VMware Carbon Black Workload

최신 데이터 센터를 위한 고급 워크로드 보호

사용 사례

- 클라우드 워크로드 보호
- 취약점 관리
- 보안 리스크 및 운영 환경 개선을 위한 워크로드 감사
- 소프트웨어 정의 데이터 센터(SDDC) 보안 태세 강화
- 서버의 레거시 안티바이러스 대체
- 워크로드 정상/비정상 행위 모니터링 및 엔드포인트 탐지 및 대응(EDR)

(특장점) 인프라 팀을 위한 보안 기능

- VMware vSphere® Client™에서 실시간으로 취약점 평가
- 우선 순위 기반 보안 취약점 관리로 보안 패치 적용 효율성 향상
- 기존 인프라 환경에 내장된 보안 활용
- 선제적인 IT 환경 관리를 통해 침해사고 사전 예방
- 별도 추가 설치 또는 부하를 발생 시키는 스캐닝이 불필요하여 워크로드에 오버헤드 요소 제거
- 서버에서 레거시 백신(Anti-Virus) 대체를 통한 컴퓨팅 사이클 재확보

(특장점) 보안 팀을 위한 보안 기능

- 알려진 또는 알려지지 않은 보안 위협으로부터 워크로드 보호
- 보안 툴을 통합하여 복잡성 감소
- 쉽고 빠른 보안 인시던트 조사
- 실시간 공격 체인 시각화 제공
- 평균 해결 시간(MTTR) 단축
- 보안 분석과 IT 운영 간 장벽 제거
- 내부 보안 전문가 및 동료로 구성된 활동적인 사용자 커뮤니티에 참여

기업 및 기관이 클라우드 트랜스포메이션과 애플리케이션 현대화를 향한 여정을 계속함에 따라, 이들에겐 강력하고 운영하기 쉬운 최신 보안 솔루션이 필요합니다. VMware Carbon BlackWorkload™는 최신 워크로드를 보호하기 위해 특별히 설계된 고급 보호 기능을 제공하여 공격 표면을 줄이고 보안 태세를 강화합니다. 이 혁신적인 솔루션은 우선 순위가 지정되는 취약점 보고 기능과 기본 워크로드 강화 기능을 업계 최고의 예방, 감지 및 대응 기능과 결합하여, 가상화된 프라이빗 및 하이브리드 클라우드 환경에서 실행되는 워크로드를 보호합니다.

VMware vSphere와 긴밀하게 통합된 VMware Carbon Black Workload는 설치 및 관리 부담을 완화하고, 여러 워크로드 보안 사용 사례에 대한 원격 분석 컬렉션을 통합하는 고급 보안을 제공합니다. 이 통합 솔루션을 통해 보안 및 인프라 팀은 보안 수명주기의 모든 지점에서 신규 및 기존 워크로드를 자동으로 보호하는 동시에 운영을 단순화하고 IT 및 보안 스택을 통합할 수 있습니다.

리스크 식별 및 워크로드 보호 강화

VMware Carbon Black Workload는 보안 및 인프라 팀이 환경 전반에서 가장 위험한 취약점과 일반적인 악용에 집중할 수 있도록 지원합니다. 취약점을 많이 찾는 것이 아니라 중요한 취약점을 찾는 것이 핵심입니다. CVSS(Common Vulnerability Scoring System), 실제 악용 가능성, 그리고 공격 빈도의 조합을 기반으로 취약점의 우선 순위를 지정하고 동급 최고의 우선 순위 지정 기능으로 패치 적용 효율성을 높입니다.

그림 1: vSphere Client에서 우선 순위 기반 보안 취약점 보고

특징

- 스캔리스(Scanless), 리스크 우선순위 기반 보안 취약점 평가
- 워크로드 인벤토리 및 수명주기 관리
- VMware vCenter® 플러그인
- 워크로드 정상/비정상 행위 모니터링
- 수많은 워크로드 아티팩트에 대한 온디맨드 방식의 쿼리 수행
- 차세대 바이러스 백신(NGAV)
- 워크로드에 대한 엔드포인트 탐지 및 대응(EDR)
- 지속적인 평가를 실행하여 시간 경과에 따른 IT 환경 추적 관리

플랫폼

- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016
- Windows 2019
- Red Hat 6/7
- CentOS 6/7
- Ubuntu 16/18/19/20
- SLES 12/15

최소 기술 요구 사항

- vSphere 6.5 이상
- VMware Tools™ 11.2 이상
- vCenter 6.7 U3 이상
- VMware Carbon Black Cloud™에 대한 인터넷 연결

자세한 정보

개인화된 데모를 설정하거나 자세한 정보를 원하시면 *contact@carbonblack.com*으로 e-메일을 보내거나 *carbonblack.com/workload*를 방문하시기 바랍니다.

자세한 정보를 원하거나 VMware Carbon Black 제품을 구매하려면

(02) 3016-6500로 연락하시기 바랍니다.

실시간 취약점 평가는 보안 및 인프라 팀이 리스크 점수 및 국가 취약점 데이터베이스에 대한 링크를 통해 취약점 컨텍스트를 이해하도록 돕습니다. 또한 리소스를 많이 사용하는 검사의 경우, 추가 관리 오버헤드 또는 설정 없이 이러한 검사의 필요성을 제거합니다. 게다가 VMware Carbon Black은 운영 보안 관리, 침해 지표(IOC), 악의적인 방법, 기법, 프로시저(TTP), 그리고 시스템에서 발생하는 일반적인 이벤트에 대한 가시성을 제공합니다.

vSphere 관리자는 vSphere Client에서 바로 워크로드 보호를 간단하게 보안 기능으로 활성화해서 사용할 수 있으며, 가상 머신 인벤토리에 대해 일괄 지원 및 수명주기 관리를 할 수 있습니다. vSphere 대시보드는 어플라이언스 상태, 인벤토리 상태, 설치 워크플로우에 대한 가시성을 제공하며, 환경에서 발견된 운영 체제 및 애플리케이션 취약점에 대한 리스크 우선 순위 목록을 인프라 팀이 볼 수 있도록 합니다. VMware Carbon Black Cloud Workload를 사용하면 환경에 대한 탁월하고 심층적인 가시성을 제공하여 리스크를 줄이고 워크로드를 강화하는 동시에 보안을 간소화하고 효율적으로 운영할 수 있습니다.

지능형 사이버 공격의 예방, 탐지 및 대응

보안 팀은 매우 동적인 가상화 데이터 센터 환경에서 보안 가시성 확보와 보안 통제에 대한 제약사항과 어려움이 많습니다. VMware Carbon Black Workload는 기본 취약점 평가 및 워크로드 하드닝 기능을 업계 최고의 차세대 바이러스 백신(NGAV), 워크로드 정상/비정상 행위 모니터링, 그리고 워크로드에 대한 엔드포인트 탐지 및 대응(EDR)과 결합하여 이러한 환경에서 실행되는 워크로드를 보호합니다.

VMware의 고급 워크로드 보호 기능을 통해 보안 팀은 시간이 지남에 따라 공격자의 행동 패턴을 분석하여, 처음 보는 공격(알려진 양호한 소프트웨어를 조작하는 공격 포함)을 감지하고 차단할 수 있습니다. 공격자가 경계 방어를 우회하는 경우, VMware Carbon Black은 데이터 침해로 확대되기 전에 보안 팀이 공격을 차단할 수 있도록 지원합니다. 인프라에 보안을 내장함으로써 사용자는 현재 시스템 상태를 쉽게 감사하여 보안 태세를 추적하고 워크로드를 강화할 수 있으며, vSphere 관리자와의 더욱 간편한 협업을 통해 알려진 취약점을 해결할 수 있습니다.

IT 및 보안 팀의 운영 단순화

VMware는 보안 제공에 있어 내재적 접근 방식, 즉, 워크로드가 배포되는 모든 곳의 인프라에 보안을 보다 간편하게 구축하는 방식을 취하고 있습니다. 이 고유한 접근 방식을 통해 VMware는 인프라 및 보안 팀에 단일 출처를 제공하여 중요 취약점 및 공격에 대한 대응을 가속하는 동시에 협업을 지원하고 마찰을 줄임으로써 보안과 운영 단순성을 둘 다 잡을 수 있습니다. 리소스를 두고 경쟁하는 여러 포인트 보안 툴을 VMware Carbon Black으로 대체하여 보안 운영을 간소화하고 IT와 보안 스택을 단순화해서 통합하세요.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com 서울시 강남구 영동대로 517 아셈타워 13층 (우) 06164 e-메일: vmware_kr@vmware.com
 Item No: 768319aq-ds-crbn-black-cld-wkld-uslet 2/21