솔루션 소개서

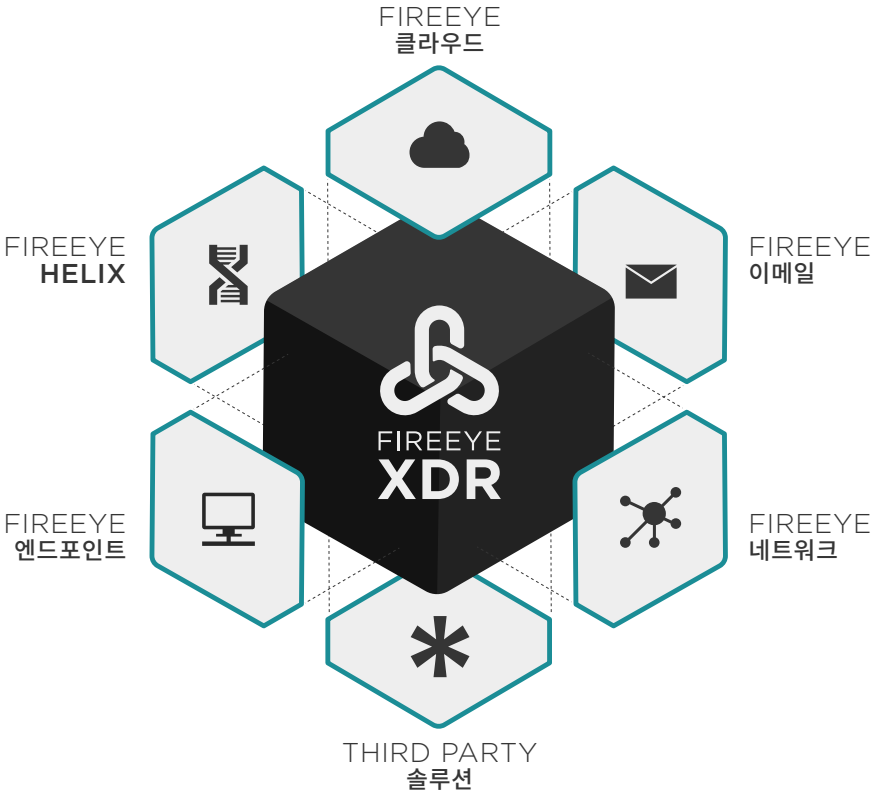
FireEye XDR을 통한 보안 아키텍처 통합

XDR(eXtended Detection and Response: 확장된 탐지 및 대응)은 끊임없이 변화하는 위협 환경과 여러 보안 솔루션의 통합 관리에 대한 니즈로 인해 생겨났습니다. XRD은 궁극적으로 엔드포인트 탐지 및 대응(EDR), 네트워크 분석 및 가시성(NDR), 이메일 보안, 보안 정보 및 이벤트 관리(Security Information and Event Management, SIEM), 보안 오케스트레이션, 자동화 및 대응(SOAR), 클라우드 보안 등과 같은 보안 및 비즈니스 기술에서의 텔레메트리(telemetry) 기능을 위협 탐지 및 대응 솔루션으로 통합하는 것입니다.

XDR이 정의되기 전에도 FireEye는 고객에게 XDR의 효과를 내는 솔루션을 제공하기 위해 노력해 왔습니다. FireEye는 침해 사고 데이터의 상관 관계를 파악하고, 최일선에서의 인텔리전스와 분석 정보를 적용하여 문제가 되는 위협의 우선순위를 정하고 이에 대응함으로써 위협의 모든 것을 파악합니다. 보안 복잡성을 줄이고 보안 담당자들의 업무 효율을 높이기 위해 FireEye XDR은 고객에게 간소화된 위협 탐지, 조사, 침해 사고 대응 기능을 제공할 뿐만 아니라 애널리스트의 역량을 높여 줍니다.

그림 1.

FireEye의 자체 기술뿐만 아니라 여러 소스를 통한 광범위한 서드파티 데이터를 연동하여 통합 제공합니다.



최근의 보안 과제

고객들은 공격자가 방어 체계를 우회하여 쉽게 침투할 수 있는 보안 솔루션을 여전히 사용하고 있습니다. 이러한 보안 투자 상황에는 다음의 3가지 위험 요소가 존재합니다.

- **앞으로 일어날 보안 위협에 대비하지 못한 채 현재 공격 상황에만 대응**
  조직은 현재 위협에 대해 사전 조치를 취하고 최신 정보를 유지해야 합니다. 하지만 대부분의 조직에 있어 아직 일어나지 앞은 잠재 위협에 대해 선제적인 보안 조치를 취한다는 것은 어려운 일입니다. 앞으로 일어날 수 있는 공격까지 검토할 전문성이나 인력을 갖추지 못하고 있기 때문입니다. 대부분 조직에서는 잠재적인 공격으로부터 자산을 보호할 수 있게 대비하는 인텔리전스가 부족합니다.

- **오류가 발생하기 쉬운 수동 프로세스에 의존하고 있는 보안**
  보안 인프라를 관리하기 위해 수동 프로세스에만 의존하고 있어 문제 상황이 발생하고 있습니다. 많은 조직의 경우 발생된 경보가 오탐이 아닌 것을 확인하기까지 많은 단계를 거쳐 일일이 검토해야 합니다. 이로 인해 경보를 점검하는 데 있어 불필요한 시간을 낭비하게 됩니다. 공격자들은 타이밍을 놓치지 않고 매일 더 많이, 더 빠르게 공격을 수행합니다.

- **보안 솔루션을 자체 개발하여 많은 투자 비용 소요**
  많은 조직이 직접 보안 솔루션을 개발함으로써 투자 비용을 절약하고 있다고 생각합니다. 하지만 안타깝게도 이러한 솔루션은 전문 벤더의 솔루션을 사용하는 것보다 더 많은 비용이 드는 경우가 많습니다. 자체 개발된 솔루션은 업데이트가 불가능하거나, 전문성 부족 또는 그 외 다른 문제로 인해 제 기능을 하지 못할 수도 있기 때문에 이미 검증된 외부 솔루션보다 보안성이 좋지 않은데도 불구하고 비용 부담은 더 커지게 됩니다.

FireEye XDR로 신속한 위협 대응 및 피해 완화

통합형 FireEye XDR 플랫폼은 보안 자산의 데이터를 통합 및 분석하여 문제가 되는 위협에 대응할 수 있습니다.

FireEye XDR 특장점

- **공격 탐지에서 향후 위협 방지로 범위 확대**
  방법: FireEye 기술은 인바운드 이메일 공격, 네트워크 기반 공격, 엔드포인트 공격을 차단합니다. 모든 위협 벡터에 대한 보안 데이터를 통합 관리함으로써 분석 업무를 단순화할 수 있습니다.

- **고도화된 공격에 대한 완전한 탐지**
  방법: FireEye는 조직 전반에 걸쳐 여러 가지 툴에서 나온 데이터의 상관 관계를 파악하여 보안 침해 사고를 확실히 탐지할 수 있도록 합니다. 그에 이어 FireEye 및 서드파티 보안 기술 솔루션 전반에서 위협 환경에 대한 정보를 활용할 수 있습니다.

- **주도권을 가진 대응**
  방법: FireEye는 조사 업무의 워크플로우를 제시합니다. 이를 통해 보안 침해 사고에 대한 워크플로우를 정형화할 수 있습니다. 궁극적으로는 보안 시스템상의 주요 문제를 해결하여 분석 시간을 우선순위에 따라 조정하고 리스크를 줄일 수 있게 됩니다.

FireEye XDR은 최고의 자동화 기술을 기반으로 업계에서 검증된 기술력과 위협 인텔리전스를 비롯한 사이버 보안 전문성으로 이루어져 있습니다. 다양한 보안 효과를 제공하지만 특히 다음의 혜택을 기대할 수 있습니다.

- **애널리스트 및 SOC 효율성 향상**: 여러 시스템상에서 발생된 여러 이벤트들의 상관 관계를 파악하여 조사
- **리스크 감소**: 위협 탐지 및 조사 프로세스를 자동화하고 대응 속도를 높여 침해 사고 예방을 위한 작업 우선순위 지정
- **위협 탐지 기능의 높은 효율성** 및 분석 정보 제공: 매일 업데이트되는 침해 사고 대응에 대한 모범 사례의 플레이북을 통해 변화하는 글로벌 위협 환경 반영
- **전략에 맞게 솔루션 기능 최적화**: 이를 통해 FireEye 솔루션과 서드파티 솔루션을 자유롭게 조합하여 운영

XDR의 높은 유연성

성능을 최적화하고 정교한 위협 상황에 맞설 수 있도록 보안 태세를 개선하려면 FireEye Endpoint Security, 이메일 보안, 네트워크 보안, Cloudvisory를 Helix와 연동할 것을 권장합니다. 이를 통해 지능형 공격 및 측면 이동(lateral movement)을 탐지하기 위한 추가 분석 기능으로 FireEye XDR 플랫폼의 성능을 향상시킬 수 있습니다.

FireEye XDR은 모든 FireEye 기술과 전문성을 연계하여 단일 플랫폼으로 제공되므로 엔드포인트, 네트워크, 클라우드, 이메일 전반의 위협을 원활하게 탐지할 수 있습니다. 다양한 서드파티 보안 툴을 쉽게 연동할 수 있으므로 기존 보안 시스템의 특성을 잘 파악하여 조직의 보안 요구사항에 맞춘 전략을 세울 수 있습니다.

자세한 정보는 파이어아이 영업팀으로 문의하시기 바랍니다.

FireEye에 대한 자세한 정보: **www.FireEye.kr**

FireEye Korea
서울특별시 강남구 테헤란로 507
WeWork 빌딩 12층 112호
02-6959-4017
korea.info@fireeye.com

FireEye 소개

FireEye는 인텔리전스 기반의 보안 솔루션을 제공합니다. FireEye는 혁신적인 보안 기술, 최고의 Threat Intelligence 및 세계적으로 인정받는 Mandiant® 컨설팅을 결합한 단일 플랫폼을 제공하여 고객 보안 운영 플랫폼을 완벽하게 확장하여 보안을 강화시킵니다. 이를 통해 FireEye는 사이버 공격에 대비하고 이를 방어 및 대응하고자 노력하는 조직의 사이버 보안 부담을 줄이고 보안 운영의 복잡성을 간소화합니다.

FIREEYE™