SOPHOS

Sophos Managed Threat Response: Beyond the Endpoint

MTR Connectors and MTR Network Sensor

Sophos MTR goes beyond the endpoint adding in telemetry from other sources including network and cloud data. By extending visibility MTR operators can enrich endpoint investigations, better detect suspicious activity, and quickly neutralize active threats.

Intro

The Sophos MTR team provides 24/7 monitoring, threat hunting, and incident response. To have the most complete picture of a customer's environment, analysts need the broadest range of telemetry to ensure they have both the visibility and context to provide the absolute best protection. MTR Connectors and the MTR Network Sensor were designed to ensure MTR operators have the most crucial data at their fingertips ensuring attackers have fewer places to hide.

Network Visibility

The Sophos MTR service provides broad visibility and response capabilities across endpoints and servers. However, there are specific scenarios where extended visibility from additional telemetry would increase the effectiveness of the MTR service.

Combining endpoint and network visibility can aid in a variety of use cases, including:

- *Detect threats at the edge:* Network telemetry enables MTR operators to spot attempts to infiltrate the network at the perimeter.
- *Identify threats on the wire:* MTR operators can investigate threats detected in DNS requests, HTTP requests, and IP packets. Detection capabilities include web-based threats such as web application exploitation, SQL injection, and more.
- *Augment investigations with enhanced telemetry:* With Sophos XG telemetry in place, MTR can access network telemetry to aid investigations and validate threats. For example, with Sophos XG ATP events the MTR team can be alerted to malware call home addresses which have been classified by SophosLabs. This allows MTR to quickly begin investigating suspect hosts and identify unprotected devices in the estate.
- *View untrusted traffic:* Though most malicious traffic on the edge of the network is successfully identified and blocked before entry, it can be useful to observe dropped traffic as part of a larger indicator of attack within a threat campaign.

Highlights

- Siloed tools make it difficult for security operators to achieve enterprise-wide visibility
- MTR Advanced customers can add additional telemetry to endpoint and server data
- MTR Connectors allow MTR operators to consolidate data from multiple sources
- The Sophos Firewall MTR Connector adds network visibility for customers running XG Firewall managed in Sophos Central
- The Sophos Cloud Optix MTR Connector provides cloud visibility with access to Cloud Optix Policy and Anomaly alerts and Amazon GuardDuty events
- The MTR Network Sensor* virtual network appliance is a simple way to add network telemetry to the MTR Advanced service by deploying in non-blocking mode

- *Additional prevention and oversight for non-MTR managed devices:*
  - Unmanaged or guest devices: Security administrators need to ensure that protection is enabled on all devices and systems within their trusted environments. This includes guest devices on their network and other machines that did not have Intercept X Advanced installed by default. Security administrators must also quickly address new networks joining their domain via company reorganization or acquisitions when they can't quickly reconfigure the new endpoints and servers.
  - Endpoints and servers with legacy operating systems: Some systems can't be upgraded without significant cost (like large industrial equipment) or lack of specialized knowledge (like custom software).
  - IoT Devices: IoT devices often present unique challenges from a security perspective. Installing an endpoint agent may not be possible due to proprietary hardware and software, but they can be identified by their activity on the network.

Network Visibility: Sophos Firewall MTR Connector

Sophos MTR Advanced customers have the ability to fully deploy Sophos XG Firewall across their environment or deploy XG Firewall in tap mode while utilizing a non-Sophos firewall. Customers must manage their XG Firewalls in Sophos Central and use XG Central Firewall Reporting.

The Sophos Firewall MTR Connector generates MTR detections from the following network security events: ATP (Command & Control), IPS, Sophos AV (email, web, FTP), and Sophos Sandstorm (sandbox).

Network Visibility: MTR Network Sensor*

Sophos MTR Advanced customers* have the option to deploy the MTR Network Sensor in order to gain network telemetry. The network sensor is an SF SW/Virtual network appliance and is ideally suited for organizations who are unable or unwilling to deploy Sophos XG Firewall. The sensor is deployed in non-blocking mode and cannot be used as a replacement for a firewall.

The MTR Network sensor leverages the XG Firewall MTR Connector to generate MTR detections from ATP (Command & Control) and premium IDS events.

Customers must enable Central Firewall Management and Central Firewall Report. These features come with 7 days of data storage in the Sophos Data Lake, which can be used by customers to perform queries and run reports. This is separate from the MTR detections and data retention used exclusively by the MTR team.

* available in North America only

CASE STUDY

XG Firewall MTR Connector Enables MTR To Identify Active Threat

CUSTOMER

A USA-based MTR Advanced customer in the education vertical (~500 devices)

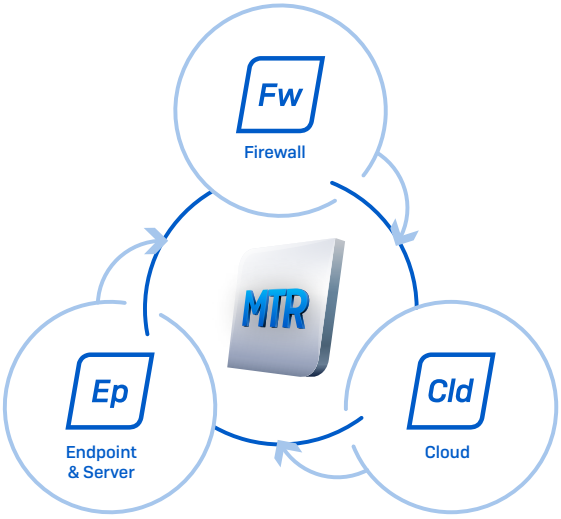
An intrusion prevention system (IPS) detected an attempted PHP remote code execution exploit, originating from a Russian IP address. While this would normally indicate the threat had been prevented via the traffic being dropped, the MTR team still investigated to confirm. Upon investigation, it was clear that active communication to this Russian IP over port 80 was still taking place after the IPS detection, indicating that the adversary had successfully circumnavigated detection and exploited the system.

Case details and instructions were provided to the customer, explaining the nature of the detection and recommending a block for the specific IP in question, as well as a geo-block for countries they do not conduct business with. The team followed up with the customer after they had made the recommended firewall configuration changes and confirmed that no more suspicious activity was present.

Cloud Visibility

By adding cloud telemetry, customers will receive around-the-clock security monitoring of major cloud platforms by a dedicated team of cybersecurity experts. The Sophos Cloud Optix MTR Connector provides Sophos MTR operators with the visibility needed to quickly identify critical cloud security events used in breach attempts across Amazon Web Services, Microsoft Azure, and Google Cloud Platform environments.

Extending cloud provider services with powerful artificial intelligence uncovers meaningful and actionable insights. Events from Sophos Cloud Optix generate MTR detections, including anomalous IAM user login activity, outbound network traffic connections, and other high-risk activity. Additional threat detections can be added via integration with the Amazon GuardDuty service, which analyzes CloudTrail, DNS and VPC flow logs.



About Sophos Managed Threat Response

The Sophos Managed Threat Response (MTR) service provides 24/7 threat hunting, detection, and response delivered by a team of Sophos experts as a fully managed service. While other managed detection and response (MDR) services simply notify you of attacks or suspicious events, with Sophos MTR, your organization is backed by an elite team of threat hunters and response experts who take targeted actions on your behalf to neutralize even the most sophisticated threats. Customers who choose to leverage Sophos MTR also receive Intercept X Advanced with EDR.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

21-02-11 DS-EN (TN)

SOPHOS