CUSTOMER CASE STUDY

Sophos secures one of the world's largest climate summits in the heart of the Amazon

COP30 AMAZONIA

Industry
United Nations Climate Change Conference

Number of users managed:
+42,000

Sophos Solutions
Sophos Endpoint

Sophos Extended Detection and Response (XDR)

Sophos Managed Detection and Response (MDR)

Sophos Central

SOPHOS

Challenges:

- **An enormous, transient attack surface** created by 60,000 devices on the network simultaneously, open public Wi-Fi with no authentication, and public computer centers where attendees regularly connected USB devices.
- **Exceptionally high volumes of hostile activity,** including 27.4 million malicious DNS requests, driven by hacktivists, state-sponsored actors, and other adversaries looking to target a high-profile global event.
- **Constantly changing temporary infrastructure,** where devices coming from approximately 190 nations required continuous monitoring, segmentation, and rapid threat containment.
- **A 24/7 operational requirement,** as diplomatic negotiations spanned global time zones, meaning the SOC needed uninterrupted visibility, automated response, and machine-speed containment.

When COP30 arrived in Belém, Brazil, deep in the Amazon region, the city was transformed almost overnight into a global digital hub. Delegations from nearly 190 countries poured in. Tens of thousands of attendees depended on uninterrupted connectivity to negotiate climate policy, exchange sensitive documents, and coordinate real-time diplomatic discussions.

The scale was immense: over 60,000 users connecting simultaneously, 42,582 credentialed participants, and more than a thousand Wi-Fi 6E access points powering 475 million network sessions across the event.

COP30, the United Nation's flagship climate change conference, needed to operate flawlessly, with cyber threats emerging from every direction.

"A breach could derail diplomatic negotiations, leak sensitive documents, damage international reputation, disrupt credentialing and logistics, and threaten critical services," Milton Sampaio, the IT coordinator for COP30, said.

A high-pressure environment built overnight

Unlike a typical enterprise network with stable infrastructure and predictable behavior, COP30's environment was a moving target. Computer centers allowed the public to use USB devices freely, and the main Wi-Fi network was completely open — with no password or authentication layer. Even with careful segmentation, a single compromised device could ripple across delegations, media, United Nations teams, and local operations.

"A breach could derail diplomatic negotiations, leak sensitive documents, damage international reputation, disrupt credentialing and logistics, and threaten critical services."

Milton Sampaio,
IT coordinator for COP30

SOPHOS

At the perimeter, attacks began immediately. COP30 saw 27.4 million malicious DNS requests, and an overwhelming concentration of threats focused on initial access attempts — 86.59% of all hostile behavior. State-backed actors, hacktivists, and opportunistic attackers all viewed COP30 as a high-value, globally visible target.

And the IT team couldn't afford to have any break in connectivity. While Brazil slept, delegates in Asia were reviewing and transmitting digital documents for the next round of negotiations. The SOC had to maintain constant monitoring and rapid response, with no tolerance for downtime.

Choosing a partner that could move at the speed of diplomacy

With so many moving parts, Sampaio and his team needed visibility, automation, and operational simplicity across thousands of unpredictable endpoints. Sophos stood out for several reasons — but the most important was the ability to unify massive amounts of telemetry into a single, intuitive dashboard that analysts could use immediately inside the COP30 security and network operations centers.

Training needed to be fast because the analysts came from various organizations with different backgrounds. According to Sampaio, the SECOP team quickly learned how to use Sophos tools, allowing them to integrate MDR operations seamlessly with Cisco, Fortinet, Vectra, Infoblox, and Microsoft products and services. This cohesive environment created a true defense-in-depth model.

Sophos Managed Detection and Response (MDR) became the backbone of endpoint protection during the event, delivering rapid detection and automated containment at the speed the environment demanded.

"Monitoring through an intuitive dashboard integrated into the COP30 SOC/NOC was essential. The team quickly learned how to use the solution," Sampaio said.

Turning complexity into clarity with MDR

For an event of this scale, the challenge wasn't just the volume of alerts, the analysts had to be able to process them quickly enough to take action if needed. Sophos Extended Detection and Response (XDR) and MDR provided the unified telemetry needed to reduce investigation time, giving the SOC a clear picture of what was happening across all the potential points of connection.

"Monitoring through an intuitive dashboard integrated into the COP30 SOC/NOC was essential. The team quickly learned how to use the solution."

Milton Sampaio,
IT coordinator for COP30

Automated playbooks and endpoint isolation proved crucial. When a device crossed behavior thresholds, Sophos MDR responded before an analyst even touched the keyboard. This prevented lateral movement within the heavily micro-segmented environment and ensured that sessions remained stable for users.

Sampaio noted that features like threat hunting queries, process-level visibility, and deep insight into system integrity allowed his team to stay ahead of attackers despite the enormous attack surface.

"Sophos XDR/MDR streamlined endpoint analysis and response, reducing investigation time," he said.

Resilience proven under global pressure

COP30 ultimately delivered a smooth and uninterrupted experience, even amid a torrent of attacks.

The numbers told the story: 27.4 million malicious DNS requests blocked, 24 million malicious firewall connections stopped, and 86.59% of threats neutralized at initial access — long before they could escalate.

All of this occurred while maintaining 100% network availability across more than a petabyte of processed traffic. The SOC closed 86.37% of all incidents, with only six percent reaching high severity, according to Sampaio.

UNFCCC's acceptance checklist — covering segmentation, perimeter security, redundancy, and operational resilience — was fully met.

"With Sophos MDR Complete augmenting our 24/7 SOC, we contained threats at the speed of diplomacy — protecting a truly global conversation in the heart of the Amazon," Sampaio said.

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

SOPHOS