MTR Sophos Managed Threat Response

Sophos Managed Threat Response (MTR) Privacy Data Sheet

SOPHOS

Sophos Managed Threat Response (MTR) Privacy Data Sheet

The purpose of this datasheet is to provide Sophos customers with information they need to understand how our offering affects their privacy considerations. In this document, we provide information about MTR data handling practices, including personal information collection, use and storage.

Product Summary

Built on our Intercept X Advanced with EDR technology, Sophos MTR fuses machine learning technology and expert analysis for improved threat hunting and detection, deeper investigation of alerts, and targeted actions to eliminate threats with speed and precision.

Information Processed by Sophos MTR

Sophos processes the following types of information as part of the MTR service:

- CustomerID
- MachineID
- UserID
- Sophos Intercept X Advanced Telemetry
- Sophos Firewall Telemetry (optional)
- Sophos Cloud Optix (optional)

Licensed endpoints communicate with Sophos infrastructure using HTTPS every 5 minutes. Product events are used to generate MTR detections, and some detections generate MTR Cases. These cases are assigned to an analyst for investigation. Sophos' case management system tracks and audits all actions taken by the analyst. The endpoints communicate with Sophos infrastructure using HTTPS. Depending on the case complexity an analyst may need to acquire more evidence from the endpoint to aid in the investigation and perform response actions to neutralize an active threat on the customer's behalf.

During the course of delivering the service and in the course of an investigation, Sophos may have access to the following information:

- Full user information—including user credentials used to login to the endpoint
- All files contained on the licensed endpoint
- Network data associated with the licensed endpoint

Depending on the case, where a specific file is part of suspicious activity, MTR analysts may access the file. However, in most instances, the MTR analyst will not access the file, but submit the file to Sophos Labs for analysis purposes. In most cases, these files are binary, PE files (Portable Executables) which do not contain personal data.

MTR analysts will only process suspicious files for the purposes of providing evidence to support a case or send to Sophos Labs for further analysis.

Sophos Engineering monitors the effectiveness of the product, planning future roadmap strategy and retirements, product development and enhancement, troubleshooting, generating statistics and reports.

Sophos Rapid Response

MTR Rapid Response offers lightning-fast assistance with identification and neutralization of active threats, delivered by an expert team of incident responders globally.

MTR Rapid Response service supports analysis of third-party log data, like firewall logs, system logs, etc. to aid in triage and define remediation actions. These logs may contain private data including IP addresses, MAC addresses, Hostnames and UserIDs. This data is stored in dedicated customer folders, which can be accessed only by authorized Rapid Response incident responders. Data is deleted when the Rapid Response term ends.

Purpose of Information Processed by Sophos MTR

Sophos processes the information noted above for the purpose of performing the service in accordance with the Sophos Services Agreement.

Sub-processors

Data processed by MTR is hosted in AWS data centers in the region(s) selected by the customer at the time of Sophos Central account creation. In some cases, specifically for the Sophos Rapid Response service, rapid response incident responders may request specific customer data, which is stored temporarily in Box environment for the duration of the rapid response engagement. Visit our Sub-processor listing to find out more about sub-processors engaged by Sophos.

Retention

Sophos applies its retention policies to delete and purge data that is no longer needed for the purpose for which the personal data was originally collected.

MTR retains endpoint and network telemetry for 7 days, MTR Detections for 90 days and MTR Cases for 2 years. After these time frames the data is deleted. Additionally, Sophos will store licensed endpoint telemetry and network telemetry from licensed XG firewalls using Central Firewall reporting in Sophos Central for 7 days, or a longer timeframe based on data retention option the customer has purchased. This data is available to be used by the customer to perform their own queries and investigations independently from the MTR, or Rapid Response services. All customer data is deleted upon termination of the service.

Upon termination of the MTR service, access to the customer interface in Sophos Central is disabled after a 10-day grace period. After this period, the data will be permanently deleted and unrecoverable.

Security

Sophos secures your information by authenticating access via username and password based on managed Active Directory group membership coupled with multi-factor authentication.

The Sophos MTR platform has achieved SOC2 Type II certification and PCI DSS v3.2 attestation to demonstrate its strong security practices, policies and internal controls environment.

For information about the security protections used in the data centers where Sophos MTR data resides, visit the AWS Security Documentation Center.

Our Commitment to Privacy

Sophos is committed to complying with data protection rules and protection of personal data processed by Sophos MTR. Sophos will access data only to enable it to provide the services you have signed up for and in the case of Sophos MTR, to identify security threats or to investigate suspicious activities that are indicative of attacks.

Access

Customer Access

MTR customers have access to Sophos Central customer portal to administer, configure and manage their estate and access information from Sophos endpoints and (optionally) XG Firewalls.

Sophos Access

Access to information processed is restricted to Sophos engineers, and the MTR Operations team. When a support ticket is raised, the Sophos support team will access your account for purposes of troubleshooting and resolving issues.

Some customer data is anonymized and may be accessed by Sophos Labs or Sophos AI teams for threat research purposes to improve our ability to detect new threats. An exception is file submission of suspicious files that may contain personal information. If these files are convicted as malicious, then they are treated as malware and will be blocked globally going forward. If these files are not convicted and are cleaned, they are permanently deleted within 30 days.

MTR Operations has system level privileges on licensed endpoints, including ability to start and stop software, delete and read files and otherwise take any actions deemed necessary for the purpose of providing the service, according to the customers' threat response mode preferences set in Sophos Central.

Disclaimer

The information contained in this privacy data sheet may change at any time and is only meant for general awareness. This MTR Privacy Data Sheet is not meant to constitute legal advice, warranty of fitness for a particular purpose or compliance with any applicable laws.