Cisco Threat Grid – Appliances

Product Overview

A Threat Grid appliance delivers on-premises advanced malware analysis with deep threat analytics and content. Organizations with compliance and policy restrictions can analyze malware locally by submitting samples to the appliance.

With a Threat Grid appliance you can analyze all samples using proprietary and highly secure static and dynamic analysis techniques. It correlates the results based on behavioral indicators derived from the historical and global context of hundreds of millions of other analyzed malware artifacts to provide a comprehensive view of malware attacks, campaigns, and their distribution. This ability helps you effectively defend against both targeted attacks and threats from advanced malware. Threat Grid's detailed reports, including the identification of important behavioral indicators and the assignment of threat scores, let you quickly prioritize and recover from advanced attacks.

Cisco® Threat Grid appliances combine two of the leading malware protection solutions: **unified malware analysis** and **context-rich intelligence**.

They empower security professionals to proactively defend against and quickly recover from cyberattacks.

© 2019 Cisco and/or its affiliates. All rights reserved.

Features and Benefits

Threat Grid appliance features and benefits are shown in Table 1.

Table 1. Features and Benefits

Feature	Benefit
Glovebox	Glovebox is a user interaction tool that provides a safe environment to dissect malware without the risk of infecting your network. Built into the appliance, analysts are able to interact with the sample while it is being analyzed including opening applications, clicking through dialogue boxes, and even reboot the virtual machine if needed.
On-premises appliance	Provides safe and highly secure on-premises static and dynamic malware analysis to maintain the confidentiality of data. Easily integrates with existing security infrastructure. Provides safe on-premises storage of malware analysis results
Advanced analytics	Delivers comprehensive security insight into malware behavior and direct links to the sample source and associated behavior in Threat Grid's extensive database. Provides easy access to all information and analysis results for further investigation.
Advanced behavioral indicators	Analyzes more than 1000 highly accurate and actionable advanced behavioral indicators with few false positives. Produces comprehensive indicators through advanced static and dynamic analysis encompassing numerous malware families and malicious behaviors. Delivers the broadest context around threats and helps you make quick and confident decisions.
Threat score	Automatically derives threat scores from proprietary analysis and algorithms that consider the confidence and severity of observed actions, historical data, frequency, and clustering indicators and samples. Prioritizes threats with confidence to reflect each sample's level of malicious behavior. Improves the prioritization of threats, which enhances the efficiency and accuracy of malware analysts, incident responders, security engineering teams, and products that consume Threat Grid's feeds.
Remote updates	Has the capability to be manually updated to help ensure an up-to-date knowledge base while complying with corporate or regulatory policies to keep all information within logical boundaries.
API for integration	Simplifies fast operationalization of threat intelligence with existing security and network infrastructure. Makes integration fast and easy with Threat Grid's representational state transfer (REST) API. Provides integration guides for a number of third-party products, including gateways, proxies, and security information and event management (SIEM) platforms.

Licensing

Threat Grid appliances require an active content subscription license to be deployed. Licenses are now customizable through the SBP platform to include any daily sample capacity between 500 and 10,000 samples per day. License PIDs are listed in the Ordering Information Section.

© 2019 Cisco and/or its affiliates. All rights reserved.

Comprehensive On-Premises Malware Analysis

For organizations with compliance and policy restrictions on submitting malware samples to the cloud, Threat Grid provides a dedicated appliance for local malware analysis backed by the full power of Threat Grid's federated threat intelligence. Threat Grid provides a global view of malware attacks, campaigns, and their distribution. It analyzes millions of samples monthly and distills terabytes of malware analysis into rich, actionable intelligence.

Security teams can quickly correlate a single malware sample's observed activity and characteristics against millions of other samples to fully understand its behaviors in a historical and global context to effectively defend against both targeted attacks and the broader threats from advanced malware. Threat Grid's detailed reports, identifying key behavioral indicators along with a threat score, help enable quick prioritization and recovery from advanced attacks with accuracy and speed. Analysis features include:

- Dynamic and static analysis engines that provide a full understanding of malware behavior
- Detailed analysis reports of all malware sample activities, including network traffic
- User-interface workflows designed for security operations center (SOC) analysts, malware analysts, and forensic investigators

Product Specifications

Product specifications are shown in Table 2.

Table 2. Product Specifications

Feature	Cisco Threat Grid M5
Form Factor	1 Rack Unit (1RU)
Dimensions	1.7 x 16.9 x 28 inches (H x W x D)
Network Interface	2x1 GB Copper + SFP+
CIMC Interface	1 GB Copper
Power options	770W AC

Environmental Specifications

Environmental specifications are shown in Table 3.

Table 3. Environmental Specifications

	Cisco Threat Grid M5
Temperature: Operating	10°C to 35°C (50°F to 95°F) (no direct sunlight, maximum allowable operating temperature derated 1°C/300 m (1°F/547 ft) above 950 m (3117 ft)
Temperature: Non-Operating	-40°C to 65°C (-40°F to 149°F) Maximum rate of change (operating and non-operating) 20°C/hr (36°F/hr)
Humidity: Operating	8% to 90% and 24°C (75°F) maximum dew-point temperature, non-condensing environment
Humidity: Non-Operating	5% to 95% and 33°C (91°F) maximum dew-point temperature, non-condensing environment
Altitude: Operating	0 to 10,000 ft (0 to 3000m); maximum ambient temperature decreases by 1°C per 300m)
Altitude: Operating	0 m to 3050 m (10,000 ft)

© 2019 Cisco and/or its affiliates. All rights reserved.

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

Next Steps:

For more information about Cisco Threat Grid uni ed malware analysis and threat analytics, visit: cisco.com/go/amptg.

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

1944846 10/19

Ordering Information

To place an order for a Cisco Threat Grid appliance, visit the Cisco ordering homepage. Table 4 provides ordering information.

Table 4. Ordering Information

Part Number	Product Description
TG-M5-BUN	**Cisco Threat Grid M5 Appliance and License Bundle**
TG-M5-K9	Cisco Threat Grid M5 Model Hardware
TGA-LIC-SUB	Cisco Threat Grid License for TG Appliance

Cisco and Partner Services

Services from Cisco and Cisco Certified Partners can help you plan and implement your integration with Threat Grid's premium threat feeds and the REST API. Planning and design services align your existing infrastructure, Threat Grid premium feed formats, and operational processes to make the best use of advanced threat feeds.