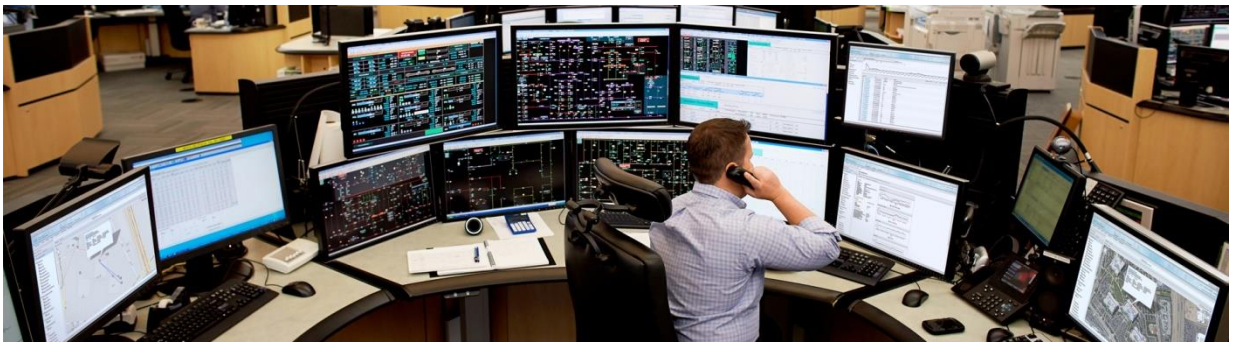

Cisco Threat Grid: Get Proactive with Advanced Malware Security

BENEFITS

- Gain deeper insight for stronger defense with static and dynamic malware analysis
- Accurately identify attacks in near real time with context-focused security analytics
- Proactively protect businesses using threat intelligence from premium threat feeds
- Accelerate threat detection and response capabilities with a powerful API that integrates and automates existing security products and processes
- Defend against threats from anywhere with the scale and power of a cloud service that analyzes hundreds of thousands of samples every day

Today's advanced malware hides in plain sight, evades defenses, and patiently waits to strike. Security teams are challenged with detecting and analyzing advanced threats while their security technologies lack the sophistication and interconnectivity needed to block them.

Organizations are coming under unrelenting attack, with security breaches occurring daily. The highest-profile attacks are creating front-page headlines. A global community of attackers is creating advanced malware and launching it through multifaceted attacks and multiple attack vectors within organizations of all sizes. Organizations are still relying on outdated tools and partially effective methods to protect their sensitive data, mainly with signature-based technology. Security teams now have a much shorter window to identify, investigate, and remediate malware. Additionally, organizations are facing significant shortages of staff with the necessary skills and experience to understand and triage advanced malware.

Cisco® Threat Grid combines static and dynamic malware analysis with threat intelligence into a single solution delivered through the cloud, as an on-premises solution, or integrated into Cisco security technologies. Threat Grid combines behavioral analysis and up-to-the-minute threat intelligence feeds with your existing security infrastructure. With Threat Grid you can understand what malware is doing or attempting to do, how large a threat it poses, and how to defend against it.

Escalating Attacks Overwhelm Traditional Security Approaches

According to the 2017 Cisco Annual Security Report, cybercriminals are designing malware that relies on tools that users trust to persistently infect and hide in plain sight on their machines. The2017 PWC Global State of Information Security report found that organizations are detecting 26 percent more incidents than they did the prior year. The 2016 Ponemon Cost of Data Breach Study found the average time to detect a breach was between 162 to 229 days, while data exfiltration begins in just hours.

According to ESG Global's 2016 survey of IT spending, 28 percent of large and midmarket enterprises say they have an ongoing shortage of IT security skills in their organization.

Security organizations are overwhelmed, fighting an uphill battle to meet the challenge of advanced threats. They have much shorter windows to identify and respond to incidents, and it's much harder to understand what's happening in a large, modern enterprise environment due in part to the lack of communication between security technologies. And with so few expert security personnel available and constrained budgets for new defenses, enterprises are vulnerable.

Cisco Threat Grid Overview

Threat Grid provides the in-depth information needed to better defend against malware. With its robust, context-rich malware knowledge base, organizations can understand what malware is doing or attempting to do, how large a threat it poses, and how to defend against it. The solution includes the following features:

Malware Analysis

Threat Grid crowdsources malware from a closed community and analyzes all samples using highly secure proprietary techniques that include static analysis, dynamic analysis, and forensic analysis. Unlike traditional sandboxing technologies, our analysis exists outside the virtual environment, identifying malicious code designed to evade detection. As part of the analysis, the Glovebox feature allows you to interact with the malware in real time, recording all activity for future playback and reporting.

Edge-to-Endpoint Integration

Threat Grid is integrated with Cisco security technologies to provide malware analysis from the network edge to the endpoint. These technologies include Cisco AMP for Networks, Cisco Next Generation Intrusion Prevention Systems, Cisco ASA with Firepower™ Services, Cisco Email Security Appliance, Cisco Web Security Appliance, and Cisco AMP for Endpoints. The combined power of Threat Grid with these detection technologies means organizations get more visibility into more places than ever before. Information is correlated, shared, and synthesized across multiple security controls so your organizations can make faster, better decisions to quickly eliminate threats and reduce the harm from breaches caused by malware.

Empowering Existing Security Technologies

Threat Grid transparently integrates with an organization's existing security infrastructure. It can automatically consume submissions from endpoint agents, deep-packet-inspection platforms, forensic investigation tools, and more through the representational state transfer (REST) API and through numerous partner solution integrations. Since Threat Grid is integrated across the Cisco security portfolio, you can analyze more samples from your existing tools instead of deploying and managing new ones using sample packs.

Threat Score

With more than 800 behavioral indicators and a malware knowledge base sourced from around the globe, Threat Grid provides more accurate, context-rich analytics about advanced malware than ever before. Malware samples submitted to Threat Grid provide a threat score that is based on two key elements: severity and confidence. Using the behavioral indicators, Threat Grid tells you if a sample is malicious, suspicious, or benign, and why. This eliminates guesswork and empowers junior security analysts to make better decisions, faster.

Glovebox

Advanced malware uses numerous evasion techniques to determine whether it is being analyzed in a sandbox. Some of these samples require user interaction. Threat Grid provides you with Glovebox, a safe environment to dissect these samples without infecting your network while the sample is being analyzed. Glovebox is a powerful tool against advanced malware that allows analysts to open applications and replicate a workflow process, see how the malware behaves, and even reboot the virtual machine.

Machine Readable Threat Feeds

Threat Grid provides highly accurate premium content feeds. These help organizations generate context-rich threat intelligence that is both actionable and specific. Using the powerful API, you can import threat information directly into your existing security technologies, including security information and event management (SIEM) solutions, gateways, proxies, visualization tools, and more to automate detection and responses for even the most sophisticated threats.

Cloud Power and Scale

Threat Grid crowdsources malware from a closed community and analyzes all samples using highly secure proprietary techniques that include static and dynamic analysis. It correlates the results with hundreds of millions of analyzed malware samples to provide a global view of malware attacks, and campaigns. Security teams can quickly correlate a single sample of observed activity and characteristics and compare it against millions of other samples to fully understand its behavior in a historical and global context.

Threat Grid's cloud solution allows users to submit thousands of samples at a time for analysis, receiving detailed reports, including the identification of important behavioral indicators and the assignment of threat scores, in just minutes. This information helps security teams rapidly prioritize and recover from advanced attacks.

On-premises Analysis

The Threat Grid appliance delivers on-premises advanced malware analysis with deep threat analytics and content. Organizations with compliance and policy restrictions submit malware samples to the appliance for analysis, helping to ensure adherence with organizational requirements. With the Threat Grid appliance, all samples are analyzed using proprietary and highly secure static and dynamic analysis techniques. It correlates the results against billions of analyzed malware artifacts without sending information out of your organization's logical boundaries.

Empower Your Security Team

Whether on premises or in the cloud, security teams can use Threat Grid to quickly correlate a single sample or hundreds of observed activities and characteristics against millions of other samples to fully understand malware behavior in a historical and global context. This helps you to 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.

How Different Security Teams Can Use Cisco Threat Grid

Table 1 illustrates how different members of your security organization can use Threat Grid.

Table 1. Threat Grid Throughout an Organization

Department/Personnel	Relevant Benefits
Incident response	• Analyzes a single submission or hundreds of submissions in minutes • Searches for malicious samples using IP addresses, file hashes, mutexes (mutual exclusion objects), domain names, registry keys, and URLs • Interacts with malware sample using Glovebox
Security operations	• Generates a threat score for all malware submissions • Provides easy to understand behavioral indicators for all analysts • Automatically submits suspicious samples for analysis
Chief information security officer	• Integrates with existing security technologies • Accelerates detection of advanced, targeted attacks • Empowers security teams to react faster

Cisco Advanced Services for Threat Grid

Integrate, Automate, and Remediate

Organizations use Threat Grid to better understand and protect their environment from today's advanced malware. Cisco Advanced Services can help your organization to fully integrate Threat Grid's dynamic malware analysis engine and automate sample submissions. Cisco Advanced Services helps you quickly take advantage of Threat Grid's threat intelligence feeds, so that you can use existing security technologies to automatically submit or consume actionable information.

> "The integration of Threat Grid into our environment provides our existing security, risk, and privacy business protection technologies with automated and integrated threat intelligence, enhancing their effectiveness and enriching our overall cyber defense posture. This advanced threat picture enables our Critical Incident Response Centers to more rapidly analyze and mitigate potential malware."
>
> **— Roland Cloutier, Global Chief Security Officer, ADP**

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.

Why Cisco?

Today's networks extend to wherever employees are, wherever data is, and wherever data can be accessed from. As a result, technologies must also focus on detecting, understanding, and stopping threats. Being threat-focused means applying visibility and context to understand and adapt to changes in the environment and then evolving protections to take action and stop threats. Threat Grid provides the deep level of analysis and threat-content needed to protect your organization today.

Next Steps

For more information or to watch real-world examples of organizations combatting advanced threats with Threat Grid visit http://www.cisco.com/go/amptg.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C22-734156-02 03/17