OpenDNS

OpenDNS is now part of Cisco.

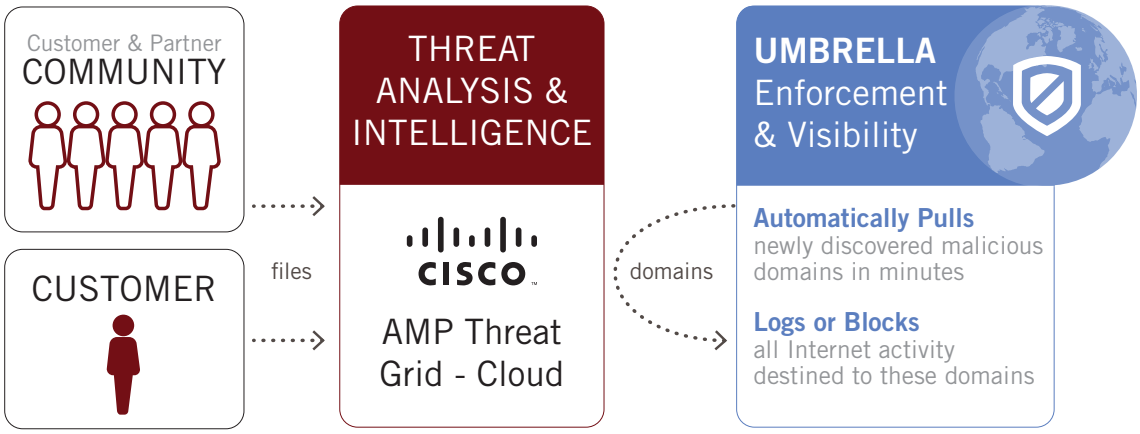
Feature Brief: Cisco AMP Threat Grid Integration

Convert Your Threat Detection and Intelligence into Global Threat Prevention

Take faster action on newly discovered malicious domains by leveraging a turn-key integration between Cisco and OpenDNS. 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.

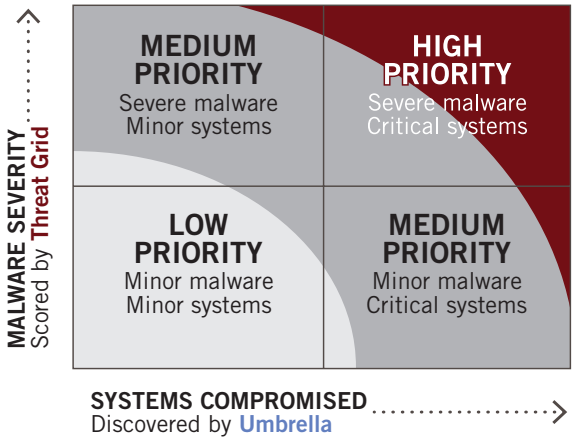
Reduce Attack Dwell Time by Eliminating Manual Configuration

Every minute, Cisco AMP Threat Grid discovers new malicious domains from every file you and others submit. These domains are the destination of command & control (C2) callbacks from compromised systems. And C2 callbacks are used to exfiltrate data to the attacker's botnet infrastructure. So we can protect against breaches by simply taking action on this threat intelligence. But we let it lie dormant in Threat Grid because manually configuring appliance- and agent-based threat defenses is slow and impossible to keep up with. By leveraging our integration, malicious domains that have a very high Threat Grid confidence score and pass OpenDNS's false positive filters will be automatically added to our DNS-based service—Umbrella. Hours of data entry are gone!



Prioritize Investigations by Correlating Malware with Systems

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.



Why Umbrella?

- **Threat Prevention** not just threat detection
- **Protects On & Off Network** not limited to devices forwarding traffic through on-prem appliances
- **Always Up to Date** no need for device to VPN back to an on-premises server for updates
- **Block by Domains for All Ports** not just IP addresses or domains over ports 80/443
- **Integrate in Seconds** does not require pro services to setup

About Threat Grid

Cisco's 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 are analyzed every month
- 7.5 minutes to analyze a single file is average
- 1,000 files can be analyzed in 15 minutes

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

Any Device. Any Port or Protocol. On or 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. 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-based systems on or off the corporate network.

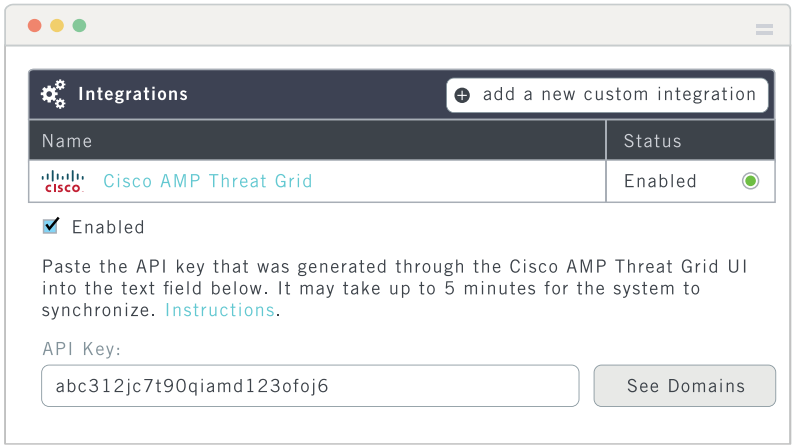
Enforcing Security Everywhere Has Never Been Faster

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

> *"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

Step 1

Step 2



Investigate Attacks Using Global and Historical Context

We have much shorter 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 a shortage of expert incident analysts. Both OpenDNS and Threat Grid provide consoles and APIs for fuller context to speed up investigations. Threat Grid shows the creation and evolution of malicious files and their relationships with indicators of compromise, whereas OpenDNS Investigate shows the creation and evolution of malicious domains and their relationships with IPs and ASNs. Together, we enable you to pivot around attackers' infrastructures and payloads so you can uncover potential threats before new attacks launch.

> *"Two-thirds of the time spent by security staff responding to malware alerts is wasted because of faulty intelligence."*
>
> — Ponemon Institute [The Cost of Malware Containment](), Jan 2015

OpenDNS

OpenDNS is now part of Cisco.

For a free trial or more sales information, contact our team:

1-877-811-2367 | sales@opendns.com | www.opendns.com