Cisco Threat Grid

Threat Grid: Advanced File Analysis Packs (Integrated) vs. Cloud Comparison

Threat Grid Advanced File Analysis Packs (Integrated)

Product Description

Cisco Threat Grid Advanced File Analysis Packs are additional sample-per-day capacity licenses available for customers who have purchased a Cisco security product along with an AMP Security license. Advanced File Analysis Packs are intended for customers who want to increase the number of samples they are allowed to submit, via their integrated device, to Threat Grid for analysis within a 24-hour period.

Threat Grid is included as an integrated component of the AMP Security license and available to numerous Cisco Security Products. Threat Grid provides a graduated threat score and determines if a file might be malicious or benign through various static and dynamic analysis engines - commonly referred to as sandboxing.

When integrated with a Cisco security product, such as Email Security Appliance, Firewalls (NGFW), Intrusion Prevention (NGIPS), and AMP for Endpoints amongst others; it allows the integrated product to determine if a file is malicious, what its threat score is, and enhance its ability to detect a wider range of known and unknown malware. Threat Grid delivers a more effective solution to protect their organizations infrastructure, services and intellectual property.

Integrations

- AMP for Networks
- AMP for Endpoints
- AMP Private Cloud
- Email Security Appliance (ESA)
- Cloud Email Security (CES)
- Web Security Appliance (WSA)
- Next Gen Intrusion Prevention System (NGIPS)
- Next Gen Firewall
- Meraki MX UTM

Threat Grid Cloud Subscription

Product Description

A full subscription to Threat Grid provides the most comprehensive analysis of advanced malware today. It is the first unified malware analysis and threat intelligence solution that securely crowd-sources malware samples from a closed community, providing a global view of malware samples, behaviors, and their associated families.

Threat Grid provides rich reporting, the ability to pivot and drill down on data elements, and interact with malware using Glovebox. An easy to use REST API automates sample submissions and threat intelligence consumption with 3rd parties to have a common analysis platform, and gain a holistic view of all malware samples.

Use Cases

- High Privacy Requirements: Threat Grid appliances provide on premises malware analysis, ensuring customers adhere to corporate and compliance mandates.
- Security Operations: Threat Grid provides an intuitive web portal for junior analysts to quickly understand the scope of a threat and respond to incidents– all driven by high-fidelity analyzed content. The portal also provides a detailed analysis and threat score for rapid prioritization of threats, as well as user interaction with the malware using Glove Box.
- Threat Intelligence: With access to a robust API to integrate sample submission, Threat Grid enriches security event and threat content, allowing customers to automate and enhance the capabilities of their existing IT security infrastructure and procedures.
- Data enrichment: Threat Grid leverages a robust big data store of analyzed malware content that is rich in historical context and fully correlated, enabling the quick development of actionable defense and IR remediation plans.
- Drill Down: Threat Grid's depth of malware analysis and data pivoting capabilities provide reverse engineers and incident responders the context, depth of data, and malware analysis they require to be effective.

Threat Grid Cloud subscription provides threat intelligence feeds, either pre-packaged or customized for a customers unique security needs, industry, and threat environment.

Feature / Capability	Integrated Threat Grid	Threat Grid Cloud Subscription
Sample Information / Metadata	X	X
Behavioral Indicators	X	X
Simple search of SHA256, IP Address, and name	X	X
Threat Score	X	X
Network Activity report	X	X
Download original Sample, PCAP Report		X
View / Download Video of sample execution		X
Process report		X
Artifacts report		X
File Activity report		X
Download artifacts		X
Pivot on data elements in report		X
Interact with malware samples in Glovebox		X
Download Report JSON		X
Malware Process Graph		X
Adjust sample analysis run time		X
Advanced search (samples, artifacts, registry, URLs, etc)		X
API integration for automation of sample uploads		X
User selectable emulation environment		X
Threat Intelligence Feeds via API		X
Default Sample Submissions per Day	200*	Scalable*
Single view of all sample submissions		X

*Scale sample limits as needed with the purchase of additional Advanced File Analysis Packs

Increase your daily sample limits with additional Advanced File Analysis Packs whether you have Threat Grid Integrated or a Threat Grid Cloud subscription.

Part #	Description
L-TGSP-S1-LIC-K9=	Cisco Threat Grid File Pk. 200 Daily Submissions. 1,3 or 5 Years
L-TGSP-S2-LIC-K9=	Cisco Threat Grid File Pk. 500 Daily Submissions. 1,3 or 5 Years
L-TGSP-S3-LIC-K9=	Cisco Threat Grid File Pk. 1500 Daily Submissions. 1,3 or 5 Years
L-TGSP-S4-LIC-K9=	Cisco Threat Grid File Pk. 5000 Daily Submissions. 1,3 or 5 Years