Never stop hunting for the riskiest 1% of threats.

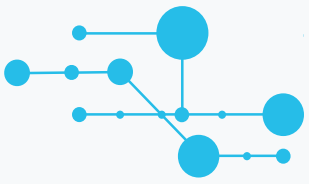
Most endpoint solutions claim to block 99% of threats – but what about the remaining 1%?

Traditional antivirus solutions are just that: traditional. Testing shows they are blind to advanced threats, including ransomware hidden in zip files, memory-based malware, and browser injections.

Advanced malware requires advanced solutions that don't just stop at prevention – it requires prevention, detection, and response. Cisco AMP for Endpoints provides that advanced solution by going beyond reactive response and enabling customers to proactively detect and hunt threats. This proactive approach is essential for tackling the unknown and riskiest 1% of threats, and why AMP for Endpoints is superior to traditional endpoint security solutions.

Prevention

Powered by Cisco Talos, Cisco AMP for Endpoints enables customers to...



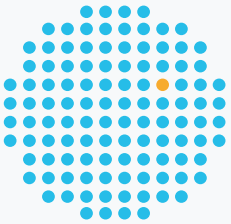
- Strengthen defenses using the best global threat intelligence, and block both fileless and file-based malware in real time.
- Detect and block malware exploits and evasion technology.

While legacy technologies...

- Fail to see malware in .zip format, including ransomware and other threats hiding in zip files.
- Show pre-execution detection "futility" – failing to catch malware in pre-execution stages.
- Come up with more false positives, including inaccurately reporting the well-known "7z software" as malicious.
- Falsely report the successful elimination of malware – when in reality malicious, potentially destructive files continue to exist on the endpoint.

Detection

Cisco protects for unknown threats by...



- Continuously monitoring and recording all file activity to quickly detect stealthy malware.
- Providing fast and accurate threat detection.

While traditional AV solutions demonstrate...

- Lack of coverage for low-prevalence threats and damaging software vulnerabilities.
- Deficiencies in process-level, drill-down analysis and investigation.

Response

Cisco is the only provider of patented retrospective security that...

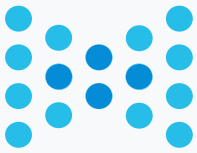
- Retrospectively stops threats at the first sign of malicious behavior.
- Rapidly contains the attack by isolating an infected endpoint and remediating malware across Windows, Macs, Linux, servers, and mobile devices (Android and iOS).

While alternative endpoint security options...

- Don't offer retrospective device and file trajectory, lacking in providing visibility to threats that can be exposed by command-line arguments.
- Demonstrate inconsistencies in providing accurate disposition of an endpoint, failing to show if an analyst's action to "stop and remove" a suspicious file was successful or not.

Efficiency

Seamlessly integrated in one end-to-end solution that...



- Has more than 15 built-in protection and detection mechanisms, including malicious activity protection, fileless-malware exploit prevention, machine-learning analysis of new threats, and sandboxing.
- Allows you to see a threat once and block it anywhere else in the environment.

While traditional AV tools...

- Require configuring many discrete elements to attain ample protection with low false positives.
- Prove the complexity of the solution by requiring multiple "process-hungry" agents to run on endpoints.
- Expose many product defects and random errors, causing confusion and at times misleading the user.