Secure Malware Analytics

(formerly Threat Grid)

Cisco Partner

https://cs.co/1page

Secure Malware Analytics is the malware analysis and malware threat intelligence engine behind all products across the Cisco Security Architecture. The system delivers enhanced, in-depth, advanced malware analysis and context-rich intelligence to help better understand and fight malware within your environments.

Benefits:

Make Decisions Faster and more Effectively:

- Rapidly analyze files and suspicious behavior across your environment.
- Get context-rich malware analytics and threat intelligence with insight into what a file is doing and quickly respond to threats.

Achieve Visibility and Control:

- When combined with Secure Endpoint and/or XDR, Secure Malware Analytics analyzes unknown files using static and dynamic analysis techniques.
- Pre- and post-execution of the master boot record, including physical and virtual hosts, OSs, applications, protocols, users, content, and network behavior.
- Malware Defense continuously monitors files and traffic even after initial scan.
- Retrospective alerts inform you of any change in disposition, including who on your network was infected and when.
- Dashboards show exactly where the threat has been, what it did, and the root causes so you can quickly contain and remediate.

Access Behavioral Indicators:

- Secure Malware Analytics appliances analyze more than 2200 highly accurate and actionable advanced behavioral indicators.
- This solution also produces comprehensive indicators through advanced static and dynamic analysis on thousands of malware families and malicious behaviors.

Solutions:

Cisco Secure Malware Analytics Cloud: Cloud-based (SaaS) threat intelligence portal which offers the full suite of features along with a robust API for comprehensive integrations.

Cisco Secure Advanced File Analysis: Sample-packs for automated submissions from integrated products, both Cisco the third party.

Cisco Secure Malware Analytics Appliance: On-premise solution for threat intelligence and advanced file analysis.

Features:

Behavioral Indicators: 2240+ indicators form the backbone of Malware Analytics. Developed by Cisco's team of cybersecurity experts.

Outside-Looking-In Approach: Architecturally designed to neutralize modern malware's evasion techniques, ensuring malware detonates to its full extent to help users better understand intentions and behaviors.

Remote Network Exits: Use selectable network exits to make outgoing traffic appear to be originating from different geographies in order to identify geographically-dependent malware.

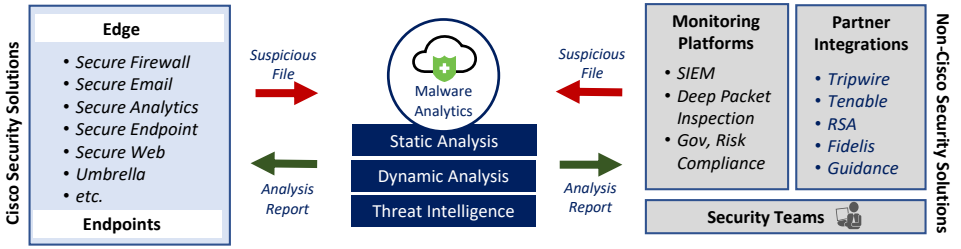
Network Simulation: Catch malware that is attempting to communicate with decommissioned internet resources by simulating network activity.

Glovebox: Interact with suspicious files in real-time in a safe environment. Control interactions to replicate scenarios that may trigger advanced malware.

Automated Playbooks: Simulate user interaction such as cursor movement and interaction with dialog boxes to ensure that malware detonates fully, leaving behind a complete set of threat intelligence data.

Rich Analysis Data: Detailed analysis of sample behaviors including sample metadata, DNS traffic, TCP/IP streams, processes, artifacts and more.

MITRE ATT&CK: Behavioral indicators written in plain language and classified according to the MITRE ATT&CK framework to understand the intentions of malware and develop a picture of malware campaigns.



Resources:

SalesConnect
At-a-Glance
Ordering Guide
Data Sheet
Secure Malware Analytics for Splunk
Secure Malware Analytics Console Integrations
Case Studies
PoV Guide
Public page

Example SKU: ***TGA-LIC-K9***