FIREEYE™

클라우드 보안

하이브리드 인프라 모니터링 및 방어

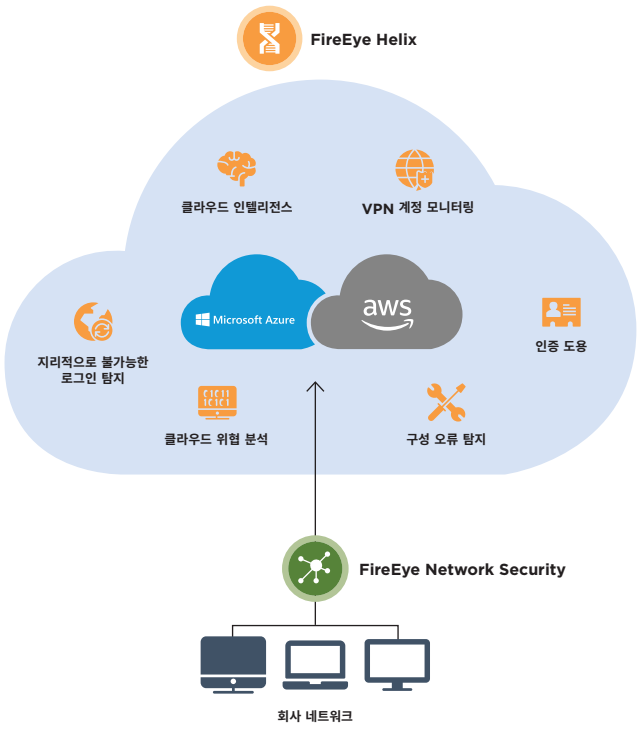
요약

- 클라우드 인프라 취약점 및 위협에 대한 실시간 가시성 확보
- 클라우드 보안 침해로 이어질 수 있는 인증 도용과 의도치 않은 구성 오류를 탐지 및 방지
- 클라우드 트레일, S3 및 ELB 로그의 모니터링과 수집을 중앙 집중화하여 보안 운영 간소화

비즈니스 운영 환경을 클라우드로 전환함에 따라 조직은 수많은 보안 문제에 직면하게 됩니다. 잘못 구성된 인증, 허점이 있는 주요 관리 기능, 보안이 되지 않은 API 등은 공격자가 클라우드 인프라에 대한 액세스 권한을 얻을 수 있는 수많은 방법 중 일부에 지나지 않습니다. 인프라에 액세스한 공격자는 애플리케이션을 탈취하여 클라우드 내에서 탐지되지 않은 채 이동하면서 인증 정보를 확보하고 기밀 데이터를 빼냅니다. 클라우드는 온프레미스 기술만큼 공격에 취약하지만, 이러한 클라우드 환경을 보호하는 데 필요한 툴을 갖춘 조직은 소수에 불과합니다.

서비스형 인프라 (IaaS) 및 서비스형 플랫폼 (PaaS) 제공업체는 보안의 공유 책임 모델을 적용하기 때문에 클라우드 내 자사의 데이터를 보호할 책임은 고객에게 있습니다. 클라우드 인프라를 방어하려면 조직이 사용자 인증을 보호하고, 취약점을 사전에 파악하며, 보안 모니터링을 중앙 집중화해야 합니다.

이와 같은 지능형 보안은 충분히 실현할 수 있습니다. FireEye Helix 는 중앙 집중화된 가시성, 구성 모니터링 및 사용자 행동 분석 기술을 사용하여 클라우드에서 지능형 공격을 탐지하는 보안 운영 플랫폼입니다.



FireEye 솔루션을 활용한 클라우드 인프라 보안

FireEye 솔루션의 기능:

가시성 및 인텔리전스를 통해 이전에 관찰된 적 없는 위협 표면화

인증 정보 도용 및 구성 관리 부실 방지

분산된 자산 추적

인증 도용 탐지

침해 당한 계정 식별 및 경보 제공

지리적으로 불가능한 로그인 탐지

지리적 위치상 물리적으로 불가능한 로그인이 관찰되는지 탐지

클라우드 구성 규칙, 분석 및 오케스트레이션

클라우드 구성 오류를 탐지하여 자동으로 복구하고 보고서 생성

침해 당한 VPN 계정 탐지

데이터 센터 로그인, 지리적 현실성, IP 이상 탐지를 활용하는 휴리스틱을 적용하여 VPN 기반 위협 식별

클라우드 인텔리전스

상황 인텔리전스로 Amazon GuardDuty 경보를 강화하여 효율적인 탐지 및 대응 지원

네트워크 모니터링

WAN 연결에 대한 비정상적인 활동을 탐지하여 회사 네트워크와 IaaS 및 PaaS 클라우드 간의 공격자 내부 이동 방지

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

FireEye Korea
서울 특별시 강남구 테헤란로 534 글라스타워 20층
02.2092.6580
korea.info@fireeye.com

FireEye, Inc. 소개

FireEye는 인텔리전스 기반의 보안 회사입니다. FireEye는 혁신적인 보안 기술, 국가 수준의 위협 인텔리전스 및 세계적으로 유명한 Mandiant® 컨설팅을 결합한 단일 플랫폼을 제공하여 고객 보안 운영의 완벽한 확장을 지원합니다. 이를 통해 FireEye는 사이버 공격에 대비하고 이를 방어 및 대응하고자 노력하는 조직의 사이버 보안 부담을 줄이고 간소화합니다.

FIREEYE™