

## 데이터 시트

# FireEye Helix

보안 운영 업무를 위한 최적의 탐지 및 인텔리전스



### 주요 기능

- **지능형 위협 탐지:** 600여 개의 FireEye 및 서드파티 보안 솔루션과 연동하여 상황별 위협 인텔리전스 및 행동 분석을 통해 상세 정보를 제공합니다.
- **침해 사고의 피해 최소화:** 최일선에서 얻은 정보를 바탕으로 보안 기능을 오케스트레이션하고 워크플로우를 자동화하여 대응을 가속화합니다.
- **모든 위협 경로 및 배포 유형에 대한 가시성 확보:** 온프레미스 또는 클라우드에서 보안 데이터 및 인프라를 차세대 SIEM으로 중앙집중화하여 위협 및 취약점을 완벽하게 파악합니다.

### 머리말

사이버 보안은 그 어느 때보다 어려운 문제로 대두되었습니다. 매일 새로운 위협이 등장하고 취약점들이 노출됨에 따라 기업들은 추가로 보안 제품을 구매하고 인력을 보강할 수밖에 없는 상황에 놓여 있습니다. 이같이 문제 상황에 놓인 후 사후 대응하는 방식은 복잡성이 가중되고, 이는 공격자들이 악용할 수 있는 또 다른 취약점이 됩니다. 효율적인 보안 운영 업무를 위해서는 종합적이고 근본적인 접근 방식이 필요합니다. FireEye Helix는 조직이 그러한 토대를 구축하는 데 도움을 드립니다.

FireEye Helix는 SaaS 보안 플랫폼으로, 조직은 이를 통해 침해 사고 탐지부터 대응에 이르는 모든 과정을 제어할 수 있습니다. 모든 FireEye 솔루션과 함께 기존 보안 솔루션을 연동하여 이를 차세대 SIEM(Security Information and Event Management, 보안 정보 및 이벤트 관리), 오케스트레이션 및 위협 인텔리전스로 강화하고 보안 투자의 효율성을 극대화합니다. 보안 전문가들에 의해 보안 전문가가 직접 설계한 이 제품은 보안 담당자가 경보 관리, 조회, 분석, 조사, 리포팅과 같은 주요 업무를 효율적으로 수행할 수 있도록 도움을 드립니다.

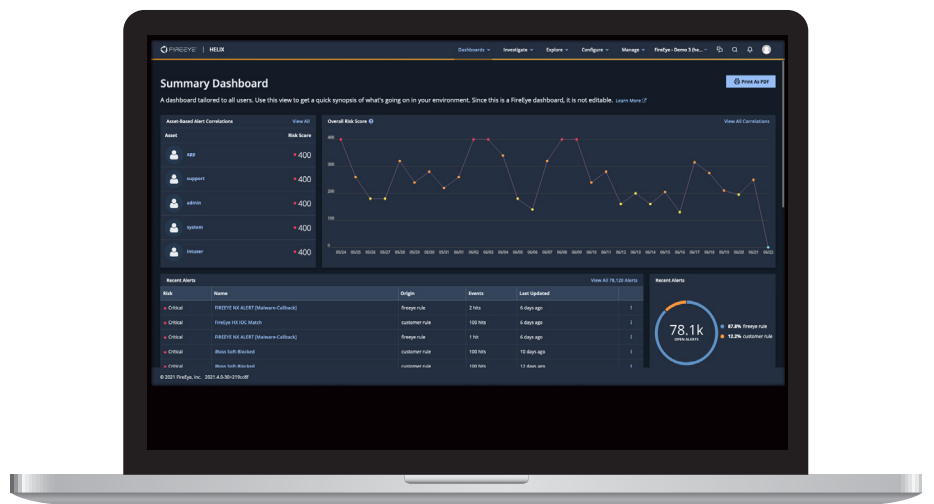


그림 1. 즉각적인 상황 인식에 효율적인 운영 인터페이스.

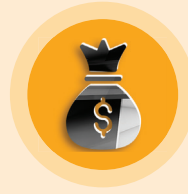
### ● ● ● FireEye Helix의 기능



여러 틀에서 나온 데이터의 연관성을 분석하여 보안 침해 사고 탐지



상황별 위협 인텔리전스와 명확한 근거에 의한 효율적인 의사 결정



보안 데이터 및 인프라 중앙집중화



**위협 인텔리전스**  
다양한 기능을 통해 최신 위협을 파악하십시오.



**차세대 SIEM**  
고도화된 사용자 행동 분석 기능으로 위협 및 취약점 탐지 성능을 개선하십시오.



**보안 오케스트레이션 및 자동화(SOAR)**  
보안 전문가가 사전에 설계한 플레이북을 기반으로 대응 체계를 자동화합니다.



**사용자 및 개체 행동 분석(UEBA)**  
머신 러닝의 경보 연관성 분석으로 내부자 위협, 측면이동(lateral movement) 또는 진행이 많이 되어 있는 공격에 대한 리스크를 확인합니다.



**워크플로우 관리**  
자동화 또는 매뉴얼 워크플로우를 통해 조사 프로세스 상에서 필요한 조치를 수행합니다.



**컴플라이언스 리포팅**  
대시보드 및 위젯을 사용자 지정으로 구성해서 가장 중요한 정보를 시각적으로 종합하여 확인할 수 있습니다.

### FireEye Helix Platform을 사용하는 방법

FireEye Helix는 다양한 FireEye의 구독 기반 솔루션들과 함께 사용할 수 있습니다. 모든 FireEye 제품과 연동되며 기존에 사용 중인 서드파티 보안 솔루션들과도 연동됩니다. 조직의 성장과 변화에 맞춰 비즈니스 운영에 지장을 주지 않으면서 FireEye 솔루션을 재구성하거나, 추가 또는 업그레이드할 수 있습니다.

FireEye에 대한 자세한 정보: [www.FireEye.kr](http://www.FireEye.kr)

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

©2020 FireEye, Inc. 저작권 소유. FireEye는 FireEye, Inc.의 등록상표입니다. 다른 모든 브랜드, 제품 또는 서비스 명칭은 각 소유자의 상표 또는 서비스 마크입니다. H-EXT-DS-US-EN-000050-07

**FireEye, Inc. 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 확장함으로써 보안을 강화시킵니다. 이를 통해 FireEye는 사이버 공격에 대비하고 이를 방어 및 대응하고자 노력하는 조직의 사이버 보안 부담을 줄이고 보안 운영의 복잡성을 간소화합니다.

