Mandiant

MD SOC CONTAINMENT

You may enroll in the MD SOC Containment feature to allow Managed Defense to contain designated endpoints. By containing endpoints, you limit the impact of threat detected in your environment. MD SOC Containment uses the containment or isolation feature of your endpoint detection and response (EDR) agents to limit network connectivity and prevent communication to compromised devices. You authorize the endpoints that Managed Defense can contain. Upon enabling this feature, you acknowledge that Managed Defense maintains full discretion to contain endpoints per the configuration you choose.

Typical MD SOC Containment scenarios include, but are not limited to, the following:

- Malware with known propagation capabilities
- Ransomware
- Hands-on attacker activity
- Detected lateral movement
- Attempted data exfiltration
- Identification of a backdoor or remote access tool
- Identification of data staging

Managed Defense supports MD SOC Containment on the following EDR technologies:

- CrowdStrike Falcon
- Microsoft Defender for Endpoint
- SentinelOne Singularity
- Trellix Endpoint Security

To set up the MD SOC Containment feature, you must configure the settings for each technology that you want to use for containment.

Configure MD SOC Containment

To configure the MD SOC Containment feature for your EDR technology, use the following steps:

> Only users with the Team Admin role are able to manage the SOC Containment setting.

1. Navigate to **Settings > Organization** and select the organization you want to opt in or out.

   > Selecting an organization is only required if your Managed Defense account has multiple organizations.

2. Make a selection for the **MD SOC Containment** setting that you want to update:
   - **Do Not Contain** (default): Does not permit Managed Defense to contain endpoints in your environment.
   - **Specific Endpoints**: Allows Managed Defense to contain endpoints that you designate through tags in your EDR host management.

     > Additional configuration is required for this selection. See **Configure MD SOC Containment for Specific Endpoints** for technology-specific details.

   - **Any Endpoints**: Allows Managed Defense to contain any endpoint in your environment.

A list of MD SOC Containment options for three EDR technologies: CrowdStrike Falcon, Microsoft Defender for Endpoint, and SentinelOne Singularity

Configure MD SOC Containment for Specific Endpoints

For any EDR technology you have selected to contain **Specific Endpoints**, select the corresponding technology tab and follow the directions to tag endpoints for containment.

CrowdStrike Falcon

Configure MD SOC Containment for CrowdStrike Falcon

Microsoft Defender for Endpoint

Configure MD SOC Containment for Microsoft Defender for Endpoint

SentinelOne Singularity

Configure MD SOC Containment for SentinelOne Singularity

Trellix Endpoint Security

Configure MD SOC Containment for Trellix Endpoint Security