Novedades: Sophos Cloud Native Security

Completa cobertura de seguridad multinube en entornos, cargas de trabajo e identidades

SOPHOS
Cybersecurity delivered.

Una única solución integrada de seguridad en la nube

La adopción de las tecnologías en la nube, como los hosts, los contenedores, los servicios de almacenamiento y la infraestructura como código, significa que las organizaciones deben aumentar su visibilidad para protegerse de los errores de configuración, el malware, el ransomware, las filtraciones, etc.

Sophos Cloud Native Security unifica las herramientas necesarias para proporcionar esa visibilidad y hacer que sus entornos en la nube sean robustos, difíciles de vulnerar y capaces de recuperarse rápidamente. Sophos Cloud Native Security, una única solución integrada disponible para Amazon Web Services, Microsoft Azure y Google Cloud Platform, combina Sophos Cloud Optix y Sophos Intercept X Advanced for Server with XDR.

Con la vista de administración única de la consola de Sophos Central, podrá buscar amenazas multinube, recibir detecciones priorizadas de incidentes, y beneficiarse de los eventos de seguridad conectados automáticamente para optimizar los tiempos de investigación y respuesta a amenazas, todo desde un único lugar.

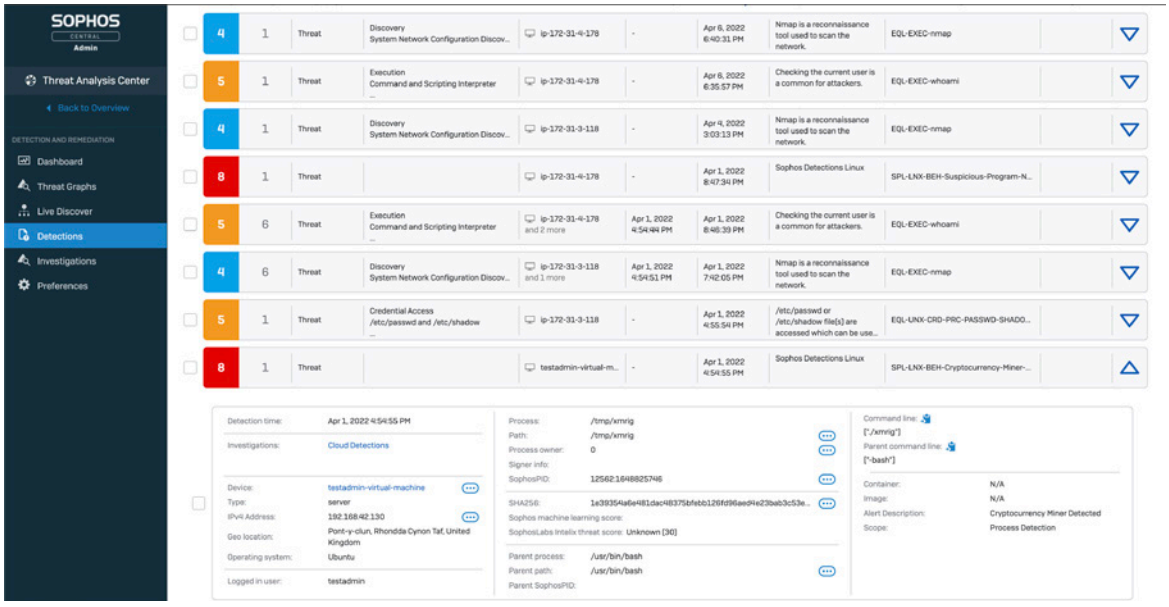
La próxima evolución de Sophos Server Protection

Para proteger sus cargas de trabajo de servidor en la nube pública, Sophos ha ampliado su protección de confianza de Windows para proteger los despliegues Linux, uno de los sistemas operativos más prolíficos en la nube.

A principios de este año, Sophos Server Protection para cargas de trabajo en la nube vio una importante evolución de las funciones para Linux y contenedores, con una nueva protección contra amenazas de comportamiento y exploits en tiempo de ejecución para identificar incidentes de seguridad sofisticados en Linux en el momento en que se producen.

Sophos Cloud Native Security ofrece las funciones de protección de cargas de trabajo necesarias para salvaguardar su infraestructura y sus datos ahora y a medida que evolucionan en la nube.

- Protéjalo todo: la nube, centros de datos, hosts, contenedores, Windows o Linux.
- Aumente el rendimiento y el tiempo de actividad con una protección ligera para hosts Windows y Linux vía agente o API para Linux.
- Identifique incidentes de seguridad sofisticados en Linux y contenedores en tiempo de ejecución sin necesidad de desplegar un módulo de kernel.
- Proteja sus hosts de Windows y sus empleados remotos contra el ransomware, exploits y amenazas desconocidas.
- Controle aplicaciones, bloquee configuraciones y supervise cambios en archivos críticos de sistema de Windows.
- Agilice las investigaciones y la respuesta a amenazas con la detección y respuesta ampliadas (XDR) para priorizar y conectar eventos.



Ejemplo de detecciones de amenazas en tiempo de ejecución en Linux de Sophos XDR en la consola de Sophos Central.

Opciones de despliegue de la protección de cargas de trabajo en la nube

Administración de Sophos Central: este agente ligero de Linux proporciona a los equipos de seguridad la información crítica que necesitan para investigar y responder a las amenazas de comportamiento, exploits y malware en Windows y Linux en un solo sitio. Al supervisar el host, esta opción de despliegue permite a los equipos administrar sus soluciones de Sophos desde un único panel intuitivo y así moverse ágilmente entre la búsqueda, la remediación y la administración de amenazas.

Integración de API: Sophos Linux Sensor es una opción de implementación muy flexible configurada de forma precisa para ofrecer el mejor rendimiento. El sensor utiliza API para integrar exhaustivas detecciones de amenazas en tiempo de ejecución, en entornos de host o contenedor, con sus herramientas de respuesta a amenazas existentes. Ofrece un mayor nivel de control para la creación de conjuntos de reglas personalizadas que contengan solo las detecciones de comportamientos en tiempo de ejecución necesarias para casos de uso de seguridad específicos.

Adicionalmente al Sophos Linux Agent, Sophos Linux Sensor proporciona:

- Más detecciones: acceso a detecciones adicionales para la explotación de aplicaciones y sistemas.
- Configuración y ajuste: opciones para modificar las listas de permitidos y bloqueados para detecciones por defecto.
- Configuración de recursos: opciones de configuración para ayudar a optimizar el uso de los recursos de los hosts.

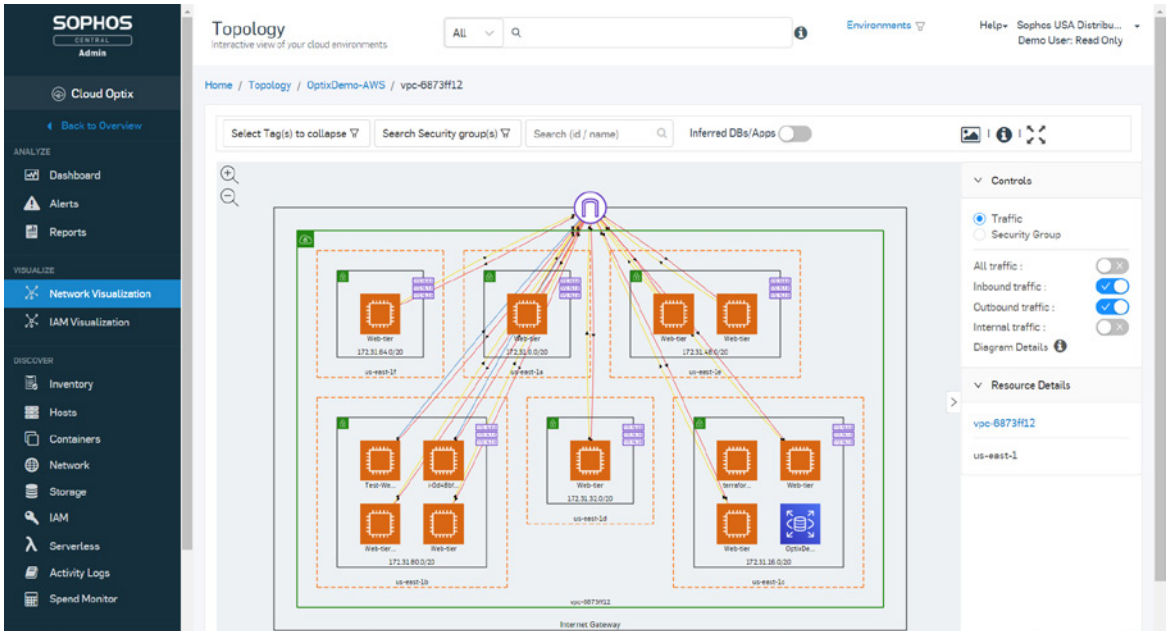
Optimice la visibilidad de lo que necesita proteger

Reducir toda la superficie de ataque en los entornos de AWS, Azure y GCP va más allá de la detección de amenazas a las cargas de trabajo en la nube y su protección. Por eso, Sophos Cloud Native Security unifica su conjunto de herramientas de seguridad en una sola herramienta para incluir la gestión de la posición de seguridad en la nube, la gestión de la posición de seguridad de Kubernetes, la seguridad de la infraestructura como código, la gestión de derechos en la infraestructura en la nube y la supervisión de los gastos en la nube.

Obtenga visibilidad, gobernanza y cumplimiento multinube

Aumente la eficiencia con herramientas de visibilidad y remediación sin agente en todos los entornos de AWS, Azure, GCP, Kubernetes, Docker Hub y de infraestructura como código en una única consola.

- Tenga una perspectiva general con visualizaciones de la topología de red exportables e inventarios de recursos bajo demanda.
- Integre los servicios de seguridad de los proveedores de la nube en una sola vista, incluidos Azure Advisor, Azure Sentinel, AWS Security Hub, Amazon GuardDuty, AWS CloudTrail, AWS IAM Access Analyzer, Amazon Detective, Amazon Inspector, AWS Systems Manager y AWS Trusted Advisor.
- Frene la TI en la sombra con la detección automática de recursos y la visualización de los despliegues de firewall y los agentes de protección de cargas de trabajo de Sophos.
- Prevenga y remedie los riesgos de configuración en servicios de hosts, de contenedores, de Kubernetes, sin servidor, de almacenamiento y de bases de datos, así como grupos de seguridad de red.
- Supervise y mantenga permanentemente las normas de seguridad y cumplimiento con políticas que se asignan automáticamente a su entorno y ahorre semanas de esfuerzo con los informes listos para auditorías. Las políticas incluyen CIS Foundations Benchmark, ISO 27001, EBU R 143, FEDRAMP FIEC, RGPD, HIPAA, PCI DSS, SOC2 y las prácticas recomendadas de Sophos.
- Realice un seguimiento comparativo de los costes de la nube para varios servicios de AWS y Azure desde una única pantalla, mejorando así la visibilidad. Reciba recomendaciones para optimizar el gasto del proveedor de la nube desde Sophos o integre los servicios de AWS Trusted Advisor o Azure Advisor.
- Reduzca la fatiga por alertas e identifique de forma eficiente mejoras inmediatas y problemas críticos con alertas clasificadas según el riesgo y codificadas por colores que muestran los pasos detallados de remediación.

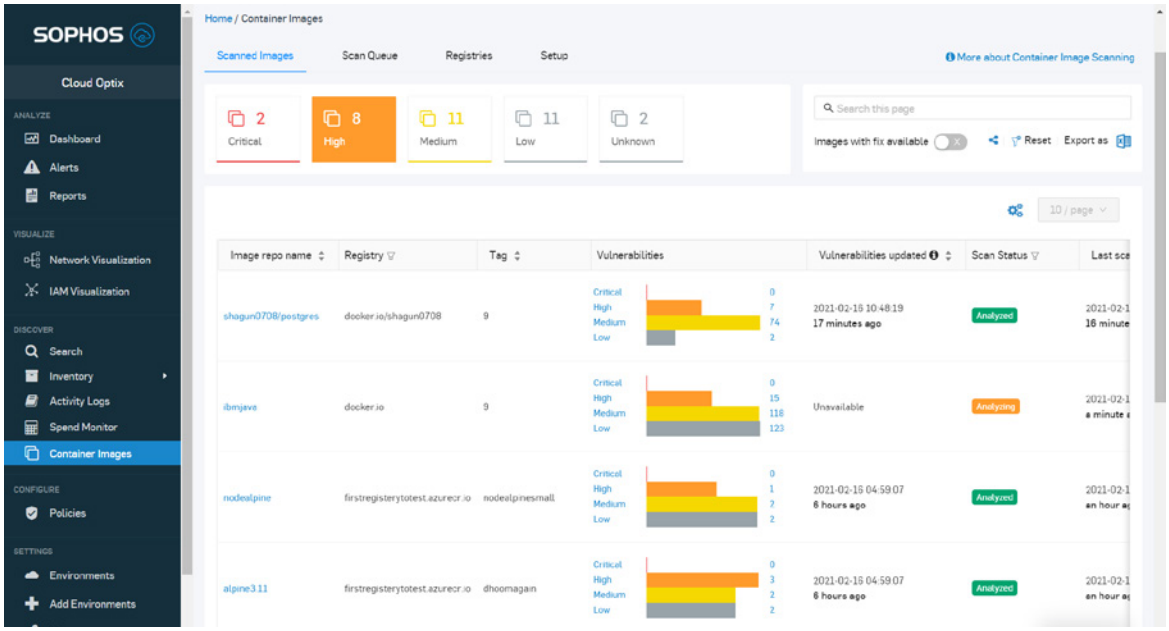


Ejemplo de visualización de topología de red de Sophos para AWS con análisis de grupos de seguridad.

Reduzca el riesgo sin ralentizar a DevOps

Permita un desarrollo rápido y seguro con una configuración de seguridad integrada y comprobaciones de cumplimiento en cualquier fase del proceso de desarrollo.

- Detecte automáticamente errores de configuración y secretos, contraseñas y claves incrustados en archivos de plantillas de Terraform, AWS CloudFormation, Ansible, Kubernetes y Azure Resource Manager.
- Evite el despliegue de contenedores con vulnerabilidades del sistema operativo e identifique las correcciones disponibles. Compatible con Amazon ECR, ACR, registros de Docker Hub, entornos de infraestructura como código e imágenes en los procesos de compilación.
- Integre fácilmente con GitHub y Bitbucket para recibir los resultados del escaneado bajo demanda en Sophos Central o utilice la API REST para escanear plantillas de infraestructura como código e imágenes de contenedor en cualquier fase del desarrollo.

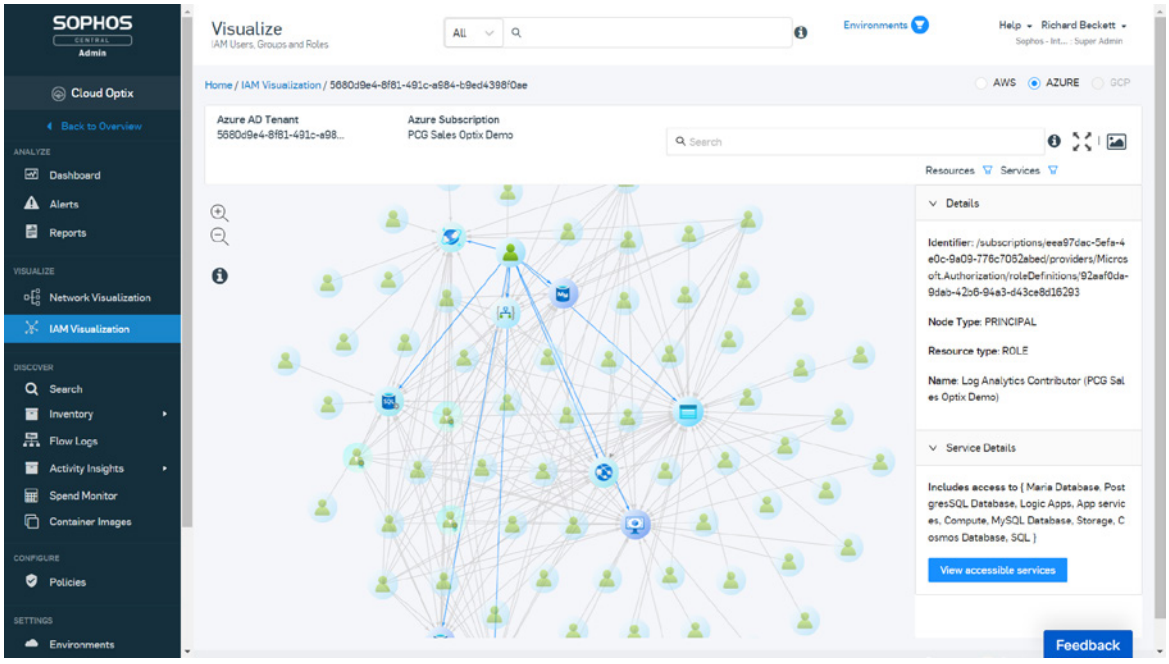


Ejemplo de resumen de los resultados de la evaluación de vulnerabilidades del escaneado de imágenes de contenedor de Sophos.

Aplique el mínimo privilegio

Gestione las identidades antes de que sean explotadas con nuestra ayuda para implementar el mínimo privilegio con la gestión de derechos en la infraestructura en la nube en entornos multinube.

- Asegúrese de que todas las identidades solo realizan las acciones necesarias para sus tareas y nada más.
- Señale patrones de acceso de usuarios y ubicaciones inusuales para identificar el mal uso o el robo de credenciales.
- Detecte roles de IAM de Microsoft Azure desactualizados, no gestionados y huérfanos utilizados para obtener acceso a entornos.
- Visualice roles de IAM de AWS complejos e interdependientes para identificar y evitar rápidamente los roles de IAM con demasiados privilegios.
- Sírvase de SophosAI para relacionar anomalías de alto riesgo dispares en el comportamiento de los usuarios del entorno de AWS para evitar brechas de seguridad.

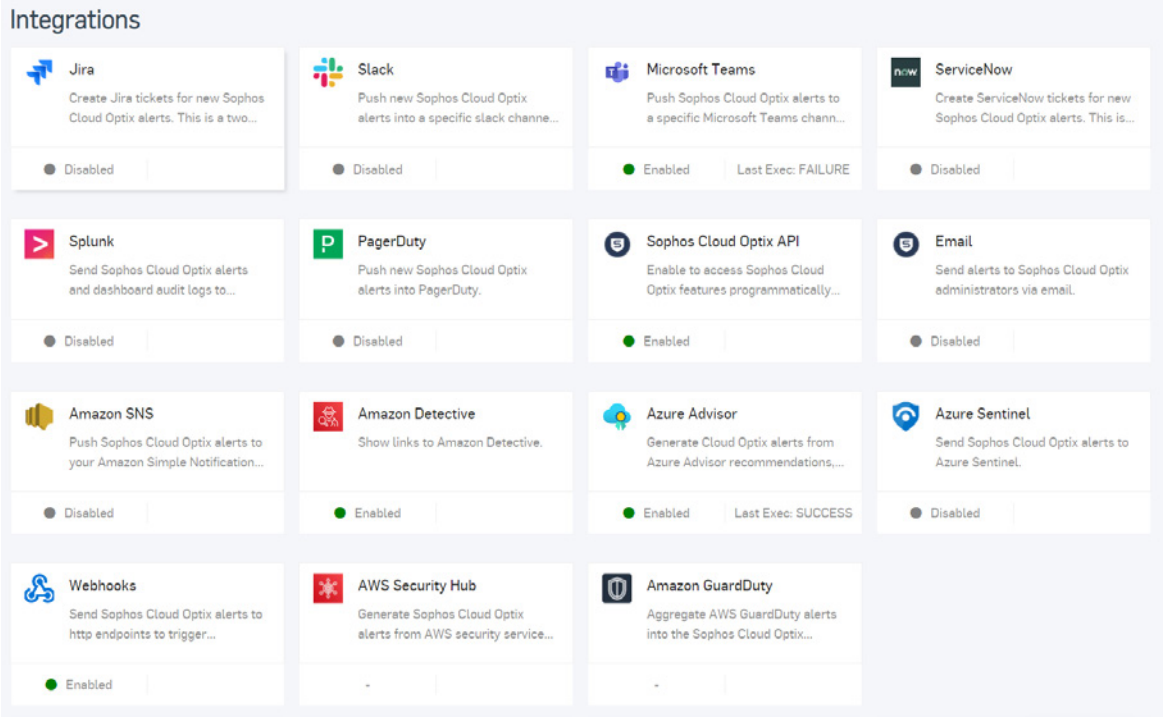


Ejemplo de visualización de IAM de Sophos para Microsoft Azure.

Agilice las operaciones de seguridad y mejore la colaboración

Mejore la agilidad en todas las organizaciones mediante la integración de alertas de la posición de seguridad del entorno en la nube con herramientas populares de SIEM, de colaboración, de flujo de trabajo y de DevOps en solo unos clics.

- Operaciones de seguridad: integración con Splunk, Azure Sentinel y PagerDuty para recibir notificaciones instantáneas sobre eventos de seguridad y cumplimiento.
- Herramientas de colaboración: envío de alertas instantáneas a Slack, Microsoft Teams o Amazon Simple Notification Service (SNS) para colaborar en temas.
- Gestión del flujo de trabajo: integre la respuesta a alertas en flujos de trabajo estándar creando incidencias de JIRA y ServiceNow desde Sophos Central con integración bidireccional para evitar la duplicación de incidencias.



Ejemplo de integraciones de Sophos populares para gestionar las alertas de gestión de la posición de seguridad en la nube.

Colaboraciones que se suman a su equipo

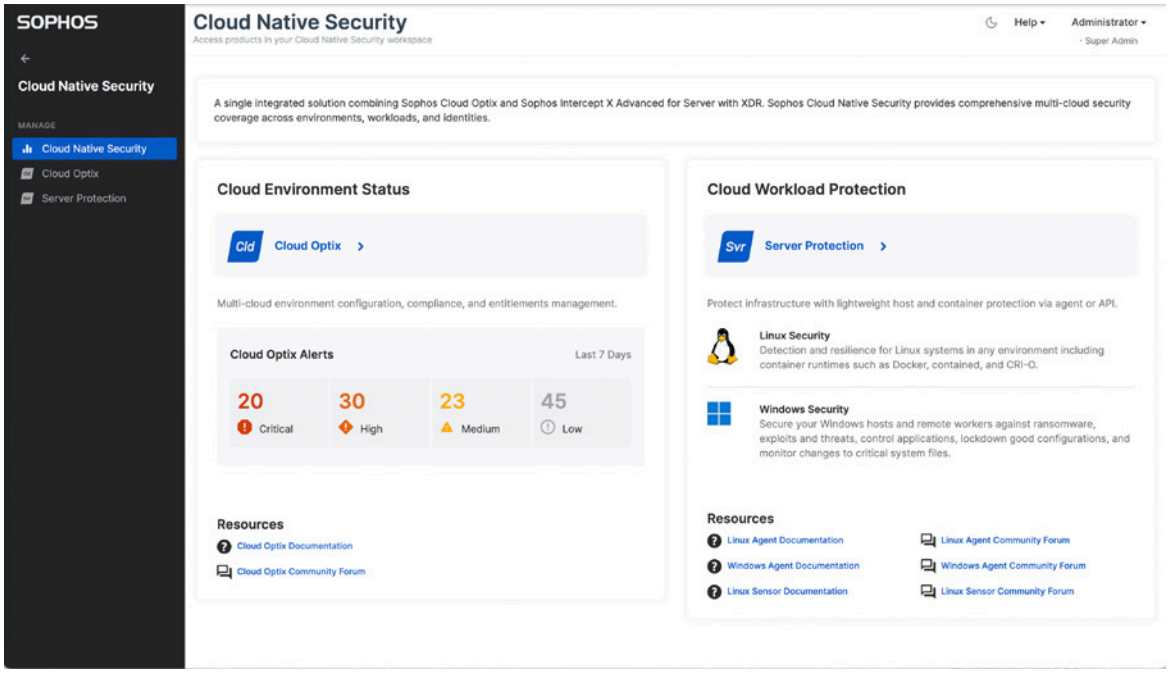
Gestione la protección a su manera: con su propio equipo de seguridad, con la ayuda de un partner de Sophos o a través del servicio Sophos Managed Threat Response (MTR) para garantizar una supervisión y respuesta 24/7.

Sophos MTR es el complemento perfecto de Sophos Cloud Native Security. Este servicio de respuesta a amenazas administrado puede trabajar con sus equipos, supervisar su entorno 24/7/365, responder a posibles amenazas, buscando indicadores de peligro, y proporcionar análisis detallados de eventos, incluyendo qué ha pasado, dónde, cuándo, cómo y por qué, a fin de evitar que ataques sofisticados comprometan sus datos y sistemas.

Disponibilidad de Sophos Cloud Native Security

Este nuevo paquete combinado está disponible para todos los clientes y la actualización se puede hacer desde Intercept X Essentials for Server, Intercept X Advanced for Server e Intercept X Advanced for Server with XDR.

Una vez activado en Sophos Central, los clientes y partners verán un nuevo elemento "CNS" en el panel de navegación de la izquierda. Este enlaza al nuevo panel de control de resumen de Cloud Native Security, que proporciona acceso a los productos Sophos Cloud Optix e Intercept X Advanced for Server with XDR.



Ejemplo del panel de control de Sophos Cloud Native Security en la consola de administración de Sophos Central.

Pruébelo gratis hoy mismo

Regístrese para una evaluación gratuita de 30 días en es.sophos.com/cloud

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com

06-07-22 ES (DD)

SOPHOS