Managed Detection and Response Service (MDR)

Thrive's Managed Detection and Response Service (MDR) combines powerful Extended Detection and Response Services (XDR) with Security Incident and Event Management (SIEM), proactive oversight by a global 24x7x365 SOC and an automation AI platform powered by ServiceNow and Security Orchestration, Automation & Response (SOAR) technologies to provide the most advanced protection against cyber threats targeted at core infrastructure and all endpoints.

Thrive's (MDR) provides proactive threat monitoring, incident response, and remediation against the daily cyber threats that can impact organizations large and small. MDR is an important component of a comprehensive cybersecurity strategy to proactively identify and respond to potential threats.

Our security professionals collaborate with your internal teams to quickly respond to security incidents of all complexity levels. This collaboration helps to remediate and neutralize threats and thoroughly investigate their root causes, while we continuously tune our detection rules to improve your security posture and increase visibility into potential threats more quickly.

Thrive's MDR includes a combination of security monitoring technologies, threat intelligence, automation, and industry certified security analysts who are responsible for monitoring and responding to security incidents to quickly analyze suspicious events to contain and remediate the threat.

Key Benefits

Outsourcing this critical security control to Thrive as your trusted cybersecurity provider allows you to free up resources and expertise to focus on your core business functions while ensuring your organization is protected.

Improved Threat Detection and Response Capabilities

Thrive's MDR provides continuous security monitoring and analysis of your organization's digital assets to identify and respond to potential threats more quickly and effectively.

Reduced Risk of Data Breaches

By detecting and responding to threats in real-time, Thrive MDR can help prevent data breaches and other cyber-attacks.

Enable Compliance

Thrive MDR can help organizations comply with industry regulations and standards, such as GDPR, HIPAA, and PCI-DSS.

Cost Savings

Thrive MDR can help organizations save costs by reducing the need for multiple layers of cybersecurity resources and preventing major business-impacting data breaches.

Managed Detection and Response Service (MDR)

Our MDR platform collects telemetry and data from servers, firewalls, network devices, applications, SaaS, Cloud, and security platforms, and adds real-time context, analytics, and alerts for a more complete understanding of the environment. When a suspicious incident is detected, pre-planned, automated responses are initiated to drastically reduce the time to respond to critical incidents. Analysis and triage are then performed by the 24x7x365 Thrive Security Operations Center (SOC) team of certified security experts to determine the threat risk and the appropriate actions to remediate or mitigate the threat.

Thrive's XDR provides Next Generation file-based and file-less malware detection & protection for servers and workstations, providing both pre-infection and post-infection detection and prevention against data exfiltration and ransomware. The platform identifies and stops breaches in real-time, automatically and efficiently with automated response and remediation playbooks and procedures. This is the most powerful tool available in today's market to mitigate escalating dangerous threats targeted at businesses, government agencies and educational institutions alike.

The Thrive MDR service is built upon three core functions to detect and respond to any suspicious activity that could indicate potential security threats before they can cause damage to your organization's systems and data.

1. **Threat Detection:** Thrive MDR utilizes a tightly integrated technology stack that includes SIEM, SOAR, and XDR platforms to collect and analyze security data from an organization's network, endpoints, and cloud infrastructure, combined with threat intelligence information to detect potential cyber threats in real-time.

2. **Incident Response:** When a potential threat is detected, Thrive's team of security analysts will investigate the incident, determine the scope of the threat, and provide guidance on how to respond. This process involves identifying, containing, investigating, and remediating the incident to minimize damage and prevent future incidents from occurring.

3. **Remediation:** Remediation is dependent on the ultimate source of the event and the access Thrive has to the impacted system(s) and/or network.
   - Thrive provides direct threat remediation for any impacted systems contracted under Thrive Managed Services. Thrive security analysts will direct our internal teams responsible for managing the impacted system on the remediation steps they will need to perform to mitigate or remediate the threat.
   - Thrive security analysts will provide guidance to clients who manage their internal systems with information detailing the impacted systems and the steps required to mitigate or remediate the threat.

Take the Next Step

To learn more about how Thrive can help your business, please visit thrivenextgen.com