Novidades: Sophos Cloud Native Security

Cobertura completa de segurança multinuvem para ambientes, cargas de trabalho e identidades

SOPHOS
Cybersecurity delivered.

Uma solução única e integrada de segurança na nuvem

A transição para as tecnologias de nuvem, como hosts, contêineres, serviços de armazenamento e Infraestrutura como Código, significa que as organizações precisam aumentar a visibilidade para proteger-se contra configurações indevidas, malwares, ransomwares, violações e mais.

O Sophos Cloud Native Security unifica as ferramentas necessárias para oferecer visibilidade e deixar seus ambientes de nuvem mais rígidos, difíceis de comprometer e rápidos na recuperação. Uma solução única e integrada para Amazon Web Services, Microsoft Azure e Google Cloud Platform, o Sophos Cloud Native Security combina o Sophos Cloud Optix e o Sophos Intercept X Advanced for Server XDR.

Em uma mesma tela, o painel de gerenciamento do Sophos Central lhe dá o poder de sair no encalço de ameaças multinuvem, receber detecções priorizadas de incidentes e beneficiar-se da conexão automática entre os eventos de segurança para otimizar os tempos de investigação e resposta a ameaças.

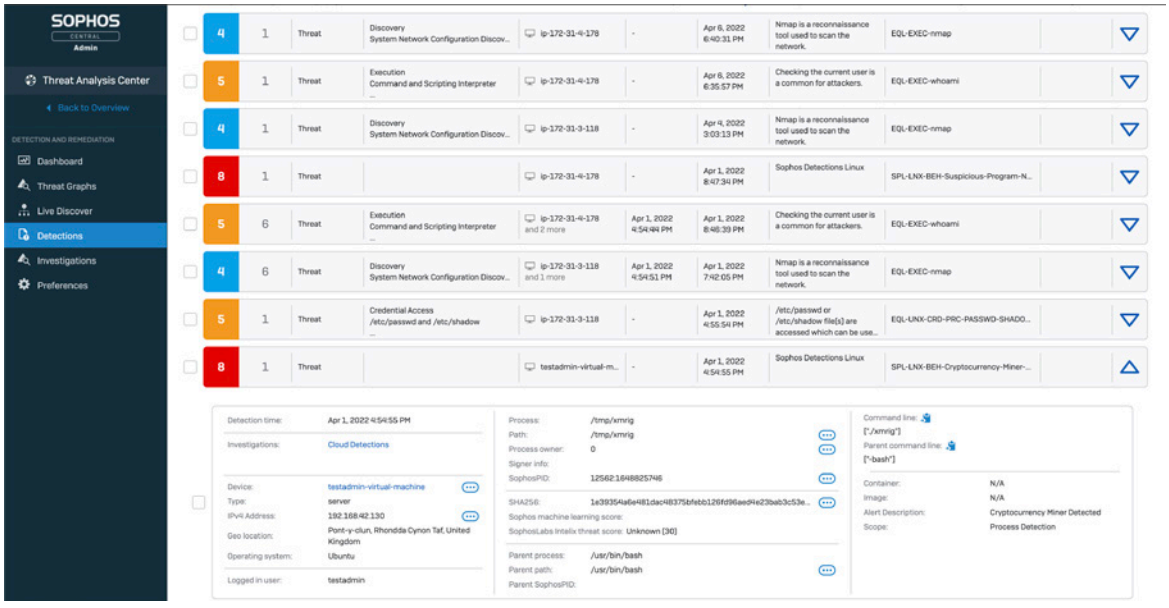
O próximo patamar na evolução do Sophos Server Protection

Para proteger suas cargas de trabalho de servidor na nuvem pública, a Sophos estendeu sua proteção Windows confiável para abranger também as implantações em Linux – um dos sistemas operacionais na nuvem mais prolíferos.

No início do ano, a proteção de servidores da Sophos para cargas de trabalho na nuvem acompanhou a grande evolução das capacidades do Linux e seus contêineres, apresentando uma nova proteção contra ameaças de exploit e comportamentais em runtime para identificar incidentes de segurança no Linux conforme acontecem.

O Sophos Cloud Native Security oferece as habilidades de proteção de carga de trabalho necessárias para proteger a sua infraestrutura e os seus dados agora e conforme evoluem na nuvem.

- Proteja tudo: nuvem, data center, host, contêiner, Windows e Linux.
- Aproveite tempo de atividade e desempenho com a proteção de host leve do Linux e do Windows através de um agente ou API para Linux.
- Identifique incidentes sofisticados de segurança em contêineres e no Linux em runtime sem implantar um módulo kernel.
- Proteja os seus hosts do Windows e trabalhadores remotos contra ransomwares, exploits e ameaças nunca antes vistas.
- Controle aplicativos, bloqueie configurações e monitore alterações a arquivos críticos do sistema Windows.
- Agilize investigações e resposta a ameaças com a detecção e resposta estendidas do XDR para priorizar e conectar eventos.



Exemplo de detecções de ameaças em tempo de execução no Linux pelo Sophos XDR no painel do Sophos Central.

Opções de implantação de proteção de carga de trabalho na nuvem

Gerenciamento do Sophos Central – Este agente leve Linux dá às equipes de segurança as informações críticas de que precisam para investigar e responder a ameaças comportamentais do Windows e Linux, exploits e malwares em um mesmo lugar. Monitorando o host, essa opção de implantação permite que as equipes gerenciem suas soluções da Sophos a partir de um único painel, sem rupturas na atividade ao mudar entre busca, correção e gerenciamento de uma ameaça.

Integração da API – O sensor Sophos Linux é uma opção de implantação altamente flexível que é ajustada para oferecer o melhor desempenho. O sensor usa APIs para integrar detecções avançadas de ameaças em runtime, em ambientes de host ou em contêiner às suas ferramentas existentes de resposta a ameaças. Ele oferece maior nível de controle para criar conjuntos de regras personalizadas contendo apenas as detecções de comportamento em runtime para atender a um caso de uso de segurança específico.

Além do agente Sophos Linux, o sensor Sophos Linux oferece:

- Mais detecções: acesso a detecções adicionais de exploração de aplicativos e sistemas
- Configuração e sintonia: opções para modificar listas de permissão e bloqueio para detecções padrão
- Sintonia de recursos: opções de configuração para ajudar a otimizar a utilização de recursos de host

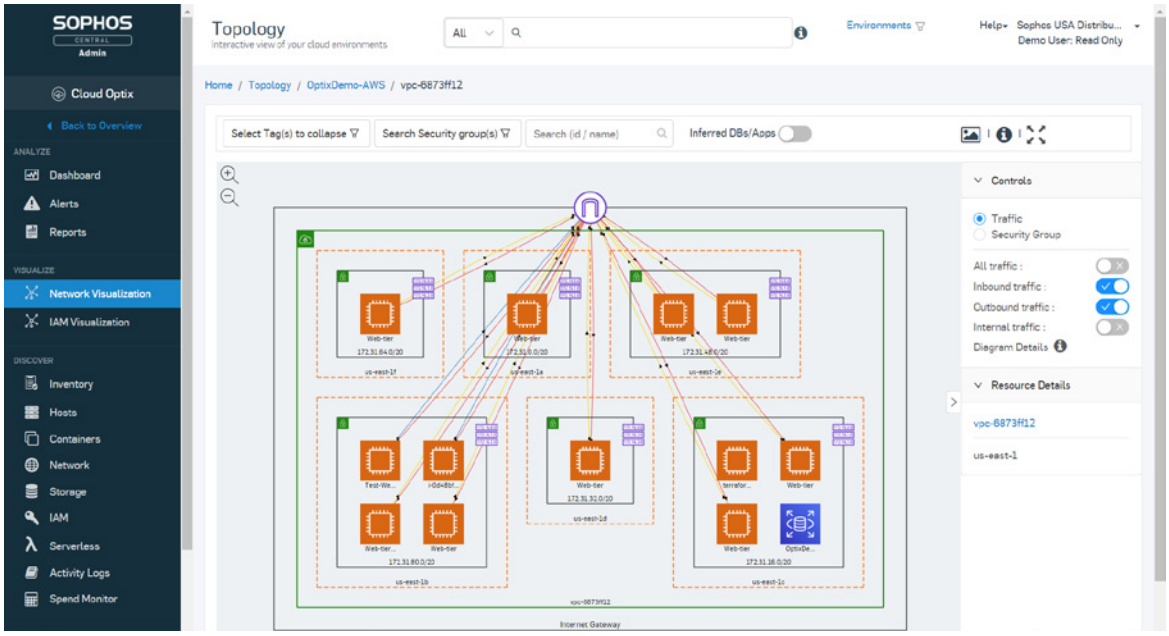
Veja mais do que você precisa proteger

Reduzir a superfície de ataque em sua totalidade em ambientes AWS, Azure e GCP vai além da proteção e detecção de ameaças a cargas de trabalho na nuvem. É por isso que o Sophos Cloud Native Security consolida seu kit de ferramentas de segurança com uma ferramenta que inclui gerenciamento de postura de segurança da nuvem, gerenciamento de postura de segurança de Kubernetes, segurança de Infraestrutura como Código, gerenciamento de direitos da infraestrutura da nuvem e monitoramento de gastos da nuvem.

Visibilidade, governança e conformidade multinuvem

Aumente a eficiência com as ferramentas de visibilidade e correção sem agente nos ambientes AWS, Azure, GCP, Kubernetes, Infraestrutura como Código e Docker Hub em um único painel.

- Veja os sistemas em sua totalidade, com inventários de ativos sob demanda e visualizações da topologia da rede exportáveis.
- Integre serviços de segurança de provedores de nuvem em uma única exibição, incluindo 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.
- Dê fim à TI sombra com a descoberta e visualização automática de ativos de agentes de proteção de carga de trabalho e implantações de firewall da Sophos.
- Previna e resolva os riscos de configuração em hosts, contêineres, Kubernetes, funções sem servidor, serviços de armazenamento e banco de dados e grupos de segurança de rede.
- Monitore e mantenha os padrões de segurança e conformidade continuamente com políticas que mapeiam automaticamente para o seu ambiente e economizam semanas de trabalho com relatórios prontos para auditoria. As políticas incluem normas CIS Foundations Benchmark, ISO 27001, EBU R 143, FEDRAMP FIEC, GDPR, HIPAA, PCI DSS, SOC2 e as práticas recomendadas da Sophos.
- Faça o acompanhamento comparativo dos custos dos vários serviços AWS e Azure lado a lado em uma única tela para melhorar a visibilidade. Receba recomendações da Sophos para otimizar os custos do provedor de nuvem ou integre-se com os serviços AWS Trusted Advisor ou Azure Advisor.
- Reduza a exaustão dos alertas e detecte eficientemente maneiras rápidas de aprimoramento e problemas críticos com a avaliação de risco e alertas codificados por cor que mostram etapas de remediação detalhadas.

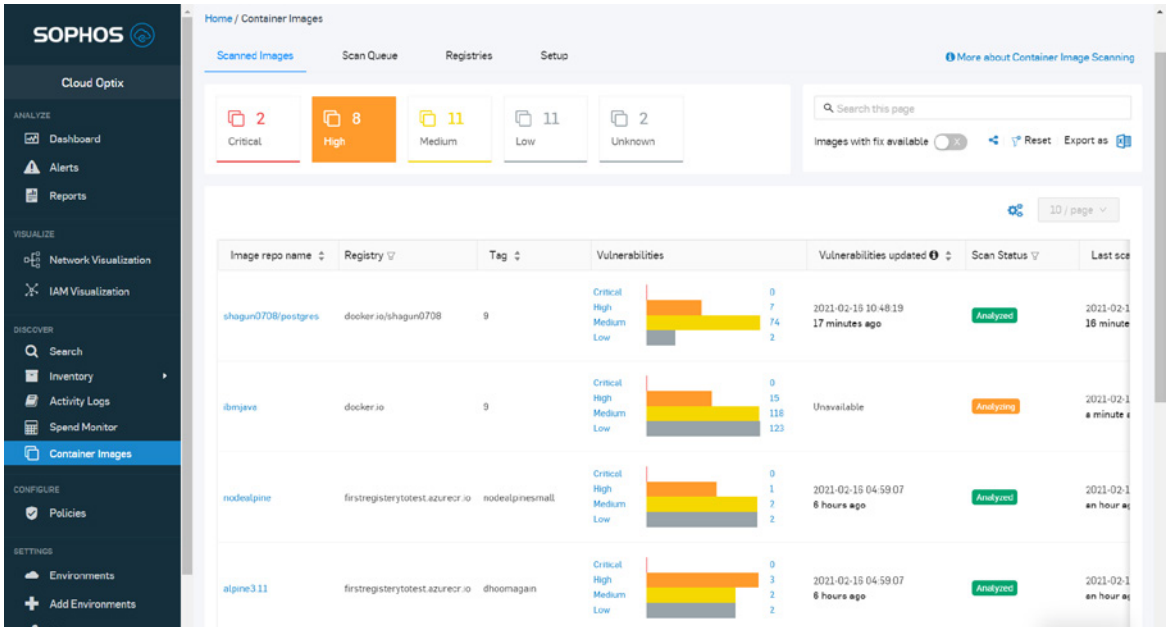


Exemplo da visualização de topologia de rede da Sophos para AWS com análise de grupo de segurança.

Reduza riscos sem perder velocidade de DevOps

Possibilite um desenvolvimento rápido e seguro com verificações integradas de configuração e conformidade de segurança em qualquer estágio do pipeline de desenvolvimento.

- Detecte automaticamente configurações incorretas, segredos, senhas e códigos incorporados em arquivos de modelo do Terraform, AWS CloudFormation, Ansible, Kubernetes e Azure Resource Manager.
- Previna a implantação de contêineres com vulnerabilidades de sistema operacional e identifique as correções disponíveis. Oferece suporte a Amazon ECR, ACR, registros do Docker Hub, ambientes de Infraestrutura como Código e imagens no pipeline de compilações.
- Faça a integração ao GitHub e Bitbucket com facilidade para receber os resultados de varreduras sob demanda no Sophos Central, ou use a API REST para fazer a varredura de modelos de Infraestrutura como Código e imagens de contêiner em qualquer estágio de desenvolvimento.

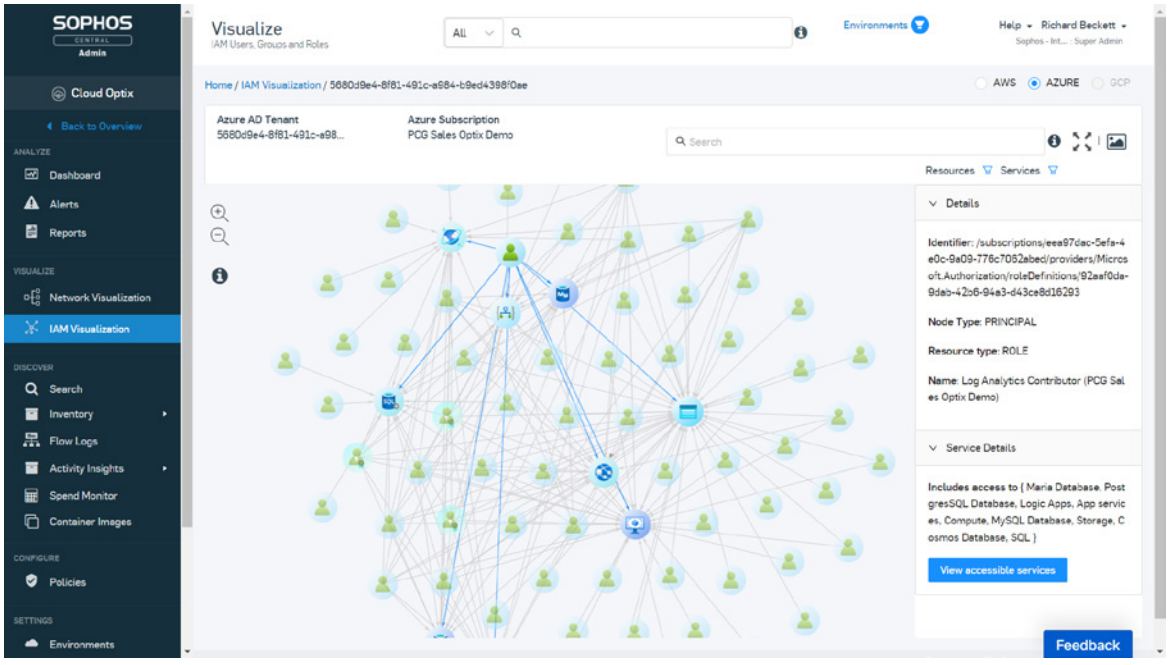


Exemplo de um resumo da Sophos dos resultados de avaliação de vulnerabilidades na varredura da imagem do contêiner.

Adote o privilégio mínimo

Gerencie identidades antes de serem exploradas com nossa ajuda para implementar o privilégio mínimo com o gerenciamento de direitos de infraestrutura de nuvem em todos os ambientes multinuvem.

- Assegure que todas as identidades executem apenas as ações necessárias para suas tarefas e nada mais.
- Identifique padrões e locais de acesso incomuns ao usuário que indicam roubo ou uso indevido de credenciais.
- Destaque as funções órfãs do Microsoft Azure IAM, não gerenciadas e desatualizadas, usadas para obter acesso aos ambientes.
- Visualize funções do AWS IAM complexas e interligadas para destacar e prevenir rapidamente funções do IAM com excesso de privilégios.
- Utilize o SophosAI para correlacionar anomalias díspares de alto risco do comportamento do usuário no ambiente AWS para prevenir violações.

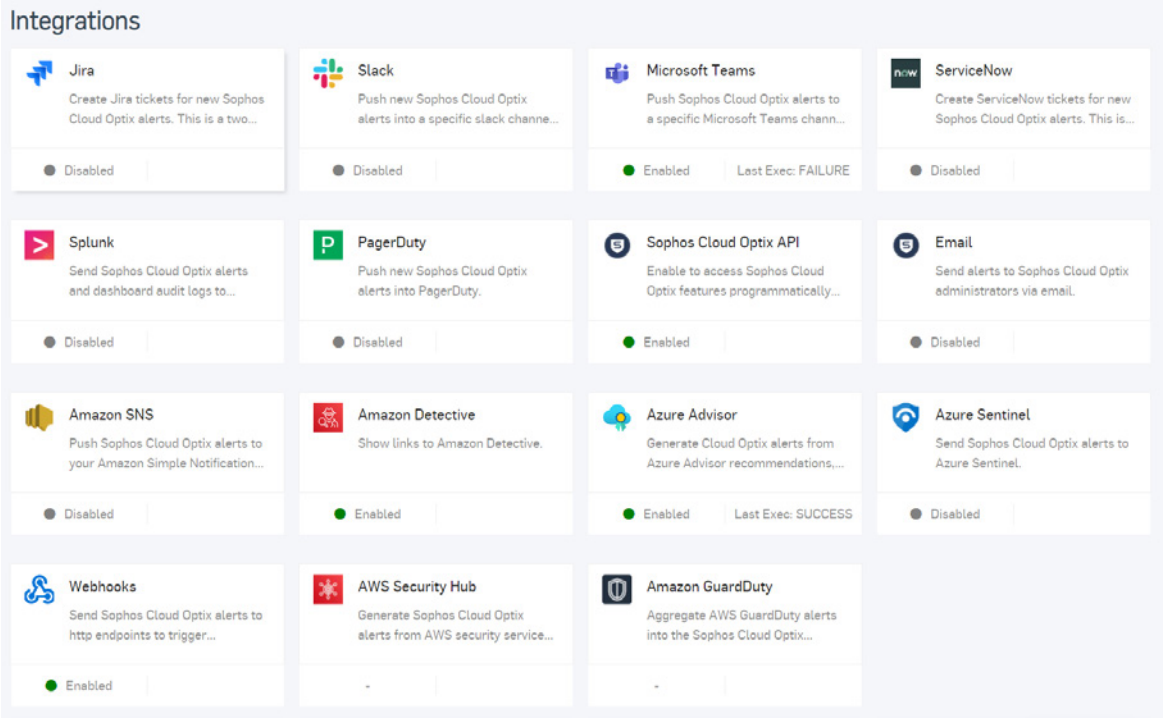


Exemplo da visualização do Sophos IAM para Microsoft Azure.

Agilize SecOps e melhore a colaboração

Aumente a agilidade entre organizações com alertas de postura de segurança do ambiente da nuvem integrados a ferramentas populares SIEM e de colaboração, fluxo de trabalho e DevOps em apenas alguns cliques.

- Operações de segurança: integram-se ao Splunk, Azure Sentinel e PagerDuty para receber notificações instantâneas sobre eventos de segurança e conformidade.
- Ferramentas de colaboração: enviam alertas instantâneos ao Slack, Microsoft Teams ou Amazon Simple Notification Service (SNS) para contribuir nos tópicos.
- Gerenciamento de fluxo de trabalho: incorpora resposta a alertas nos fluxos de trabalho padrão criando tíquetes JIRA e ServiceNow diretamente no Sophos Central com integração de duas vias para evitar duplicação de tíquetes.



Exemplo de integrações populares da Sophos para administrar alertas de gerenciamento de postura de segurança na nuvem.

Parcerias que expandem a sua equipe

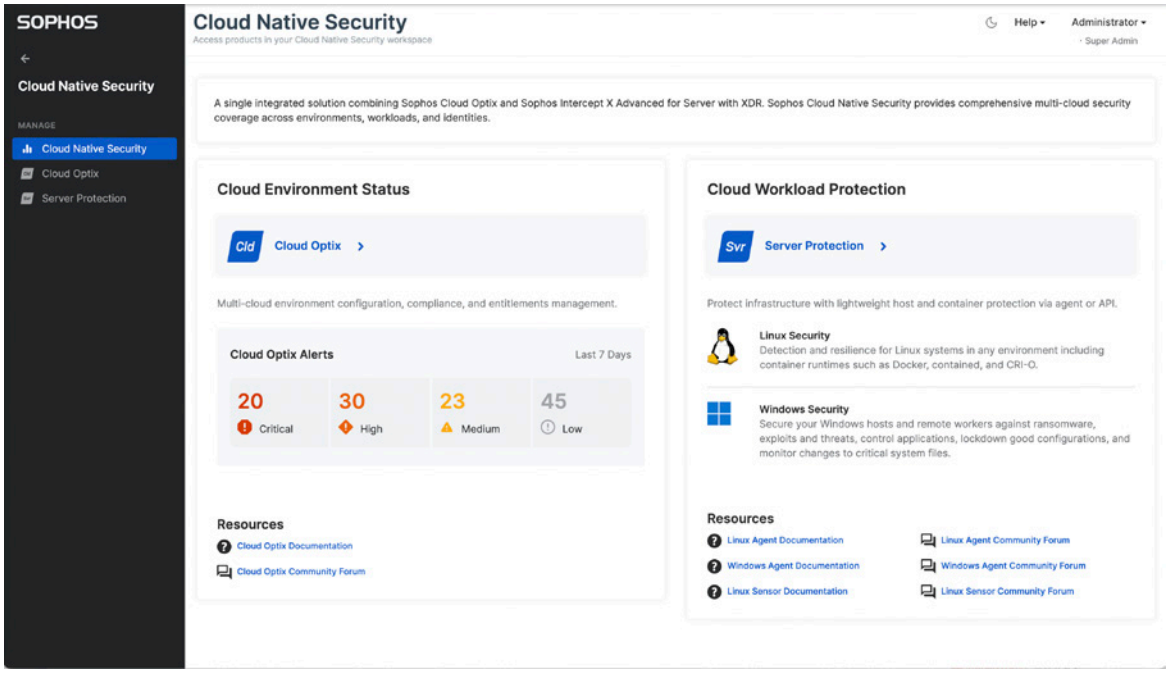
Gerencie sua proteção do seu jeito — com o respaldo da sua própria equipe de segurança, com a ajuda de um parceiro Sophos ou através do serviço Sophos Managed Threat Response (MTR) para garantir 24 horas diárias de monitoramento e resposta.

O Sophos MTR é o complemento perfeito ao Sophos Cloud Native Security. Esse serviço gerenciado de resposta a ameaças pode trabalhar com suas equipes, monitorar seu ambiente 24 horas por dia, 365 dias por ano, responder a ameaças potenciais, pesquisar indicadores de comprometimento e fornecer análises detalhadas sobre eventos, incluindo o que aconteceu, onde, quando, como e por que, de modo a prevenir que ameaças sofisticadas comprometam seus dados e sistemas.

Disponibilidade do Sophos Cloud Native Security

Esse novo pacote combinado está disponível a todos os clientes, e você pode fazer upgrade para o Intercept X Essentials for Server, Intercept X Advanced for Server e Intercept X Advanced for Server with XDR.

Uma vez conectados e ativos, clientes e parceiros notarão o novo item "CNS" no painel de navegação esquerdo do Sophos Central. Ele interliga o novo painel sintetizado do Cloud Native Security, dando acesso aos produtos Sophos Cloud Optix e Intercept X Advanced for Server with XDR.



Exemplo do painel do Sophos Cloud Native Security no painel de gerenciamento do Sophos Central.

Experimente agora gratuitamente

Registre-se para uma avaliação gratuita de 30 dias em sophos.com/cloud

Vendas na América Latina
E-mail: latamsales@sophos.com

Vendas no Brasil
E-mail: brasil@sophos.com

22-07-06 PTBR (DD)

SOPHOS