11- Cisco AMP for Endpoints

Ahmed Sultan
Senior Technical Instructor
ahmedsultan.me/about

Introduction

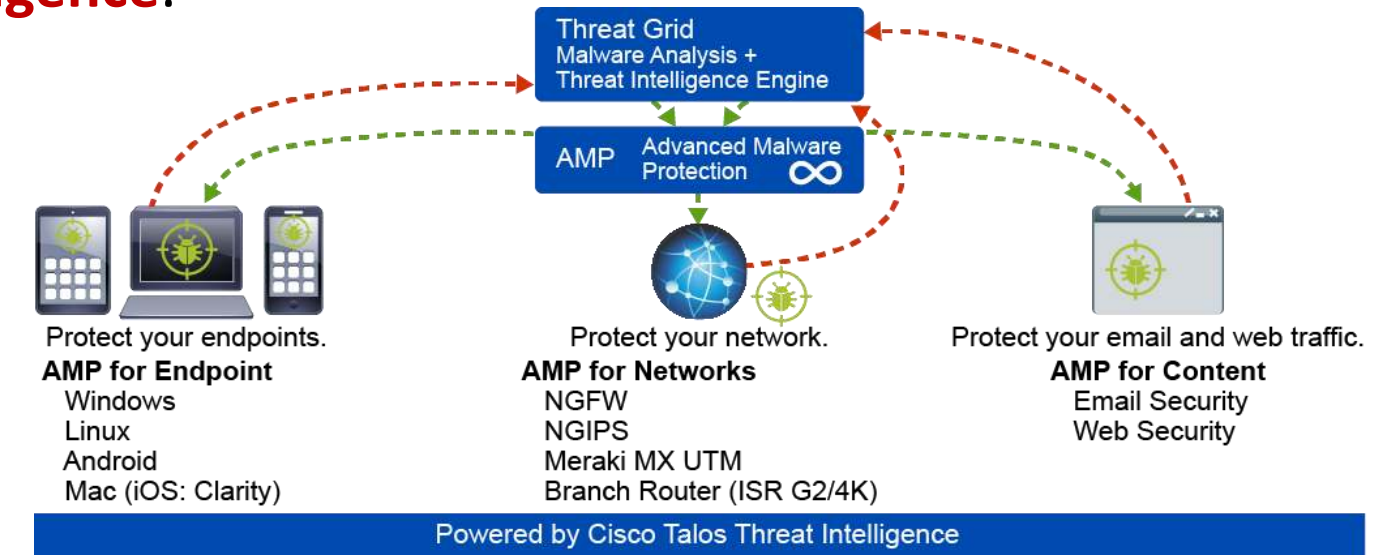
- Securing your endpoints is markedly different than securing your network.
- In legacy network architectures, you can use your network to protect your endpoints.
- That strategy is less-useful in modern, mobile and cloud-based environments, because you cannot guarantee that your endpoints will always be behind your network.
- As your corporate endpoints connect to business partner networks, to hosted environments, and to other networks that you do not control, you must focus on protecting the endpoint independently of protecting the network.

Introduction (cont.)

- Cisco Advanced Malware Protection (AMP) accelerates security response by providing visibility and clarity to previously unknown artifacts in exchanged files, and by seeing a threat once and blocking it everywhere.
- Cisco AMP is available both on **network devices** and on **endpoints**, thus addressing security both of network and security.
- In the context of AMP for Endpoints, the AMP solution is positioned as Endpoint Protection Platform (EPP), which provides many capabilities to protect endpoints.

Cisco AMP for Endpoints Architecture

- The power of the AMP architecture is the integration between different components, such as **Cisco Firepower NGFW**, **Cisco Email Security Appliance (ESA)**, and **Cisco Web Security Appliance (WSA)**.
- The AMP cloud, where the detection of malware occurs, is powered by **Talos Threat Intelligence**.

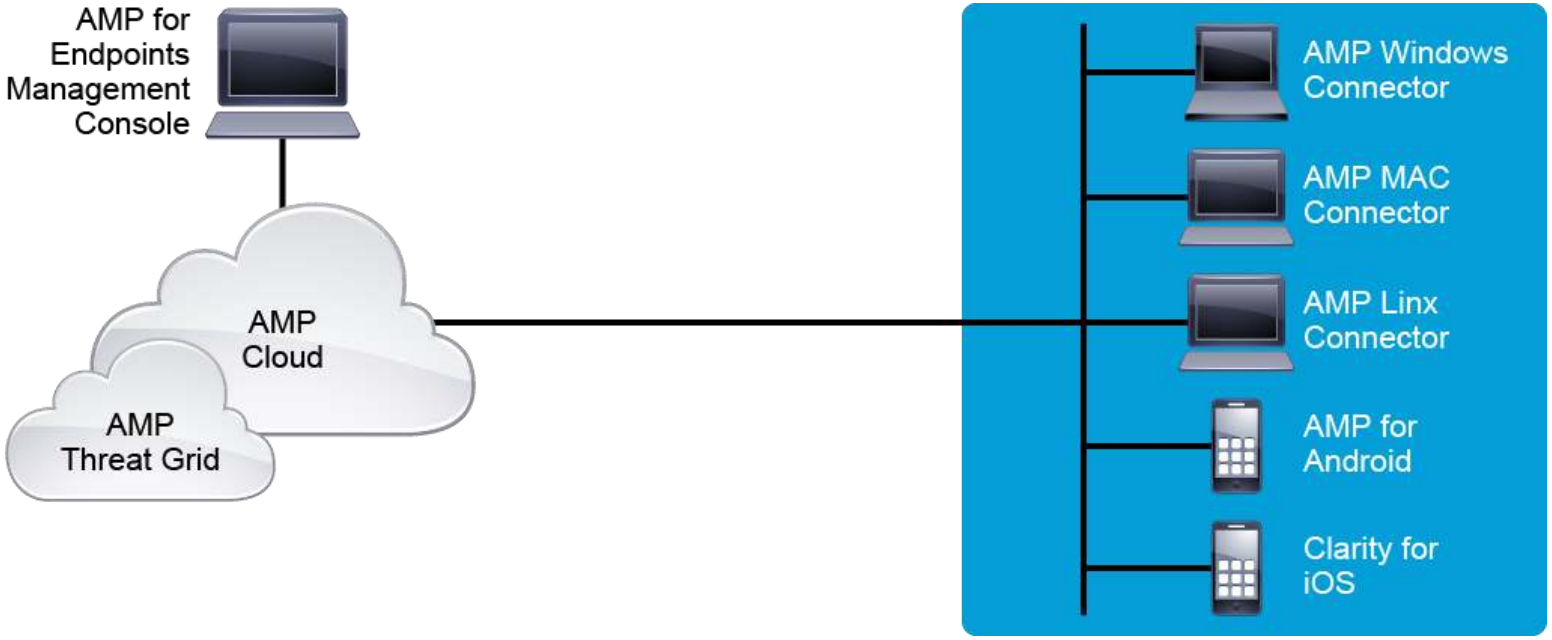


Cisco AMP for Endpoints Architecture (cont.)

- Any component in the AMP architecture can submit a file to AMP cloud for analyses.
- If a file is unknown to AMP cloud, the file can be further submitted to Threat Grid cloud sandbox for analyses.
- Files can also be submitted to Threat Grid manually by users.
- When Threat Grid issues a conviction, the Cisco AMP Cloud informs all AMP components worldwide of the conviction.

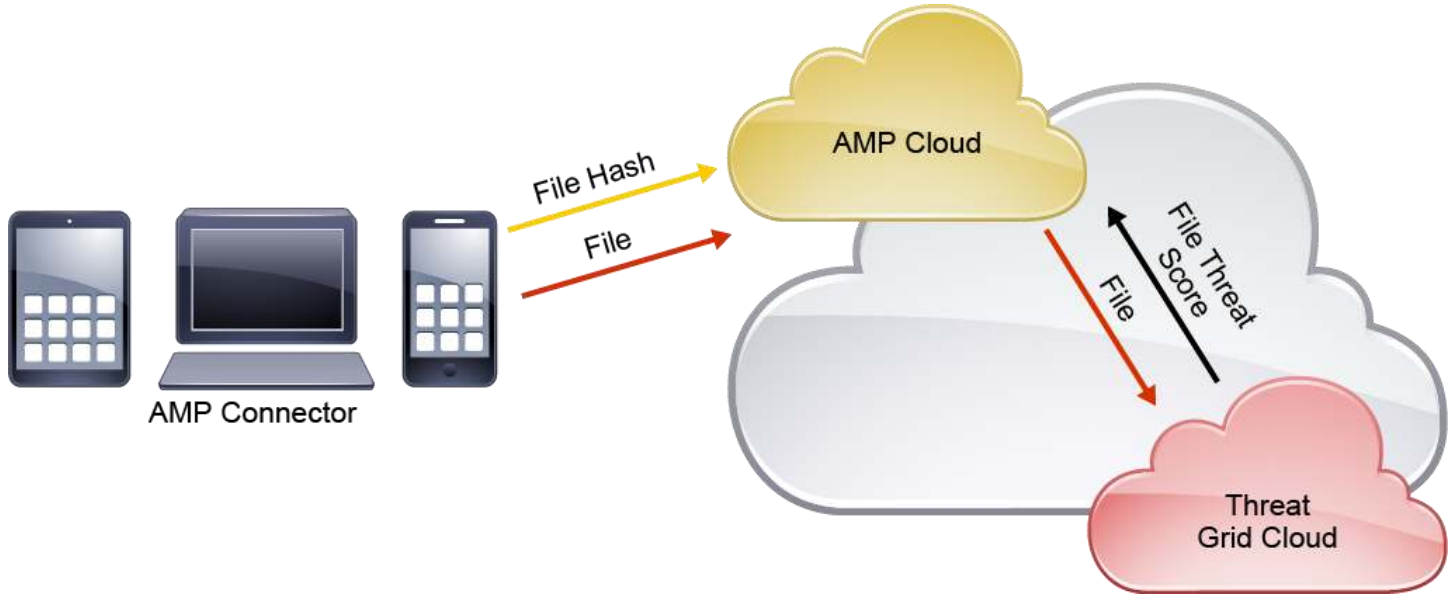
Cisco AMP for Endpoints Architecture (cont.)

- The figure illustrates the AMP for Endpoints solution components.



Cisco AMP for Endpoints Architecture (cont.)

- The most common AMP for Endpoints deployment type is to use public cloud.



Cisco AMP for Endpoints Architecture (cont.)

- When a file is moved, executed, or copied, the AMP connector calculates its hash (and additional feature sets, if needed) and queries the AMP cloud for the file verdict.
- Only file hash is sent to the cloud at this point.
- For the files that are already known to the cloud, the verdict can be **clean** or contain **malware**.
- If the file is unknown to the cloud, the returned verdict is unknown.

Cisco AMP for Endpoints Architecture (cont.)

- If the verdict is unknown, the AMP connector can be configured to send the whole file for the **sandbox** analysis.
- The file is sent to the AMP cloud and submitted to the **Threat Grid Cloud sandbox** for analyses.
- Files can also be submitted to Threat Grid manually by users, either through the AMP or Threat Grid console.
- When **Threat Grid** issues a conviction, it updates the verdict in the AMP cloud.
- The AMP cloud then informs all components that have seen the file previously about the verdict through the retrospective event.

Explore Cisco AMP for Endpoints [Lab]

Demo Lab