Cisco Threat Grid Cloud

Product Overview

Cisco Threat Grid crowd-sources malware from a closed community and analyzes all samples using proprietary, highly secure techniques that include static and dynamic (sandboxing) analysis. It correlates the results with hundreds of millions of other analyzed malware artifacts to provide a global view of malware attacks, campaigns, and their distribution. Security teams can quickly correlate a single samples of observed activity and characteristics against millions of other samples to fully understand its behaviors in a historical and global context. This ability helps analysts effectively defend against both targeted attacks and the broader 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 combines two of the leading malware protection solutions: unified malware analysis and context-rich intelligence. It empowers security professionals to proactively defend against and quickly recover from cyber attacks.

Features and Benefits

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

Table 1. Features and Benefits

Feature	Benefit
Advanced analytics	• Delivers comprehensive security insight into malware behavior • Provides direct links to the sample source and associated behavior in Threat Grid's extensive database • 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
Glovebox	• Provides a safe environment to dissect malware without the risk of infecting your network • Allows analysts to open applications and replicate a workflow process, see how the malware behaves, and even reboot the virtual machine
Threat scores	• Improves 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 • 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
API for integration	• Simplifies fast operationalization of threat intelligence with existing security and network infrastructure • Makes integration fast and easy with Cisco 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
Standard feed formats	• Provides easy-to-integrate normalized feeds in a number of standardized formats - including JavaScript Object Notation (JSON), Structured Threat Information Expression (STIX), and comma-separated values (CSV) - and as Snort rules • Customized feed formats available for particular security products • Easily and consistently tracks trends over time and produces actionable reports

Advanced Intelligence, Analysis, and Reporting

Threat Grid's cloud-based service provides the most robust, context-rich threat intelligence available. Threat Grid securely analyzes millions of files and correlates them against hundreds of millions of other analyzed malware artifacts. This gives you both a global and a historical view of malware. The ability to pivot and drill down on each data element allows analysts to dive deeper during analysis, identifying malicious files masquerading as benign. Robust search, correlation, and reporting capabilities provide detailed information on malware artifacts, indicators, and samples. Detailed analysis reports include all malware sample activities, including those involving network traffic and malware artifacts.

Table 2. Supporting Platforms and Operating Systems

Product Family	Platfor Supported
Threat Grid portal	• Windows 7 64 bit • Windows 7 64 bit (Korean) • Windows 7 64 bit (Japanese) • Windows 10
Threat Grid dynamic analysis	Supported file types for analysis: • .BAT - Batch files • .CHM - Compiled HTML Help - Microsoft Compiled HTML Help • .DLL - See: PE32 and PE32+ • .ISO - ISO image files • .HTA - HTML Application • .HWP, .HWT, .HWPX - Available on the win7-x64-kr VM only (specific to Hancom Office) • .JAR - Java Archives • .JS - JavaScript • .JSE - Encoded JavaScript • .JTD, .JTT, .JTDC, .JTTC: Available on the win7-x64-jp VM only (specific to Ichitaro) • .LNK - Windows shortcut files • .MSI - Microsoft Installer files • MHTML - Mime HTML Files • Microsoft Office Documents, including .DOC, .DOCX, .RTF, .XLS, .XLSX, .PPT, .PPTX • PDF - Portable Document Format (detailed static forensics, including Javascript resources) • PE32 Files and Executables (.EXE) • Libraries (.DLL) • .PE32+ files - Available on the win7-x64 VM only • Executable (.EXE) • Libraries (.DLL) • .PS1 - Powershell • .SWF - Flash Files • URLs (As Internet Shortcut file, or submit the URL directly. Detailed static forensics or Javascript resources.) • .VBE - Encoded Visual Basic • .VBN - Virus Bin - See .ZIP • .VBS - Visual Basic Script • .WSF - Windows Script File • .XML and XML Based Office Document Types (.DOCX, .XLSX, .PPTX) • XML - Extensible Markup Language (.XML), An XML that is from Office will be opened in the corresponding program • (Office 2003). All other XML will be opened in IE • ZIP - Archive and Quarantine Formats, as well as .BZ2, .GZip, .XZ • ZIP (.ZIP) as a container, no nesting of archives, no password or 'infected'. We do not support nested ZIP archives due to known unpacking attacks, such as zip bombs and quines, including 42.zip, which is a well-known attack against AV services • Quarantine file types including .SEP, .VBN

Comprehensive Premium Feed Content

Cisco Threat Grid crowd-sources malware from a closed partner and customer community, providing a global view of malware attacks, campaigns, and their distribution. It analyzes millions of samples monthly and distills terabytes of rich, actionable content into clearly categorized and easily consumable threat-intelligence feeds. This helps you effectively defend against the broadest variety of threats and reduces the damage from attacks. Threat Grid provides several categories of prepackaged premium feeds that address numerous threat types, including:

- Various Trojans, including remote-access Trojans (RATs) and malware families known to spread additional malware and exhibit specific behaviors such as downloading executables.
- Malware that attempts to establish outbound network communications and exhibits anomalous network activity. Examples include PDF files and Microsoft Office documents that initiate malicious network activity, malware that communicates over various protocols and channels, the use of nonstandard or mismatched network protocols, and communications with known sinkholes. Threat Grid uses specific behavioral indicators to generate its feeds. These include network indicators that are used to help determine outbound communications.
- Malicious activities on the host, including modifications to the Windows host files and dynamic-link libraries (DLLs), and hijacking techniques to install malicious files and maintain persistence on the host without registry modifications.
- Malware exhibiting high threat scores as determined by Threat Grid.Licensing

Table 2 shows the platforms supported by Cisco Threat Grid.

Licensing

Threat Grid capabilities include deep analytics and results, including process mapping and registry changes, network connections, and videos of malware execution in the environment, if applicable. You can access batch feeds of analyzed intelligence data, and you can create custom feeds from the broader set of Threat Grid data. Threat Grid has been integrated into the Cisco Advanced Malware Protection (AMP) license to provide a limited number of samples to be analyzed per day. Customers easily can add more daily sample submissions through Advanced File Analysis packs.

Threat Grid Cloud subscribers may submit samples either directly through the cloud portal or automated through the Threat Grid API. All cloud service elements are licensed in terms of 1, 3, or 5 year content subscriptions. The standard Threat Grid Cloud subscription includes 3 user accounts, while more user accounts can be added a la carte in groups of 1, 5 or 10 users. For subscribers who need additional daily submission capacity, Advanced File Analysis packs can be purchased in packs of 200, 500, 1500 or 5000 samples/day.

Table 3 shows the number of analyst accounts created with the ability to log in to the Threat Grid portal for investigation and analysis and the corresponding number of files that can be submitted manually or through the API to the Threat Grid cloud for static and dynamic analysis.

Table 3. Analyst Accounts

Threat Grid Cloud Base Subscription	
L-TG-CL-K9=	Threat Grid Cloud Access, 3 User Accounts
Threat Grid Cloud User Accounts	
L-TG-CL-U1-K9=	1 Additional Cisco Threat Grid Cloud Account
L-TG-CL-U5-K9=	5 Additional Cisco Threat Grid Cloud Account
L-TG-CL-U10-K9=	10 Additional Cisco Threat Grid Cloud Account
Threat Grid Advanced File Analysis Packs	
L-TGSP-S1-LIC-K9=	Threat Grid Advanced File Analysis – 200 Daily Samples
L-TGSP-S2-LIC-K9=	Threat Grid Advanced File Analysis – 500 Daily Samples
L-TGSP-S3-LIC-K9=	Threat Grid Advanced File Analysis – 1500 Daily Samples
L-TGSP-S4-LIC-K9=	Threat Grid Advanced File Analysis – 5000 Daily Samples

Cisco and Partner Services

Services from Cisco and Cisco Certified Partners are available to help you plan and implement integration with Threat Grid's premium threat feeds and representational state transfer (REST) API. Planning and design services align your existing infrastructure, Threat Grid premium feed formats, and operational processes, so you can make the best use of advanced threat feeds. Meet our partners.

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 unified malware analysis and threat analytics, visit cisco.com/go/amptg.