데이터 시트

FortiEDR™

실시간 엔드포인트 보호, 탐지 및 자동 대응

FortiEDR™은 유연한 배포 옵션과 예측 가능한 운영 비용으로 단일 통합 플랫폼에서 현재 및 기존 운영 체제는 물론 제조 및 OT 시스템을 갖춘 워크스테이션과 서버를 비롯한 모든 통신 장치에 대하여 설정된 사고 대응을 통해 실시간 자동 엔드포인트 보호 기능을 제공합니다.

실시간 사전 예방 위험 완화 및 IoT 보안

공격면을 사전에 축소하는 예방 조치를 지원합니다. 예를 들어 취약성 평가 및 사전 예방적 위험 완화 기반 정책 등 취약점이 있는것으로 알려진 모든 애플리케이션의 통신 관리도 지원할 수 있습니다.

사전 보호

파일 기반 멀웨어의 감염을 방지하는 맞춤형 커널 레벨 차세대 머신러닝 기반 안티바이러스(NGAV) 엔진을 통해 1차 방어선을 제공합니다.

사후 보호

FortiEDR은 엔드포인트가 손상된 경우에도 지능형 공격을 실시간으로 탐지하고 중지하는 유일한 솔루션입니다. 피해가 발생하지 않고, 데이터가 손실되지 않으며, 아무런 문제가 없습니다. FortiEDR은 체류 시간을 없애고 자동화된 EDR(Endpoint Detection and Response) 기능 집합을 제공하여 사고를 탐지, 완화, 조사, 대응, 해결합니다.

지원되는 플랫폼

- Windows XP SP2/SP3, 7, 8.x 및 10.x, Windows Server 2003 R2, 2008 R1, 2008 R2, 2012, 2012 R2, 2016, 2019
- macOS Yosemite(10.10), El Capitan (10.11), Sierra(10.12), High Sierra (10.13), Mojave(10.14), Catalina(10.15)
- VDI 환경: VMware Horizons 6 및 Citrix XenDesktop/XenApp
- Red Hat Enterprise Linux 6.8, 6.9, 6.10 및 7.x
- CentOS 6.8, 6.9, 6.10 및 7.x
- Ubuntu 16.04, 18.04

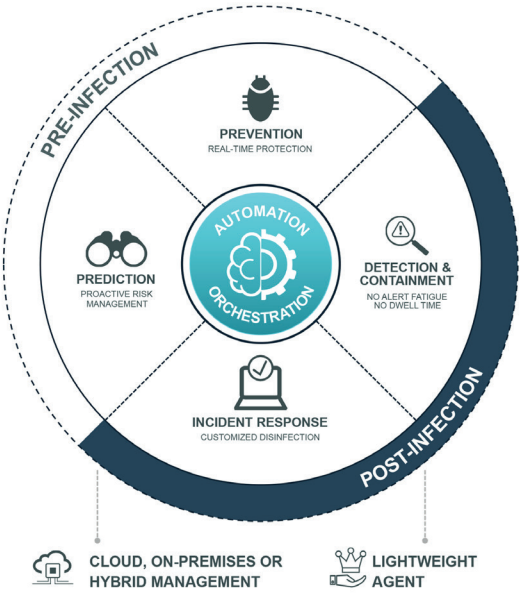
HIPAA COMPLIANT

PCI DSS COMPLIANT

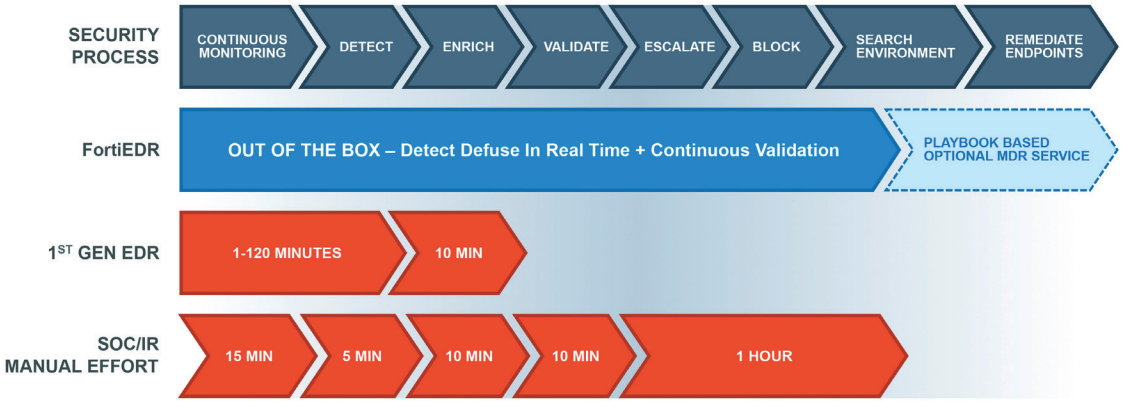
하이라이트

포괄적인 엔드포인트 보안 플랫폼

FortiEDR은 지능형 위협을 탐지하고 이미 손상된 장치에서도 실시간으로 침해 및 랜섬웨어 피해를 막음으로써 자동으로 사고에 대응하고 해결하여 데이터를 보호하고, 시스템 가동 시간을 보장하며, 비즈니스 연속성을 유지하도록 처음부터 제작된 유일한 엔드포인트 보안 솔루션입니다. FortiEDR은 현재 및 기존 운영 체제를 갖춘 워크스테이션과 서버부터 POS 및 제조 컨트롤러에 이르기까지 모든 것을 보호합니다. 네이티브 클라우드 인프라로 제작된 FortiEDR은 클라우드 또는 보안 환경 내의 온프레미스에 구축되거나 하이브리드로 구축될 수 있습니다.



장점



FortiEDR은 보안 프로세스를 자동화하고 과도한 알림이나 지체 시간 없이 감염 후 실시간 보호를 제공합니다.

보호

FortiEDR을 사용하면 플랫폼 전반에서 설정된 사고 대응을 통해 사전 예방적인 실시간 자동 엔드포인트 보호를 받을 수 있습니다. 실시간 감염 후 차단으로 침해를 막아 유출 및 랜섬웨어 암호화로부터 데이터를 보호합니다.

관리

FortiEDR은 직관적인 인터페이스를 갖춘 단일 통합 콘솔을 제공합니다. 사람이 수동으로 작업할 필요가 없도록 클라우드 관리형 플랫폼이 루프를 닫고 일상적인 엔드포인트 보안 작업을 자동화합니다.

확장성

네이티브 클라우드 인프라를 사용하며 설치 공간이 작은 FortiEDR을 구축하고 빠르게 확장함으로써 수십만 개의 엔드포인트를 보호할 수 있습니다.

유연성

FortiEDR은 다양한 엔터프라이즈 사용 사례를 처리할 수 있습니다. 클라우드 관리 플랫폼을 보안 환경 내의 온프레미스에 또는 보안 클라우드 인스턴스에 구축할 수 있습니다. 엔드포인트는 온라인과 오프라인 모두에서 보호됩니다.

비용

침해 전의 운영 비용과 조직에 미치는 침해 피해를 없앰으로써 비용을 낮추고 예측할 수 있으며 TCO 상승을 억제할 수 있습니다.

특징

검색 및 예측

FortiEDR은 보안 팀이 다음을 수행할 수 있도록 취약성 평가 및 검색 기능을 갖춘 최첨단 자동 공격면 정책 제어를 제공합니다.

- 로그(Rogue) 장치(예: 보호되지 않거나 관리되지 않는 장치) 및 IoT 장치를 검색하고 제어합니다.
- 애플리케이션 및 등급을 추적합니다.
- 시스템 및 애플리케이션 취약성을 검색하고 가상 패치 적용을 통해 완화합니다.
- 사전 예방적 위험 완화 기반 정책을 통해 공격면을 줄입니다.

방지

FortiEDR은 머신러닝 안티바이러스 엔진을 사용하여 멀웨어를 실행되기 전에 차단합니다. 이 크로스-OS NGAV 기능은 구성 가능하며 간단한 단일 에이전트에 내장되어 있으므로 사용자는 추가 설치 없이 모든 엔드포인트 그룹에 안티멀웨어 보호를 할당할 수 있습니다.

- 머신러닝 커널 기반 NGAV를 사용합니다.
- 지속적으로 업데이트되는 클라우드 데이터베이스의 실시간 위협 인텔리전스 피드를 통해 더 많은 결과를 얻습니다.
- 단절된 엔드포인트를 오프라인 보호 기능을 통해 보호합니다.
- USB 장치 제어

검색 및 완화

FortiEDR은 파일에 기반하지 않은 멀웨어 및 기타 고급 공격을 실시간으로 탐지 및 제거하여 데이터를 보호하고 위반을 방지합니다. FortiEDR은 의심스러운 프로세스 흐름과 동작을 탐지하는 즉시 해당 프로세스가 요청하는 아웃바운드 통신과 파일 시스템 액세스를 차단함으로써 잠재적 위협을 즉시 완화합니다. 이 단계는 데이터 유출, 명령 및 제어(C&C) 통신, 파일 변조, 랜섬웨어 암호화를 방지합니다. 동시에 FortiEDR 백엔드는 잠재적 자동 사고 대응 플레이북 정책을 적용할 수 있도록 계속해서 추가 증거를 수집하고, 더 많은 이벤트 데이터를 생성하고, 사고를 분류합니다. FortiEDR은 물리적으로 데이터 침해 및 랜섬웨어 피해를 실시간 방지함으로써 이미 손상된 장치에서도 자동으로 비즈니스 연속성을 보장합니다.

- 메모리 기반 공격과 "자급자족" 공격(공격자가 피해자의 윈도우 운영체제를 사용해 탐지를 피하는 방법) 등 몰래 침투한 공격을 매우 정확하게 탐지하는 OS 중심 탐지를 활용합니다.
- 침해를 실시간으로 차단하고 위협 체류 시간을 없앱니다.
- 전체 로그 기록을 분석합니다.
- 랜섬웨어 암호화 및 파일/레지스트리 변조를 방지합니다.
- 위협 타입을 지속적으로 검증합니다.
- 신호 대 잡음비(Signal-to-Noise Ratio)를 개선하고 알림 피로를 없앱니다.

대응 및 해결

여러 환경을 파악하고 있는 맞춤형 플레이북을 사용하여 사고 대응 작업을 설정합니다. 사고 대응 및 해결 프로세스를 간소화하고, 이미 탐지된 위협에 의해 이루어진 악의적인 변경을 수동으로 또는 자동으로 롤백합니다. 이러한 작업을 단일 장치에서 또는 환경 전반의 모든 장치에서 수행할 수 있습니다.

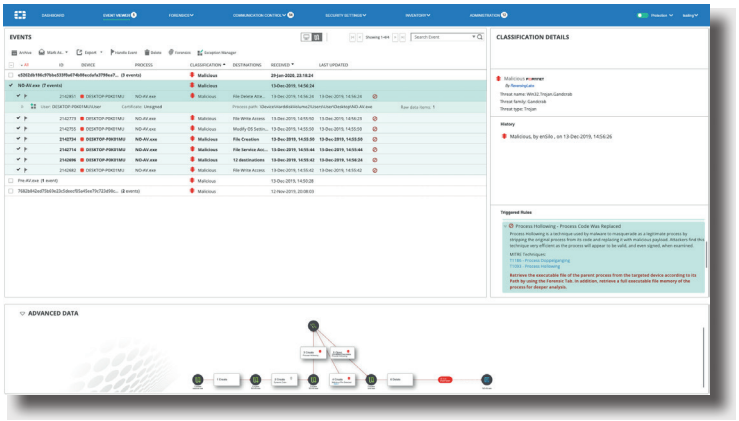
- 사고 분류를 자동화하고 신호 대 잡음비를 개선합니다.
- 플레이북 자동화를 통해 사고 대응 절차를 표준화합니다.
- 파일 제거, 악성 프로세스 종료, 영구적 변경 되돌리기, 사용자에게 알림, 애플리케이션 및 장치 격리, 티켓 열기 등의 사고 대응 작업을 자동화하여 보안 리소스를 최적화합니다.
- 사고 분류 및 공격 대상(예: 엔드포인트 그룹)에 따라 상황에 맞는 사고 대응을 활성화합니다.
- 특허를 받은 코드 추적 기능을 통해 공격 체인 및 악의적인 변경 사항을 완벽하게 파악합니다.
- 시스템 가동 시간을 유지하면서 정리 및 악의적인 변경 사항 롤백을 자동화합니다.
- 선택적인 관리형 탐지 및 대응(MDR) 서비스를 제공합니다.

특징

조사 및 추적

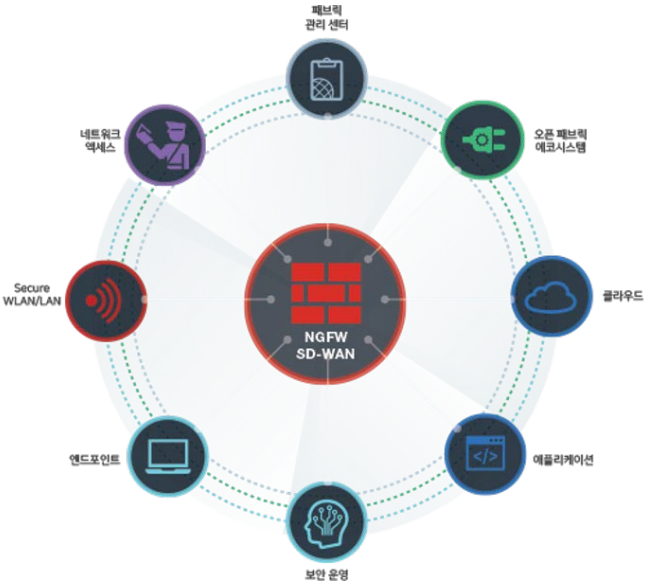
FortiEDR은 감염 전후에 모두 멀웨어에 대한 자세한 정보를 사용하여 더 많은 데이터를 확보함으로써 침투된 엔드포인트에 대한 포렌식을 수행합니다. 고유의 가이드 인터페이스가 유용한 안내와 모범 사례를 제공하며 합당한 후속 단계를 보안 분석가들에게 제안합니다.

- 최종 사용자의 중단을 최소화하면서 조사를 자동화합니다.
- 자동으로 위협을 완화하고 차단함으로써 보안 분석가가 스스로의 속도에 맞춰 추적할 수 있도록 합니다.
- 특허를 받은 코드 추적 기술이 장치가 오프라인 상태일 때에도 스모킹 건(Smoking Gun)을 가리키는 전체 공격 체인 및 스택 가시성을 제공합니다.
- 메모리 기반 위협 추적을 위해 메모리 내 공격의 메모리 스냅샷을 보존합니다.
- 가이드 인터페이스는 이벤트가 의심스럽거나 악의적인 것으로 플래깅된 이유를 명확히 설명하고, 해당 MITRE 공격 프레임워크를 나열하고, 포렌식 조사를 위한 논리적 단계를 표시합니다.



가이드 인터페이스는 이벤트가 의심스럽거나 악의적인 것으로 플래깅된 이유를 명확히 설명하고, 해당 MITRE 공격 프레임워크를 나열하고, 포렌식 조사를 위한 논리적 다음 단계를 표시합니다.

보안 패브릭 통합



FortiEDR은 포티넷 보안 패브릭 아키텍처를 활용하며 FortiGate, FortiNAC, FortiSandbox, FortiSIEM 등 여러 보안 패브릭 구성 요소와 통합됩니다.

FortiGate

FortiEDR 커넥터를 사용하면 엔드포인트 위협 인텔리전스 및 애플리케이션 정보를 FortiGate와 공유할 수 있습니다. FortiEDR 관리는 침투 공격 후 IP 주소를 일시 중단하거나 차단하는 등 FortiGate에 대한 향상된 대응 조치를 지시할 수 있습니다.

FortiNAC

FortiEDR은 엔드포인트 위협 인텔리전스 및 검색된 자산을 FortiNAC와 공유합니다. Syslog 공유를 통해 FortiEDR 관리는 장치 격리와 같은 향상된 대응 조치를 FortiNAC에 지시할 수 있습니다.

FortiSandbox

FortiEDR과 FortiSandbox의 네이티브 통합 기능은 클라우드의 샌드박스에 파일을 자동으로 전송하여 실시간 이벤트 분석 및 분류 작업을 지원합니다. 또한 FortiSandbox와 위협 인텔리전스를 공유합니다.

FortiSIEM

FortiEDR은 위협 분석 및 포렌식 조사를 위해 FortiSIEM에 이벤트 및 알림을 보냅니다. FortiSIEM에는 FortiEDR OOTB 전용 파서가 포함되어 있으며, FortiEDR과 더욱 긴밀히 통합하기 위해 JSON 및 REST API를 활용할 수도 있습니다.

FortiGuard Labs

FortiEDR과 FortiGuard Labs의 네이티브 통합을 통해 최신 인텔리전스를 확보함으로써 실시간 사고 분류를 지원하여 정확한 사고 대응 플레이북을 활성화할 수 있습니다.

서비스

FortiEDR 구축 서비스
구축 서비스는 성공적인 구축을 보장하기 위한 전문가의 도움을 제공합니다. 아키텍처 및 계획, 구성, 설치, 플레이북 설정, 환경 조정, 교육을 포함합니다.

FortiResponder 관리형 탐지 및 대응(MDR) 서비스
FortiResponder 관리형 탐지 및 대응(MDR) 서비스는 숙련된 분석가 및 플랫폼에 의한 상시 위협 모니터링, 알림 분류, 사고 처리 기능을 고객에게 제공합니다.

고도로 숙련된 전문가가 모든 알림을 검토 및 분석하고, 고객을 안전하게 보호하기 위한 조치를 취하고, 사고 대응자 및 IT 관리자들에게 문제 해결 및 다음 단계에 대한 세부적인 권장 사항을 제공하기 때문에 고객은 언제나 안심할 수 있습니다. FortiResponder MDR 서비스는 기존 운영을 확장하고 SOC의 성숙도를 더욱 향상시킬 수 있도록 도와줍니다.

사양

관리, 아키텍처 및 플랫폼 지원
단일 통합 관리 콘솔이 예방, 탐지 및 사고 대응 기능을 제공합니다. 확장 REST API를 사용하여 모든 콘솔 작업 그리고 그 이상을 지원할 수 있습니다.

- **오프라인 보호** - 보호 및 탐지가 엔드포인트에서 이루어지므로 단절된 엔드포인트를 보호합니다.
- **네이티브 클라우드 인프라** - FortiEDR은 클라우드에서 멀티테넌트 관리를 제공합니다. 이 솔루션은 클라우드 네이티브, 하이브리드 또는 온프레미스로 구현될 수 있습니다. 보안 환경도 지원합니다.
- **가벼운 엔드포인트 에이전트** - FortiEDR은 1% 미만의 CPU, 최대 120MB의 RAM, 20MB의 디스크 공간을 활용하며 네트워크 트래픽을 최소화합니다.

FortiEDR은 Windows, macOS 및 Linux 운영 체제를 지원하며 오프라인 보호를 제공합니다.

- Windows(32비트 및 64비트 버전 모두) XP SP2/SP3, 7, 8, 8.1 및 10
- Windows Server 2003 R2 SP2, 2008 R1 SP2, 2008 R2, 2012, 2012 R2, 2016 및 2019
- macOS 버전: Yosemite(10.10), El Capitan(10.11), Sierra(10.12), High Sierra(10.13), Mojave(10.14) 및 Catalina(10.15)
- Linux 버전: RedHat Enterprise Linux 및 CentOS 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7 그리고 Ubuntu LTS 16.04.5, 16.04.6,
- 18.04.1 및 18.04.2 서버, 64비트
- VMware 및 Citrix 내 VDI(Virtual Desktop Infrastructure) 환경. VDI 환경: VMware Horizons 6 및 7 그리고 Citrix XenDesktop 7

www.fortinet.com/kr

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