엔드포인트 보안 솔루션 비교

Cisco에 대한 최근 서드파티 연구 조사 결과

가장 빠른 탐지 속도

100% 보안 침해 탐지율

출처: 2016 NSS Labs BDS 테스트 보고서

보고서 전문 보기

	Cisco AMP for Endpoints	Carbon Black Endpoint Security	CrowdStrike Falcon	CylancePROTECT
탐지				
통합된 탐지 기술 수	14 Cisco AMP Threat Grid에서는 정적/동적 분석 및 행동 휴리스틱(heuristics) 기술을 사용합니다. 외부 가상 머신을 가동하여 샌드박스 인식형 악성코드를 차단합니다. 여러 엔진을 통해 각 파일의 위험 여부를 평가하고 판정합니다. 1:1 SHA 매칭, 퍼지 핑거프린팅(ETHOS), 머신 러닝(SPERO), IOC, 디바이스 플로우 상관관계 분석, TETRA, ClamAV, 명령줄 캡처, 위협 추적 등의 기법을 사용합니다.	4 Carbon Black은 화이트리스팅, 머신 러닝, 행동 분석, 차세대 안티바이러스 기술을 사용합니다.	4 CrowdStrike Falcon은 공격 지표(파일리스 악성코드), 머신 러닝, 블랙리스트/화이트리스트, 알려진 익스플로잇 차단 기술을 사용합니다.	1 Cylance는 알고리즘을 유일한 탐지 방법으로 사용합니다. 개별 클라이언트에 구축된 수학 모델의 현재성에 효율성이 좌우됩니다. 모델 업데이트에 따라 일부 클라이언트는 바이러스를 탐지할 수도, 탐지하지 않을 수도 있습니다.
지속적 분석과 회귀적 탐지	✓ Cisco AMP for Endpoints 솔루션은 이벤트 호라이즌(특정 시점)을 넘어 지속적인 분석을 활용하고 처음에는 정상으로 나타나거나 초기 방어를 우회하고 나중에 악성으로 식별되는 지능형 악성코드를 회귀적으로 탐지, 경고, 추적, 분석 및 치료할 수 있습니다.	제한적 Carbon Black은 이벤트 호라이즌(특정 시점)을 넘어 지속적인 분석을 활용하고 처음에는 정상으로 나타나거나 초기 방어를 우회하고 나중에 악성으로 식별되는 지능형 악성코드를 회귀적으로 탐지, 경고, 치료할 수 있습니다. Cb Defense(별도의 제품)도 필요합니다.	✓ CrowdStrike Falcon은 DVR 기능을 통해 엔드포인트에 대한 5초 가시성까지 제공합니다. Falcon은 이벤트 호라이즌(특정 시점)을 넘어 지속적인 분석을 활용하고 처음에는 정상으로 나타나거나 초기 방어를 우회하고 나중에 악성으로 식별되는 지능형 악성코드를 회귀적으로 탐지, 경고, 치료할 수 있습니다.	✓ Cylance는 이벤트 호라이즌(특정 시점)을 넘어 지속적인 분석을 활용하고 처음에는 정상으로 나타나거나 초기 방어를 우회하고 나중에 악성으로 식별되는 지능형 악성코드를 회귀적으로 탐지, 경고, 치료할 수 있습니다.
디바이스 경로 분석	지속적 Cisco AMP는 호스트가 파일(악성코드 파일 포함)과 상호 작용하는 방법을 엔드포인트 환경 전체에서 매핑합니다. 이 방법을 통해 파일 전송이 차단되거나 파일이 격리되었는지를 확인할 수 있습니다. 위협의 범위를 파악하고 아웃브레이크 제어를 제공하며 최초 감염자를 찾아낼 수 있습니다.	✓ 조사를 위해 많은 내용을 담은 프로세스 트리를 제공합니다. 그래프의 시각 효과를 높이는 요소가 많습니다.	✗ CrowdStrike는 디바이스 경로 분석을 제공하지 않지만 속성 추적은 가능합니다. 누가 악성코드를 개발했는지 밝히는 게 중요하지만, 대개는 재발을 막는 수준에 머무릅니다.	제한적 Cylance Optics(별도의 제품)가 필요합니다.

	Cisco AMP for Endpoints	Carbon Black Endpoint Security	CrowdStrike Falcon	CylancePROTECT
탐지(계속)				
탐지 수단	**다수** Cisco AMP는 퍼지 핑거프린팅(ETHOS), 머신 러닝(SPERO), 동적 파일 분석(Threat Grid), 1:1 SHA 매칭 등 여러 탐지 방식을 사용하며 모두 Talos에서 지원합니다.	**다수** 150가지 행동. 경로 분석은 없습니다. 행동 IoC가 없습니다. 이벤트는 시그니처, 취약점, 특정 시점 분석을 기반으로 합니다.	**다수** 120개 로컬 이벤트 유형의 실시간 스트리밍, 해시 및 행동 차단, 인증 정보 도용 및 권한 에스컬레이션, 부트 섹터, 프로세스, 스택, 기타 기술을 사용합니다.	**단일** Cylance는 1백만 가지 이상의 기능 및 속성을 사용하는 머신 러닝 모델을 주로 사용합니다. SHA256 검사로 이를 보완합니다.
동적 파일 분석	**Threat Grid** 자동화된 디토네이션 엔진이 여러 기법을 통해 관찰, 분해, 분석을 수행합니다. 샌드박스 인식형 악성코드를 통과시키지 않습니다.	✗ 샌드박싱 기술을 위해 파트너와의 통합 지점이 필요합니다.	✗ 통합 지점이 없습니다. 분류된 네트워크의 외부에 온프레미스 시스템을 구축하지 않습니다. NGIPS, BDS, BPS와 같은 지원 시스템과 통합하지 않습니다.	✗ 통합 지점이 현재는 없습니다.
파일 분석 구축 모델	**모두** Threat Grid 샌드박스가 AMP for Endpoints 솔루션 내부에 완전히 통합됩니다. 파일 분석도 온프레미스 솔루션이 될 수 있습니다. AMP Threat Grid는 전용 분석 메커니즘 및 100가지의 기타 우회 차단 기술을 사용하므로 분석 및 샌드박싱을 회피하려는 악성코드도 이를 탐지하지 못합니다. Threat Grid는 호스트, 네트워크, 정적/동적 분석, 실행 전/후 마스터 부트 레코드 분석 등 가장 다양한 분석 기술을 사용합니다.	✗ 샌드박싱 기술을 위해 파트너와의 통합 지점이 필요합니다.	✗ 통합 지점이 없습니다. 모든 파일 분석에 머신 러닝으로 충분하다고 주장합니다.	✗ 통합 지점이 없습니다.
API 지원	✓ 이벤트, IOC, 디바이스 데이터를 풀링하는 데 REST API 액세스를 사용합니다. 환경에 맞게 스크립트를 작성하고 API를 맞춤화할 수 있습니다.	✓ 개방형 API	✓ 개방형 API	**일일 보고서** 위협, 디바이스, 이벤트, 지표, 해제, 정책의 범주에 대한 일일 보고서를 CSV 형식으로 내보낼 수 있습니다.
파일 경로 분석	✓ 보안 침해의 범위(해당 악성코드에 감염된 엔드포인트 수)를 파악합니다. 최초 감염자, 즉 해당 환경에서 악성코드가 가장 먼저 나타난 컴퓨터, 그 계보, 호스트 간 이동 경로를 찾아냅니다.	**제한적** 범위가 로컬 호스트 프로세스에 집중되며 "파일" 및 그 이동 경로의 관점에서 추적하지 않습니다.	**제한적** 공격 지표를 사용하여 범위가 로컬 호스트 프로세스에 집중되며 "파일" 및 그 이동 경로의 관점에서 추적하지는 않습니다. Linux, Mac, 모바일에 대한 가시성 격차로 인해 거시적 관점에서 전체 상황을 파악하기가 어렵습니다.	✗ 현재는 지원되지 않습니다. Cylance Optics에서 제공될 가능성이 있습니다.

알고 계십니까?

23%가 넘는 조직이 2011년부터 취약점을 갖고 있었습니다.

그중 하나가 되지 마십시오

(출처: 2016년 중기 사이버 보안 보고서)

	Cisco AMP for Endpoints	Carbon Black Endpoint Security	CrowdStrike Falcon	CylancePROTECT
탐지				
화이트리스트/ 블랙리스트	✓ AMP for Endpoints에서는 미탐을 블랙리스트에, 오탐을 화이트리스트에 포함시켜 Cisco Talos에서 설정한 분류를 재정의할 수 있습니다.	✓ Bit9은 화이트리스트/블랙리스트 선두 주자 중 하나입니다. 지금은 Carbon Black Enterprise Protection으로 불리며 Carbon Black이 제공하는 엔드포인트 보안 아키텍처의 기초입니다.	✓ CrowdStrike는 미탐을 블랙리스트에, 오탐을 화이트리스트에 포함시켜 관리자가 Falcon에서 설정한 분류를 재정의할 수 있는 기능을 제공합니다.	✓ Cylance는 미탐을 블랙리스트에, 오탐을 화이트리스트에 포함시켜 관리자가 Cylance에서 설정한 분류를 재정의할 수 있는 기능을 제공합니다.
소프트웨어 취약점	✓ 취약한 애플리케이션의 수 및 심각도, 해당 환경에서 이 애플리케이션이 확인된 엔드포인트 수를 파악합니다. 각 애플리케이션의 취약점을 관련 CVE 항목과 연결합니다.	✗ IBM BigFix와 통합해야 CVE 관련 취약점 정보를 호스트에 제공할 수 있습니다.	✗ 네트워크에서 호스트와 관련된 CVE를 구체적으로 검색할 방법이 없습니다. Falcon은 시스템에 대한 익스플로잇을 탐지하는 데 IoA(indicator of attack)를 사용합니다. CVE는 시스템의 연구 정보 내에 있습니다.	✗ 네트워크에서 호스트와 관련된 CVE를 구체적으로 검색할 방법이 없습니다.
통합형 ATP(advanced threat protection)(공격 디토네이션)	✓ 내장된 샌드박싱 기능, 이벤트 상관관계 분석, 1,200여 가지의 IoC, 수십억 개의 악성코드 아티팩트, 이해하기 쉬운 위협 점수를 활용할 수 있습니다.	✗ Carbon Black 자체는 폐쇄 루프형 ATP를 제공하지 않습니다. Carbon Black은 FireEye, Palo Alto Networks 등과 같은 다른 벤더와 통합할 수 있으나 별도의 라이선스, 지원, 관리가 필요합니다.	**제한적** CrowdStrike는 샌드박스가 없지만 머신 러닝, 익스플로잇 차단, IoA, 블랙리스팅/화이트리스팅을 사용하여 메모리에서 실행 중인 익스플로잇과 함께 악성코드를 차단할 수 있습니다.	✗ Cylance는 안티바이러스에 중점을 두며 알고리즘을 유일한 탐지 방법으로 사용합니다. 개별 클라이언트에 구축된 수학 모델의 현재성에 효율성이 좌우됩니다. 모델 업데이트에 따라 일부 클라이언트는 바이러스를 탐지할 수도, 탐지하지 않을 수도 있습니다. Cylance는 고도로 우회적인 파일리스 악성코드를 탐지하는 기능이 없습니다.
샌드박스 인식형 악성코드	✓ AMP Threat Grid는 전용 분석 메커니즘 및 100가지의 기타 우회 차단 기술을 사용하므로 분석 및 샌드박싱을 회피하려는 악성코드도 이를 탐지하지 못합니다.	**제한적** Carbon Black은 자체 ATP 또는 샌드박스가 없습니다. Palo Alto Networks, FireEy 또는 기타 솔루션과 통합해야 악성코드 디토네이션 기능을 제공할 수 있습니다. ATP 또는 샌드박스 인식형 악성코드를 탐지할 수 있는 서드파티 통합이 없습니다.	**제한적** CrowdStrike는 파일이 실행될 때 고정 파일 데이터 및 행동 데이터를 모두 수집하고 이를 클라우드에 보내 머신 러닝을 통해 파일이 악성일 가능성을 나타내는 점수를 부여합니다. 알려진 행동 기능이 있을 경우 파일이 더 이상 피해를 주지 않도록 차단하지만 파일을 제거하지는 않습니다. 지표(익스플로잇 차단)가 없을 경우 해당 자산은 위험한 상태가 됩니다(작업이 차단되지 않음). CrowdStrike가 비활성화되거나 제거될 경우 이전 악성코드가 계속 자산에 남아 있으므로 해당 자산은 위험한 상태가 됩니다.	✗ Cylance는 안티바이러스에 중점을 두며 알고리즘을 유일한 탐지 방법으로 사용합니다. 개별 클라이언트에 구축된 수학 모델의 현재성에 효율성이 좌우됩니다. 모델 업데이트에 따라 일부 클라이언트는 바이러스를 탐지할 수도, 탐지하지 않을 수도 있습니다. Cylance는 고도로 우회적인 파일리스 악성코드를 탐지하는 기능이 없습니다.

	Cisco AMP for Endpoints	Carbon Black Endpoint Security	CrowdStrike Falcon	CylancePROTECT
대응				
악성코드 치료	✓ 악성으로 분류된 파일을 자동으로 격리하고 계속 활동을 분석합니다. 알 수 없는 파일 속성이 변화할 경우 대상 파일을 격리합니다.	**제한적** Carbon Black은 악성코드를 치료할 수 있으나 Cb Defense, Cb Response, Cb Protection 또는 전체 플랫폼이 있어야 합니다.	**제한적** CrowdStrike Falcon은 알려진 행동 기능이 있을 경우 파일이 더 이상 피해를 주지 않도록 차단하지만 파일을 제거하지는 않습니다.	✓ 차단에 중점을 둡니다. Cylance는 수학 모델에 의해 정상으로 분류된 적이 있는 파일을 격리할 수 있습니다.
악성코드 게이트웨이 확인	✓ 악성코드 및 기타 파일의 진입 지점을 공개하여 대응팀이 신속하게 침입 경로를 평가하고 재발을 방지할 적합한 조치를 마련할 수 있게 합니다.	**제한적** 서드파티 솔루션과의 통합 지점이 있어야 합니다.	✓ Falcon은 사고 발생의 침입 경로를 규명하는 데 사용할 수 있습니다.	✗ 침입 경로를 규명하는 기능이 없습니다.
맞춤형 탐지	✓ 관리자가 엔드포인트 활동에 따라 엔드포인트 및 네트워크 컨트롤 플레인 전 범위에서 의심스러운 파일 및 표적 공격을 차단하는 종합적인 보호 조치를 신속하게 시행할 수 있습니다.	✓ 맞춤형 파일 해시를 추가하여 맞춤형 탐지 및 차단을 수행할 수 있습니다.	✓ 맞춤형 파일 해시를 추가하여 맞춤형 탐지 및 차단을 수행할 수 있습니다. MD5 및 SHA256이 지원됩니다.	✓ 맞춤형 파일 해시를 추가하여 맞춤형 탐지 및 차단을 수행할 수 있습니다.
파일 검색 및 가져오기	✓ 관리자가 조직 내에서 의심스러운 파일을 추적하고 설치 기반에서의 확산 현황을 파악하며 임의의 엔드포인트에서 파일을 수집하여 추가 포렌식 및 분석을 실시할 수 있습니다.	✓ 엔드포인트에서 파일을 검색하고 가져올 수 있습니다.	**제한적** 파일 검색은 가능하지만 가져올 수 없습니다.	✗ 검색 기능이 없습니다.
취약한 애플리케이션 가시성	✓ 해당 환경의 취약한 애플리케이션을 공개하여 관리자 및 대응 팀이 더 효과적인 지침과 정보로 패치 관리 프로세스를 지원할 수 있게 합니다.	✗ 알려진 취약점이 엔드포인트에 있더라도 독자적으로 보고할 수 없습니다. IBM BigFix와의 통합이 필요합니다.	✗ 알려진 취약점이 엔드포인트에 있더라도 보고할 수 없습니다.	✗ 알려진 취약점이 엔드포인트에 있더라도 보고할 수 없습니다.

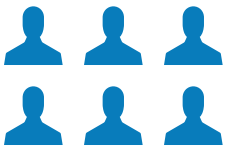
알고 계십니까?

보안 침해의 평균 비용은
157만 달러에 달합니다.

자세히 보기

	Cisco AMP for Endpoints	Carbon Black Endpoint Security	CrowdStrike Falcon	CylancePROTECT
아키텍처				
운영 체제 지원	**다수** Windows(XP 이상), Mac OS, Linux, Android	**다수** Windows, Mac OS, Linux	**듀얼** Windows, Mac OS	**단일** 머신 러닝은 Windows, Mac에서만 사용 가능, SHA256 검사 이용
구축 모델	**모두** 순 클라우드 또는 온프레미스 오퍼링으로 제공됩니다.	**모두** 제품에 따라 온프레미스 또는 클라우드에 구축됩니다.	**단일** 클라우드에서만 구축됩니다, 현재로서는 전용 구축을 위한 온프레미스 설치가 지원되지 않습니다.	**단일** 클라우드에서만 구축됩니다. 온프레미스 설치가 지원되지 않습니다.
오프라인 지원	✓ TETRA 및 ClamAV가 루트킷 탐지 및 오프라인 보호를 제공합니다.	✓ Carbon Black은 차세대 AV 기능을 제공하고자 최근 Confer를 인수했습니다.	✓ Falcon은 호스트가 네트워크에 연결되지 않더라도 계속 실행됩니다.	✓ 오프라인에서 85% 효율성을 제공합니다.
폐쇄 루프형 탐지, 다른 플랫폼과의 통합	✓ Cisco Firepower NGIPS, Cisco ISE 및 기타 AMP 플랫폼(예: AMP on Email, Web Security)과 통합됩니다.	**제한적** 개방형 API. 공통 스크립팅 언어를 수집할 수 있습니다. Palo Alto Networks, Check Point, Blue Coat, Cyphort, Fidelis, Damballa, Splunk, Red Canary 등 기타 솔루션과 통합됩니다.	✓ Falcon API 및 Falcon Streaming 서드파티용 API.	✓ 데이터 내보내기용 CylanceProTECT API, 제품 통합용 CylanceV.
위협 인텔리전스				
일일 고유 악성코드 샘플 수	**다수** Talos는 매일 최대 150만 개의 고유한 악성코드 샘플을 처리합니다. 자세한 내용은 talosintel.com을 참조하십시오.	**200,000** Cb Collective Defense Cloud는 80억 개 이상의 파일에 대한 평판 점수를 보유하고 있으며 매일 약 20만 개가 추가됩니다. 또한 20여 개 이상의 전문 파트너가 제공하는 위협 인텔리전스를 활용하면서 안전한 소프트웨어와 악성 소프트웨어의 이진을 구별합니다.	**공개되지 않음**	**공개되지 않음**
매일 차단되는 위협 수	**200억 개** 매일 수천억 개의 이벤트를 모니터링하면서 200억 개 이상의 위협을 차단합니다.	**공개되지 않음**	**공개되지 않음** CrowdStrike의 주장에 따르면 매일 총 300억 개 이상의 이벤트(정상, 미확인, 악성)를 모니터링하면서 수백만 개의 위협을 차단합니다.	**공개되지 않음**
매일 검사된 이메일 메시지 수	**6000억 개** 검사된 6,000억 개 중 85% 이상이 스팸입니다.	✗ Carbon Black은 이메일 벡터링에 참여하지 않습니다.	✗ CrowdStrike는 이메일 벡터링에 참여하지 않습니다.	✗ Cylance는 이메일 벡터링에 참여하지 않습니다.
매일 모니터링되는 웹 요청 수	**160억 개** 참고로 Google은 매일 35억 개의 검색을 처리합니다. 즉 Talos는 Google에서 확인하는 검색보다 78% 더 많은 웹 활동을 모니터링합니다.	✗ Carbon Black은 웹 벡터링에 참여하지 않습니다.	✗ CrowdStrike는 웹 벡터링에 참여하지 않습니다.	✗ Cylance는 웹 벡터링에 참여하지 않습니다.
매일 모니터링 및 처리되는 URL	**920억 개** Talos는 OpenDNS Umbrella와의 통합으로 매일 DNS 요청을 통해 920억 개 이상의 인터넷 기반 URL을 확인할 수 있습니다. 참고로 2017년 1월 기준으로 인터넷에는 18억 개의 웹 사이트(Netcraft)가 있습니다. Cisco Talos와 Umbrella Threat Intelligence는 매일 전체 활성 상태의 인터넷을 최대 51회 모니터링합니다.	✗ Carbon Black은 웹 벡터링에 참여하지 않습니다.	✗ CrowdStrike는 웹 벡터링에 참여하지 않습니다.	✗ Cylance는 웹 벡터링에 참여하지 않습니다.

	Cisco AMP for Endpoints	Carbon Black Endpoint Security	CrowdStrike Falcon	CylancePROTECT
위협 인텔리전스(계속)				
자동화된 인텔리전스 피드	✓ ATP Gateway, AMP Endpoint, Network-based ATP, NGFW, NGIPS, Email Security + AMP, Web Security + AMP, DNS security, Cloud Security 구성 요소, Threat Intelligence Director 등 모든 Cisco Security 제품과 함께 구성하고 교환할 수 있습니다.	✓ 엔드포인트 제품과 함께 구성하고 교환할 수 있습니다.	✓ 엔드포인트 제품과 함께 구성하고 교환할 수 있습니다.	✓ 엔드포인트 제품과 함께 구성하고 교환할 수 있습니다.
위협 인텔리전스 공유	✓ Aegis, Crete, Aspis 프로그램을 통해 수백여 파트너, 고객, 사업자와 데이터를 공유합니다. Cisco는 Cyber Threat Alliance 창립 회원입니다.	✗ Carbon Black은 위협 인텔리전스를 다른 업체와 공유하지 않습니다.	✗ CrowdStrike는 위협 인텔리전스를 다른 업체와 공유하지 않습니다.	✗ Cylance는 위협 인텔리전스를 다른 업체와 공유하지 않습니다.



알고 계십니까?

Cisco Talos는 250명 이상의 연구진으로 구성된 세계 최대 규모의 위협 인텔리전스 전문 조직입니다.

무슨 일을 하는지 알아보십시오

	Cisco AMP for Endpoints	Carbon Black Endpoint Security	CrowdStrike Falcon	CylancePROTECT
통합				
통합	✓ Rest API	**제한적** 개방형 API. 공통 스크립팅 언어를 수집할 수 있습니다. Palo Alto Networks, Check Point, Blue Coat, Cyphort, Fidelis, Damballa, Splunk, Red Canary 등 기타 솔루션과 통합됩니다.	✓ 서드파티를 위한 Falcon API 및 Falcon Streaming API.	**제한적** A10, 시만텍에서 엔진을 실행할 수 있습니다.