Managed Threat Detection

Supplement your existing non-Sophos endpoint protection with 24/7 monitoring and detection delivered as a fully-managed service

Bring Your Own Protection

Few organizations have the right tools, people, and processes in-house to effectively manage their security program around-the-clock. There is a lot of dependence on automated endpoint protection, but what happens if bad actors are able to circumvent that protection? Will anyone notice before it is too late?

Sophos Managed Threat Detection provides 24/7 threat monitoring and detections to ensure that whatever suspicious activity evades your endpoint protection will not go unnoticed. The service is designed to run in parallel with non-Sophos endpoint protection products, which means organizations can continue to use their current endpoint protection while still being monitored by Sophos threat experts.

Detection

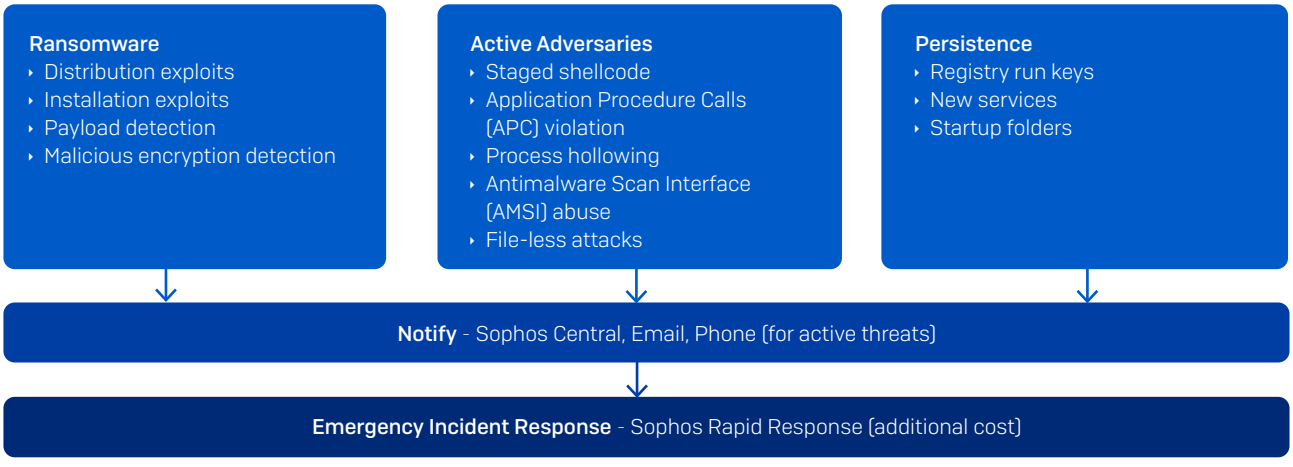
Managed Threat Detection is available in "Notify" threat response mode. Customers will receive alerts if a high severity threat evades their endpoint protection solution. This includes a variety of behavioral activity commonly seen before ransomware attacks.

Examples of detection events include:

- Staged shellcode such as those is commonly found in CobaltStrike Beacon or Metasploit Meterpreter
- New scheduled task which runs $PS, including activity in locations which are commonly used for persistence by malware and threat actors (i.e. registry runkeys, services, Windows startup items)
- Ransomware and behavioral activity that other protection products may miss

Highlights

- 24x7 monitoring and detection of suspicious activity
- Designed to run in parallel with third party endpoint protection products
- "Notify" threat response mode
- Analyst validation of all high severity detections
- Notifications provided with remediation recommendations
- Sophos Rapid Response is available for additional incident response



SOPHOS

Notification and Response

Clear communication is absolutely critical when running a security operations program. This is why the Managed Threat Detection service provides a steady stream of information, including weekly and monthly reports, email notifications, and a dashboard in Sophos Central.

Customers will receive email notifications with case status updates. This includes alerts when action is required and when cases are resolved. All Cases are validated by an analyst and notifications will incorporate a case synopsis, a list of affected devices, and remediation recommendations.

Additionally, broadcasts will be sent alerting customers to breaking industry news explaining the latest findings on the threat, what steps Sophos is taking, and what customers can do to stay protected.

When active threats are detected in a customer environment Sophos operators will reach out via phone. This ensures that critical information is not delayed. Customers can update their Managed Threat Detection authorized contact information and preferences in their Sophos Central dashboard at any time. The dashboard also provides a summary of all relevant Managed Threat Detection activity giving customers the most up to date information wherever and whenever they need it.

If incident response help is needed to respond to a threat the Sophos Rapid Response team is available as an additional service. Sophos Rapid Response provides fast emergency assistance to investigate and neutralize active threats. Whether it is an infection, compromise, or unauthorized access attempting to circumvent (or has successfully breached) your security controls, the team has seen it all and stopped it all. Sophos customers have a built-in speed advantage since the Rapid Response incident response team will have immediate access to the telemetry and data recorder provided by the Managed Threat Detection agents.

	Managed Threat Response (MTR) Standard	Managed Threat Response (MTR) Advanced	Managed Threat Detection
Third-party endpoint protection compatible	✗	✗	✓
24/7 monitoring	✓	✓	✓
Adversarial detections	✓	✓	✓
Reports, Dashboard	✓	✓	✓
Threat notification	✓	✓	✓
Sophos Firewall MTR Connector	✗	✓	✓
Sophos CloudOptix MTR Connector	✗	✓	✗
Multiple OS support	✓	✓	✗ (Win10/2012r2+ only)
Analyst-initiated leadless threat hunting	✗	✓	✗
Sophos endpoint health check	✓	✓	✗
Real-time protection	✓	✓	✗
Containment and neutralization	✓	✓	✗
Communication via phone	✗ (active threats only)	✓	✗ (active threats only)

Thailand : E-Rong Consultants Co.,Ltd. I Tel : 02-664-6588 I E-mail : sales@e-rong.co.th