Advanced Threat Detection

Overview

Cisco Cloud Web Security consists of multiple security technologies designed to protect your network throughout the full attack continuum. Cisco Cloud Web Security Premium adds Advanced Threat Detection (ATD) services to Cisco Cloud Web Security Essentials and provides additional features that enhance the protection of your network from advanced cyber threats.

- Advanced Malware Protection (AMP) operates in the during and after phases of the attack continuum.
  - In the during phase, scans file reputation to automatically detect and block known and emerging malware threats in real time.
  - In the after phase, performs behavioral analysis of suspicious files in a virtual sandbox environment to prevent malicious files from affecting your network. Cumulative analysis and intelligence information about the files collected from the community are shared through a sandbox report.
  - Tracks the spread of any file within your network and continuously monitors file reputation over time. If a file reputation changes to malicious or is found by file sandboxing to be malicious, AMP provides retrospective alerting in the after phase. AMP identifies every instance of the file within your network to address the problem of malicious files passing through perimeter defenses that are later deemed a threat.
- Cognitive Threat Analytics (CTA) extends Cisco Cloud Web Security into the after phase of the attack continuum.
  - Actively monitors your network to spot behavior outside the norm.
  - Automatically detects suspicious activity inside your network.
  - Using behavioral analysis of network traffic to detect anomalies, identifies symptoms of malware infection or data breach.
  - Reduces the time to discover threats operating inside your network.

- Performs independent (of any global feeds) analysis of your web traffic to detect attacks targeted against your network.
- Delivers local security intelligence specific to your network environment.
- Uses advanced statistical modeling and machine-learning to identify new threats.

Note AMP and CTA are activated as part of the provisioning process for Cisco Cloud Web Security Premium. No additional configuration within Cisco ScanCenter is required.

Caution In cases where the size of the executable file is larger than 128KB, streaming of the file to the browser begins before the file scan is completed. If the AMP scan finds the file to be malicious, a TCP Reset is sent to the browser to stop the file download. However, if the TCP Reset gets blocked, the connection is closed, but the partially downloaded file remains available.

Additional Benefits

- Continuous monitoring reduces time-to-detect and helps you prioritize the investigation of attacks on your network.
- Identifies hosts infected by malware or compromised with advanced threat infections that were able to sneak by other security measures.
- Provides context information including user identities, threat indicators, descriptions of malicious behavior, and precision ratings of verdicts.
- Uncovers persistent, complex infections that penetrated other defenses to establish command-and-control (C&C) communication channels.
- Proactively detects and blocks malware by analyzing Web traffic metadata, making it harder for the attack to evade the ATD system.
- Fuzzy fingerprinting automatically detects polymorphic variants of known malware.
- Provides a bigger picture of the threat by focusing on the attacker rather than just the exploit or particular malware.
- Rather than just react to attacks, helps you stay ahead of the attacker through the use of machine learning and advanced statistical and predictive modeling.
- Adaptive capabilities that respond to new threats as they emerge.
- No need to manually create and maintain rule sets.

Reports Tab

In the during phase, AMP examines the reputation of select file types traversing your network perimeter. If the file reputation is malicious, AMP blocks the file and reports to Cisco ScanCenter. Information on malware blocked inline by AMP is found in the **Malware Analysis** section of the **Reports** tab.

Dashboard Tab

Information on files sandboxed by AMP during the after phase is found in the **Dashboard** tab and **AMP Blocks** section. See Dashboard.

Threats Tab

Incidents and their general details are listed in the **Threats** tab.

- CTA incident—CTA analyzes network traffic collected in Web proxy logs to detect anomalies. Behaviors that do not conform to an established standard are possible threats and are reported to Cisco ScanCenter as incidents.
- AMP retrospective incident—In cases where the file reputation is clean or unknown at the time of download, but later the file reputation changes to malicious or is found by file sandboxing to be malicious, AMP reports the file to Cisco ScanCenter as a retrospective incident.

For more information on the **Threats** tab, see Web Portal.