SOPHOS

MAXIMIZE CYBER RESILIENCE FOR MSPS WITH SOPHOS MANAGED THREAT RESPONSE (MTR)

A Sophos whitepaper September 2020

Introduction

Today's adversaries have MSPs firmly locked in their sights. From nation states like China to criminal groups like GandCrab and REvil, the one-to-many relationship between a MSP and their portfolio of customers offers adversaries a springboard to quickly and efficiently devastate multiple targets at once.

Adversaries understand the existential threat they pose to the MSP industry's credibility and this makes them an even more attractive target. It is every MSP's nightmare to have to contact every single customer and inform them that the worst has happened. One incident could result in a loss of faith and a loss of custom that forces a MSP to close its doors for good.

The social pressure that a successful breach poses greatly increases an adversary's chances of a lucrative payout to their ransomware or blackmail and further incentivizes their efforts in targeting and breaching MSPs. Seven figure ransom requests are not unheard of, with some groups exfiltrating terabytes of customer data and threatening to publicly release it online should the ransom not be paid.

It is essential that a MSP not only invest in prevention technologies for themselves and their clients, but to also ensure mature detection and response capabilities are in place so that threats that evade prevention are swiftly detected and responded to before they escalate into high-impact incidents.

Sophos Managed Threat Response (MTR) provides you with piece of mind knowing you are backed by an expert team of threat hunters, threat analysts, and incident responders. The service provides around-the-clock monitoring over your managed assets, hunting, threat detection, and real-time incident investigation. When a threat is detected the Sophos MTR team responds in collaboration with your team, or entirely on your behalf. Rather than wait until a breach occurs and scrambling to enlist assistance, Sophos MTR are already there, defending against new and emergent threats, working alongside you to contain and neutralize them.

- Defend your clients by defending yourself
- Union of technology, people, and process
- Augmenting your security team with response experts
- Rapid Response for when the worst happens
- Integrated insight across endpoint, network, and cloud
- High efficacy signals for efficient investigation

Defend your clients by defending yourself

MSPs continue to be targeted by advanced adversaries. This underlines the importance of a MSP defending themselves with equal, if not greater effort than they defend their clients with.

Partnering with another service provider like Sophos MTR provides you with a pragmatic approach to risk reduction. Layer your own defenses with additional oversight and the added expertise of a managed service so that even the most capable adversaries will struggle to get past your defenses.

Union of technology, people, and process

Effective defenses against cybersecurity incidents requires a multi-layered approach with a union of technology, people, and process. The NIST Cybersecurity Framework refers to five core functions: Protect, Detect, Respond, Recover, Identify. Across all these core functions technology solutions exist to aid in their successful execution, but technology alone cannot solve the problem of cybersecurity.

Sophos MTR fuses Sophos technology with human expertise and response, enhanced with industry-leading machine learning. Included with the MTR service is Sophos Intercept X Advanced, our industry leading prevention technology with a broad range of protection and detection capabilities for ransomware, exploitation, file-less and file-based malware, adversarial behaviors and TTPs (tactics, techniques, and procedures), and more. Also included is Sophos EDR (Endpoint Detection and Response), capturing enhanced system telemetry that can be leveraged to hunt down threats and IT operations issues, as well as enable remote access to systems to investigate and respond to incidents.

Augment your security team with response experts

Responding to threats requires experience. While many MSPs have mature security operations, the volume and scale of incidents they've seen may be minimal. Sophos MTR acts as a virtual expansion of your existing team with extensive experience in threat detection and response.

In addition, with Sophos MTR hunting, investigating, and responding to threats, this frees up your existing teams to work on more strategic efforts or important projects that are important to the growth and success of your business.

Rapid Response for when the worst happens

For customers not already protected by Sophos MTR, Sophos Rapid Response offers a fixed-cost, lightning-fast incident response service to identify and neutralize active threats. When experiencing an active incident second matter. That is why the Rapid Response service is able to onboard customers within hours, and most are triaged within 48.

Whether you offer your own response service or not, Sophos Rapid Response provides specialist assistance to navigate even the most complex of incidents.

Integrated insight across endpoint, network, and cloud

The adage "you're only strongest as your weakest point" still remains true. Adversaries overwhelmingly breach an organization through the point where the defenses are weakest, yet this weakness could exist or emerge anywhere. It could be a misconfigured cloud-hosted server, a phishing email to an end-user, or an exploit of a web application.

Sophos MTR offers integrations (known as MTR Connectors) with Sophos Intercept X endpoint protection, Sophos XG Firewall, and Sophos Cloud Optix, ensuring that our security operations team have visibility across all key areas where an adversary may place their first digital step inside your environment. With fewer blind spots, threats can be identified and neutralized earlier in the attack chain, ejecting adversaries before they are able to action on their objectives.

High efficacy signals for investigation

Many security services rely solely on SIEMs aggregating logging data from multiple sources, filtering that data in the hopes of identifying signals worthy of investigation. The signal to noise ratio of these kinds of solutions results in a lot of time wasted investigating signals that are not truly indicative of adversarial or malicious activity. Time is a limited resource and when an adversary has successfully circumnavigated defenses, seconds matter.

Sophos MTR takes full advantage of Sophos Intercept X and other MTR Connector products, using product telemetry as well as system telemetry, to find the signals that are actionable and worthy of deeper inspection. With less time spent sifting through data to find signals to investigate, our operators spend more time on active investigations, with full access to the broad spectrum of data that would typically be gathered in a SIEM to assist them with their investigation.

Additional, in partnership with SophosAI, research machine learning models are trained on Sophos MTR data and deployed into our platform to learn from our human expertise, automating detection of classes of threats so that our operators can focus on the next emergent class of threat.

Designed for MSPs

Unlike other MTR services that claim to be designed for MSPs, the Sophos MTR team will take proactive action – either collaborating with you or completely on your behalf - whereas others will simply offer the solution for the MSP to implement.

We understand that threat notification is not the solution rather it is a starting point. Not all MSP organizations have the right tools, people, and processes in-house to effectively manage their security program around-the-clock while proactively defending against new and emerging threats. Going beyond simply notifying you of attacks or suspicious behaviors, the Sophos MTR team takes targeted actions on your behalf to neutralize even the most sophisticated and complex threats.

The words "breach" and "incident response" are not words that a managed service provider typically like the sound of. However, reports and studies continue to show us that SMBs are the most attacked and subsequently the most vulnerable. As these responsibilities of maintaining cyber resiliency for your clients grows, so does the need to be as most prepared for attack. Too often do we see SMB victims of cyberattacks seek reparation from the guardians in which they trusted the security of their business – the MSP. Hackers are using tactics that quite simply can catch MSPs off guard or simply circumvent the most robust endpoint protection products - in the event of a breach would you not want to have an immediate contact of expert threat analysts to support you?

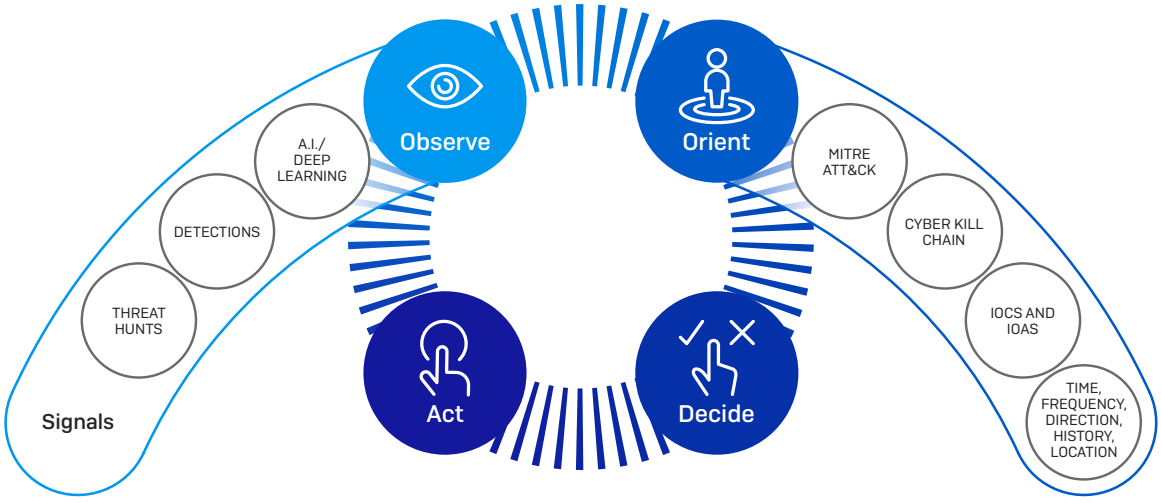
The Sophos MTR investigative framework for threat hunting and response is based on the military concept known as the OODA loop: Observe, Orient, Decide, Act.

Observe: Select key points of data that help establish a narrative of activity that is occurring on your clients' devices or within an environment.

Orient: Analysts validate observables which can create indicators. Validation is performed by applying the data points to the MITRE ATT&CK Matrix, the Cyber Kill Chain, and an analyst's tribal knowledge.

Decide: Analyst reviews previously compiled data points to determine what is required in the Act phase to come to a confident decision in the identification of malicious activity.

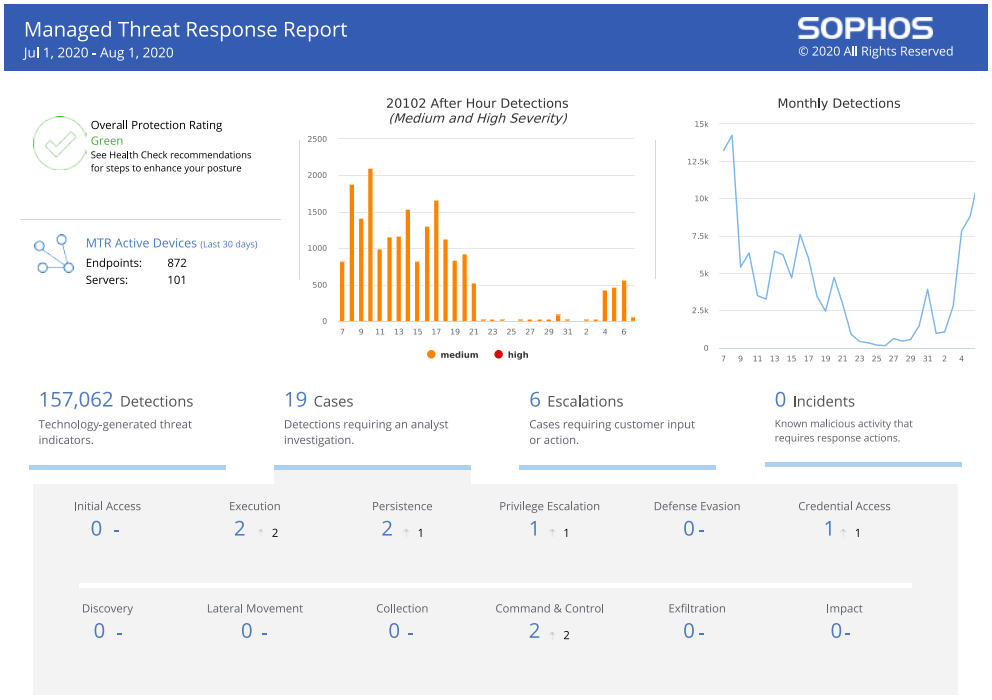
Act: If enough information has been gathered, enabling the analyst to answer the key questions in the Decide phase, then the analyst will move forward and take the necessary actions.



Monthly Activity Reporting

The MTR team constantly reviews alerts, investigates anomalous activity, and responds to confirmed threats with speed and precision based upon your selected preferences. In addition to providing comprehensive assessments of attacker activity and corresponding response actions as they occur, the MTR team also provides monthly activity reports summarizing case activities and providing the context needed to understand threats, assess organizational risk, and prioritize actions. .

These monthly reports provide MSPs with an Overall Protection Rating, which is an aggregate analysis of the security posture improvement recommendations that have been implemented versus those that have not been implemented. These health check recommendations can include things like enabling anti-exploitation features to protect against credential theft or privilege escalation, or enabling malicious traffic detection to hinder communication to command and control servers.



Example of Monthly MTR Service Report

Flexible Licensing Options

Sophos MTR features two service tiers (Standard and Advanced) to provide a comprehensive set of capabilities for organizations of all sizes and maturity levels. Regardless of the service tier selected, MSPs can take advantage of any of the three response modes (notify, collaborate, or authorize) to fit your needs.

Sophos MTR: Standard

24/7 Lead-Driven Threat Hunting
Confirmed malicious artifacts or activity (strong signals) are automatically blocked or terminated, freeing up threat hunters to conduct lead-driven threat hunts. This type of threat hunt involves the aggregation and investigation of causal and adjacent events (weak signals) to discover new Indicators of Attack (IoA) and Indicators of Compromise (IoC) that previously could not be detected.

Security Health Check
Keep your Sophos Central products--beginning with Intercept X Advanced with EDR--operating at peak performance with proactive examinations of your operating conditions and recommended configuration improvements.

Activity Reporting
Summaries of case activities enable prioritization and communication so your team knows what threats were detected and what response actions were taken within each reporting period.

Adversarial Detections
Most successful attacks rely on the execution of a process that can appear legitimate to monitoring tools. Using proprietary investigation techniques, our team determines the difference between legitimate behavior and the tactics, techniques, and procedures (TTPs) used by attackers.

Sophos MTR: Advanced *Includes all Standard features, plus the following:*

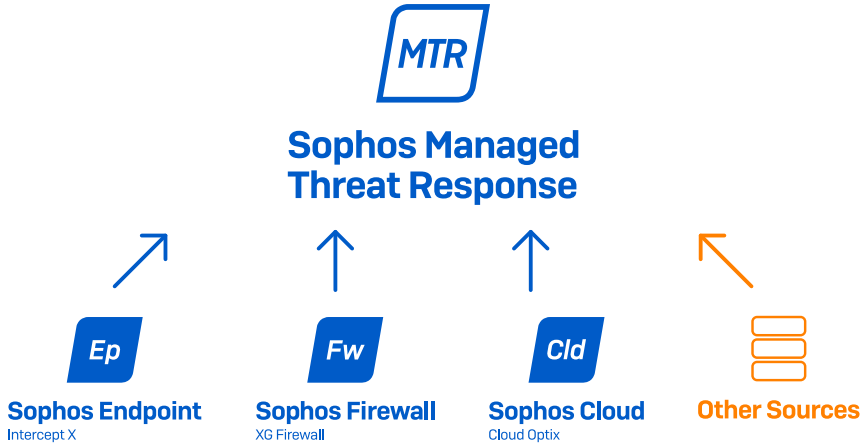
24/7 Leadless Threat Hunting
Applying data science, threat intelligence, and the intuition of veteran threat hunters, we combine your company profile, high-value assets, and high-risk users to anticipate attacker behavior and identify new Indicators of Attack (IoA).

Enhanced Telemetry
Threat investigations are supplemented with telemetry from other Sophos Central products extending beyond the endpoint to provide a full picture of adversary activities.

Proactive Posture Improvement
Proactively improve your security posture and harden your defenses with prescriptive guidance for addressing configuration and architecture weaknesses that diminish your overall security capabilities.

The Sophos Next-Gen Difference

Sophos combines the necessary elements of a layered security environment into an easy to navigate platform that gives you visibility and protection that is scalable. These combined layers of security within Sophos Central are also synchronized to share information across products to stop threats in real time, making it one of the most effective and comprehensive cybersecurity system. Adding the Sophos Managed Threat Response service to the stack elevates your MSP security offering and brings the reassurance of a trusted security operation center (SOC) to MSPs of any size.



Learn more about Sophos advanced Managed Threat Response service or speak with a cybersecurity expert to get started.

Learn more about Sophos Managed Threat Response at

www.sophos.com/MTR

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

20-09-10 WPEN (DD)

SOPHOS