Cisco Umbrella

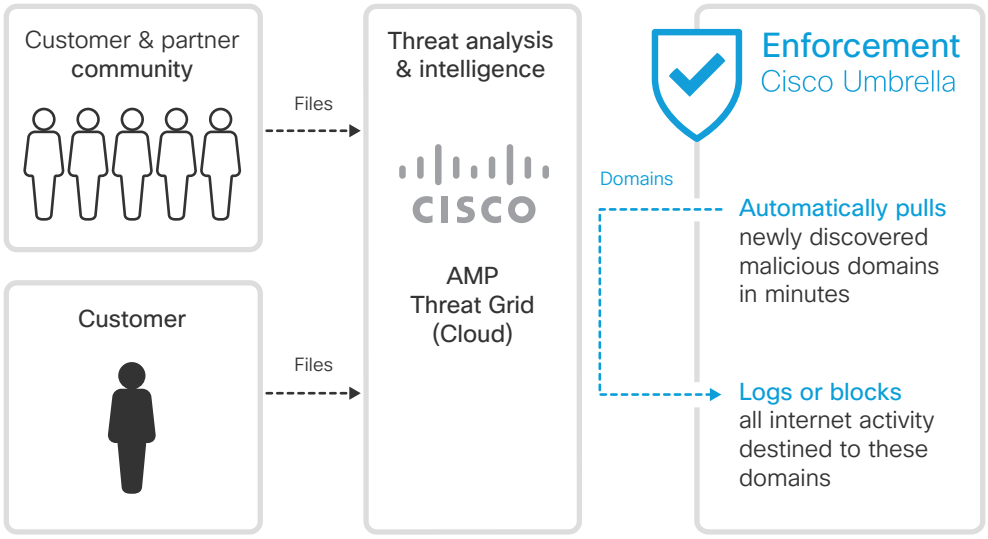
FEATURE BRIEF

Convert your threat analysis and intelligence into global prevention with Cisco Umbrella and AMP Threat Grid.

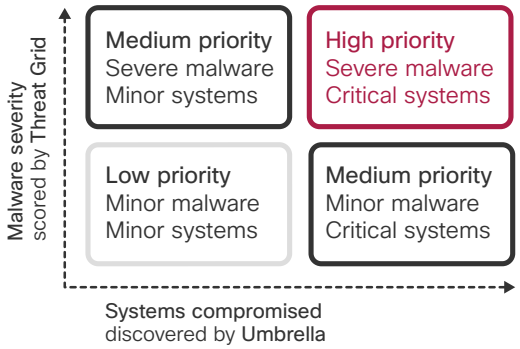
Take faster action on newly discovered malicious domains by leveraging a turn-key integration between Cisco Umbrella and Cisco AMP Threat Grid. Through security automation, dwell time is reduced from hours or days to only minutes. And by gaining internet-wide visibility in real-time, you will discover more compromised systems.

Reduce attack dwell time by eliminating manual configuration

Every minute, Cisco AMP Threat Grid discovers new malicious domains from files submitted by customers and partners. These domains are the destinations of command & control (C2) callbacks from compromised systems that are used to exfiltrate data to the attacker's botnet infrastructure. You can protect against breaches by taking action on this threat intelligence or this data might lie dormant in Threat Grid because manually configuring appliance and agent-based threat defenses is slow and impossible to maintain. By leveraging our integration, malicious domains that have a very high Threat Grid confidence score and pass Umbrella's false positive filters will be automatically added to the Umbrella cloud-delivered enforcement service. Hours of data entry are gone!



In real-time, Umbrella will identify compromised systems based on any internet activity destined to malicious Threat Grid domains. Response teams will know which malicious domains and files to further investigate based on "critical" (CEO's laptop, POS server) vs. "minor" (public kiosk, intern's desktop) systems compromised by "severe" (ransomware, APT) vs. "minor" (commodity exploit kit) malware.



About AMP Threat Grid

Threat Grid is a cloud-based unified malware analysis and threat intelligence system that identifies key behavioral indicators, providing accurate threat content enriched with global and historical context.

By the numbers

- 6-10 million files analyzed monthly
- 7.5 minutes on average to analyze a single file
- 1,000 files analyzed in 15 minutes

For more information, please visit cisco.com/go/amptg

About Cisco Umbrella

Umbrella is a cloud security platform that is built into the foundation of the internet. It analyzes DNS and IP activity to predict current and emerging threats, and block them before they reach your network or endpoints.

By The Numbers

- 85 million users
- 100 billion daily Internet requests
- 7 million malicious destinations enforced at any given time

Any device over any port or protocol, on and off the network

While most malware exploits Windows-based systems, attackers that target specific enterprises will design malware to compromise any device to exfiltrate the data. DNS is used by every device on your network, so Umbrella protects any device – managed and unmanaged. The C2 callbacks may use web or non-web ports and protocols. DNS precedes the callbacks, so Umbrella logs or blocks internet activity, including data exfiltration, over any port or protocol. And compromised systems may roam on or off the corporate network. Using lightweight and transparent clients to forward DNS, Umbrella protects Windows or Mac OS X systems on or off the corporate network.

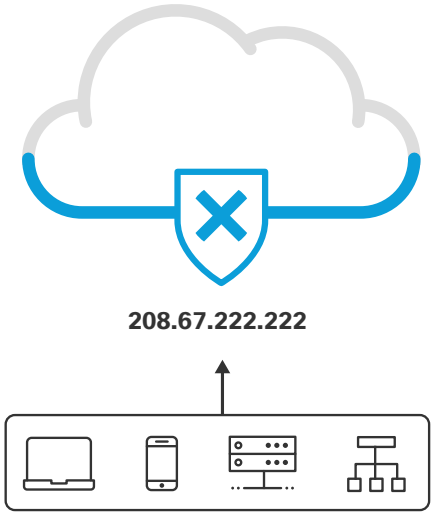
"Organizations that have automated tools report that an average of 60 percent of malware containment does not require human input or intervention and can be handled by automated tools."

Ponemon Institute
The Cost of Malware Containment, Jan 2015

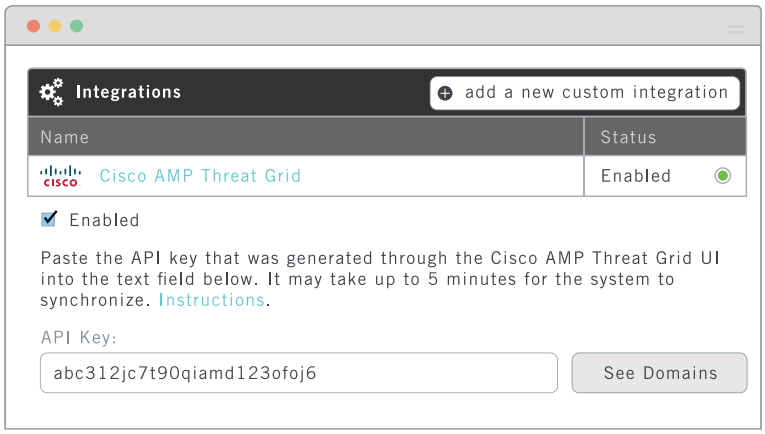
Enforcing security everywhere has never been so easy

Simply point DNS to the Umbrella global network and paste your Threat Grid API key into the Umbrella dashboard. The set up takes only minutes and the experience is transparent to your networks, devices, and users. Together, Umbrella and Threat Grid's cloud-delivered, API-based services enforce security everywhere.

Step 1



Step 2



Investigate attacks using global and historical context

We have short windows to identify and respond to attacks before damage happens. And it's much harder to understand what's happening in large, digital business environments, especially with the current shortage of expert incident analysts. Both Umbrella and Threat Grid provide threat intelligence consoles and APIs that give you more complete context about threats and help speed up investigations. Threat Grid shows the behavior and indicators of compromise of malicious files when they run on endpoints, whereas Cisco Umbrella Investigate gives insight into the internet infrastructure (domains, IPs, ASNs, etc.) used for attacks. Investigate shows the creation and evolution of malicious domains and their relationships with IPs, ASNs, and malware. Together, we enable you to pivot around attackers' infrastructures so you can investigate incidents faster and uncover potential threats before new attacks launch.

About Cisco Umbrella Investigate

Investigate provides threat intelligence about domains, IPs, ASNs, and malware across the internet. Leveraging a diverse dataset of 80+ billion daily DNS requests and live views of the connections between different networks on the internet, we apply statistical models and human intelligence to pinpoint attackers' infrastructures and predict future threats.