

# 기능 및 규격

- Cloud Workload Protection Platform (CWPP)

# Cloud Workload Protection Platform (CWPP)

## 개요

VMware의 워크로드 보안 제품인 Carbon Black Cloud의 주요 기능 및 규격에 대해 에디션 별로 명시하여 정보제공요청서 혹은 제안요청서에 대응할 수 있도록 한다.

VMware 특징점은 붉은색으로 표기한다.

## 기능 요건

### 일반 및 관리

#### 콘솔

- HTML 5 기반의 웹 콘솔 환경 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud-Workload/services/cbc-workloads-oer/GUID-C09ECFC2-7703-4BED-A272-44ABBD3A6B0D.html>
- 벤더 커뮤니티를 통한 보안 리포트 및 위협 색적 방안 수시 제공
  - <https://community.carbonblack.com>
- 여러 조직 별 관리 콘솔 생성 및 관리하는 멀티테넌시 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-ECCB09F4-34DB-4CBC-AA97-ACBD1431FFB9.html>

#### 관리

- 역할 관리
  - 콘솔 사용자 별 역할 부여
    - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-CF5ACD2C-A534-46C8-AE06-E1884DB37B58.html>
  - 모범사례 역할 제공
    - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-6B8FB45E-28AD-4986-B5D0-3EB83C5FF2DA.html>
  - 역할 커스터마이징 제공
    - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-2E02B16B-185E-434F-83C9-DD1F8ECBFDB7.html>
- 범주 별 알림 제공
  - 일반 (경보 및 위협)
    - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-5D9EA7FC-4C46-4B6D-8D2B-467651EF1F28.html>
  - 쿠버네티스
    - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-E01F991F-7360-4C32-BD38-69ECFB5E2949.html>
- 보안 스택의 통합을 위한 API 및 SDK 제공
  - <https://developer.carbonblack.com/reference/carbon-black-cloud/platform-apis/>
- 로그 추출 및 SIEM 연동 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-4B780445-68B5-4B65-9E69-AF2AD9B33C46.html>
  - 기본 데이터 저장 기간 확장 지원

### 에이전트 운영 환경

- 공통
  - 운영체제 별 에이전트 그룹 분류 제공
    - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-225A2814-B26C-4404-B031-EABD5BF84894.html>
  - Active Directory 기반 에이전트 그룹 분류 제공
    - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-741989BE-4844-4953-B7FE-89A05A81EBE7.html>
  - Hostname 기반 에이전트 그룹 분류 제공
    - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-741989BE-4844-4953-B7FE-89A05A81EBE7.html#GUID-BDBF769E-BC7E-4A7B-BBF8->

- 92A0193359E0\_GUID-15D63B9E-8500-4B50-A8E9-6465E04C4F8E
- IP 서버넷 기반 에이전트 그룹 분류 제공
  - [https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-741989BE-4844-4953-B7FE-89A05A81EBE7.html#GUID-BDBF769E-BC7E-4A7B-BBF8-92A0193359E0\\_GUID-15D63B9E-8500-4B50-A8E9-6465E04C4F8E](https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-741989BE-4844-4953-B7FE-89A05A81EBE7.html#GUID-BDBF769E-BC7E-4A7B-BBF8-92A0193359E0_GUID-15D63B9E-8500-4B50-A8E9-6465E04C4F8E)
- 에이전트 그룹 분류 기준 별 호환 정의 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-741989BE-4844-4953-B7FE-89A05A81EBE7.html#use-of-logical-operators-for-sensor-group-criteria-2>
- 에이전트 활동 이용자 안내 여부 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-C8423E18-7163-46E7-9E94-9169CEFD6782.html>
- 에이전트 이용자 통제 여부 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-FF935B8B-5737-4CC2-85D4-DE5B5EEFE358.html>
- 이용자의 에이전트 삭제 시도 시 코드 요청 방안 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/cbc-sensor-installation-guide/GUID-6D511596-6A71-486D-ABAC-59B8345AF14D.html>
- 지원 운영체제 및 에이전트 버전 단위 라이프사이클 기간 명시
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/cbc-sensor-support-policy/GUID-9D4D7BB4-A1B8-4255-BA20-932B15934FFE.html>
- 복제형 VDI 인식 및 정리 방안 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-406CD399-F536-4150-8CFA-E48F1DC17E32.html>
- 자산 단위 격리 여부 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-C8769B0F-5184-4028-B915-56AFFE315989.html#quarantine-a-device-triggered-by-an-alert-2>
- 에이전트 설치 및 업그레이드 편의성 제공 (시스템 리부트 불필요)
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/cbc-sensor-installation-guide/GUID-1521D596-AE7A-4882-8A40-9741B7E807D3.html>
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/cbc-sensor-installation-guide/GUID-C974F5C4-BD57-4F16-85CD-D6F934BB3F4A.html>
- Windows
  - 데스크탑 및 서버 지원
    - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/cbc-oer-win-sensor-on-desktop/GUID-D51C23FB-C043-48E3-B01D-66F3573C72ED.html>
    - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/cbc-oer-win-sensor-on-server/GUID-149AAA9E-05D0-4208-B210-B1EF04C9C8B6.html>
  - Windows 보안센터 연동 제공
    - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-968C0E1F-170B-4EDB-80BE-731CBBEFF847.html>
  - AMSI 지원
    - [https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-E6EAE58C-466D-4C44-AF87-F3CA86B9737F\\_copy-xdr.html](https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-E6EAE58C-466D-4C44-AF87-F3CA86B9737F_copy-xdr.html)
  - ARM64 칩셋 지원
    - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/cbc-oer-win-sensor-on-desktop/GUID-D51C23FB-C043-48E3-B01D-66F3573C72ED.html>
- Linux
  - 커널 기반한 다양한 운영체제 지원
    - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/cbc-oer-linux-sensor/GUID-3CBCD489-F097-4722-ABF9-B6A7EDC1F51D.html>
  - ARM64 칩셋 지원
    - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/cbc-oer-linux-sensor/GUID-B8767EEB-29E5-4F26-9B1A-0EDB17B72B63.html>
- Mac
  - Kernel Extensions 기반 지원
    - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/cbc-sensor-installation-guide/GUID-D2BF71B6-2352-4DE1-841A-E727CC75232E.html>
  - System Extensions 기반 지원
    - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/cbc-sensor-installation-guide/GUID-50A83AD4-3D85-415A-9C4D-DD3FFA6D637E.html#GUID-50A83AD4-3D85-415A-9C4D-DD3FFA6D637E>
  - ARM64 칩셋 지원
    - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/cbc-audit-and-remediation-oer/GUID-9ABB1F2E-1C08-439A-B4FB-F455FDDEF7F1.html>

## Prevention

### 예방

- 네이티브 프로그램과 일반적인 스크립팅 언어를 활용하는 악성 파일리스 및 파일 지원 스크립트를 방지
  - Advanced Scripting Prevention

- <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud-on-VMware-Cloud-Services-Platform/services/carbon-black-cloud-on-csp-user-guide/GUID-98F6D21F-E6F0-48CB-926A-40F1D489E585.html>
- **악의적인 활동에 사용되는 일반적이고 널리 퍼져 있는 TTP와 Carbon Black의 위협 분석 부서에서 탐지한 일상적인 TTP 행위에 대응**
  - Carbon Black Threat Intel
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud-on-VMware-Cloud-Services-Platform/services/carbon-black-cloud-on-csp-user-guide/GUID-98F6D21F-E6F0-48CB-926A-40F1D489E585.html>
- 자격 증명을 획득하는 위협 행위자에 대응하고 이러한 활동을 나타내는 악의적인 TTP 행위에 대응
  - Credential Theft
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud-on-VMware-Cloud-Services-Platform/services/carbon-black-cloud-on-csp-user-guide/GUID-98F6D21F-E6F0-48CB-926A-40F1D489E585.html>
- 보안 소프트웨어 제거 또는 비활성화, 데이터/스크립트 난독화 또는 암호화, 신뢰할 수 있는 프로세스를 악용하여 악성 활동을 숨기고 위장하는 등 위협 행위자가 탐지를 피하기 위해 사용하는 일반적인 TTP 행위에 대응
  - Defense Evasion
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud-on-VMware-Cloud-Services-Platform/services/carbon-black-cloud-on-csp-user-guide/GUID-98F6D21F-E6F0-48CB-926A-40F1D489E585.html>
- 위협 행위자가 재시작, 자격 증명 변경, 기타 액세스를 차단할 수 있는 기타 중단을 통해 시스템에 대한 액세스 권한을 유지하기 위해 사용하는 일반적인 TTP 행위에 대응
  - Persistence
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud-on-VMware-Cloud-Services-Platform/services/carbon-black-cloud-on-csp-user-guide/GUID-98F6D21F-E6F0-48CB-926A-40F1D489E585.html>
- 위협 행위자가 운영 체제의 버그 또는 잘못된 구성을 통해 상승된 액세스 권한을 획득했음을 나타내는 동작을 해결하고 이러한 활동을 방지하기 위한 TTP 행위에 대응
  - Privilege Escalation
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud-on-VMware-Cloud-Services-Platform/services/carbon-black-cloud-on-csp-user-guide/GUID-98F6D21F-E6F0-48CB-926A-40F1D489E585.html>
- 지정 프로세스에 대해 보안 위협 행위의 유형 별 허용 및 불허 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-1A8BDB2B-BE96-4739-950D-99F194E7458C.html>
- **프로세스 범주에 대해 보안 위협 행위의 유형 별 허용 및 불허 기능 제공**
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud-on-VMware-Cloud-Services-Platform/services/carbon-black-cloud-on-csp-user-guide/GUID-B3A6CD73-9FE7-41C1-945B-D878527A0B63.html>
- **프로세스 종료 및 파일 삭제 등을 통한 공격 중단 지원**
  - <https://docs.vmware.com/en/VMware-Carbon-Black-EDR/7.7.1/vmw-cb-edr-ug/GUID-6B68C4D7-C113-4D55-BD34-B93331A5C052.html>

## 검사

- USB 장치 정보에 기반한 허용 및 불허 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-19B3084E-7092-494C-8484-5B333F423135.html>
- 안티바이러스 시그니처 기반 검사 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-84D98399-8E46-42DF-8ED5-F90E65069954.html>
- 에이전트 설치 전 존재한 맬웨어 차단을 위한 백그라운드 검사 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-8FECF4D4-3FFA-4102-91EA-2CD042C7FD84.html>
- 컴퓨터 성능을 위한 실행 파일 (exe, dll, scripts) 포커스 검사 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-79EE2C6A-2102-4C2A-BB3B-BB51E7CCB884.html>
- 컴퓨터 자원 절약을 위한 낮은 우선 순위 백그라운드 검사 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-8FECF4D4-3FFA-4102-91EA-2CD042C7FD84.html>
- 빠른 색적을 위한 높은 우선 순위 백그라운드 검사 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-8FECF4D4-3FFA-4102-91EA-2CD042C7FD84.html>
- 평판 기반 검사 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-84BBD4DA-CA1C-437D-A42D-95FDE82B6E81.html>
- 엄격하게 제어되는 환경 운영을 위해 바이너리 실행 전 검사 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-3CCF9929-0913-4F2A-8086-087A423CFE88.html>
- 실시간 원격 접속 및 진단 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-DED51138-E9A8-4BCC-873E-5768DAB596BE.html>
- 에이전트 상태 보고 확인
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/cbc-sensor-installation-guide/GUID-C8423E18-7163-46E7-9E94-9169CEFD6782.html>
- 메모리 덤프
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-DED51138-E9A8-4BCC-873E-5768DAB596BE.html>
- 네트워크 드라이브 스캔 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID->

[E7A4C98A-9A41-4B36-A5D0-5CC9B9EF44B0.html](#)

- 맬웨어 격리/삭제/추출 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-F855AA34-7058-455E-B17A-B2E9265B5974.html>
- 클라우드 분석 제공
  - 샌드박스 분석
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-3CCF9929-0913-4F2A-8086-087A423CFE88.html>

## Standard

### 보호

- 사용자화 침해지표 경보 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-D15FC6CD-4360-4816-BCF7-AF2D9538529C.html>
- USB 장치 통제 경보 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-C51FFEEC-AB70-4C15-873D-3BD2FA85EE25.html>
- 클라우드 분석 경보 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-03EDC0BC-375F-4F4E-B611-B94265B56018.html>
- 심각도 분석 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-95388BA8-00FA-432C-ABC0-7C3353D19D35.html>
- 유사 경보의 자동 그룹화 통한 행위 기반 경보 시야 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-7AE51D2D-0DAD-43E5-BE01-D664B4BD8C0A.html>
- 경보 및 조사 기능 연동
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-15C429CA-7129-4171-BB0B-3F7132DA01EF.html>
- 경보 대응 빠른 방안 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-C8769B0F-5184-4028-B915-56AFFE315989.html>
- 경보 내 유형 별 필터 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-4718F7A2-1CCA-4FA2-8491-03A405F551E3.html>
- 경보 관련 근본원인분석 및 시각화 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-FBE02855-EB56-45CA-9E4A-A69D1903FBF6.html>

### 행위 탐지 및 대응

- 모든 프로세스 근본원인분석 및 시각화 조사 제공
  - 부모 및 자식 프로세스에 대한 상관 관계 분석
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-AA8ABBA8-C8D7-434F-85D0-DE4BE78E5E42.html>
- 파일 수정 여부 수집
  - <https://docs.vmware.com/en/VMware-Carbon-Black-EDR/7.7.1/vmw-cb-edr-ug/GUID-9CF0F950-E9B8-45C7-9FD5-887866657AAF.html>
- 레지스트리 수정 여부 수집
  - <https://docs.vmware.com/en/VMware-Carbon-Black-EDR/7.7.1/vmw-cb-edr-ug/GUID-9CF0F950-E9B8-45C7-9FD5-887866657AAF.html>
- 네트워크 접속 등 연결에 대한 정보 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-EDR/7.7.1/vmw-cb-edr-ug/GUID-9CF0F950-E9B8-45C7-9FD5-887866657AAF.html>
- TTPs and MITRE 기법 참조 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-857AA662-6DA1-4265-99E7-A65B7E1F50CC.html>
- 악성 이벤트 의심 내역 조사 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-A9A1FD79-AC43-4CAC-B1D8-4B0A69FF8407.html>
- 스크립트 기반 공격 조사 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-187BF058-1719-4E57-9A5A-E9D338D62C99.html>

## Workload Protection

- 하이퍼바이저 커널 기반 모듈 제공
  - vCenter를 통해 배포 명령 내릴 수 있는 ESXi 하이퍼바이저 VIB 패키지 제공
  - Instant Clone VDI 등의 인식에 도움

- [https://docs.vmware.com/en/VMware-Carbon-Black-Cloud-Workload/1.2/carbonblack\\_workload/GUID-071DC7EC-3CB1-487B-BBB9-CD670513EA70.html](https://docs.vmware.com/en/VMware-Carbon-Black-Cloud-Workload/1.2/carbonblack_workload/GUID-071DC7EC-3CB1-487B-BBB9-CD670513EA70.html)
- 하이퍼바이저 관리자와 웹 콘솔 간 보안 명령 중계 가상 애플라이언스 제공
  - [https://docs.vmware.com/en/VMware-Carbon-Black-Cloud-Workload/1.2/carbonblack\\_workload/GUID-E2ED3713-315B-4EEE-A3E8-A7A09A011101.html](https://docs.vmware.com/en/VMware-Carbon-Black-Cloud-Workload/1.2/carbonblack_workload/GUID-E2ED3713-315B-4EEE-A3E8-A7A09A011101.html)
- 하이퍼바이저 관리자와 웹 콘솔 간 보안 명령 중계에 프록시 통한 이중 보안 방안 제공
  - [https://docs.vmware.com/en/VMware-Carbon-Black-Cloud-Workload/1.2/carbonblack\\_workload/GUID-E579E334-80F1-4876-8AA0-F29BAB441887.html](https://docs.vmware.com/en/VMware-Carbon-Black-Cloud-Workload/1.2/carbonblack_workload/GUID-E579E334-80F1-4876-8AA0-F29BAB441887.html)
- 하이퍼바이저 관리자와 가상 애플라이언스 통합하여 인프라 및 보안 간 동일 시야 방안 제공
- 엄격하게 제어되는 환경을 운영하여 워크로드를 안전하게 보호하고 인터넷 트래픽에 직접 노출되지 않도록 가상 애플라이언스 제공
  - Sensor Gateway
  - [https://docs.vmware.com/en/VMware-Carbon-Black-Cloud-Workload/1.2/carbonblack\\_workload/GUID-CC4071BA-E3A5-4E3D-A659-AF2F14B508C6.html](https://docs.vmware.com/en/VMware-Carbon-Black-Cloud-Workload/1.2/carbonblack_workload/GUID-CC4071BA-E3A5-4E3D-A659-AF2F14B508C6.html)

## Advanced

### Audit & Remediation

- Osquery 통한 에이전트 배포 환경의 규정 준수 및 위협도 실시간 검사 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-3DD4AC73-3531-4023-85A1-09D469214920.html>
- Osquery 템플릿 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-129D4F84-1BF0-49F3-BF95-83002FD63217.html>
- Osquery 사용자화 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-3DD4AC73-3531-4023-85A1-09D469214920.html>
- CIS Benchmarks 수행 및 보고 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-E5EFA185-AB06-41A0-ABF4-9BA4CD1E1032.html>

### Vulnerability Management

- Windows 운영체제 및 애플리케이션 취약점 확인 및 평가 제공
  - [https://docs.vmware.com/en/VMware-Carbon-Black-Cloud-Workload/1.1/carbonblack\\_workload/GUID-12E5C0BF-566D-43F3-BB41-63DEE1E182E3.html](https://docs.vmware.com/en/VMware-Carbon-Black-Cloud-Workload/1.1/carbonblack_workload/GUID-12E5C0BF-566D-43F3-BB41-63DEE1E182E3.html)
- Linux 운영체제 및 애플리케이션 취약점 확인 및 평가 제공
  - [https://docs.vmware.com/en/VMware-Carbon-Black-Cloud-Workload/1.1/carbonblack\\_workload/GUID-12E5C0BF-566D-43F3-BB41-63DEE1E182E3.html](https://docs.vmware.com/en/VMware-Carbon-Black-Cloud-Workload/1.1/carbonblack_workload/GUID-12E5C0BF-566D-43F3-BB41-63DEE1E182E3.html)
- CVSS 기반 위협 계측 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-F99243BC-3CD5-4EEE-B9D5-CE31A112BD66.html>
- CVE-ID 기준 안내 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-3621AFA1-668C-4E9E-923E-E8E9D01AE99E.html>

## Enterprise

### Enterprise EDR

- 인증 이벤트 조사 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-18D2C498-DD6A-4731-BD61-7EF7B471401E.html>
- 바이너리 자동 상세 보고 제공
- **바이너리 수집 제공**
- 강화된 데이터 조사 쿼리 제공
  - <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-18D2C498-DD6A-4731-BD61-7EF7B471401E.html>
- 위협 정보와 보안담당자의 쿼리를 추가해 사용자화 침해지표 목록 생성 및 관리 제공
- 이상징후 분류 경고 연동
  - [https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-1759B0E7-A08A-48CC-954B-E75017A3A02B\\_copy-xdr.html](https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-1759B0E7-A08A-48CC-954B-E75017A3A02B_copy-xdr.html)

## Add-on

### Host Based Firewall

- <https://carbonblack.vmware.com/resource/vmware-carbon-black-cloud-host-based-firewall-solution-brief?path=/carbon-black-host-based-firewall>

## Extended Detection and Response (XDR)

- Network Detection and Response
  - <https://carbonblack.vmware.com/resource/carbon-black-xdr-technical-overview#network-connection-visibility>
- Host Intrusion Detection System
  - <https://carbonblack.vmware.com/resource/carbon-black-xdr-technical-overview#ids-observations>
- Anomaly Classification
  - [https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-1759B0E7-A08A-48CC-954B-E75017A3A02B\\_copy-xdr.html](https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-1759B0E7-A08A-48CC-954B-E75017A3A02B_copy-xdr.html)

## Extended Data Retention

- <https://blogs.vmware.com/security/2021/05/announcing-increased-data-retention-for-vmware-carbon-black-cloud.html>

## Managed Detection

- <https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-datasheet-managed-detection.pdf>

## Managed Detection and Response

- <https://www.vmware.com/products/managed-detection-and-response.html>

# 기능 매트릭스

FEATURE	Prevention	Standard	Advanced	Enterprise
Policy-Based Prevention	☑	☑	☑	☑
Up-to-Date Threat Intel	☑	☑	☑	☑
Malware Detection & Deletion	☑	☑	☑	☑
Prevention Alerts	☑	☑	☑	☑
Alert Triage	☑	☑	☑	☑
Bypass & Quarantine	☑	☑	☑	☑
Process Banning		☑	☑	☑
Event Investigation		☑	☑	☑
Behavioral EDR		☑	☑	☑
Device Control		☑	☑	☑
API, Event Forwarder		☑	☑	☑
Audit and Remediation			☑	☑
> Live Query			☑	☑
> Live Response			☑	☑
> CIS Benchmarks			☑	☑
Vulnerability Management			☑	☑
Enterprise EDR				☑
> Anomaly Classification				☑
Watchlists				☑
Process Trees				☑
Workload Protection		☑	☑	☑
> vSphere Integration		☑	☑	☑

> Sensor Gateways		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Host Based Firewall		add-on	add-on	add-on
Extended Detection and Response (XDR)		add-on	add-on	add-on
> Network Detection and Response		add-on	add-on	add-on
> Host Intrusion Detection System		add-on	add-on	add-on
Extended Data Retention	add-on	add-on	add-on	add-on
Managed Detection		add-on	add-on	add-on
Managed Detection and Response		add-on	add-on	add-on

# 고지사항

총판인 에티버스의 해석 및 검토의견은 특정한 효력이 없으며, 진행과 결정을 보다 수월하도록 돕기 위한 참고 용도로서 제공됩니다. 사업 진행 시, 특히 정보제공요청서 작성 등에는 수행을 책임지는 담당자와 함께 충분한 검토하여 진행하시기 바랍니다.