Cisco Threat Grid

Unified Malware Analysis and Threat Intelligence

Companies are finding themselves under a multitude of common and advanced malware attacks. As a security professional or IT manager, you probably struggle to find time to investigate every attack, let alone prioritize the most dangerous ones that should be addressed first.

Struggle no longer. With Cisco Threat Grid, you can perform malware analysis and ingest context-rich threat intelligence on site in a standalone appliance, with a cloud-based subscription, or as an integrated part of your existing Cisco security technologies. Or you can integrate the solution with your existing network and security infrastructure, including mail gateways; security information and event management (SIEM); and governance, risk management, and compliance (GRC) platforms. Drawing on this large static and dynamic malware-analysis solution, you get timely, context-rich, actionable intelligence to identify malware and mitigate its damage.

Cisco Threat Grid is deployed in multiple locations around the world, where it has helped security operations center and incident response teams take more effective and consistent action (Figure 1).

Benefits

- **Transparent integration** with existing security solutions for better detection
- **Greater effectiveness** of security and response teams
- **Faster investigation and response** to security incidents
- **Seamless** malware analysis from your existing Cisco security tools

Two Crucial Weapons to Fight Malware: Analysis and Threat Intelligence

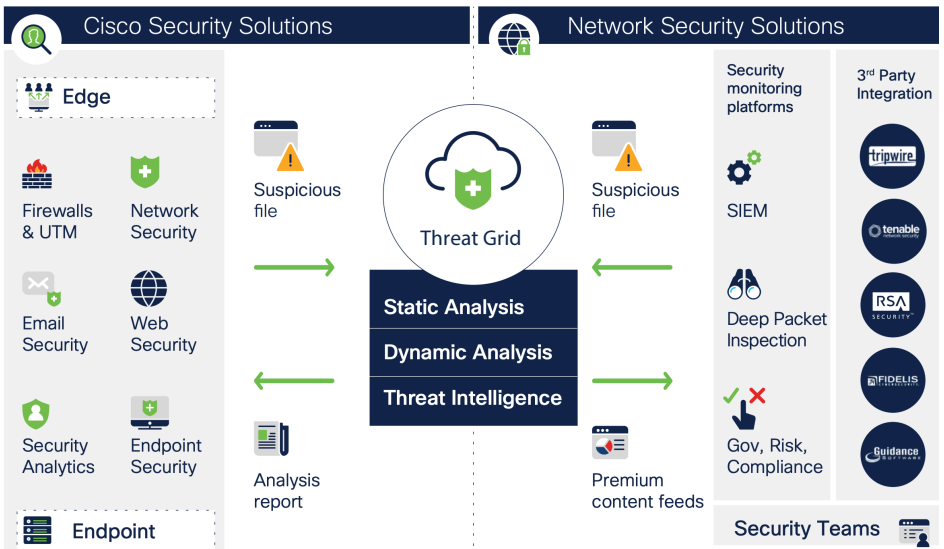
Cisco Threat Grid delivers context-driven analytics to accurately identify attacks in near real time. The solution analyzes millions of files and correlates them against hundreds of millions of other analyzed malware artifacts. Customers gain a global and historical view of malware attacks, campaigns, and their distribution.

With Cisco Threat Grid, you can:

- Use the threat score and behavioral indicators to rapidly identify, prioritize and recover from advanced malware
- Automate malware protection features for faster detection and response
- Easily integrate premium feeds into existing security technologies such as SIEM, intrusion detection systems, gateways, and proxies to detect and block malware faster

Cisco Threat Grid gives you accurate detection and defense against advanced attacks. Robust search, correlation, and reporting capabilities provide detailed information on current and historical malware artifacts, indicators, and samples. Detailed analysis reports include all malware sample activities, including network traffic and artifacts.

Figure 1. Edge to endpoint integration



Cisco Threat Grid has been integrated across the Cisco portfolio, from edge to endpoint, including the following products:

- Cisco Next-Gen Firewall
- Cisco Email Security
- Cisco Web Security Appliance
- AMP for Endpoints
- Cisco Umbrella

A subscription to Cisco Threat Grid provides users with access to the robust representational state transfer (REST) API. You can automate the submission of suspicious files to Threat Grid for analysis from nearly any existing security platform.

Next Steps:

For more information on Threat Grid Cloud and Appliances visit: cisco.com/go/amptg.

"Threat Grid is revolutionizing the way that organizations use accurate and context rich malware analysis and threat intelligence to defend against advanced cyberattacks."

Jon Olstik,
ESG Group