솔루션 개요

자동화된 실시간 사고 대응으로 엔드포인트 보안 강화

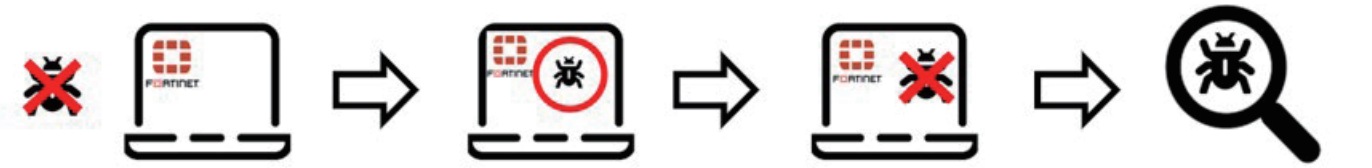
종합 요약

지능형 공격은 몇 분, 때로는 몇 초 만에 엔드포인트를 손상시킬 수 있습니다. 1세대 EDR(Endpoint Detection and Response) 도구로는 이를 따라잡을 수 없습니다. 수동 분류 및 대응이 필요하기 때문에 너무 느릴 뿐만 아니라 많은 알림이 생성됩니다. 이러한 솔루션은 보안 운영 비용을 높이고 사고 대응 프로세스를 느리게 만들기 때문에 운영 중단을 일으키고 시스템 사용자를 방해합니다.

2016년 1월 1일 이후로, 매일 평균 4,000건 이상의 랜섬웨어 공격이 발생했습니다.[1]

FortiEDR은 감염 전, 후 모두에 엔드포인트에 대한 고급 실시간 위협 방지를 수행함으로써 이러한 결점을 해결합니다. FortiEDR은 사전에 공격면을 줄이고, 멀웨어 감염을 방지하고, 잠재적 위협을 실시간으로 탐지 및 완화합니다. 또한 자동 및 효율적으로 랜섬웨어 피해를 차단함으로써 보안 운영을 간소화하고 사용자 및 프로덕션 장비를 온라인 작동 상태로 유지합니다.

FortiEDR의 사전 보호 절차



엔드포인트에 있는 FortiEDR 에이전트가 대부분의 파일 기반 멀웨어 사전 실행을 차단하여 감염을 방지합니다.

감염이 발생하면 FortiEDR이 실시간으로 위협을 탐지하고 완화하여 피해를 억제합니다.

위협이 억제되면 FortiEDR이 환경설정 및 클라우드 기반 인텔리전스를 기반으로 사고 대응을 조율합니다.

FortiEDR이 메모리, 스냅샷을 보존하고 포렌식 조사를 위한 지침을 제공합니다.

FortiEDR이 엔드포인트 보안을 강화하는 방법

FortiEDR은 다양한 방지, 탐지, 대응 기능을 시스템 리소스가 제한된 장치에서도 쉽게 구축할 수 있는 가벼운 설치 공간 안에 통합하는 차세대 엔드포인트 보호 솔루션입니다. FortiEDR의 주요 기능으로는 검색 및 위험 완화, 차세대 안티바이러스(NGAV), 동작 기반 탐지, 실시간 차단, 자동 사고 대응, 포렌식 조사, 위협 추적, 가상 패치 기능이 있습니다(그림 1). FortiEDR은 포티넷 보안 패브릭 아키텍처를 활용하며 FortiGate, FortiNAC, FortiSandbox, FortiSIEM 등의 보안 패브릭 구성 요소와 통합됩니다.

사전 예방적 위험 완화

FortiEDR은 기존 엔드포인트에 설치된 FortiEDR 수집기를 사용하여 관리되지 않는 장치 및 애플리케이션을 지속적으로 스캔함으로써 보안팀에 완벽한 가시성을 제공합니다. 분석가는 애플리케이션 등급, 취약점, 실시간 위협 인텔리전스를 기반으로 통신 제어 정책을 할당할 수 있습니다. 사전 예방적 위험 완화는 보호되지 않은 엔드포인트 수를 최소화하고 공격면을 줄입니다.

실시간 방지

FortiEDR에는 파일 기반 멀웨어로부터 보호하기 위한 머신러닝(ML) 기반 AV 엔진이 통합되어 있습니다. FortiEDR은 엔드포인트가 인터넷에 연결되어 있지 않은 경우에도 엔드포인트를 보호합니다. 작은 설치 공간과 다양한 운영 체제를 지원하는 FortiEDR은 제조업의 운영에서 실시간 운영 체제 및 프로세스 컨트롤러를 실행하는 POS(Point-of-Sale) 터미널과 같은 리소스가 제한된 장치에 구축될 수 있습니다.

자동 탐지 및 차단

FortiEDR은 동작 기반 탐지를 사용하여 잠재적 위협을 자동으로 식별하고 완화합니다. 이 접근 방식은 메모리 안에 숨어 있고 디스크는 건드리지 않음으로써 기존의 AV 방어를 쉽게 회피할 수 있는 파일레스(Fileless) 멀웨어에 특히 효과적입니다. 파일레스 위협은 합법적인 시스템 리소스를 이용하여(이를 자급자족이라고도 함) 완전히 메모리 안에서 공격을 실행하거나 랜섬웨어와 같은 다른 공격 벡터를 제공함으로써 악의적인 목표를 달성합니다.

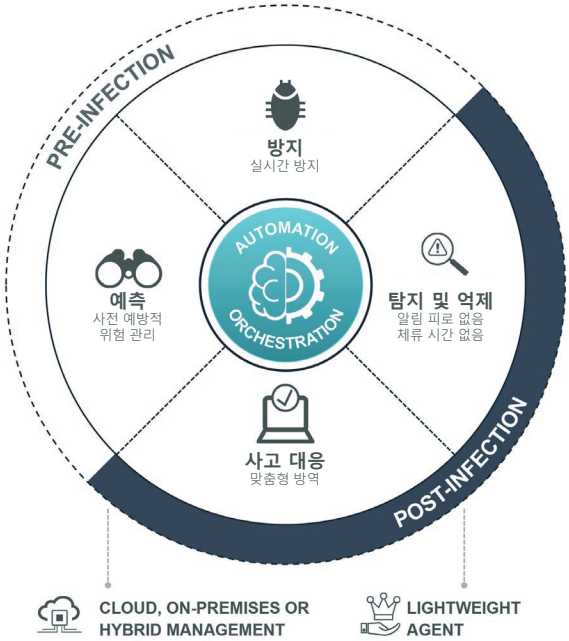


그림 1: FortiEDR은 엔드포인트 탐지 및 대응을 개선하기 위해 감염 전/후 기능 제공

의심스러운 동작이 발생할 때 FortiEDR은 요청된 모든 아웃바운드 통신을 차단하고 파일 시스템에 대한 액세스를 차단함으로써 공격을 즉시 막습니다. 동시에 FortiEDR 클라우드 기반 백엔드가 적절한 대응 조치를 위해 위협을 지속적으로 분류하고 노이즈를 제거하여 보안 분석 및 운영을 간소화합니다.

조율된 사고 대응

FortiEDR에는 조율되고 자동화된 사고 대응 및 해결을 지원하는 맞춤형 플레이북이 함께 제공됩니다. 플레이북에 의해 실행되는 일반적인 자동 작업에는 악성 프로세스 종료, 파일 제거, 잔존 위협 정리, 악의적 변경 사항 롤백, 사용자 알림, 애플리케이션 및 장치 격리, 티켓 열기 등이 있습니다.

모든 엔드포인트의 위험 허용도가 동일한 것은 아닙니다. 예를 들어, 제조 현장의 컨트롤러 시스템은 고가용성을 요구하므로 직원의 노트북보다 위험 허용도가 낮습니다. 보안 팀은 플레이북을 사용하여 위협 분류 및 엔드포인트 그룹을 기준으로 적절한 작업을 시작하는 상황 기반 사고 대응을 설계할 수 있습니다. 이 접근 방식은 일관된 사고 대응을 보장하고, 보안 팀이 일상적인 업무에 소비하는 시간을 줄이고, 기업이 엔드포인트 보안 정책을 위험 허용도에 맞출 수 있도록 도와줍니다.

포렌식 조사

FortiEDR에는 알림에 대한 명확한 설명을 제공하고 포렌식 조사를 위한 논리적 단계를 제안하는 고유한 유도형 인터페이스가 있습니다. FortiEDR은 ATT&CK 데이터베이스와 같은 신뢰할 수 있는 소스로부터 공격 기술에 대한 세부 정보를 가져와서 자동으로 더 많은 데이터를 확보합니다. 특허받은 코드 추적 기술을 통해 보안 팀은 사이버 공격 체인을 완벽하게 파악할 수 있습니다. FortiEDR은 조사에 도움이 되도록 공격의 메모리 스냅샷도 저장합니다.

비즈니스적 이점

FortiEDR은 엔드포인트 보호, 사고 대응, 보안 운영, 비즈니스 연속성 측면에서 상당한 비즈니스 가치를 제공합니다.

실시간 보호로 보안 향상

실시간으로 작동하고 머신러닝을 활용하는 FortiEDR은 실시간으로 침해를 차단하고 데이터 손실 및 랜섬웨어 피해를 방지함으로써 탐지와 대응 사이의 시간 간극을 없앱니다. FortiEDR은 기업의 엔드포인트 보호를 향상시킬 뿐만 아니라 방어기재를 우회하는 위협의 영향도 최소화합니다.

보안 운영 최적화

FortiEDR은 표준화된 맞춤형 사고 대응 프로세스를 통해 보안 워크플로를 최적화합니다. FortiEDR은 반복 작업을 자동화하고 오탐지를 최소화함으로써 직원의 시간을 절약하고 알림 피로를 줄입니다. FortiEDR은 자동으로 알림을 통합하고, 이벤트를 연결하고, 일관성 있는 공격 현황 그래프를 제공함으로써 사고 대응 및 포렌식 조사를 간소화합니다.

비즈니스 연속성 보장

FortiEDR은 실행 중인 시스템에서 대응 및 해결을 지원함으로써 운영 중단을 방지하고 사용자의 생산성을 유지합니다. FortiEDR은 제한된 시스템 리소스로 레거시 장비를 지원함으로써 유효 수명을 늘립니다. 보안 팀은 FortiEDR을 사용하여 악성 피해를 롤백하고 비용이 많이 드는 시스템의 재이미징을 예방 할 수 있습니다.

FortiEDR 특징 요약

감염 전		감염 후			
검색 및 예측	방지	탐지	완화	대응 및 조사	해결 및 롤백
사전 예방적 위험 완화	**실행 전 보호**	**실시간으로 위협 탐지**	**침해 및 데이터 손실 차단**	**전체 공격 가시성**	**방역**
• 로그(Rogue) 장치 및 IoT 검색 • 애플리케이션 및 평판 • 취약점 • 위험 기반 정책이 공격면을 줄임	• 커널 수준 • 머신러닝 및 무서명 애플리케이션	• 알림에 대한 피로 없음 • 멀웨어 분류 제공 • IOC 표시 • 전체 공격 체인 제공	• 최초이자 유일한 실시간 감염 후 차단 • 아웃바운드 통신 차단 • 데이터 유출 방지 • 데이터 변조 및 랜섬웨어 암호화 방지	• 맞춤형 사고 대응 플레이북 • 체류 시간 없앰 • 포렌식 데이터 캡처 • 파일레스 공격에 대한 메모리 스냅샷 • 시간이 될 때 위협 추적	• 악성 변경 사항 롤백 • 잘못된 파일 제거 • 지속성 정리 • 재이미지/재구축 없앰 • 비즈니스 연속성 보장 • 외부 해결 도구를 위한 REST API 출력

포티넷 구축 및 MDR 서비스

- 포티넷 Professional Services는 아키텍처 계획, 구성, 플레이북 설정 및 맞춤설정, 교육에 대한 전문가 지원을 제공합니다.
- 포티넷의 MDR 서비스인 FortiResponder는 24x7 위협 모니터링, 알림 분류, 원격 해결 서비스를 제공함으로써 사용자가 안심할 수 있도록 합니다.
- 인증된 포티넷 MSSP 파트너는 완전 관리형 SOC를 비롯한 MDR 서비스를 제공합니다.

결론

지능형 위협 및 랜섬웨어가 꾸준히 더 늘어나고 복잡해짐에 따라 기업은 엔드포인트를 포함하여 전반적으로 보안 조치를 강화해야 합니다. FortiEDR은 가볍고 배포가 용이한 차세대 엔드포인트 보호, 탐지, 대응 기능을 제공합니다. 보안 팀은 FortiEDR을 통해 엔드포인트 보안을 강화함으로써 사고 대응 속도를 높이고, 보안 운영을 간소화하며, 프로덕션 라인 및 지식 근로자의 작업 중단으로 인한 비용 손실을 방지할 수 있습니다.

FortiEDR의 일반적인 사용 사례

운영 기술 보안

FortiEDR은 운영 기술(OT) 환경에서 위협을 방지, 탐지, 완화하는 동시에 운영의 중단을 방지하기 위해 시스템을 온라인 상태로 유지합니다. FortiEDR은 취약점을 발견하며 다음 유지 보수 기간까지 시스템을 공격으로부터 보호하기 위해 가상 패치 적용과 같은 완화 장치를 제공합니다. FortiEDR은 장치 성능에 영향을 미치지 않으면서 레거시 장비 및 보안 시스템을 지원하는 적은 설치 공간이 특징입니다.

POS(Point-of-Sale) 보안

FortiEDR은 POS(Point-of-Sale)에서 신용 카드 정보를 보호하여 소스 공격을 차단합니다. PCI DSS(Payment Card Industry Data Security Standard) 인증을 받은 FortiEDR은 시스템 손상 시 데이터 유출을 방지합니다. FortiEDR은 가상 패치를 제공하여 POS 시스템을 취약점으로부터 보호합니다. FortiEDR은 설치 공간이 작아 레거시 POS 장비에 적합하며 OS 지원이 기본 제공됩니다.

[1] "How To Protect Your Networks from Ransomware," U.S. Federal Bureau of Investigation, 2020년 2월 3일 액세스.

FORTINET

www.fortinet.com/kr

서울특별시 강남구 영동대로 325 에스타워 14 /15층 전화: 080-559-8989 Email: **kr-callcenter@fortinet.com**

580266-0-0-EN