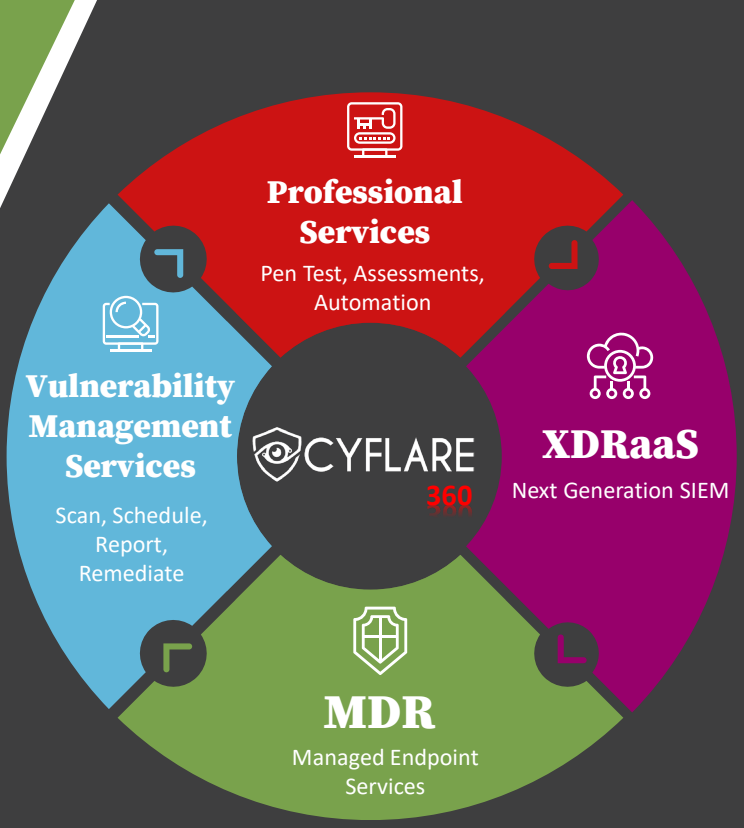
CYFLARE
The threat stops here.

MANAGED DETECTION AND RESPONSE (MDR) SERVICES

Supercharge your security posture and let our security analysts monitor your detections around the clock.



As an MDR service provider, we believe clients must know exactly what use cases and detection types our SOC analysts respond to and at what priority rather than a generic answer of simply responding to everything.

As a client responsible for securing the endpoints in your organization, you must know exactly which use cases are monitored by the SOC, at what priority, and what timeframe for response. With the simple event table below, it is easy to know exactly what use cases we monitor for and what severity we assign to them.

Use Case	Severity	Description
Remediation Event	Medium	A threat was identified and preemptively mitigated by the source tool. A full SOC investigation, and notification to be completed regarding the threat with appropriate recommended actions.
Potentially Unwanted Application (PUA)	Medium	A threat was identified with the classification of a PUA. A full SOC investigation, and notification to be completed regarding the threat with appropriate recommended actions.
Blacklist or Whitelist Threats	Medium	After a threat is identified, one of the recommended actions is to add the file, hash, or application to a blacklist or whitelist/exclusion depending on the nature of the threat.
Malware Identified	High	A threat was identified with one of the following malicious classifications: Malware, Ransomware, Trojan, Adware, Spyware, Worm, Virus, Exploit, etc. A full SOC investigation, and notification to be completed regarding the threat with appropriate recommended actions.
Failure to Remediate	High	A threat was identified and not preemptively mitigated by the source tool. A full SOC investigation, and notification to be completed regarding the threat with appropriate recommended actions depending on the nature of threat.

NOTE: Outbound Threat Protection SLAs follow standard CyFlare SLAs.

Advanced Endpoint Services

Detect and remediate threats immediately.

Use Case	Severity	Description
Installation and Removal of Agents	Low	An inbound request is received regarding the installation or removal of an agent from an endpoint post-deployment.
Agents Updated	Low	An inbound request is received regarding updating an agent or group of agents post-deployment. Also, proactive outbound recommendations to update an agent or group of agents for security best practice and hygiene.
Policy/Configuration Change	Low	An inbound request is received regarding changes to a policy or configuration change post-deployment. This includes detect or protect policies upon detection of threats, engines enabled, and items captured by agents for deep visibility.
Device Control (USB/Bluetooth)	Low	An inbound request is received regarding a new device control rule to be created, changed, or deleted post-deployment for endpoint peripherals.
Reboot Required	Low	An inbound request or outbound request is made for a reboot required on an endpoint for the agent to function as expected.
User Management	Low	An inbound request is made to create, change, or delete a user from the endpoint management console post-deployment.
Exclusion Management	Medium	An inbound request is made to enable exclusions for file paths, applications, or hashes to avoid sensitive items from being scanned or affected by EDR post-deployment.

NOTE: Outbound Threat Protection SLAs follow standard CyFlare SLAs.

Our Managed Endpoint Solutions

CyFlare Takes You Further

Bundled security solutions via ONE pull the full attack storyline together.

With the CyFlare ONE platform, your investment in an advanced endpoint solution extends beyond any other service provider's capabilities. Clients who rely on CyFlare to monitor multiple security solutions receive extraordinary benefits when it comes to a thorough investigation, containment, and eradication.

With multiple solutions working together to identify potential Indicators of Compromise (IoC) to the SOC and the ability to systematically interconnect these systems through APIs, it is now possible to enable an intelligent SOC that pulls the full attack storyline together and systematically eradicates the threat.

The table below identifies a sample of scenarios and integrated value-adds for bundled services.

Bundled Services Benefits	
Use Cases	**Extended Detection and Response (XDR)**
Remediation Event	▪ Identify root cause if caused by an external actor, IP or domain ▪ Identify potential account takeover activity ▪ Identify lateral movement if available ▪ Enrich with external threat intelligence
Failure to Remediate	▪ View real-time lateral movement ▪ Visualize event story line by Kill Chain Phase and 360-degree Panoramic view ▪ Identify related early stage Indicators such as reconnaissance or account takeover related events ▪ User Behavior Analytic anomalies
Potentially Unwanted Application (PUA)	▪ Identify machines using the same application on the network ▪ 0-day file sandboxing from XDR Service Network Traffic Analysis ▪ New application usage anomaly detection

Extended Detection and Response (XDR) Services consist of a cloud-native Next Generation SIEM platform continuously monitored by the CyFlare SOC. Clients who subscribed to both the Managed Endpoint solution and XDR Services realize significant efficiencies by allowing the SOC to investigate, contain, and remediate across the cloud, perimeter, network,

Transparent Day-to-Day Access

A co-managed or managed security investment.

Many of our clients need a 24x7 SOC to address security events but still want the ability to use the tool, manage policies and help themselves when they need to. Like all CyFlare's managed security services we always allow fully privileged access to the console so that you can fully realize your investment. The CyFlare SOC is always just a ticket away to get assistance when you need it.

Managed endpoint services are offered in two distinct operating modes offering unmatched options compared to competitive solutions. Those management levels are as follows:

- **Co-Managed:** API Integration with CyFlare ONE + SOC Access to source tool UI for security event investigation
    - Does not include typical day to day management actions such as reporting, troubleshooting agent issues, upgrading agents, account handling, and other policy configurations.
    - Configuration change requests and guidance will be provided when necessary for improving the security of the endpoint.
- **Managed:** Managed Endpoint solutions have each gone through the CyFlare Center of Excellence process to be sure resources are trained, systems are integrated, operations are in place to comprehensively manage all aspects of the endpoint solution including design, deployment, configuration, maintenance, and thorough incident response.

Engaging Your CyFlare SOC

Support can be requested at any time by calling into the SOC, placing a ticket via email or ticketing portal or contacting your Customer Success Manager. Additionally, tickets can be escalated by requesting escalation with the SOC, changing the severity of the ticket, or emailing escalation@cyflare.com. This is all communicated during onboarding and reiterated within each ticket sent from the SOC.

Want a free demo? Contact us!

Email us at **sales@cyflare.com** or call 1-877-729-3527