Google Cloud
Security

Datasheet

Mandiant Managed Defense

Service Highlights:

- Human-led hunting performed by Mandiant frontline experts
- Unparalleled visibility of threat actor activity and tactics through Google Threat Intelligence
- Expert alert triage, investigation, and prioritized escalation with curated recommendations.
- Seamless monitoring for telemetry integrated into Google SecOps and technology partner products

24x7 threat detection, investigation, and response from Mandiant experts for your security stack

Mandiant Managed Defense delivers expert-led threat detection, hunting, investigation, and response capabilities on top of the AI-infused Google Security Operations (SecOps) platform, leveraging applied threat intelligence, helping to ensure that your organization is ready to defend against adversaries.

The Managed Defense service is most effective when a broad set of security telemetry sources are integrated into Google SecOps. Customers are empowered to use the available default Google SecOps parsers to streamline alert and event ingestion.

Customers can also benefit from using Managed Defense Technology Partner products. 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, file acquisition, and closing out alerts.

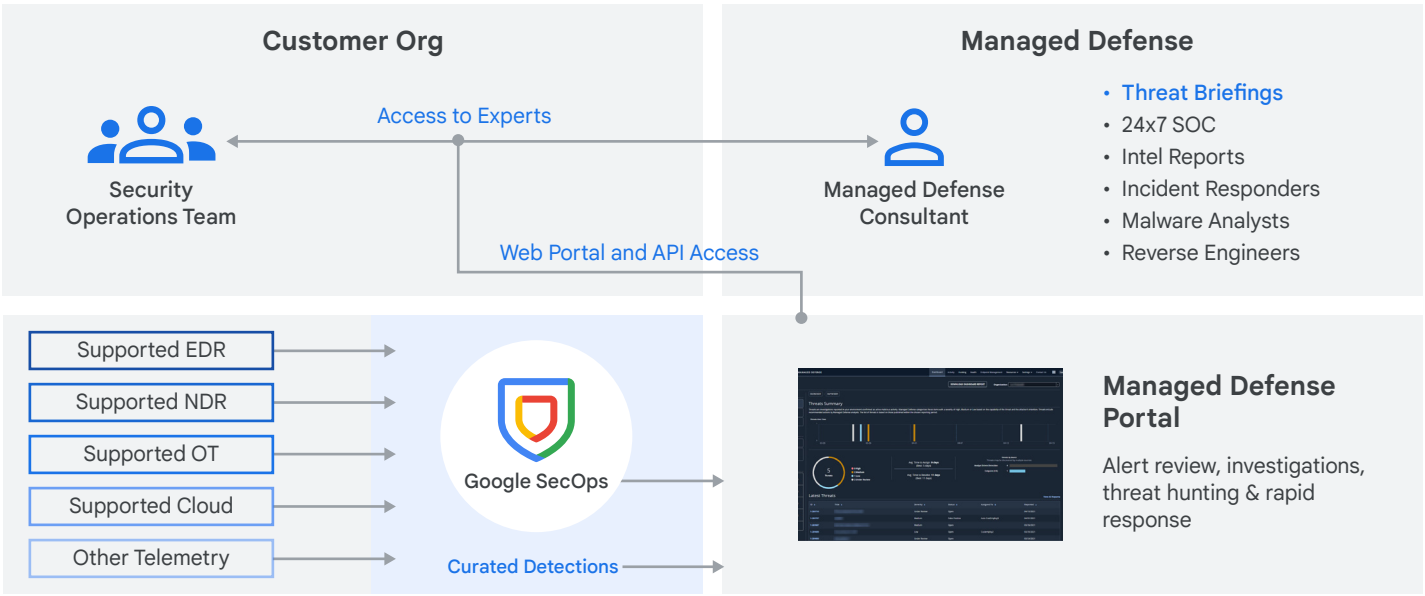

FIGURE 1: Sample architecture of Managed Defense for Google Security Operations

Managed Defense support for curated detections

Through the curated detections available within Google Security Operations, Managed Defense can review an expanded set of log sources while performing triage and initiating investigations. As customers integrate new telemetry sources into Google Security Operations, the log data will be parsed into the Security Operations Unified Data Model and curated detection rules will be applied. Alerts that are generated by these rules become available to Managed Defense for triage investigation.

Curated detections coverage is dependent on a customer's Google SecOps license. Support for curated detections is currently in Preview*.

About curated detections:

The Google Threat Intelligence (GCTI) team provides and manages a set of YARA-L rules to help customers identify threats to their enterprise. These predefined rules are called curated detections. Curated detections can be enabled within a customer-owned Google Security Operations instance.

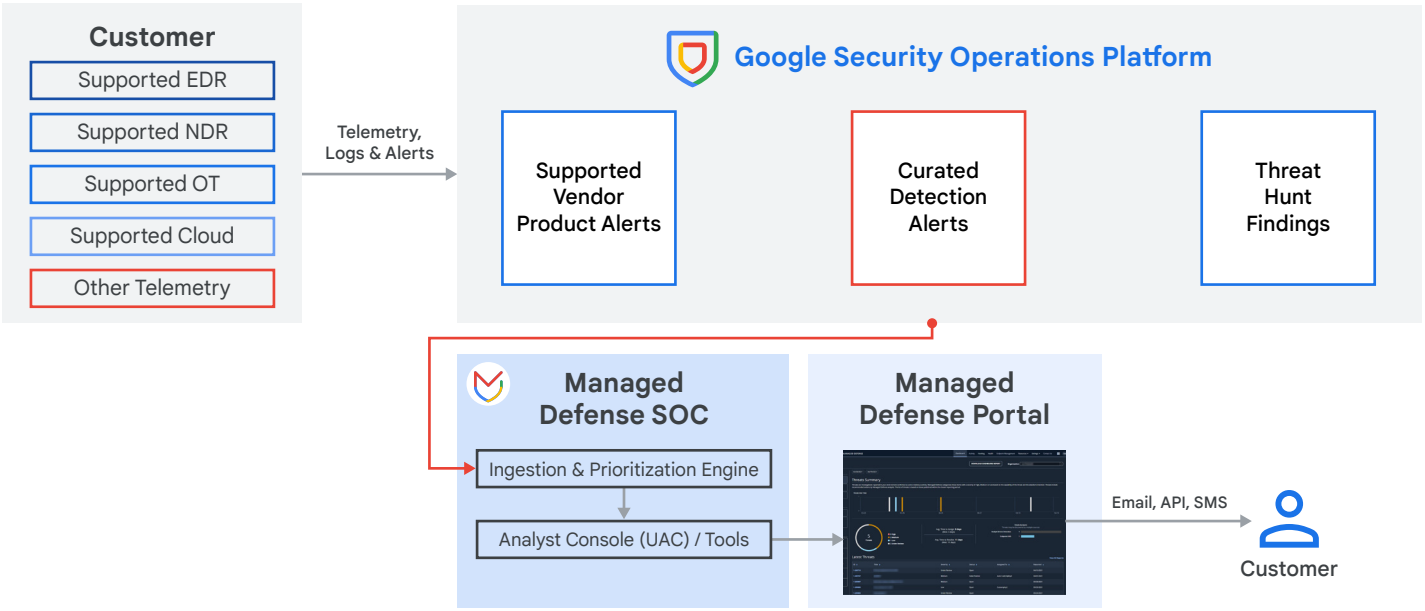

FIGURE 2: The Managed Defense SOC ingests, triages, investigates, and responds to alerts from curated detections, supported technology vendors, and threat hunting findings, providing customers with detailed Investigation reports via the Managed Defense Portal.

* Review the Google Cloud product launch stages to learn more about Preview programs.

Explore Managed Defense for Google SecOps supported technology partners

Managed Defense supports threat hunting, alert triage, investigation, and rapid response capabilities for your technology stack. The integrations with supported technology partners enables Managed Defense to take deeper remediation actions, for example host containment and automated file acquisition. Explore the supported technology partners.

Category	Vendor	Product Supported	Product License Requirements	Required SecOps Parsers
Endpoint detection and response (EDR)	Crowdstrike	Falcon Insight XDR	Falcon Data Replicator	Alerts: CS_DETECTS Telemetry: CS_EDR
	SentinelOne	Singularity XDR	Cloud Funnel	Alerts: SENTINELONE_ALERT Telemetry: SENTINELONE_CF
	Microsoft	Defender for Endpoint	Microsoft Defender for Endpoint Plan 2Azure Blob Storage	Alerts: MICROSOFT_GRAPH_ALERT Telemetry: MICROSOFT_DEFENDER_ENDPOINT
Identity	Microsoft	Defender for Identity	One of the following: Endpoint Plan 2 Defender for Business Defender for Identity license	Alerts: MICROSOFT_GRAPH_ALERT
Network detection and response (NDR) and Firewall	Corelight	Open NDR	N/A	Alerts and Telemetry: CORELIGHT
	Palo Alto Networks	Next-Generation Firewall	N/A	PAN_NGFW

Explore Managed Defense Standard supported technology partners

Managed Defense supports threat hunting, alert triage, investigation, and rapid response capabilities for your technology stack. The integrations with supported technology partners enables Managed Defense to take deeper remediation actions, for example host containment and automated file acquisition. Explore the supported technology partners.

Category	Vendor	Product Supported	Product License Requirements	Required SecOps Parsers
Endpoint detection and response (EDR)	Crowdstrike	Falcon Insight XDR	Falcon Data Replicator	Alerts: CS_DETECTS Telemetry: CS_EDR
	SentinelOne	Singularity XDR	Cloud Funnel License	Alerts: SENTINELONE_ALERT Telemetry: SENTINELONE_CF
	Microsoft	Defender for Endpoint	One of the following: Endpoint Plan 2 Defender for Business Defender for Identity license	Alerts: MICROSOFT_GRAPH_ALERT Telemetry: MICROSOFT_DEFENDER_ENDPOINT
	Trellix	Endpoint Security Versions (HX) 9.1-10.0	N/A	N/A
Identity	Microsoft	Defender for Identity	One of the following: Endpoint Plan 2 Defender for Business Defender for Identity license	Alerts: MICROSOFT_GRAPH_ALERT
Network detection and response (NDR) and Firewall	Corelight	Open NDR	N/A	Alerts and Telemetry: CORELIGHT
	Palo Alto Networks	Next-Generation Firewall	N/A	N/A
	Trellix	Network Security (NX) Version 9.1-10.0 Network Forensic Packet Capture (PX) Version 6.1-6.2	N/A	N/A
Email	Trellix	Email Security (EX)	N/A	N/A
Operational Technology	Nozomi Networks	N/A	Trellix Helix	N/A
	Forescout	N/A		
	Claroty	Continuous Threat Detection		
	Armis	Centrix™		

Make Google part of your security team.

Learn more about Mandiant Managed Defense.

Google Cloud

For more information visit cloud.google.com