Mandiant

MANAGED DEFENSE SUPPORTED TECHNOLOGIES

Mandiant Managed Defense (Managed Defense) delivers Managed Detection and Response (MDR) services using supported security detection technologies. The Managed Defense service is most effective when visibility is maximized by using a broad set of Supported Technologies. Services delivered on each platform are subject to the capabilities of the technology and the permissions granted to Managed Defense.

Security Technologies that Managed Defense Supports

The following tables list the supported security technologies, required Google Security Operations parsers, and supported alert types from each vendor that are processed as part of providing security event monitoring and threat hunting services.

Indicators of Compromise (IOCs) and signatures created by customers are not within the scope of Managed Defense service delivery. Managed Defense does not generally escalate rules where activity has been blocked. For instance, an email may be quarantined before you receive it or traffic may be dropped by an inline network security device. This escalation is only possible if the activity is related to other malicious activity.

Corelight

Product	Description	Required SecOps Parsers	Managed Defense Supported Alert Types
Open NDR	Suricata alerts and Zeek logs are supported by Managed Defense.	Alerts and Telemetry: **CORELIGHT** (https://docs.cloud.google.com/chronicle/docs/ingestion/parser-list/corelight-changelog)	• Suricata Alerts

CrowdStrike

Product	License requirement	Description	Required SecOps Parsers	Managed Defense Supported Alert Types
CrowdStrike Endpoint Security	CrowdStrike Falcon Enterprise or higher	CrowdStrike Falcon Enterprise, Elite, and Complete are supported for Endpoint Protection Platform (EPP) alerts.	**CS_ALERTS** (https://docs.cloud.google.com/chronicle/docs/ingestion/parser-list/cs-alerts-changelog)	Endpoint Protection (EPP) alerts
CrowdStrike Falcon Next-Gen Identity Security	CrowdStrike Falcon Next-Gen Identity Security	Managed Defense supports ingestion and monitoring of alerts from the CrowdStrike Falcon Identity Protection (IDP) module.	**CS_ALERTS** (https://docs.cloud.google.com/chronicle/docs/ingestion/parser-list/cs-alerts-changelog)	Identity Protection (IDP) alerts

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Product	License requirement	Description	Required SecOps Parsers	Managed Defense Supported Alert Types
Falcon Endpoint Telemetry	Falcon Data Replicator license	CrowdStrike Falcon Enterprise, Elite, and Complete are supported by Managed Defense. Falcon Data Replicator is required for service.	**CS_EDR** (https://docs.cloud.google.com/chronicle/docs/ingestion/parser-list/cs-edr-changelog)	N/A

Microsoft

Product	License requirement	Description	Required SecOps Parsers	Managed Defense Supported Alert Types
Defender for Endpoint	One of the following: • Endpoint Plan 2 • Defender for Business • Defender for Identity license	Microsoft Defender for Endpoint Plan 2 or Defender for Business is required for service delivery. Managed Defense uses the **Endpoint Detection and Response** (https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/overview-endpoint-detection-response?view=o365-worldwide) features of the platform.	Alerts: **MICROSOFT_GRAPH_ALERT** (https://docs.cloud.google.com/chronicle/docs/ingestion/parser-list/microsoft-graph-alert-changelog) Telemetry: **MICROSOFT_DEFENDER_ENDPOINT** (https://docs.cloud.google.com/chronicle/docs/ingestion/parser-list/microsoft-defender-endpoint-changelog)	• Antivirus • Endpoint Detection and Response (EDR)
				The following signatures are monitored in real-time by the Managed Defense SOC. All other signatures are leveraged for hunting and do not adhere to Managed Defense Service Level Objectives. • Suspected over-pass-the-hash attack (forced encryption type) • Suspicious additions to sensitive groups • Data exfiltration over SMB • Suspected Golden Ticket usage (forged authorization data) • Malicious request of Data Protection API master key

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Product	License requirement	Description	Required SecOps Parsers	Managed Defense Supported Alert Types
Defender for Identity	One of the following: • Endpoint Plan 2 • Defender for Business • Defender for Identity license	Microsoft Defender for Identity alerts is supported for customers who have provided Managed Defense access to Microsoft Security Graph.	Alerts: **MICROSOFT_GRAPH_ALERT (https://docs.cloud.google.com/chronicle/docs/ingestion/parser-list/microsoft-graph-alert-changelog)**	• Suspicious service creation • Suspected Kerberos SPN exposure • Suspected Golden Ticket usage (ticket anomaly) • Suspected Golden Ticket usage (nonexistent account) • Suspected SID-History injection • Suspected overpass-the-hash attack (Kerberos) • Suspected Skeleton Key attack (encryption downgrade) • Suspected DCShadow attack (domain controller replication request) • Suspicious VPN connection • Suspected DCShadow attack (domain controller promotion) • Suspected use of Metasploit hacking framework • Suspected Brute Force attack (SMB) • Suspected NTLM authentication tampering • Suspected WannaCry ransomware attack • Suspected NTLM relay attack • Suspected SMB packet manipulation (CVE-2020-0796 exploitation) • Suspected Golden Ticket usage (ticket anomaly using RBCD) • Suspected rogue Kerberos certificate usage • Suspected exploitation attempt on Windows Print Spooler service • Suspected AS-REP Roasting attack • Exchange Server Remote Code Execution (CVE-

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Product	License requirement	Description	Required SecOps Parsers	Managed Defense Supported Alert Types
				2021-26855) • Suspicious modification of a sAMNameAccount attribute (CVE-2021-42278 and CVE-2021-42287 exploitation) • Suspicious modification of the Resource Based Constrained Delegation attribute by a machine account • Suspicious disable of audit filters of AD CS

Operational Technology applications

Product	Description	Required SecOps Parser	Managed Defense Supported Alert Types
Claroty CTD	Alerts from Claroty CTD are supported by Managed Defense.	**CLAROTY_CTD (https://docs.cloud.google.com/chronicle/docs/ingestion/parser-list/claroty-ctd-changelog)**	• Alerting events `blocked` or `not blocked` are informational and passed on in the alert context as one of the following: ◦ `attempted` ◦ `failed` ◦ `succeeded`
Claroty xDome	Alerts from the Threat category are supported by Managed Defense.	**CLAROTY_XDOME (https://docs.cloud.google.com/chronicle/docs/ingestion/parser-list/claroty-xdome-changelog)**	• Events in the Threat category, malicious addresses, or infected devices
Forescout eyeInspect	Alerts from Forescout eyeInspect are supported by Managed Defense	**FORESCOUT_EYEINSPECT (https://docs.cloud.google.com/chronicle/docs/ingestion/parser-list/forescout-eyeinspect-changelog)**	N/A
Nozomi Guardian	INCIDENT and SIGN alerts are supported by Managed Defense.	**NOZOMI_GUARDIAN (https://docs.cloud.google.com/chronicle/docs/ingestion/parser-list/nozomi-guardian-changelog)**	• All alerts are forwarded to the SOC based on Severity

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Palo Alto Networks

Product	License requirement	Description	Required SecOps Parsers	Managed Defense Supported Alert Types
Next Generation Firewall	N/A	Palo Alto Next Generation Firewalls (PAN NGFW) threats that are not blocked are supported by Managed Defense. Managed Defense can integrate with a WildFire Free or Advanced license for additional detection of malware. Data Filtering logs can optionally provide additional context for investigations.	Alerts: **PAN_FIREWALL (https://docs.cloud.google.com/chronicle/docs/ingestion/parser-list/pan-firewall-changelog)**	• Threats • WildFire • Data Filtering**

SentinelOne

Product	License requirement	Description	Required SecOps Parsers	Managed Defense Supported Alert Types
Singularity	Cloud Funnel license	SentinelOne Singularity Complete is supported by Managed Defense. A Cloud Funnel license is required for Managed Defense service delivery.	Alerts: **SENTINELONE_ALERT (https://docs.cloud.google.com/chronicle/docs/ingestion/parser-list/sentinelone-alert-changelog)** Telemetry: **SENTINELONE_CF (https://docs.cloud.google.com/chronicle/docs/ingestion/parser-list/sentinelone-cf-changelog)**	• Threats

Trellix

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Product	Minimum Version	Maximum Version	Description	Required SecOps Parsers	Managed Defense Supported Alert Types
Email Security (EX)*	9.1	10.0	Trellix Email Security Server Edition on-premises.	N/A	• Trellix Alert Type: ◦ Malware Object
Email Security Cloud	N/A	N/A	Trellix Email Security Cloud Edition is software as a service application.	N/A	
Endpoint Security (HX)*	5.3	10.0	Trellix Endpoint Security can be deployed in on-premises, cloud, or virtual appliance configuration for Managed Defense service delivery.	N/A	• Real-Time IOCs

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Product	Minimum Version	Maximum Version	Description	Required SecOps Parsers	Managed Defense Supported Alert Types

Helix Security Platform	N/A	N/A	Trellix Helix Enterprise can be connected to Managed Defense service delivery by granting Managed Defense access to the instance through Trellix IAM.	N/A	• Helix alerts with the following tags:
					  ◦ MD-ACTION
					  ◦ MD-INFO
					• Helix alerts with the following tags are also covered for MD for OT customers:
					  ◦ ICS-ACTION
					  ◦ ICS-INFO

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Product	Minimum Version	Maximum Version	Description	Required SecOps Parsers	Managed Defense Supported Alert Types
Network Security (NX)*	9.1	10.0	Trellix Network Security can be deployed in on-premises, cloud, or virtual appliance configuration in either inline or passive modes for Managed Defense service delivery.	N/A	• Trellix Alert Types: ◦ Domain Match ◦ Malware Callback ◦ Malware Object ◦ Web Infection ◦ Infection Match • Suricata Alerts (with optional Mandiant NTAP feature enabled)

* *Managed Defense follows the* ***End of Life Policy for Trellix Supported Technology*** *(https://www.trellix.com/assets/legal/support-policy-product-support-eol.pdf). In general, this End of Life Policy typically means that the most recent two software revisions for each product are supported.*

** *Alerts are leveraged for hunting and/or for additional context and do not adhere to Managed Defense Service Level Objectives noted in the* ***Managed Defense Service Description*** *(https://docs.mandiant.com/home/md-service-description).*

Security Technology Monitors

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

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.

Onboarding Responsibilities

The table defines the responsibilities of the Managed Defense team and customers during onboarding:

Onboarding Phase	Managed Defense	Customer
Initialization		
Conduct Managed Defense Kick-Off Meeting	✔	
Provide user information for Mandiant Advantage Portal account creation		✔
Create new Mandiant Advantage Portal Users	✔	

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Onboarding Phase	Managed Defense	Customer
Provision Managed Defense Portal API Clients (Optional)	✔	
Integrate with Managed Defense Portal API (Optional)		✔
Provide Managed Defense Service Documentation	✔	
Technology Enablement		
Deploy Supported Technologies for Managed Defense		✔
(Google Security Operations Only) Grant Managed Defense analysts access to Google Security Operations		✔
(Google Security Operations Only) Grant Managed Defense access to monitor data ingestion details by linking Google Cloud Project to Managed Defense		✔
(Microsoft Defender for Endpoint Only) Configure Azure Storage to receive data from Microsoft Defender for Endpoint (Customer is responsible for costs associated with the Azure Storage and data transfer)		✔
(Microsoft Defender for Endpoint Only) Configure Azure API permissions for Managed Defense as an MSSP for Microsoft Defender for Endpoint		✔
(SentinelOne Singularity Only) Provision and maintain Amazon S3 or Google Cloud Storage to export endpoint telemetry with Cloud Funnel		✔
(SentinelOne Singularity Only) Create API tokens for Managed Defense at Global or Account level		✔
(CrowdStrike Falcon Only) Create CrowdStrike Support ticket to make Managed Defense a parent of your CrowdStrike deployment		✔
(CrowdStrike Falcon Only) Create API key for Managed Defense access to Falcon tenant(s)		✔
Configure Supported Technologies for Managed Defense		✔
Provision Supported Technology for Managed Defense	✔	
Test Supported Technology Alerts	✔	✔
Endpoint Agents		
Install endpoint agent software on supported operating systems		✔

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Onboarding Phase	Managed Defense	Customer
Configure Endpoint Groups and Services		✔
Perform Endpoint Services Testing	✔	✔
Authorize Managed Defense to Contain Endpoints (Optional)		✔
Finalization		
Confirm Onboarding Complete	✔	✔

Connectivity

This section summarizes customer roles and responsibilities for connectivity of supported technology.

- Provide information and remote access to enable the deployment of Managed Defense Supported Technology.
- Provide and maintain network connectivity between Managed Defense and Managed Defense Supported Technologies.
- Permit Managed Defense to access supported technologies to retrieve Security Alerts and Events.
- Address issues pertaining to lack of visibility within the monitored environment, such as loss of endpoint agent visibility, loss of network visibility, or unknown system traffic.

Mandiant recommends implementing strong network segmentation on security technologies connected to Managed Defense. Outbound connectivity from security technologies should be restricted to the minimum ports and protocols necessary.

Maintenance

This section summarizes customer roles and responsibilities for the maintenance of supported technology.

Managed Defense support for security technologies is currently categorized by the partnership agreements in place with various security vendors. The partnership agreements facilitate deep collaboration between the Managed Defense team and the vendor that can allow for deeper response and orchestration actions to be taken on behalf of customers. For example, host containment and file acquisition. These partnership agreements also clarify which alert, event, and log sources will be fully supported by Managed Defense.

- Customers must have an active software license and support contract for all Managed Defense Supported Technologies.
- Customers are responsible for ongoing maintenance, deployment, and management of Supported Technologies.
- Customers shall provide Managed Defense Consultant with at least 24 hours notice for planned network maintenance that may affect communications of Supported Technology with Managed Defense.
- Customers must identify and notify Managed Defense when changes within the environment may impact Managed Defense visibility and coverage. Managed Defense has no obligation to provide services for network segments and endpoints that are not visible to Managed Defense Supported Technology.
- Mandiant does not maintain backups of any supported security technologies connected to the Managed Defense service. Customers are responsible for all backups of all supported technologies connected to the Managed Defense service.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Mandiant

Customers are responsible for the rotation of credentials in authentication tokens provided to Managed Defense and must notify their Managed Defense Consultant (MDC) before changing any credentials. Failure to inform Managed Defense of new credentials may lead to a service delivery outage.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.