

인텔리전스 기반 보안운영 플랫폼

# FireEye® HELIX

최강의 통합 보안 운영 솔루션과 서비스! IT환경에서 고객을 보다 자유롭고 편리하게

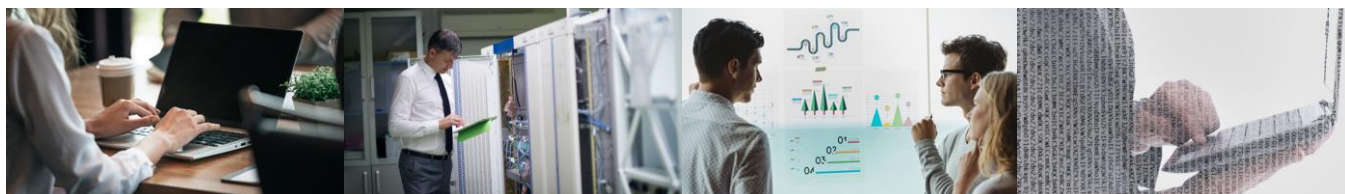
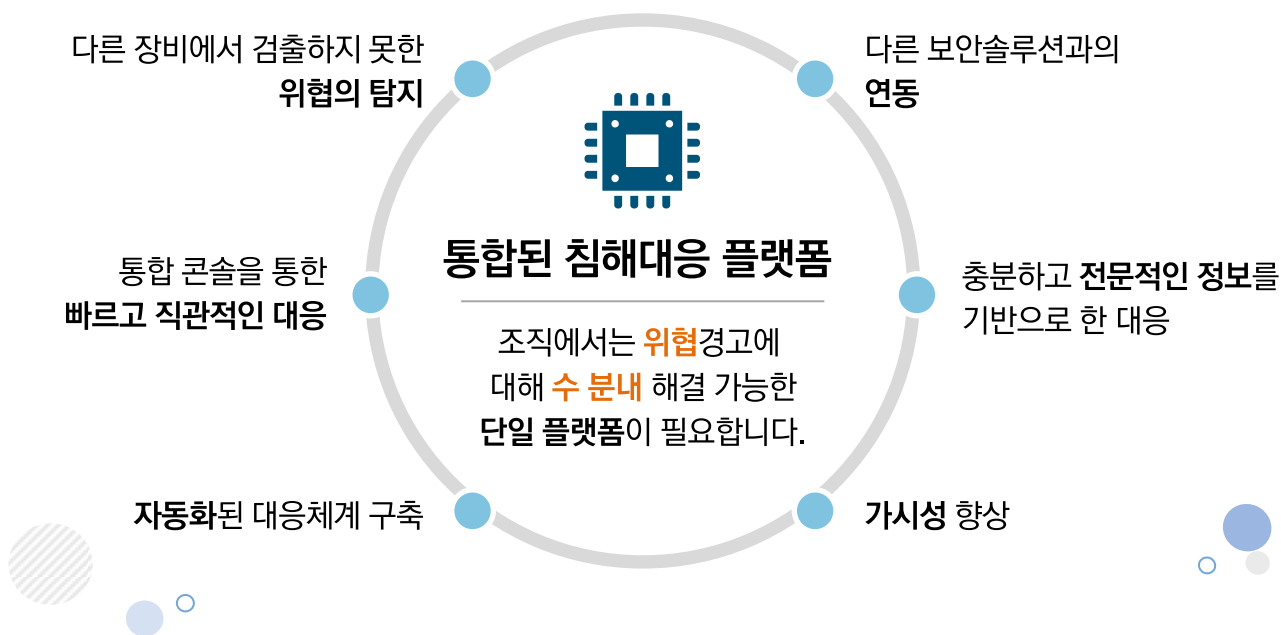


## 보안운영관련 현안

### >>> 보안운영관련 조직의 현안

| 가시성 부족        | 너무 많은 보안장비     | 너무 많은 보안 이벤트  |
|---------------|----------------|---------------|
| <p>99 day</p> | <p>85</p>      | <p>10 k</p>   |
| 제한된 대응시간      | 인텔리전스 부족       | 비용의 증가        |
| <p>20 min</p> | <p>32 days</p> | <p>\$ 4 M</p> |

### >>> 통합관리의 필요성



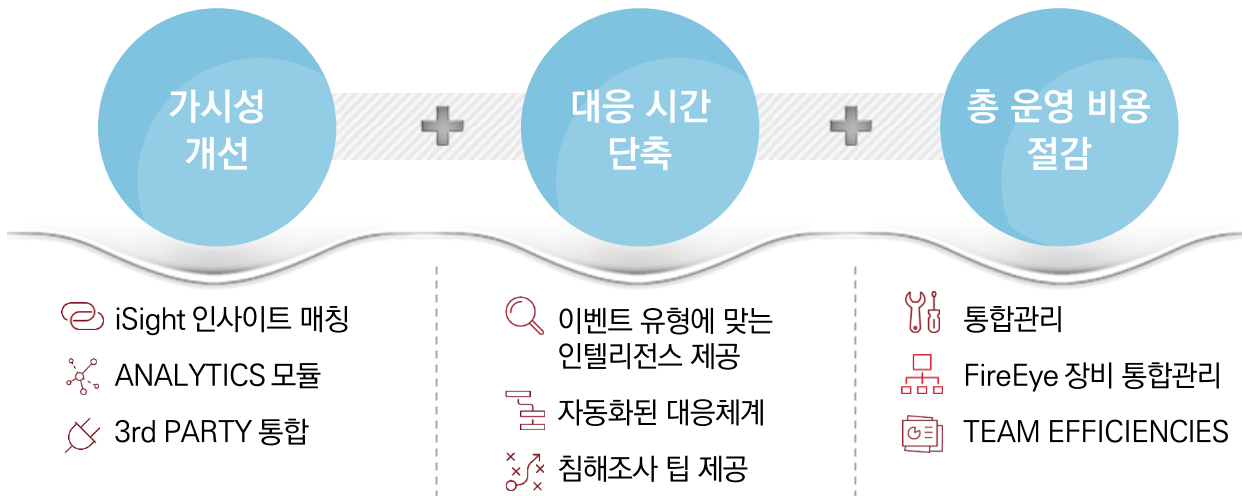
## FireEye HELIX

### Intelligence-led Security Operations Platform

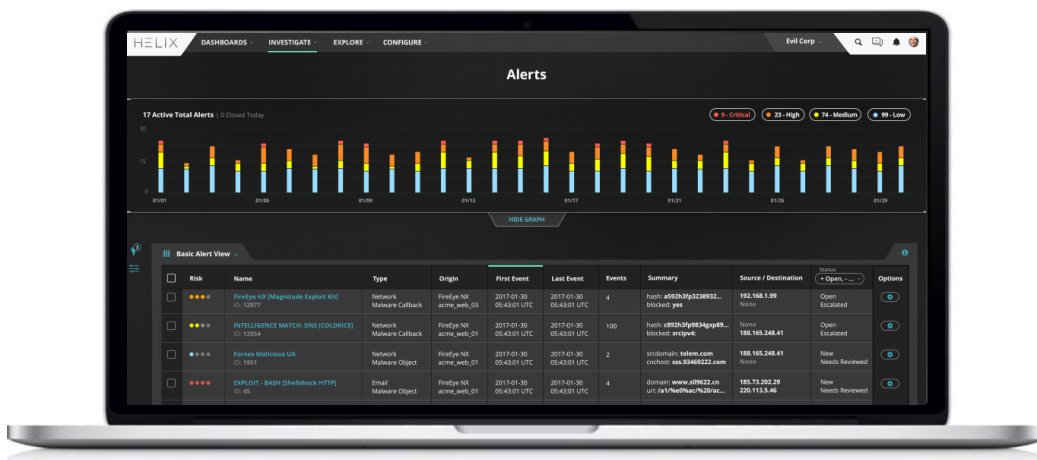
사이버 보안은 그 어느 때보다 어려운 문제로 대두되었습니다. 매일 새로운 위협이 등장하고 취약점들이 노출됨에 따라 기업들은 제품을 추가로 구매하고 인재를 보강해야 한다는 압력을 받고 있습니다. 이 같은 사후 대응적 방식은 복잡성을 가중시키고, 이 같은 복잡성은 공격자들이 악용할 또 다른 취약점이 됩니다. 효율적인 보안 운영을 위해서는 종합적이고 근본적인 접근 방식이 필요합니다. FireEye HELIX는 조직이 그러한 토대를 구축하는 데 도움을 줍니다.

FireEye HELIX는 간단한 방식으로 모든 조직에 첨단 보안을 제공하는 보안 운영 플랫폼입니다. 이전에 볼 수 없었던 위협을 노출시키고 전문가가 인텔리전스를 활용해 결정을 내릴 수 있도록 함으로써, 방어 시스템에 대한 제어력을 다시 확보해 주고 보안 투자 효과를 극대화합니다. FireEye HELIX는 모든 FireEye 솔루션과 함께 사용할 수 있으며, 타사 제품을 비롯하여 모든 보안 솔루션을 연결하고 개선할 수 있는 효율적이고 확장성이 뛰어난 토대가 됩니다. 보안 전문가에 의해, 보안 전문가를 위해 설계된 이 제품은 보안팀이 경보 관리, 검색, 분석, 조사 및 보고와 같은 주요 업무를 효율적으로 수행하도록 지원합니다.

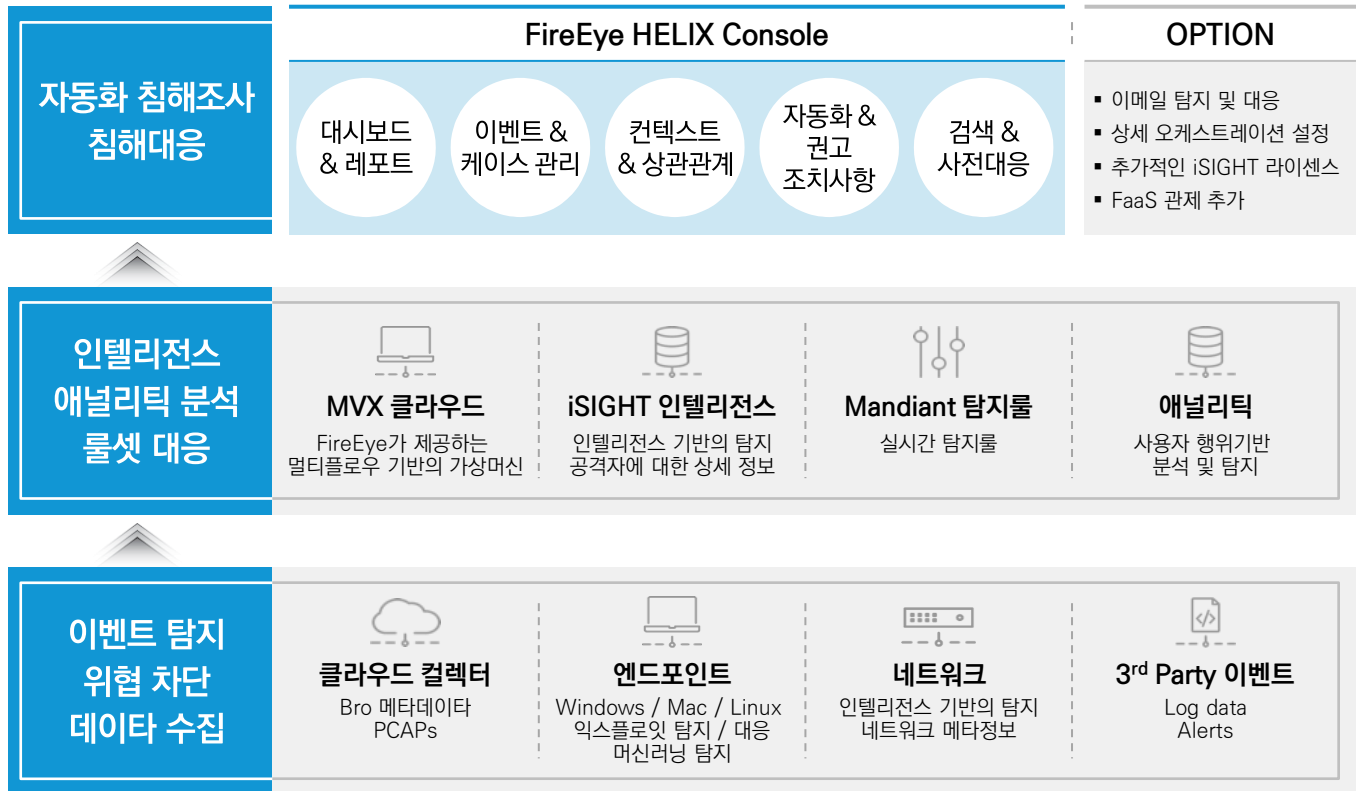
### 사용자 이점



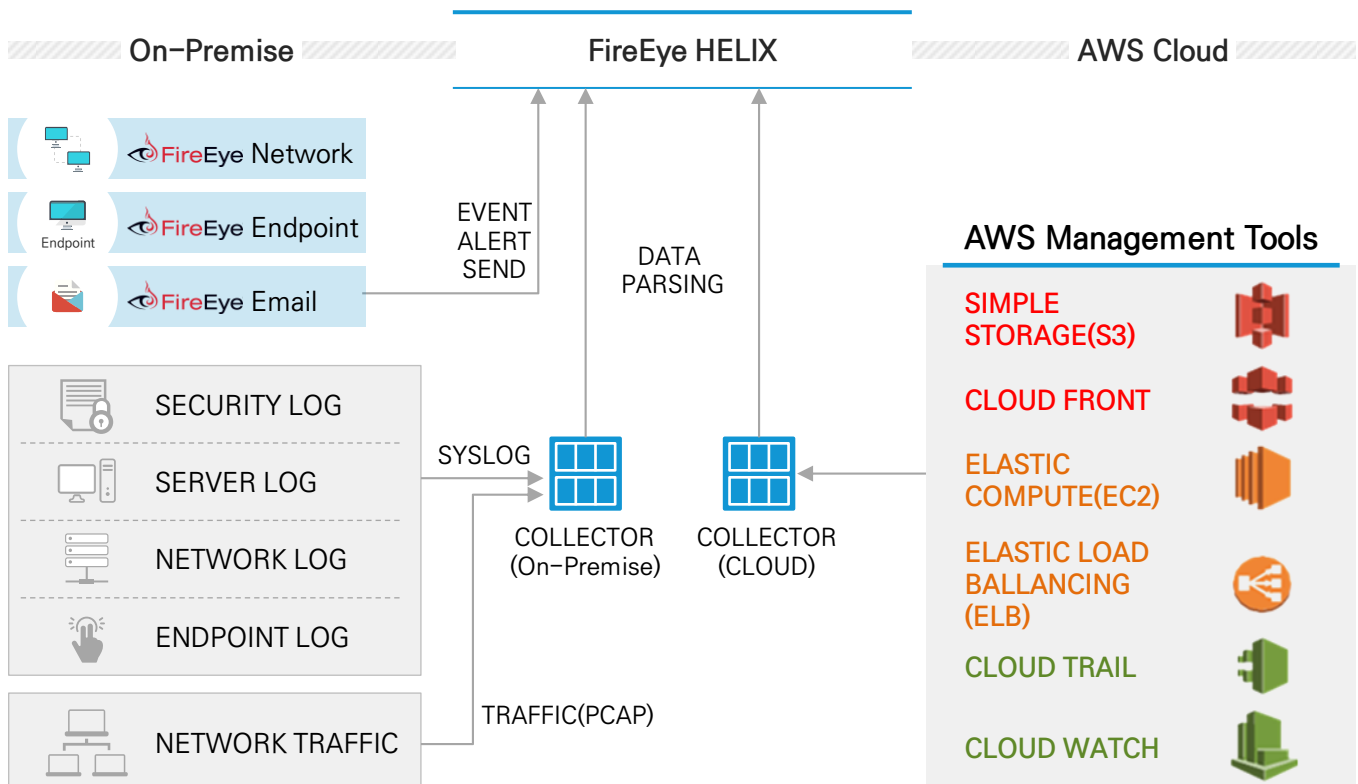
즉각적인 상황 인식을 위한 운영 인터페이스



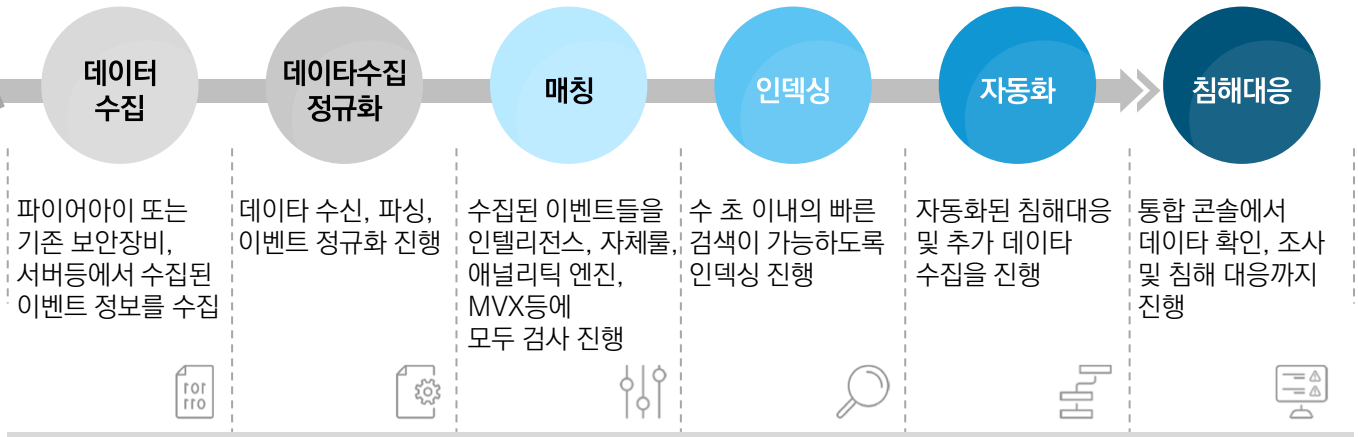
## FireEye HELIX 구조



## FireEye HELIX 구현



## FireEye HELIX 동작방식



## FireEye HELIX 기능

| 분석                                                                                                 | API                                                                          | 상황(컨텍스트)                                                                           |
|----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| 데이터에서 숨겨진 패턴 및 비정상적인 상태를 찾아 탐지 기능을 더욱 강화하고, 조사 프로세스에 상황 정보를 제공합니다.                                 | 타사 제품과 통합하고 고객 환경에 원활하게 통합할 수 있는 유연한 개방형 API를 지원합니다.                         | 인텔리전스, 경보, 호스트 및 사용자 데이터 전체에서의 상황 정보를 비롯한 관련 데이터가 자동으로 통합되므로 빠르게 의사 결정을 내릴 수 있습니다. |
| 컴플라이언스                                                                                             | 탐지                                                                           | 디바이스 및 정책 관리                                                                       |
| 미리 정의되거나 사용자 지정된 대시보드 및 위젯을 통해 컴플라이언스 요구 사항을 충족하는 동시에 사용자에게 가장 중요한 정보를 시각적으로 취합하고 표시하고 탐색합니다.      | 기존 데이터에 FireEye 전문 규칙과 FireEye iSIGHT 인텔리전스를 적용하여 다른 툴로는 감지할 수 없는 위협을 확인합니다. | 환경 전체의 구성, 정책 및 상태를 관리합니다.                                                         |
| 역할 기반 접근 제어                                                                                        | 인텔리전스                                                                        | 오케스트레이션                                                                            |
| 역할 기반 그룹을 만들어 콘솔에 액세스할 수 있는 세분화된 권한을 할당할 수 있습니다.                                                   | FireEye의 최신 인텔리전스 위협을 국가 및 산업별로 분류하여 탐지, 강화, 탐색 및 학습합니다.                     | 제품 통합 및 특정 경보에 대해 정의된 작업을 통해 조사 및 대응 프로세스를 자동화하고 시간을 단축합니다.                        |
| 조사 워크벤치                                                                                            | 워크플로우 관리                                                                     |                                                                                    |
| 유연한 보안작업의 전환과 신속한 탐지를 지원하기 위해 인프라 전체에 있는 모든 소스의 경보 및 이벤트 데이터에 대해 완벽한 인덱싱, 보관, 검색 및 악성코드 분석을 수행합니다. | 자동화된 워크플로우 및 수동 워크플로우를 통해 조사 프로세스 전체의 단계를 체계화, 할당, 협력 및 실행합니다.               |                                                                                    |



## FireEye HELIX 적용

- 서버팜에 대한 보호
  - 웹해킹 및 서버에 대한 공격 또는 이상행위 탐지
- SOC 운영 도구 (통합 모니터링 및 보안 운영)
- AWS Cloud 보안 및 감사를 위한 솔루션
  - AWS Cloud에 대한 가시성 확보
  - AWS Cloud에서의 이상행위에 대한 모니터링 및 Cloud 사용에 대한 Audit
- 침해조사를 위한 도구
  - Investigative Tips
- 보안 시스템 자동화
  - Automation & Orchestration



**HELIX** DASHBOARDS INVESTIGATE EXPLORE CONFIGURE

**FireEye Rules** [85] Customer Rules

| Risk | Name                                                              | Rule Pack               | Distinguishers            | Status  |
|------|-------------------------------------------------------------------|-------------------------|---------------------------|---------|
| **** | NEXPOSE METHODOLOGY [Unique URI]<br>ID: 1.1.2626                  | Web Application Attacks | srcipv4,srcipv6,xfwdforip | Enabled |
| **** | EXPLOIT - APACHE STRUTS [CVE-2017-9805 Remote...]<br>ID: 1.1.2606 | Web Application Attacks | srcipv4,srcipv6           | Enabled |
| **** | WEBSHELL METHODOLOGY [POST Response.WHT...]<br>ID: 1.1.2398       | Web Application Attacks | srcipv4,srcipv6           | Enabled |
| **** | METHODOLOGY - LFI [Null-Byte URI]<br>ID: 1.1.2185                 | Web Application Attacks | srcipv4,srcipv6,xfwdforip | Enabled |
| **** | EXPLOIT - CISCO VPN [CVE-2014-3393 URI]<br>ID: 1.1.1572           | Web Application Attacks | srcipv4,srcipv6,xfwdforip | Enabled |

**HELIX** DASHBOARDS INVESTIGATE EXPLORE CONFIGURE

**8520: WINDOWS METHODOLOGY [Remote AT Usage]**

\*\*\*\* Low windows, schedule, task, faas-full-coverage

First Seen: 2018-02-17 18:39:05 Last Seen: 2018-02-19 18:39:04

Log Events  
MetaClasses [1]  
auth, windows  
2018-02-17 18:40 UTC

Most Recent Event | Windows Process

| eventid       | username | args                                       | hostname |
|---------------|----------|--------------------------------------------|----------|
| 4688          | kminks   | at \\victim-1 12:36 net.exe use \\victi... | msg      |
| process       |          | c:\windows\system32\at.exe                 |          |
| accountdomain |          | mandiant                                   |          |

(주)아이티언은 기술력을 바탕으로 고객과 신뢰를 쌓아 온 기술 중심의 회사로써 진화하는 침해 위협을 빠르고 쉽게 분석하고 대응 할 수 있도록 클라우드 보안분야의 최신 전문기술을 적용한 FireEye의 HELIX를 제공하여 고객의 가치를 높이는 보안전문 회사입니다.

(주)아이티언

14057, 경기도 안양시 동안구 시민대로 401(관양동, 대륭테크노타운 15차 1211호)

ES사업부

Tel : 070-4055-1000, [essales@itian.co.kr](mailto:essales@itian.co.kr), <http://www.itian.co.kr>



주식회사아이티언



FireEye

FireEye®는 인텔리전스 기반 SaaS(Security-as-a-Service)의 리더입니다.

FireEye는 고객 보안 운영의 완벽한 확장을 위해 혁신적인 보안 기술, 국가 수준의 위협 인텔리전스 및 세계적으로 유명한 맨디언트 컨설팅을 결합한 단일 플랫폼을 제공합니다. 이를 통해 FireEye는 사이버 공격에 대비, 방어 및 대응하고자 노력하는 조직의 사이버 보안 부담을 간소화합니다. FireEye는 포브스 글로벌 2000 기업 중 940개 이상의 기업을 포함해 67개국의 5,000여 기업을 고객으로 보유하고 있습니다.