Carbon Black.

행위기반 엔드포인트 보호 솔루션

- Endpoint Detection and Response -

VISION

A WORLD SAFE FROM CYBER ATTACKS

We envision a world where people live and work in our connected way of life, free from the threat of cyber attacks. This is our ultimate purpose, and it informs everything we do and every product we build.

MISSION

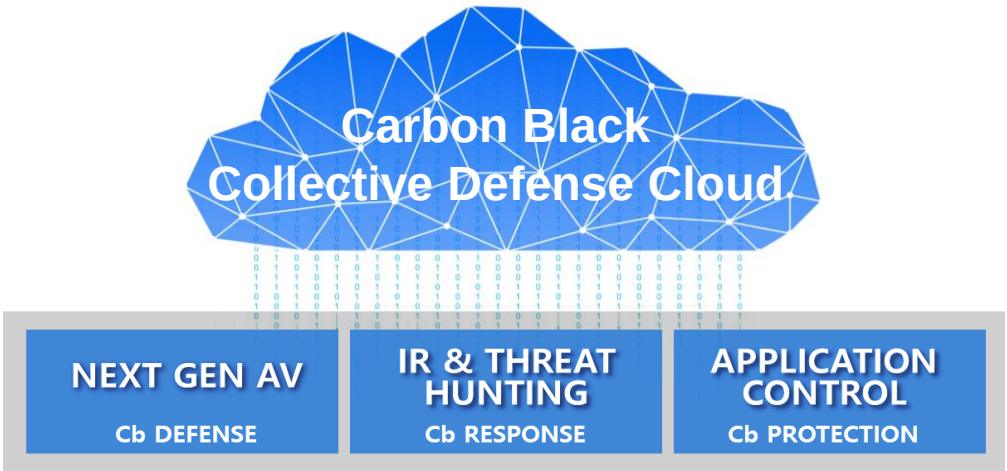
TRANSFORMING ENDPOINT SECURITY WITH BIG DATA AND ANALYTICS

In order to fulfill our vision, we believe cyber security needs a new approach—one that harnesses the power of big data, analytics, and cloud computing to defeat increasingly sophisticated adversaries.

Carbon Black.

Carbon Black 은 APT 공격, 랜섬웨어 등 알려지지 않은 공격에 대해 행위기반으로 탐지하고 차단하는 EDR 솔루션 입니다.

매일 35만개의 새로운 멀웨어가 만들어지고 있으며, 공격자들의 기술은 Anti-Virus 를 앞질러 가고 있습니다. Carbon Black 은 이러한 기존 백신의 패턴기반 탐지 한계를 뛰어넘는 엔드포인트 및 인프라 보안 솔루션 입니다. (2018 AV-테스트 Report)



Carbon Black 제품 유형

IR & THREAT HUNTING **Cb Response**	• 모든 위협 행위를 실시간 탐지 및 대응 • Cyber Kill Chain 시각화를 통해 공격경로 파악 • 포렌식 분석 및 원격 호스트 격리
NEXT GEN AV **Cb Defense**	• 기존 AV를 대체하는 차세대 바이러스 백신 • 행위기반 탐지 및 차단 • Cloud 사용으로 빠르고 손쉬운 보안환경 구축
APPLICATION CONTROL **Cb Protection**	• 승인되지 않은 어플리케이션 실행 차단 (Whitelist) • POS, ATM, MES, 의료기기 등 Mission Critical 업무의 시스템 임의 변경 차단 • LockDown, 매체제어(USB)를 통한 중요 시스템 보호

Goodus
Breathing Life into Technology

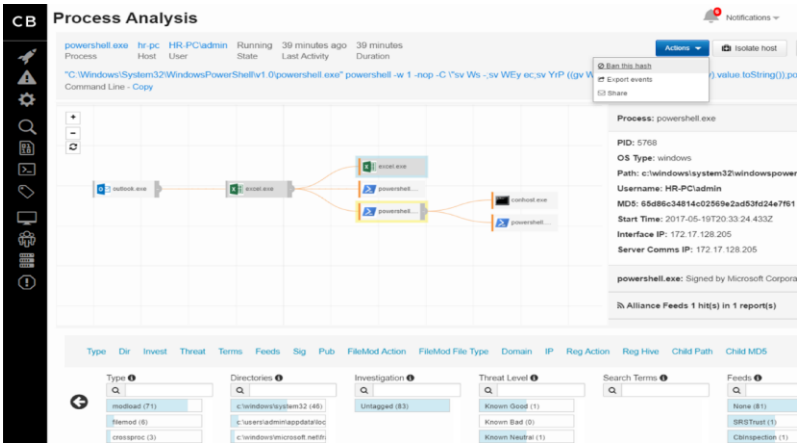
Carbon Black.

CB RESPONSE

업계 최고의 인시던트 대응 및 위협 검색

Cb Response는 보안 운영 센터(SOC) 팀을 위해 설계된 업계 최고의 인시던트 및 위협 대응 솔루션으로, 필터링 되지 않은 엔드포인트의 모든 행위 데이터를 기록합니다.
저장된 데이터를 통해 보안담당자가 실시간으로 위협을 검색하고 전체 공격에 대한 Kill-Chain을 시각화 할 수 있습니다.

이 솔루션은 Carbon Black Cloud와 연계하여, 식별된 위협 및 행위데이터에 대한 위협정보를 엔드포인트에 적용합니다.



엔드포인트에서 실행되는 프로세스 트리 가시화를 통해 한 눈에 실행 경로 파악

핵심기능

- **엔드포인트의 모든 Process Activity 중앙 관리**
  보안전문가가 위협을 실시간으로 탐지하고 공격이 발생한 후 심층적인 조사를 수행하는데 필요한 정보를 제공

- **원격 조치를 위한 Live Response**
  감염된 호스트에 안전하게 연결하여 파일을 다운/업로드, 프로세스 중단, 메모리 덤프 등을 수행 가능

- **Attack Chain 시각화 및 탐색**
  직관적인 Attack Chain 시각화를 제공하여 근본 원인을 빠르고 쉽게 식별

- **Open APIs 를 통해 관제솔루션(SIEM, SMS 등) 연동**
  기존의 보안 스택에 통합할 수 있는 강력한 파트너 ecosystem 을 제공

USE CASES

- 위협 검색
- 인시던트 대응
- 경보 확인 및 분류
- 근본 원인 분석
- 포렌직 분석
- 호스트 격리

BENEFITS

- 신속한 end-to-end 대응 및 조치
- 신속한 IR 및 위협 탐지기능과 필터링 되지 않은 엔드포인트 시각화
- 신속한 공격자 식별 및 활동과 근본원인 파악
- 감염 대상에 대한 Secure 원격 접근
- 자동 위협검색을 통해 향후 발생가능한 공격 차단

FEATURES

- Out-of-the-box 및 사용자 지정 가능한 행위 탐지
- 다양한 사용자 정의를 지원하는 Threat Intel Feeds
- 자동화된 Watchlists Query 탐지
- 중앙집중식 데이터 처리 및 바이너리 검색
- 대화형태의 Attack Chain 시각화
- 빠른 조치를 위한 Live Response
- Open APIs 및 120개 이상의 3rd Party 와 통합
- On-prem, Virtual Private Cloud, SaaS, MSSP

PLATFORMS

- Windows
- MacOS
- Redhat Linux
- CentOS Linux
- SUSE
- Oracle RHCK
- Clouds or On-Premise

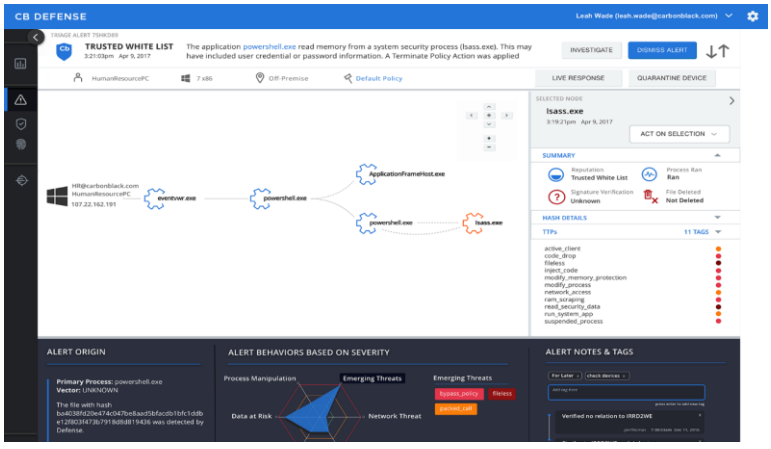
Goodus
Breathing Life into Technology

Carbon Black.

CB DEFENSE

NGAV+ Endpoint Detection and Response

Cb Defense는 업계 최고의 차세대 바이러스 백신(NGAV) 및 엔드포인트 탐지 및 대응(EDR) 솔루션 입니다. 클라우드 기반 엔드포인트 보호 플랫폼인 Cb Predictive Security Cloud를 통해 제공 됩니다.
Cb Defense 는 AV 를 대체할 수 있는 인증을 받았으며, 최소의 관리 노력으로 최상의 보안을 제공하도록 설계되었습니다.



Zero-Day 및 행위기반 공격을 빠르게 파악하고
엔드포인트의 감염확산을 차단

핵심기능

- **단일 Agent, 클라우드 플랫폼**
  단일 Agent 로 동작하며, 엔드포인트 보호 플랫폼인 Cb Predictive Security Cloud 를 통해 제공

- **공격행위의 스트리밍 기반 분석을 통한 최소 오탐**
  독보적인 데이터 기반 방지 기술은 Malware, Fileless Attack 및 Ransomware와 같은 알려지지 않은 위협을 차단함

- **완벽한 엔드포인트 활동의 시각화**
  엔드포인트 활동에 대한 명확하고 포괄적인 시각화를 제공하므로, 손쉬운 검색 및 분석/추적 기능을 제공

- **보안 및 IT조직의 운영 효율성 향상**
  Web-Based 관리를 통해 보안조직과 IT조직 구분없이 실시간 사고 대응, 실시간 조사를 할 수 있는 편리한 메뉴 구성

USE CASES

- 기존 AV 대체 및 확장
- 여러 엔드포인트를 하나의 에이전트로 통합
- Cloud기반 솔루션으로 별도관리서버 필요없음

BENEFITS

- 알려진/알려지지 않은 공격으로부터의 향상된 방어
- 보안 갭을 줄이기 위한 엔드포인트의 완전한 가시성
- 경고창을 없애고, 잠재적인 위협 우선순위 측정
- 인시던트에 대한 쉬운 조사
- 더 빠른 평균 해결시간(MTTR)
- 단순화된 운영, 인프라가 필요없음

FEATURES

- 멀웨어 방지를 위한 시그니처 및 클라우드 기반 피드
- 스트리밍 분석을 통해 파일리스 공격 방지
- 온/오프라인 예방
- 유연한 예방 정책
- 사용자 임의로 대시보드 구성 및 대화식 Attack Chain 시각화
- Live Response : 실시간 조치
- PCI 및 HIPAA 호환
- Open APIs 는 Security Stack 과 통합

PLATFORMS

- Windows 7/8/10,
- Server 2008, 2012, 2016, 2019
- MacOS 10.15+
- Linux RHEL, CentOS, SUSE, OpenSUSE, Amazon Linux, Ubuntu

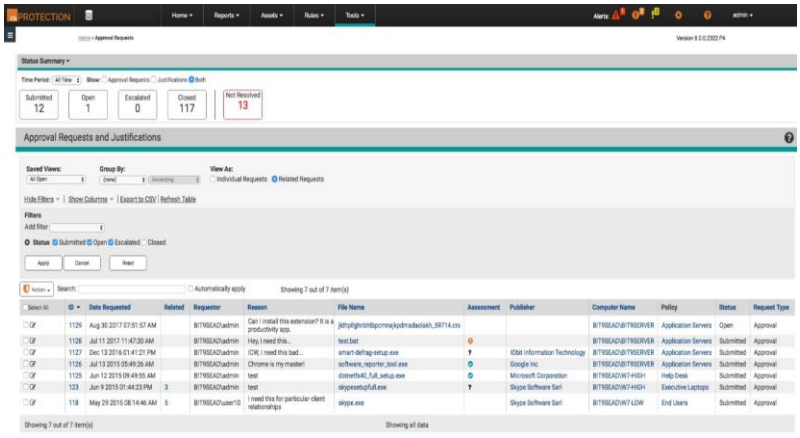
Goodus
Breathing Life into Technology

Carbon Black.

CB PROTECTION

어플리케이션 제어 및 인프라 보안

CB Protection은 서버 및 주요 시스템을 잠그고 원치 않는 변경을 방지하며, 규제 요구 사항을 지속적으로 준수하는 데 사용되는 업계 최고의 응용 프로그램 제어 제품입니다.



원하지 않는 변경으로 부터 엔드포인트 시스템을 보호

핵심기능

- **승인되지 않은 어플리케이션 실행 차단(Lock Down)**
  어플리케이션 및 파일에 대한 원치 않는 변경을 방지하며, Malware Attack을 차단하고 서버환경 보호

- **Whitelist 기반의 어플리케이션 제어**
  "bad" 를 차단하고, "good" 을 허용하는 간편한 정책 설정을 통한 어플리케이션 제어 및 외부매체제어 (USB)를 통해 중요 시스템을 보호

- **외부매체 지속적인 규정 준수**
  PCI-DSS, HIPAA / HITECH, SOX, NERC CIP, GDPR 및 NIST 800-53 과 같은 규제 표준 및 프레임 워크의 많은 요구사항을 충족

USE CASES

- 고정된 기능의 장치 : POS 단말기, ATM, MES 시스템, 의료기기 등
- Mission Critical한 엔드포인트 및 생산설비용 서버 등
- 서버 도메인 컨트롤러, 전자 메일 등 서버, 데이터 및 거래 플랫폼

BENEFITS

- Malware, Ransomware 및 차세대 공격 차단
- 엔드포인트 에이전트 통합
- 원치 않는 시스템 구성 변경 방지
- 주요 규제 요구사항에 대한 IT 위험 및 감사제어 충족
- PCI DSS 요구사항에 대한 직접제어 수행

FEATURES

- 어플리케이션 제어
- 파일 무결성 모니터링 및 제어
- 장치 제어
- 메모리 보호
- 평판 서비스
- Open APIs

PLATFORMS

- Windows XP, Server, Vista, Embedded, POS
- MacOS X
- Redhat Linux
- CentOS Linux
- Oracle RHCK Linux

Goodus
Breathing Life into Technology

침해사고 발생 시 원인 분석을 위한 시간을 75% 단축함으로,

신속하게 침해대응 및 조치를 할 수 있도록 지원

포레스터 선정, 탐지율 1위

- 탐지분야 5개 항목에서 최고점수 획득
- SOC센터에게 필요한 완전한 가시성 제공
- 위협 요소 사전 탐지 기능 제공

DEMO 및 견적요청

ms.securitybiz@goodus.com

ABOUT CARBON BLACK

카본 블랙은 차세대 엔드 포인트 보안을 제공하는 선도 업체입니다. 카본 블랙은 포춘 100 대 기업 중 30 곳을 포함하여 전 세계 3,700여 고객사에 서비스를 제공하고 있습니다. 사이버 보안 혁신 업체 인 카본 블랙은 애플리케이션 제어, EDR (Endpoint Detection and Response) 및 NGAV (Next-Generation Antivirus) . 새로 도입 된 대용량 데이터 및 분석 클라우드 플랫폼 인 Cb Predictive Security Cloud - 카본 블랙 솔루션을 활용하여 고객은 맬웨어, 중계기 및 비 악성 코드 공격을 포함한 가장 진보 된 사이버 위협으로부터 방어 할 수 있습니다. 클라우드, 전제 또는 관리 서비스를 통해 배포 된 카본 블랙 솔루션을 사용하면 중요한 시스템을 잠그고 위협 요소를 추적하고 기존 안티 바이러스를 대체 할 수 있습니다.

서울특별시 강남구 선릉로 514 성원빌딩 14F / Tel) 070-7017-4100

http://www.goodus.com

Goodus

Breathing Life into Technology