CUSTOMER CASE STUDY

Sophos protege a maior cúpula climática do mundo, realizada no coração da Amazônia

COP30 AMAZONIA

Setor:
Conferência das Nações Unidas sobre Mudança Climática

Número de usuários gerenciados:
+60.000

Soluções Sophos:
Sophos Endpoint

Sophos Extended Detection and Response (XDR)

Sophos Managed Detection and Response (MDR)

Sophos Central

SOPHOS

Desafios:

Uma enorme superfície de ataque transitória criada por mais de 60.000 dispositivos conectados simultaneamente, 42.582 participantes credenciados, Wi-Fi público aberto sem autenticação e centros de computação públicos onde os participantes poderiam usar pen drives em dispositivos disponibilizados pelo evento.

Volumes excepcionalmente altos de atividade maliciosa, incluindo 27,4 milhões de requisições DNS maliciosas, impulsionadas por hacktivistas, atores patrocinados por Estados e outros adversários que buscavam atingir um evento global de grande visibilidade.

Infraestrutura temporária em constante mudança, onde dispositivos provenientes de aproximadamente 190 países exigiam monitoramento contínuo, segmentação e contenção rápida de ameaças.

Uma exigência operacional 24/7, já que as negociações diplomáticas abrangiam vários fusos horários, exigindo visibilidade ininterrupta, resposta automatizada e contenção na velocidade das máquinas.

Quando a COP30 chegou a Belém, Brasil, no coração da Amazônia, a cidade foi transformada quase da noite para o dia em um hub digital global. Delegações de cerca de 190 países participaram do evento. Dezenas de milhares de participantes dependiam de conectividade ininterrupta para negociar políticas climáticas, trocar documentos sensíveis e coordenar discussões diplomáticas em tempo real.

A escala foi imensa: mais de 60.000 dispositivos conectados simultaneamente, 42.582 participantes credenciados e mais de mil pontos de acesso Wi-Fi 6E que suportaram 475 milhões de sessões de rede durante o evento.

A COP30, principal conferência climática das Nações Unidas, precisava operar sem falhas, com ameaças cibernéticas surgindo de todas as direções.

“Uma violação poderia comprometer negociações diplomáticas, vazar documentos sensíveis, prejudicar a reputação internacional, interromper credenciamento e logística e ameaçar serviços críticos”, afirmou Milton Sampaio, coordenador de TI da COP30.

“Uma violação poderia comprometer negociações diplomáticas, vazar documentos sensíveis, prejudicar a reputação internacional, interromper credenciamento e logística e ameaçar serviços críticos.”

Milton Sampaio,
IT coordinator for COP30

SOPHOS

Um ambiente de alta pressão construído da noite para o dia

Diferente de uma rede corporativa tradicional com infraestrutura estável e comportamento previsível, o ambiente da COP30 era um alvo em constante mudança. Os centros de computação permitiam o uso livre de dispositivos USB e a rede Wi-Fi principal era totalmente aberta — sem senha ou autenticação. Mesmo com segmentação cuidadosa, um único dispositivo comprometido poderia se espalhar entre delegações, mídia, equipes da ONU e operações locais.

No perímetro, os ataques começaram imediatamente. A COP30 registrou 27,4 milhões de requisições DNS maliciosas, com uma concentração esmagadora de ameaças em tentativas de acesso inicial — 86,59% de todo o comportamento hostil. Atores patrocinados por Estados, hacktivistas e atacantes oportunistas viram a COP30 como um alvo de alto valor e visibilidade global.

E a equipe de TI não podia permitir nenhuma interrupção na conectividade. Enquanto o Brasil dormia, delegados na Ásia revisavam e transmitiam documentos digitais para a próxima rodada de negociações. O SOC precisava manter monitoramento constante e resposta rápida, sem tolerância à indisponibilidade.

Escolhendo um parceiro que acompanhe a velocidade da diplomacia

Com tantas variáveis em movimento, Sampaio e sua equipe precisavam de visibilidade, automação e simplicidade operacional em milhares de endpoints imprevisíveis. A Sophos se destacou por vários motivos — mas o principal foi a capacidade de unificar grandes volumes de telemetria em um único painel intuitivo que os analistas puderam usar imediatamente dentro dos centros de operações de segurança e rede da COP30.

O treinamento precisava ser rápido porque os analistas vinham de diferentes organizações e tinham experiências diversas. Segundo Sampaio, a equipe SECOP aprendeu rapidamente a usar as ferramentas da Sophos, o que permitiu integrar as operações de MDR de forma fluida com produtos e serviços da Cisco, Fortinet, Vectra, Infoblox e Microsoft. Esse ambiente coeso criou um verdadeiro modelo de defesa em profundidade.

Sophos Managed Detection and Response (MDR) tornou-se a base da proteção de endpoints durante o evento, oferecendo detecção rápida e contenção automatizada na velocidade que o ambiente exigia.

"O monitoramento por meio de um painel intuitivo integrado ao SOC/NOC da COP30 foi essencial. A equipe aprendeu rapidamente a usar a solução", afirmou Sampaio.

Transformando complexidade em clareza com MDR

Para um evento dessa escala, o desafio não era apenas o volume de alertas — os analistas precisavam processá-los com rapidez suficiente para agir quando necessário. Sophos Extended Detection and Response (XDR) e MDR forneceram a telemetria unificada necessária para reduzir o tempo de investigação, dando ao SOC uma visão clara do que estava acontecendo em todos os potenciais pontos de conexão.

Playbooks automatizados e o isolamento de endpoints mostraram-se cruciais. Quando um dispositivo ultrapassava os limites de comportamento definidos, o Sophos MDR respondia antes mesmo de um analista tocar no teclado. Isso evitava a movimentação lateral dentro do ambiente fortemente microssegmentado e garantia que as sessões permanecessem estáveis para os usuários.

Sampaio observou que recursos como consultas de threat hunting, visibilidade em nível de processo e insights aprofundados sobre a integridade do sistema permitiram que sua equipe se mantivesse à frente dos atacantes, apesar da enorme superfície de ataque.

"O Sophos XDR/MDR simplificou a análise e a resposta em endpoints, reduzindo o tempo de investigação", disse ele.

Resiliência comprovada sob pressão global

A COP30, no fim, ofereceu uma experiência fluida e ininterrupta, mesmo em meio a uma torrente de ataques.

Os números contam a história: 27,4 milhões de requisições DNS maliciosas bloqueadas, 24 milhões de conexões maliciosas de firewall interrompidas e 86,59% das ameaças neutralizadas ainda no acesso inicial — muito antes que pudessem escalar.

> "O monitoramento por meio de um painel intuitivo integrado ao SOC/NOC da COP30 foi essencial. A equipe aprendeu rapidamente a usar a solução."
>
> **Milton Sampaio, IT coordinator for COP30**

Tudo isso ocorreu mantendo 100% de disponibilidade da rede em mais de um petabyte de tráfego processado. O SOC encerrou 86,37% de todos os incidentes, com apenas 6% alcançando alta severidade, segundo Sampaio.

A lista de verificação de aceitação da UNFCCC — cobrindo segmentação, segurança de perímetro, redundância e resiliência operacional — foi totalmente atendida.

“Com o Sophos MDR Complete ampliando nosso SOC 24/7, contivemos ameaças na velocidade da diplomacia — protegendo uma conversa verdadeiramente global no coração da Amazônia”, afirmou Sampaio.

Para começar com as soluções Sophos hoje e encontrar uma solução que acompanhe suas necessidades, fale com um especialista.

To get started with Sophos solutions today and find a solution that scales to your needs, speak to an expert today.

SOPHOS