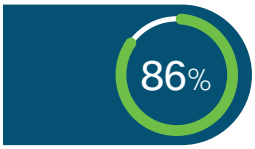
Compare Endpoint Security Solutions

	Cisco AMP for Endpoints	Carbon Black Endpoint Security	CrowdStrike Falcon	CylancePROTECT
Detection				
Number of integrated detection techniques	13 Cisco AMP for Endpoints employs a 1:1 SHA matching engine (public, private, or hybrid); TETRA AV; sandboxing; ETHOS fuzzy fingerprinting; SPERO machine learning; cloud IOCs and reputation analytics; CLI capture; memory, fileless, script, and mutation protection; vulnerable software; CTA (threat analytics); custom hash detections, ClamAV signatures, and application blocking.	4 Carbon Black employs whitelisting, machine learning, behavioral analytics, and next-gen antivirus.	4 CrowdStrike Falcon employs indicators of attack (for fileless malware), machine learning, blacklists and whitelists, and known exploit blocking.	3 Cylance employs algorithms as its only detection method. Efficacy is derived from the currency of the math model deployed to individual clients. Depending on the model updates, some clients may detect malware and some may not. SHA 256 lookupos and Sandboxing are other technologies that they employ.
Continuous analysis and retrospective detection	✓ The Cisco AMP for Endpoints employs continuous analysis beyond the event horizon (point in time) and can retrospectively detect, alert, track, analyze, and remediate advanced malware that may at first appear clean or that evades initial defenses and is later identified as malicious.	Limited Carbon Black employs continuous analysis using Cb Defense.	✓ CrowdStrike Falcon offers DVR capability down to a 5-second visibility of the endpoint.	✓ Cylance employs continuous analysis
Device trajectory	Continuous Cisco AMP maps how hosts interact with files, including malware files, across your endpoint environment. It can see if a file transfer was blocked or if the file was quarantined. It can scope the threat, provide outbreak controls, and identify patient zero.	✓ Very rich process tree for investigation. Shows a lot of eye candy which makes the investigation process visually appealing.	✗ CrowdStrike does not provide device trajectory, but it does provide attribution trajectory. It is important to know who developed that malware, but most people would rather stop it and keep it from coming in again. Recent misses and conflicting information between NSA, CIA, and CrowdStrike regarding the two largest and most public hacks in recent times, have made many question the accuracy of attribution capabilites.	Limited Requires a separate product known as CylanceOptics which allows customers to ensure the understanding of root cause.
Detection measures	Multiple Cisco AMP uses several methods of detection, including fuzzy fingerprinting (ETHOS), machine learning (SPERO), dynamic file analysis (Threat Grid), and 1:1 SHA matching, all supported by Talos, the world's largest threat intelligence group.	Multiple 150 behaviors, no trajectory. No behavioral IoCs. Events are based on signatures, vulnerabilities, and point-in-time analysis..	Multiple 120 local event types streamed in real time, hash and behavioral blocking, credential theft and privilege escalation, boot sector, process, stack, and other techniques.	Multiple Cylance primarily depends on a machine learning model that uses more than 1 million features and attributes. This is suplemented with SHA256 checks.
Dynamic file analysis	Threat Grid An automated detonation engine observes, deconstructs, and analyzes using several methods. It's impervious to sandbox-aware malware.	✗ Needs an integration point with a partner for sandboxing technology	✗ Lacks an integration point. Does not deploy an on-premises system outside classified networks. Does not integrate with supporting systems such as NGIPS, BDS, or BPS.	✗ Lacks an integration point; currently does not exist.

	Cisco AMP for Endpoints	Carbon Black Endpoint Security	CrowdStrike Falcon	CylancePROTECT
Detection (continued)				
File analysis deployment model	Both The Threat Grid sandbox is fully integrated within the AMP for Endpoints solution. File analysis can also be an on-premises solution. Because AMP Threat Grid uses a proprietary analysis mechanism and 100 other anti-evasion techniques, it is virtually undetectable by malware trying to avoid analysis and sandboxing. Threat Grid uses the widest set of analysis techniques, including but not limited to host, network, static, and dynamic analysis, as well as pre- and post-execution analysis of the master boot record.	✗ Needs an integration point with a partner for sandboxing technology.	✗ Lacks an integration point. Claims that machine learning is sufficient for all file analysis.	✗ Lacks an integration point.
API support	✓ Use REST API access to pull events, IOCs, and device data. You can script and customize the API to fit the environment.	✓ Open API	✓ Open API	✓ Open API for integration from several products. Key OEM partners also leverage CylanceProtect technology within their own products. ForcePoint, A10, Outlier API, and BRICATA.
File trajectory	✓ Gain visibility into the scope of a breach (how many endpoints are affected by subject malware). Discover patient zero: when the malware was first seen on which computer in your environment, what its parentage is, and how it moves between hosts.	Limited Scope is focused on local host processes and does not track from the aspect of "file" and where it has traveled.	Limited Scope is focused on local host processes using indicators of attack and does not track from the aspect of "file" and where it has traveled. Due to visibility gaps with Linux, Mac, and mobile, a complete picture is hard to determine.	Limited Requires CylanceOptics focused on local host processes using indicators of attack and does not track from the aspect of "file" and where it has traveled. Due to visibility gaps with Linux, Mac, and mobile, a complete picture is hard to determine.



Cisco Advanced Malware Protection Customer Statistic

86% of surveyed customers were able to improve security effectiveness with AMP for Endpoints.

Validated Published: Apr. 7, 2017 TVID: 5BE-4DD-685 Source: TechValidate survey of 927 users of Cisco Advanced Malware Protection

	Cisco AMP for Endpoints	Carbon Black Endpoint Security	CrowdStrike Falcon	CylancePROTECT
Prevention				
Whitelists and blacklists	✓ With AMP for Endpoints, you can blacklist false negatives and whitelist false positives, giving you the power to override dispositions set by Cisco Talos.	✓ Bit9 was one of the first to whitelist and blacklist. Now called Carbon Black Enterprise Protection, it is the base of the endpoint security architecture that Carbon Black provides.	✓ CrowdStrike provides the capability to blacklist false negatives and whitelist false positives, giving administrators the power to override dispositions set by Falcon.	✓ Cylance provides the capability to blacklist false negatives and whitelist false positives, giving administrators the power to override dispositions set by Cylance.
Software vulnerabilities	✓ View the number and severity of vulnerable applications, and how many endpoints the application has been seen on within the environment. Link vulnerabilities for each application to the associated CVE entries.	✗ Needs to integrate with IBM BigFix to provide hosts with vulnerabilities related to CVE	✗ No way to specifically search for CVEs related to hosts on the network. Falcon uses indicators of attack (IoA) to detect exploits on a system. CVEs are located within the research information on the system.	✗ No way to specifically search for CVEs related to hosts on the network.
Integrated advanced threat protection (attack detonation)	✓ AMP for Endpoints employs built-in sandboxing capabilities, plus event correlations, more than 1200 IoCs, billions of malware artifacts, and easy-to-understand threat scores.	✗ By itself, Carbon Black does not offer a closed-loop ATP. Carbon Black may integrate with other vendors such as FireEye and Palo Alto Networks with separate licensing, support, and management.	Limited CrowdStrike does not have a sandbox, but instead uses machine learning, exploit blocking, indicators of attack (IoA), and blacklisting and whitelisting to block malware along with exploits running in memory.	✗ Cylance is focused on antivirus and employs algorithms as its only detection method. The efficacy is derived from the currency of the math model deployed to individual clients. Depending on the model updates, some clients may detect a virus and some may not. Cylance does not possess the ability to detect highly evasive and fileless malware.
Sandbox-aware malware	✓ Because AMP Threat Grid uses a proprietary analysis mechanism and 100 other anti-evasion techniques, it is virtually undetectable by malware trying to avoid analysis and sandboxing.	Limited Carbon Black does not employ its own ATP or sandbox. It must integrate with Palo Alto Networks, FireEye, or others to provide malware detonation capabilites. None of the third-party integrations can detect ATP or sandbox-aware malware.	Limited CrowdStrike collects both static file data and behavioral data as the file runs, sends this data to the cloud, and through machine learning gives the file a score that indicates how likely the file is to be malicious. If it has a known behavioral capability, it will prevent the file from causing harm, but it does not remove the file. If it does not have an indicator (anti-exploit), then the asset may be at risk (action not blocked). If CrowdStrike gets disabled or removed, the asset is at risk because the previous malware code still resides on the asset.	✗ Cylance is focused on antivirus and employs algorithms as its only detection method. The efficacy is derived from the currency of the math model deployed to individual clients. Depending on the model updates, some clients may detect a virus and some may not. Cylance does not possess the ability to detect highly evasive and fileless malware

	Cisco AMP for Endpoints	Carbon Black Endpoint Security	CrowdStrike Falcon	CylancePROTECT
Response				
Malware remediation	✓ Automatically quarantines files deemed malicious and continuously analyzes activity. If an unknown file disposition changes, the target file will be quarantined.	Limited Carbon Black can remediate malware, but it depends on if you have CarbonBlack Defense, CarbonBlack Response, CarbonBlack Protection, or the whole platform.	Limited If CrowdStrike Falcon determines a known behavioral capability, it will prevent the file from causing harm, but it does not remove the file.	✓ The primary focus is on prevention. Cylance does have the ability to quarantine files that were previously marked as clean by the math model.
Malware gateway determination	✓ Exposes the entrypoint for malware and other files to aid responders in quickly assessing root cause and implementing proper enforcement against further instances.	Limited Only with integration point to third-party solution.	✓ Falcon can be used to determine the root cause of the incident.	✗ No capability to determine the root cause.
Custom detection	✓ Helps administrators quickly enforce full protection against questionable files and targeted attacks across both endpoint and network control planes, based on endpoint activity.	✓ Custom detection and blocking can be done by adding custom file hashes.	✓ Custom detection and blocking can be done by adding custom file hashes.	✓ Custom detection and blocking can be done by adding custom file hashes.
File search and fetch	✓ Enables administrators to hunt for any questionable file in an organization, see the dispersion through an installed base, and pull the file off any endpoint for further forensics and analysis.	✓ Files can be searched for and fetched from the endpoint.	Limited Files can be searched for but not fetched.	✗ No search.
Vulnerable application visibility	✓ Exposes the vulnerable applications in an environment, aiding administrators and responders in better instructing and informing the patch management process.	✗ Does not report known vulnerabilities if they exist on the endpoint alone; needs integration with IBM BigFix.	✗ Does not report known vulnerabilities if they exist on the endpoint.	✗ Does not report known vulnerabilities if they exist on the endpoint.

DID YOU KNOW?

The average cost of a breach is

$1.57 million

Learn more

	Cisco AMP for Endpoints	Carbon Black Endpoint Security	CrowdStrike Falcon	CylancePROTECT
Architecture				
Operating system support	Many Windows (XP or later), Mac OS, Linux, and Android	Many Windows, Mac OS, and Linux	Dual Windows and Mac OS	Singular Machine learning available only on Windows, Mac using SHA256 checks
Deployment model	Both Offered as a pure cloud or on-premises offering.	Both Depending on the product, it is on premises or in the cloud.	Singular Deploys only in the cloud; no on-premises installations for private sector at this time.	Singular Deploys only in the cloud; no on-premises installations.
Offline support	✓ TETRA and ClamAV provide rootkit detection and offline protection.	✓ Carbon Black provides offline support with CB Defense	✓ Falcon will continue to run when the host is not connected to a network.	✓ 85% efficacy offline.
Closed-loop detection, integration with other platforms	✓ Integrates with Cisco Firepower NGIPS, Cisco ISE, and other AMP platforms, such as AMP on Email and Web Security.	Limited Open API. Can ingest common scripting languages. Integrates with solutions from Palo Alto Networks, Check Point, Blue Coat, Cyphort, Fidelis, Damballa, Splunk, Red Canary, and others.	✓ Falcon API and Falcon Streaming API for third parties.	✓ CylanceProTECT API for data export and CylanceV for product integration.
Threat Intelligence				
Unique malware samples per day	1.5 million Talos processes ~1.5 million unique malware samples every day. Visit talosintel.com for more information.	200,000 The Cb Collective Defense Cloud contains reputation scores on more than 8 billion files, adding approximately 200,000 per day, while also using threat intelligence from more than 20 threat partners to distinguish good software and binaries from malicious ones.	Not disclosed	~500,000 Cylance sees about 450-500,000 bad samples per day
Threats blocked per day	20 billion 20 billion threats blocked per day from hundreds of billions of events viewed.	Not disclosed	Not disclosed CrowdStrike claims to view 30 billion total events per day (clean, unknown, and malicious), of which it is assumed that several million threats are blocked each day.	Not disclosed
Email messages scanned per day	600 billion Of the 600 billion scanned, more than 85% are spam. AMP endpoint directly benefits from AMP for Email through the sharing of intellignece within the AMP everywhere architecture. Once seen anywhere, on any vector, instantly protect everywhere, across all vectors.	✗ Carbon Black does not participate in email vectoring.	✗ CrowdStrike does not participate in email vectoring.	✗ Cylance does not participate in email vectoring.
Web requests monitored per day	16 billion For perspective, Google processes 3.5 billion searches per day. This means that Talos sees 78% more web activity than Google sees searches. AMP endpoint directly benefits from AMP for Web and DNS through the sharing of intelligence within the AMP everywhere architecture. Once seen anywhere, on any vector, instantly protect everywhere, across all vectors.	✗ Carbon Black does not participate in web vectoring.	✗ CrowdStrike does not participate in web vectoring.	✗ Cylance does not participate in web vectoring.

	Cisco AMP for Endpoints	Carbon Black Endpoint Security	CrowdStrike Falcon	CylancePROTECT
Threat Intelligence (continued)				
URLs seen and processed per day	120 billion Through the Talos integration of the Umbrella platform, Talos can see over 120 billion Internet-based URLs every day via DNS request. For perspective, as of January 2017, the Internet is powered by 1.8 billion websites (Netcraft). Cisco Talos and Umbrella Threat Intelligence sees the entire active Internet ~51 times each day.	✗ Carbon Black does not participate in web vectoring.	✗ CrowdStrike does not participate in web vectoring.	✗ Cylance does not participate in web vectoring.
Automated intelligence feeds	✓ Configurable and exchanged with all Cisco Security products: ATP Gateway, AMP Endpoint, Network-based ATP, NGFW, NGIPS, Email Security + AMP, Web Security + AMP, DNS security, Cloud Security components, Threat Intelligence Director(s), etc.	✓ Configurable and exchanged with endpoint product.	✓ Configurable and exchanged with endpoint product.	✓ Configurable and exchanged with endpoint product.
Threat intelligence sharing	✓ Data sharing with 100s of partners, customers, and providers through Aegis, Crete, and Aspis programs. Cisco is a founding member of the Cyber Threat Alliance.	✗ Carbon Black does not share its threat intelligence with others.	✗ CrowdStrike does not share its threat intelligence with others.	✗ Cylance does not share its threat intelligence with others but does belong to VirusTotal.

DID YOU KNOW?

Cisco Talos consists of over 250 researchers, making it one of the largest threat intelligence organizations in the world.

See what they do

	Cisco AMP for Endpoints	Carbon Black Endpoint Security	CrowdStrike Falcon	CylancePROTECT
Integration				
Integrations	✓ Rest API	✓ Open API. Can ingest common scripting languages. Integrates with solutions from Palo Alto Networks, Check Point, Blue Coat, Cyphort, Fidelis, Damballa, Splunk, Red Canary, and others.	✓ Falcon API and Falcon Streaming API for third parties.	✓ Open API for integration from several products. Key OEM partners also leverage CylanceProtect technology within their own products. ForcePoint, A10, Outlier API, and BRICATA.