브로셔

HPE GreenLake Management Services의 관리형 보안으로 위험 완화

HPE GreenLake

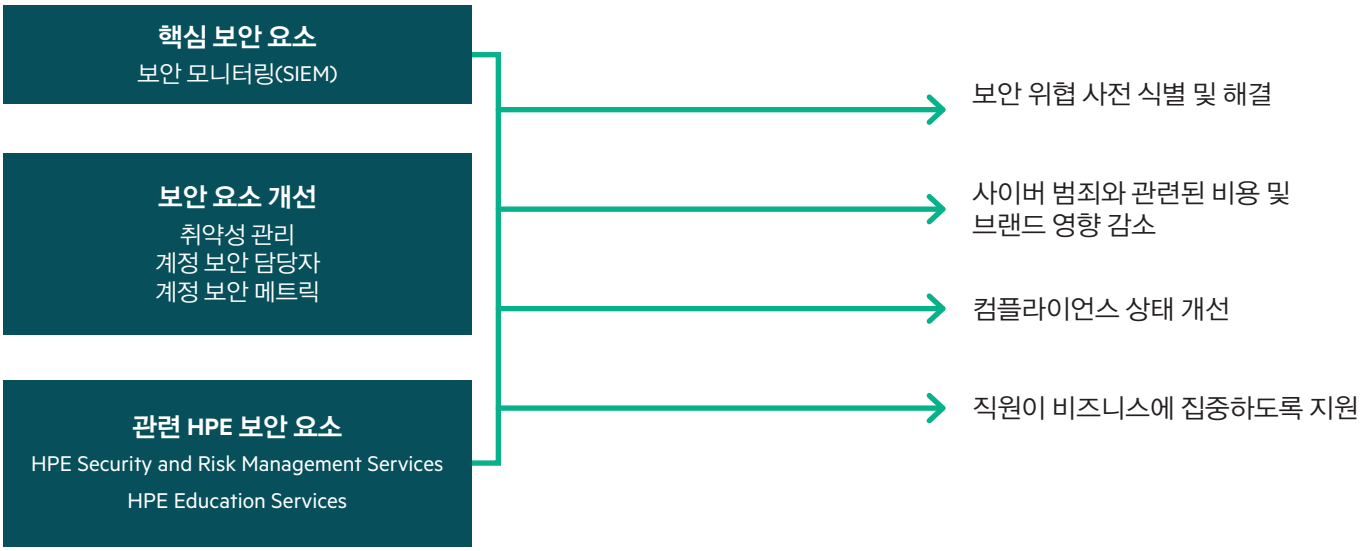
완전한 보안, 위험, 컴플라이언스 포트폴리오의 일부인 HPE GreenLake Management Services의 관리형 보안

관리형 보안은 계정 보안 담당자의 지원과 함께 보안 모니터링, 권한이 부여된 액세스 관리, 취약성 관리, 보안 강화, 컴플라이언스 관리가 포함된 서비스를 제공하여 HPE GreenLake Management Services 고객의 환경을 개선합니다.

관리형 서비스 공급자를 통해 운영 위험 관리
데이터 침해 및 사이버 보안 사고를 방지하고, 식별하며, 억제하려는 노력에도 불구하고 IT 인프라의 보안 격차로 공격과 침해를 신속하게 탐지하는 데 방해가 될 수 있습니다. 이러한 사고는 평판 훼손, 비즈니스 손실, 규정 위반으로 인한 불이익, 민사 소송, 예상치 못한 중단 시간, 핵심 정보 손실 등으로 대규모 재정 비용이 발생할 수 있습니다.

위험 및 위험과 관련된 보안 및 컴플라이언스 관련 지출 증가를 인지하더라도 IT 보안 관리는 여전히 기술 격차, 고립된 툴, 복잡성, 자동화 부족 등 여러 문제가 존재합니다. 운영을 타사 서비스 공급자에게 아웃소싱하는 것을 고려할 때 관련 문제는 증가합니다. 운영은 아웃소싱이 가능하지만 운영의 보안 및 컴플라이언스 위반의 위험은 아웃소싱할 수 없기 때문에 발생합니다.

HPE GreenLake Management Services: 관리형 보안



관리형 보안으로 운영 위험 줄이기

관리형 보안은 HPE GreenLake Management Services 계약에서 핵심적인 추가 항목으로, 운영 위험을 감소하도록 보안 전문 기술과 경험, 프로세스 간소화, 전체적인 관리 솔루션을 지원하여 아웃소싱한 리소스 관련 위험으로부터 보호할 수 있습니다. 제공되는 서비스에는 다음이 포함됩니다.

보안 모니터링: HPE 보안 분석가가 엔드 투 엔드 사고 관리를 모니터링하며, 사고 감지, 대응, 억제, 복구, 사고 후 분석 및 후속 조치를 포함한 SOC(보안 운영 센터) 활동을 제공합니다. 보안 사고를 신속하게 식별 및 해결하기 위해 로그 수집 시설에서 SOC의 요청에 따라 공유 가능한 모든 사고 기록을 저장하고 상호 연결합니다.

권한이 부여된 액세스 관리: 관리 및 시스템 권한을 HPE 보안 분석가가 지속적으로 보안, 관리, 모니터링함으로써 IT 시스템 및 관련 데이터의 기밀성, 무결성, 안정성을 보장합니다. 이 서비스는 데이터 도난, 데이터 손실, 규정 미준수로 인한 불이익, 평판 훼손 등의 위험을 대폭 줄여줍니다.

취약성 관리: 업계를 선도하는 스캔 기술과 강력한 보안 관리 프로세스의 지원을 통해 감지한 보안 취약성을 신속하게 식별, 평가, 우선순위 지정, 해결합니다. 정기 및 임시 방식의 온디맨드 스캔과 취약성 메트릭을 분기별로 공유합니다.

보안 강화: 공격 표면을 줄이고 보안 위험을 완화하는 최전선에 안전한 플랫폼 구성이 있습니다. 이 서비스는 HPE GreenLake Management Services에 기본 보안 구성을 제공하여 HPE 보안 성공 사례를 충족하도록 플랫폼을 구성할 수 있으며 SOC 플랫폼에 고품질 원격 측정 기능을 제공할 뿐만 아니라 더욱 안전하게 구성된 온프레미스 장비를 제공합니다.

SO(Security Officer): SO는 서비스형으로 배정되었으며, 보안 및 규정 요건, 감사 거버넌스, 위험 관리 등과 관련하여 해당 조직(SOC 포함)과 HPE의 관계 유지를 담당합니다. 또한 SO는 상호 합의한 보안 프로세스와 사고 대응 계획 관련 지침이 포함된 보안 핸드북을 관리합니다.

IT 보안 격차 해소

2020년 6월 HPE는 Ponemon Institute에서 수행한 IT 보안 격차 해소 관련 연구를 후원했습니다. 3개 지역과 10개 국가에서 4,189명의 IT 및 IT 보안 전문가가 설문조사에 참여했습니다.

- 61%는 네트워크 내부에 도달한 공격이 가장 큰 손해를 입힐 수 있다고 답했습니다.
- 35%만 데이터 도난 또는 권한 없는 엔티티의 데이터 수정 및 보기로 이어질 수 있는 사이버 보안 침해가 발생하기 전에 IT 인프라 내부의 공격을 신속하게 탐지할 수 있다고 확신했습니다.
- 경영진의 29%만 IT 보안 격차 해소에 매우 효과적으로 대응한다고 답했습니다.

응답자의 답변에 따르면 보안이 침해된 합법적 사용자와 부주의한 사용자가 IT 인프라에서 중대한 내부자 위협이 되고 있습니다.

위험 관리로 안심

Ponemon Institute는 IT 보안 격차를 "조직의 인력, 프로세스, 기술로 계속 변하는 위협 환경에 대응할 수 없음"이라고 설명합니다.[1]

HPE GreenLake Management Services의 관리형 보안으로 보안 위협을 식별 및 완화하는 데 필요한 인력, 프로세스, 기술을 확보할 수 있습니다. HPE의 관리형 서비스 분야의 오랜 경험과 엔드 투 엔드 보안 관리 제공 역량, 최근 원격 인프라 관리 분야에서의 혁신 기술 등으로 데이터, 애플리케이션, 인프라의 보안을 보장할 수 있습니다.

믿을 수 있는 보안 관리

사이버 보안은 오래전부터 영구적인 기능일 뿐만 아니라 비즈니스 활동에 따른 비용이었지만 데이터 침해 그리고 데이터 침해로 인한 중단 시간, 수익 손실, 중대한 평판 훼손 등과 관련된 문제 해결에 완전히 준비되지 않은 조직이 많습니다. HPE GreenLake Management Services의 관리형 보안 서비스로 자산의 보안 상태에 안심하고 사이버 보안 관련 운영 부담을 덜어 위험을 줄일 수 있습니다.

[1] HPE가 후원한 Ponemon Institute **IT 보안 격차 해소** 보고서 다운로드(hpe.com/kr/ko/resources/servers/ponemon-it-security-report.html)

완전한 보안, 위험, 컴플라이언스 포트폴리오

관리형 보안은 IT 보안 격차를 식별 및 해소하고 지속적인 모니터링 및 관리를 지원하는 HPE GreenLake Management Services의 서비스 포트폴리오 중 하나입니다. 보안, 위험, 컴플라이언스 포트폴리오에 다음도 포함됩니다.

관리형 IT 컴플라이언스: 규정 및 거버넌스 컴플라이언스에 대한 단일 대시보드의 엔터프라이즈급 가시성으로 1,500개 이상의 제어에 대한 컴플라이언스를 추적하는 동시에 멀티클라우드 환경에서 중대한 규칙 위반이 발생할 경우 비즈니스 이벤트 모니터링으로 경보를 보냅니다.

관리형 재난 복구: 믿을 수 있는 안정적인 관리형 재난 복구 서비스로 재난 발생 시 데이터를 빠르고 간편하게 복구하십시오. 정책 기반 자동화, 내장형 암호화, 초고효율 데이터 축소 기술로 데이터 보호를 간소화할 수 있습니다.

관리형 백업: 데이터 센터, 클라우드, SaaS 벤더 전반에서 운영 요구 사항에 따라 데이터 백업을 조정하십시오. 비즈니스 복구 서비스 수준 계약을 충족하도록 설계된 접근 방식으로 백업 관리를 간소화할 수 있습니다.

소프트웨어 자산 관리(SAM): 소프트웨어 자산 관리 및 라이선스 최적화 솔루션은 인벤토리, 애플리케이션 사용, 구매 주문 데이터, 라이선스 권리, 계약 기간 등을 분석함으로써 너무 많이 또는 너무 적게 사용하는 라이선스를 모니터링/관리하고 라이선스 소비를 최적화합니다.

A&PS(Advisory and Professional Services):

- 보안 분석 및 로드맵 서비스
- 취약성 분석 서비스(침투 테스트)
- 변혁 워크샵
- 백업 복구 영향 분석
- 재난 복구 기술 분석
- 보안 컴플라이언스 평가
- 보안 교육 프로그램
- ISO 22301 비즈니스 연속성 관리

자세히 알아보기

hpe.com/managementservices

올바른 구매 결정을 위해
HPE 프리세일즈 담당자와 상의하십시오.

채팅하기(세일즈)

전화하기

최신 정보 보기

HPE GreenLake 알아보기

Hewlett Packard Enterprise

a00107277KOP, 제2차 개정판