3. TREND MICRO MDR

MANAGED DETECTION AND RESPONSE SERVICE

Trend Micro Managed Detection and Response (MDR) is a service that provides detection and response services on behalf of its customers. It monitors customer network, server, email, and endpoint data (24/7), and using advanced analytics and artificial intelligence (AI) techniques to correlate and prioritize alerts according to severity. Customers have access to the MDR experts who, along with the institutional collective knowledge of the security vendor, can provide actionable remediation plans and guidance. Trend Micro experts perform a root cause analysis to get an understanding of how attacks are initiated, how far they spread, and what remediation steps need to be taken.

Customers can choose to monitor endpoint, network, email, or server security products:

- **Endpoints** with Trend Micro Apex One™ and Trend Micro Apex One™ Endpoint Sensor record system behaviors and activity. Metadata on this, along with alerts and detections, are sent to the Trend Micro MDR service.

- **Networks** equipped with Trend Micro™ Deep Discovery Inspector™ provide advanced network detection across over 100 protocols and all network ports. The MDR service collects network data from Deep Discovery Inspector as well as detections and alerts.

- **Servers** protected by Trend Micro™ Deep Security™, send log information to the MDR service so that Trend Micro analysts can perform detection and response services.

- **Email** protected by Trend Micro Cloud App Security can also subscribe to Managed XDR for messaging, allowing Trend Micro staff to extend root cause analysis and sweeping back to Microsoft® Office 365® for a proactive response.

While Trend Micro offers individual services for the above, the true strength of the service is the ability to correlate alerts and data from multiple technologies for better detection. Detection improves with the number of threat vectors served.

The service can correlate and prioritize contextual threat information from multiple sources and deliver an automated response. This will be done with the help of three specific enhancements:

- AI-augmented detection and correlation of high-risk threats
- Automated prioritization of threat information across user endpoints, networks, email, and servers
- Orchestration and response automation

When the MDR service detects a threat, Trend Micro MDR analysts immediately work to ensure that the organization is protected with updated threat information. An IoC sweep then determines the impact of the attack. Once the scope is known, Trend Micro analysts perform a root cause analysis to determine the source and spread of the attack. Customers are advised of remediation that may need to occur. Throughout this process Trend Micro is in constant communication with the customer.

*Figure: Trend Micro Managed Detection and Response*