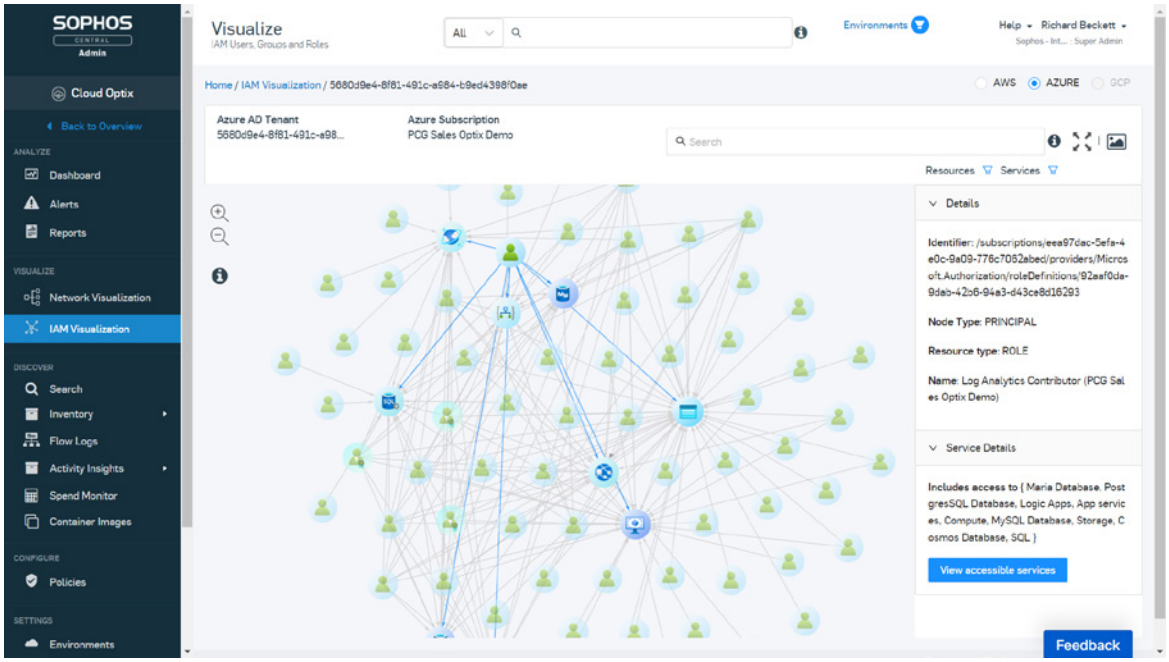


Esempio di riepilogo dei risultati della scansione dell'immagine di Sophos Container alla ricerca di vulnerabilità.

Applica Il Principio Di Assegnazione Di Meno Privilegi Possibili

Con il nostro aiuto, puoi gestire le identità prima che possano essere sfruttate in un attacco, concedendo meno privilegi possibili nei tuoi ambienti multicloud grazie alla gestione degli entitlement per l'infrastruttura cloud.

- Assicurati che tutte le identità possano svolgere solo ed esclusivamente le azioni strettamente necessarie per il proprio lavoro.
- Identifica pattern e luoghi di accesso utente insoliti, per individuare eventuali casi di furto o utilizzo improprio delle credenziali.
- Individua i ruoli IAM di Microsoft Azure orfani, non gestiti e obsoleti, utilizzati per ottenere l'accesso agli ambienti.
- Visualizza i ruoli IAM di AWS con rapporti di connessione reciproca stretti e complessi, per identificare rapidamente e bloccare i ruoli IAM con privilegi eccessivi.
- Utilizza SophosAI per mettere in correlazione anche le anomalie ad alto rischio più eterogenee nei comportamenti degli utenti in ambiente AWS, per prevenire i tentativi violazione.

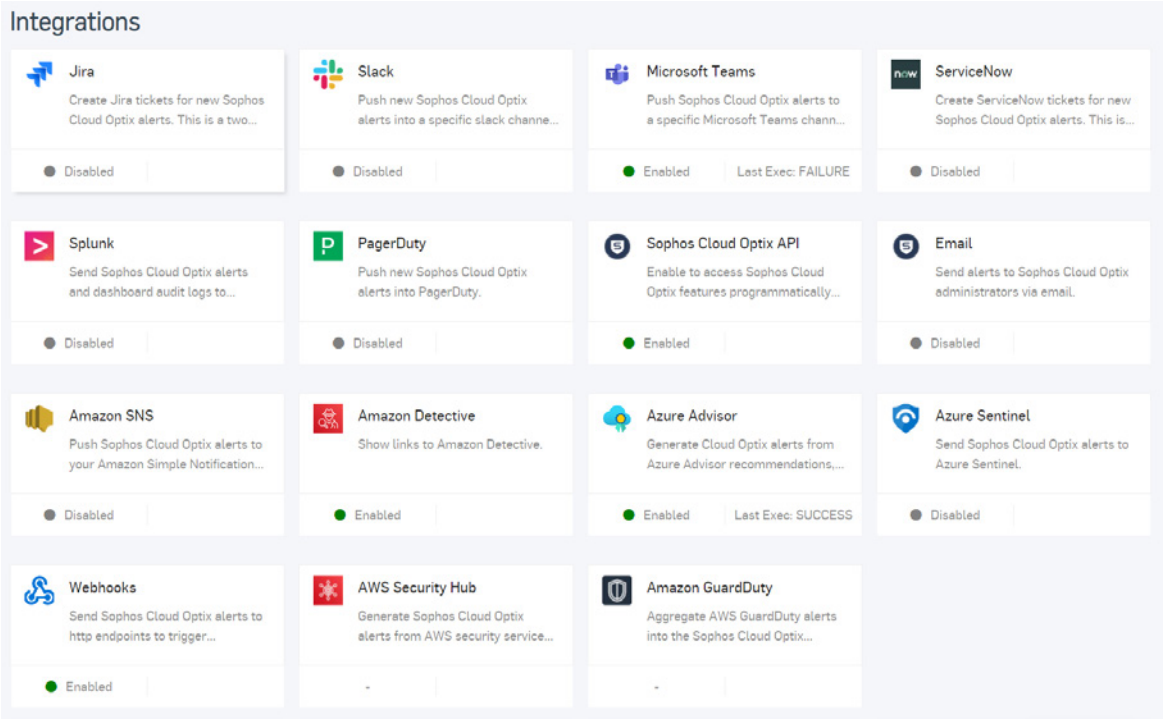


Esempio della visualizzazione Sophos dei ruoli IAM per Microsoft Azure.

Snellisci Le SecOps E Ottimizza La Collaborazione

Aumenta l'agilità dei sistemi per le organizzazioni, grazie all'integrazione di avvisi sul profilo di sicurezza dell'ambiente cloud nei più comuni strumenti per collaborazione, flusso di lavoro e SIEM, oltre a strumenti di DevOps a portata di pochissimi clic.

- Security Operations: integrazione con Splunk, Azure Sentinel e PagerDuty, per ricevere notifiche immediate sugli eventi di sicurezza e conformità.
- Strumenti di collaborazione: invia avvisi immediati su Slack, Microsoft Teams o Amazon Simple Notification Service (SNS), per collaborare immediatamente su argomenti specifici.
- Gestione del flusso di lavoro: incorpora la risposta agli avvisi nei flussi di lavoro standard, grazie alla creazione di ticket JIRA e ServiceNow direttamente da Sophos Central, con integrazione bidirezionale per evitare l'apertura di due casi per lo stesso problema.



Esempio delle integrazioni Sophos più utilizzate, per la gestione degli avvisi relativi al profilo di sicurezza sul cloud.

Partnership Che Estendono Le Capacità Del Tuo Team

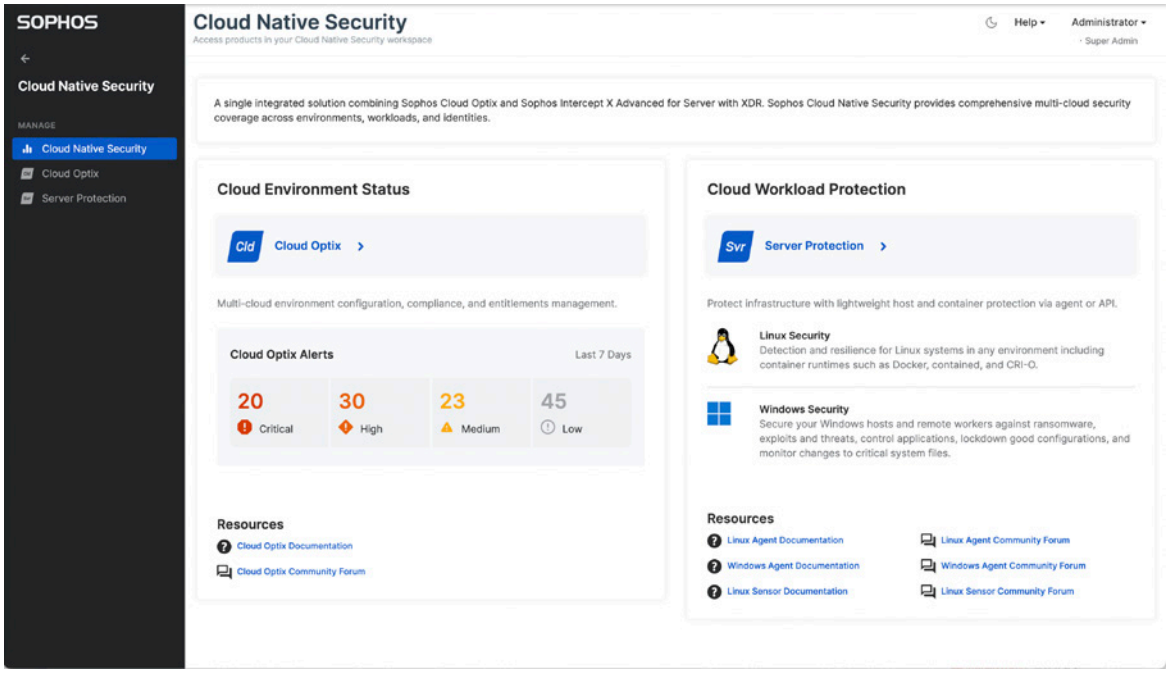
Gestisci la protezione a modo tuo: puoi dirigere il tuo team di sicurezza interno con l'aiuto di un Partner Sophos, oppure puoi affidarti al servizio Sophos Managed Threat Response (MTR), per usufruire di capacità di monitoraggio e risposta 24/7.

Sophos MTR è ideale per completare Sophos Cloud Native Security. 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.

Disponibilità Di Sophos Cloud Native Security

Questo nuovo pacchetto unico è disponibile per tutti i clienti, tramite upgrade da Intercept X Essentials for Server, Intercept X Advanced for Server e Intercept X Advanced for Server with XDR.

Una volta completata l'attivazione in Sophos Central, i clienti e i Partner troveranno una nuova voce "CNS" nel riquadro di navigazione a sinistra. Cliccando su questa voce, si aprirà una nuova dashboard di riepilogo per Cloud Native Security, che include accesso ai prodotti Sophos Cloud Optix e Intercept X Advanced for Server with XDR.



Esempio della dashboard di Sophos Cloud Native Security nella console di gestione di Sophos Central.

Effettua subito una prova gratuita

Registrati per ricevere una prova gratuita di 30 giorni su: sophos.it/cloud

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

© Copyright 2022. Sophos Ltd. Tutti i diritti riservati.
Registrata in Inghilterra e Galles con N° 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Regno Unito
Sophos è un marchio registrato da Sophos Ltd. Tutti gli altri nomi di società e prodotti qui menzionati sono marchi o marchi registrati dei rispettivi titolari.

22-07-06 IT (DD)

SOPHOS