

SECURITY TECHNOLOGY MONITORS

You are responsible for management and routine monitoring of the Managed Defense Supported Technology, and any intermediate systems that support communication with Managed Defense. This includes being responsible for identifying and taking all actions needed to bring devices online in the event of an outage and applying updates and patches. Since your security technologies must be in a good state of health for Managed Defense to provide our services, we provide a set of monitors to assist you with this monitoring. The following table lists the available monitors for customer-managed Trellix Supported Technologies.

Monitor Name	Technology	Details
VPN Connectivity	Trellix Endpoint Security, Trellix Network Security, or Trellix Network Forensics	Appliance disconnects from the Managed Defense VPN
Degraded State	Trellix Endpoint Security, Trellix Network Security, or Trellix Network Forensics	Delayed responses for a period of 30 minutes
Device API Errors	Trellix Endpoint Security, Trellix Network Security, or Trellix Network Forensics	Unsuccessful API calls
Endpoint Discovery	Trellix Endpoint Security	Endpoints not discovering for a 24-hour period
MMD API Response	Trellix Endpoint Security, Trellix Network Security, or Trellix Network Forensics	Delayed API response times for a 15-minute period
MD Hunting Sweep Error Detected	Trellix Endpoint Security	Excessive errors within one minute



Managed Defense monitoring of Microsoft Defender for Endpoint Supported Technology is limited to monitoring and notifications on connectivity with Managed Defense.