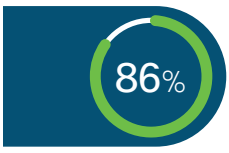
# Compare Next-Generation Endpoint Security

| | Cisco AMP for Endpoints | Carbon Black Endpoint Security | CrowdStrike Falcon | CylancePROTECT with CylanceOptics |
|---|---|---|---|---|
| **Detection** | | | | |
| Layers of integrated detection techniques | 15<br>Cisco AMP for Endpoints employs a detection lattice: exploit prevention uses deception technology to protect applications in memory and provides script and memory control. System Process Protection monitors all processes. AMP offers a 1:1 SHA matching engine (public, private, or hybrid); Tetra antivirus; Threat Grid sandboxing; ETHOS fuzzy finger-printing; 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<br>Carbon Black employs whitelisting, machine learning, behavioral analytics, and next-generation antivirus. | 4<br>CrowdStrike Falcon employs cloud-based antivirus and indicators of compromise (IOC) detection, indicators of attack (IOA, for fileless malware), machine learning, blacklists and whitelists, and known-exploit blocking. | 4<br>Cylance employs Script Control, Memory Defense, Execution Control, and Device Control. 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. Anything repackaged with MPress will be detected as malicious. |
| Endpoint agents required | 1<br>One single, lightweight AMP for Endpoints agent and its UI (Cisco Threat Response) provide all capabilities listed in this chart. Unless otherwise noted, no other Cisco product is required to meet listed functionality. | 2<br>As of the date of this comparison, two endpoint agents are required to achieve all functionality described here. | 2<br>As of the date of this comparison, two endpoint agents are required to achieve all functionality described here. | 2<br>As of the date of this comparison, two endpoint agents are required to achieve all functionality described here. |
| Continuous analysis and retrospective detection | ✓<br>AMP for Endpoints employs continuous analysis beyond the event horizon (point in time). It 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<br>Carbon Black employs continuous analysis using Cb Defense. | ✓<br>CrowdStrike Falcon offers DVR capability down to a 5-second visibility of the endpoint. | ✓<br>Cylance employs continuous analysis. |
| Device trajectory | ✓<br>Continuous. The Cisco AMP for Endpoints client and its associated UI (Cisco Threat Response) maps how hosts interact with files, including malware, 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. | ✓<br>Carbon Black has a very rich process tree for investigation and makes the investigation process visually appealing. | ✗<br>CrowdStrike does not provide device trajectory but 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<br>Using CylanceProtect and your own security information and event management (SIEM) tools, Cylance can augment visibility using Focus View, Intelligent Query, and locating patient zero. |
| Multiple detection measures | ✓<br>Cisco AMP uses several methods of detection, including fuzzy fingerprinting (ETHOS), machine learning, AI, dynamic file analysis (Threat Grid), and 1:1 SHA matching, all supported by Talos, the world's largest threat intelligence group. | ✓<br>Carbon Black detects 150 behaviors but has no trajectory and no behavioral IOCs. Events are based on signatures, vulnerabili-ties, and point-in-time analysis. | ✓<br>Falcon can detect 120 local event types streamed in real time and uses hash and behavioral blocking, credential theft and privilege escalation, boot sector, process, stack, and other techniques. | ✓<br>Cylance uses a machine learning model that uses 2.68 million features and attributes. This is suplemented with SHA-256 checks. |

| | Cisco AMP for Endpoints | Carbon Black Endpoint Security | CrowdStrike Falcon | CylancePROTECT with CylanceOptics |
|---|---|---|---|---|
| **Detection (continued)** | | | | |
| Dynamic file analysis | ✓ ThreatGrid is fully integrated into AMP for Endpoints and is not a separate product. This automated detonation engine observes, deconstructs, and analyzes using several methods. It's effectively impervious to sandbox-aware malware and all other forms of runtime detection by malware – some of which haven't even been employed by malware yet. | ✗ Needs an integration point with a partner for sandboxing technology. Vendors like FireEye and Palo Alto can provide functionality for Carbon Black. | Limited Falcon Sandbox offers cloud and on-premises deployments but does not integrate with supporting systems such as NGIPS, BDS, or BPS. | ✗ Cylance does not believe that sandboxes work and focuses on deriving its own artifacts. |
| File analysis deployment model | ✓ Both on premises and cloud. Threat Grid detonation technology is fully integrated in AMP for Endpoints. File analysis can also be separated into an on-premises solution for customers who have cloud restrictions. Because AMP Threat Grid uses a proprietary analysis mechanism and 100 other antievasion techniques, it is completely 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. | Limited Falcon Sandbox offers cloud and on-premises deployments but does not integrate with supporting systems such as NGIPS, BDS, or BPS. | ✗ Uses mathematics to derive its own artifacts. |
| API support | ✓ Use RESTful API access to pull events, indicators of compromise (IOCs), and device data. You can script and customize the API to fit the environment. | ✓ Open API. | ✓ Open API. | ✓ RESTful API for integration from several products. Key OEM partners also leverage CylanceProtect technology within their own products, including ForcePoint, A10, Outlier API, and Bricata. |
| File trajectory | ✓ AMP for Endpoints uses the Cisco Threat Response UI to help you gain visibility into the scope of an attack or 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. No additional Cisco product is required. | Limited Carbon Black's scope focuses on local host processes and does not track from the aspect of the file and where it has traveled. | Limited CrowdStrike focuses on local host processes, using indicators of attack, and does not track from the aspect of a file and where it has traveled. Due to visibility gaps with Linux, MacOS, and mobile OSs, a complete picture is hard to determine. | Limited Uses pivot to see locations of a hash or file. CylanceOptics provides additional intelligence. |




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 with CylanceOptics |
|---|---|---|---|---|
| **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 applications 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 ability to blacklist false negatives and whitelist false positives, giving administrators the power to override dispositions set by Falcon. | ✓ Cylance offers whitelisting for aspects of the product that need it: memory protection, script control, and threats. It also offers blacklisting for those scenarios when needed. |
| Software vulnerabilities | ✓ With AMP you can view the number and severity of vulnerable applications, and how many endpoints the application has been seen on within the environment. You can link vulnerabilities for each application to the associated Common Vulnerabilities and Exposures (CVE) entries. | ✗ Carbon Black needs to integrate with IBM BigFix to provide hosts with vulnerabilities related to CVE. | ✗ There's 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 in the research information on the system. | ✗ Cylance claims to know what is bad even before it comes out using math models. Even with a Cylance math model over a year--and, in some cases, a math model over two years old--Cylance claims to block 100% of threats. This logic makes visibility of vulnerable software irrelevant. NSS Labs AEP results provide a great view of how this 92% prevention actually works: 84.6% catch rate for unknown threats and 54% for vulnerable software. |
| Integrated advanced threat protection (attack detonation) | ✓ AMP for Endpoints employs built-in sandboxing capabilities (via its full integration of ThreatGrid), plus event correlations, more than 1200 IoCs, billions of malware artifacts, and easy-to-understand threat scores. AMP Endpoint is a full AV client as well and meets PCI/HIPAA audit requirements as an AV replacement. | ✗ 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 Falcon Sandbox includes 700 generic behavior indicators. | ✗ Cylance is focused solely on predictive, pre-execution prevention. |
| Sandbox-aware malware | ✓ AMP uses a proprietary analysis mechanism and 100 other antievasion techniques. It is undetectable by malware trying to avoid analysis and sandboxing. | Limited Carbon Black does not employ its own advanced threat protection (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 Falcon Sandbox cannot detect sandbox-aware malware. 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 the file has a known behavioral capability, CrowdStrike will prevent the file from causing harm, but it does not remove it. If the file 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 does not believe that sandboxes work and focuses on deriving its own artifacts. Cylance employs Script Control, Memory Defense, Execution Control, and Device Control. 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. Anything benign repackaged with Mpress will be detected as malicious. |

DID YOU KNOW?

The average cost of a breach is

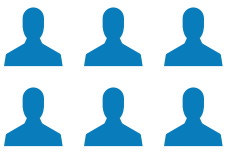
**$1.57 million**

Learn more

| | Cisco AMP for Endpoints | Carbon Black Endpoint Security | CrowdStrike Falcon | CylancePROTECT with CylanceOptics |
|---|---|---|---|---|
| **Response** | | | | |
| Malware remediation | ✓ Automatically quarantines files deemed malicious and continuously analyzes activity. If an unknown file disposition changes, the target file is quarantined. | Limited. Carbon Black can remediate malware, but the functionality depends on whether you have Cb Defense, Cb Response, Cb Protection, or the whole platform. | Limited. If CrowdStrike Falcon determines a known behavioral capability, it can 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 entry point for malware and other files to help responders quickly assess root cause and implement 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. | ✓ Determines root cause with CylanceOptics. Intelligent Query can be used to augment results. |
| 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 | ✓ AMP with the Cisco Threat Response UI lets administrators 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. | ✓ Built-in search and pivot of machines, hashes, and more. CylanceOptics Intelligent Query offers the ability to hunt throughout the environment and take action. |
| Vulnerable application visibility | ✓ AMP dynamically exposes the vulnerable applications in an endpoint 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; requires 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. |
| Integrated DNS-level protection | ✓ Exposes malicious domains associated with malware, giving users the ability to dynamically block access through Umbrella integration. Prevents command and control callbacks for data exfiltration, and stops execution of ransomware encryption. Provides up-to-minute threat data and historical context about domains, IPs, and file hashes for faster investigation. | Limited. Infoblox services are required, which provides domain reputation to Carbon Black for correlation and enforcement. | Limited. Falcon DNS requires Falcon Overwatch, which is delivered as a managed service where DNS monitoring and alerting takes place. | ✗ Lacks DNS-level protection. Cylance is focused on stopping threats that reach the endpoint rather than preventing threats from entering the network in the first place. |
| Extensive threat information across threat vectors | ✓ AMP is directly tied to Talos Threat Intelligence, so AMP can immediately see anything Talos sees. AMP can instantly defend the endpoint against threats seen by your own or another organization's firewall, web URL, DNS entry, other endpoint, or email gateway. Because AMP is built on the Unity framework, AMP has a global view of threats across all threat vectors. | ✗ Lacks information from different threat vectors such as firewalls, endpoints, and email gateways. | ✗ Lacks information from different threat vectors such as firewalls, endpoints, and email gateways. | ✗ Lacks information from different threat vectors such as firewalls, endpoints, and email gateways. Malicious URLs and malicious domains are not Cylance's concern. |

| | Cisco AMP for Endpoints | Carbon Black Endpoint Security | CrowdStrike Falcon | CylancePROTECT with CylanceOptics |
|---|---|---|---|---|
| **Architecture** | | | | |
| Operating system support | ✓ Windows (XP or later), MacOS, Linux, Android, and iOS. Cisco AMP is the only antimalware software available for iOS, as part of the Apple-Cisco API partnership. | ✓ Windows, MacOS, and Linux. | ✓ Windows, MacOS, and Linux. | Limited The primary focus of the rich toolset is on Windows. MacOS and Linux do have math models. Mobile OSs are not supported. |
| Deployment model | Both AMP is 100% managed in the cloud, reducing TCO. It's also offered as on-premises solution for organizations with cloud restrictions, such as the U.S. government. | Both Depending on the product, it is on premises or in the cloud. | Cloud only Deploys only in the cloud; no on-premises installations for the private sector. | Cloud only Deploys only in the cloud. There are no on-premises installations, but at the time of this analysis, one for U.S. government is on the roadmap. |
| Offline support | ✓ Offline protection is constant with Exploit Prevention and the AMP engine. | ✓ Carbon Black provides offline support with Cb Defense. Carbon Black scored 92.3% in block rate for offline threats in the latest NSS Labs AEP test. | ✓ Falcon continues to run when the host is not connected to a network; however, the efficacy of this function has never been publicly proven. | ✓ Cylance is built to run fully offline using locally installed math models. CylanceProtect with CylanceOptics scored 85% in offline efficacy in the latest NSS Labs AEP test. |
| Closed-loop detection; integration with other platforms | ✓ Integrates with Cisco Firepower NGFW, Firepower NGIPS, ISE, and other AMP platforms, such as AMP for Email and Web Security. This integration is relevant when organizations own several platforms, but owning several platforms is not required to fulfill any of the funtionality of AMP for Endpoints referenced in this comparison. | 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 approximately 1.5 million unique malware samples every day. | 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 450,000 to 500,000 bad samples per day. There's no confirmation whether these are unique or total. |
| Threats blocked per day | 20 billion AMP for Endpoints blocks 20 billion threats per day from hundreds of billions of events viewed. | Not disclosed | Not disclosed CrowdStrike claims to view 100 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 | 400 billion Of the 400 billion emails scanned, more than 85% are spam. AMP for Endpoints directly benefits from AMP for Email through the sharing of intelligence in the AMP Unity architecture. Once a threat is seen anywhere, on any vector, you're instantly protected 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. The company claims that every customer has some type of email gateway; Cylance focuses exclusively on the endpoint. |

| | Cisco AMP for Endpoints | Carbon Black Endpoint Security | CrowdStrike Falcon | CylancePROTECT with CylanceOptics |
|---|---|---|---|---|
| **Threat Intelligence (continued)** | | | | |
| Web requests monitored per day | 16 billion<br>Google processes 3.5 billion searches per day. This means that Talos sees 78% more web activity than Google sees searches. AMP for Endpoints directly benefits from AMP for Web and DNS through the sharing of intelligence within the AMP Unity architecture. Once a threat is seen anywhere, on any vector, you're instantly protected everywhere, across all vectors. | ✗<br>Carbon Black does not participate in web vectoring. | ✗<br>CrowdStrike does not participate in web vectoring. | ✗<br>Cylance does not participate in web vectoring. The company claims that it is futile to analyze web requests, and that knowing about malicious URLs is useless for protecting endpoints that can run the Cylance toolset. IoS, Android and most Linux systems are out of scope for Cylance tools. |
| URLs seen and processed per day | 125 billion<br>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 about 51 times each day. | ✗<br>Carbon Black does not participate in web vectoring. | ✗<br>CrowdStrike does not participate in web vectoring. | ✗<br>Cylance does not participate in web vectoring. |
| Automated intelligence feeds | ✓<br>Intelligence feeds are configurable and exchanged with all Cisco security products: advanced threat protection gateways, AMP for Endpoints, network-based advanced threat protection, NGFW, NGIPS, Email Security with AMP, Web Security with AMP, DNS security, Cloud Security components, Threat Intelligence Director, and more. | ✓<br>Configurable and exchanged with endpoint product. | ✓<br>Configurable and exchanged with endpoint product. | ✓<br>Configurable and exchanged with endpoint product. Cylance claims that intelligence feeds are not required due to the superiority of its AI/machine-learning model. |
| Threat intelligence sharing | ✓<br>Cisco shares data with hundreds of partners, customers, and providers through Aegis, Crete, and Aspis programs. Cisco is a founding member of the Cyber Threat Alliance. | ✗<br>Carbon Black does not share its threat intelligence with others. | ✗<br>CrowdStrike does not share its threat intelligence with others. | ✗<br>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 with CylanceOptics |
|---|---|---|---|---|
| **Integration** | | | | |
| Integrations | ✓ | ✓ 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. | ✓ RESTful API for integration from several products. Key OEM partners also leverage CylanceProtect technology in their own products, including ForcePoint, A10, Outlier API, and Bricata. |
| **Other Services** | | | | |
| Cybersecurity insurance | ✓ The Cisco, Apple, Allianz, and Aon collaboration for cyberinsurance is an industry first. Collectively, we provide a holistic framework to decisively act on cyberrisk, giving organizations streamlined access to the right tools and cyberinsurance to strengthen security, reduce risk, and cover the complete cost of a breach if needed. | ✗ None offered. | Limited Up to $1 million breach prevention warranty with Falcon EPP " in the event that a customer using EPP Complete experiences a breach within their protected environment that EPP Complete should have prevented." Thus, if you experience a breach and Falcon cannot detect it, there is no coverage. | ✗ None offered. |
| Threat intelligence sharing | ✓ Cisco Active Threat Analytics provides 24x7 threat analysis and incident monitoring, Cisco Collective Security Intelligence Enrichment (including Talos), log and telemetry collection, metadata extraction, rules-based analytics, full packet capture, high-touch incident support, a customer portal, and proactive threat hunting. | Limited Cb ThreatSight offers alert validation by analyzing and prioritizing alerts; trend monitoring; and context for alerts for root-cause analysis. | Limited Falcon Overwatch provides 24/7 operations and alert prioritization. | Limited Managed Prevention and Response adds varying levels of monitoring and threat intelligence (offered 24/7), threat identification, and alerting. |