McAfee Cloud Workload Security

하이브리드 인프라 워크로드를 보호합니다. 더 안전하게 더 빠르게 더 간편하게

기업 데이터 센터가 진화함에 따라 매일 점점 더 많은 워크로드가 클라우드 환경으로 마이그레이션되고 있습니다. 대부분의 조직은 컨테이너를 포함하여 끊임 없이 변화하는 사내 및 클라우드 워크로드가 혼합된 하이브리드 환경에 놓여있습니다. 이러한 클라우드 환경(개인 및 공용)에는 보호를 위해 새로운 접근 방식과 도구가 필요하므로 보안 과제가 발생합니다. 조직은 잘못된 구성, 악성 프로그램 및 데이터 침해의 위험에 대한 완벽한 방어와 함께 모든 클라우드 워크로드에 대한 중앙 집중식 가시성이 필요합니다.

McAfee® Cloud Workload Security(McAfee® CWS)는 사각지대를 없애고 고급 위협 방어를 제공하며 다중 클라우드 관리를 간소화할 수 있도록 탄력적인 워크로드 및 컨테이너를 탐색하여 방어하는 작업을 자동화합니다. McAfee는 자동화된 단일 정책이 가상 개인, 공용 및 다중 클라우드 환경을 통과하는 이동 중인 워크로드를 효과적으로 방어할 수 있도록 보호 성능을 제공합니다. 따라서 사이버 보안 팀은 탁월한 운영 능력을 갖출 수 있습니다.

첨단 워크로드 보안: 사용 사례

자동화된 탐색

관리되지 않은 워크로드 인스턴스 및 Docker 컨테이너는 보안 관리에 틈을 만들며 공격자들에게 조직에 침투하는 데 필요한 발판을 제공할 수 있습니다. McAfee CWS는 AWS(Amazon Web Services), Microsoft Azure, OpenStack 및 VMware 환경 전반에서 탄력적인 워크로드 인스턴스 및 Docker 컨테이너를 탐색하며 새로운 인스턴스를 지속적으로 모니터링합니다. 환경 전반에 대한 중앙 집중식의 완전한 시야를 확보하고 위험 노출을 야기하는 운영 및 보안 사각 지대를 제거합니다.

네트워크 트래픽에 대한 통찰력 확보

McAfee CWS는 클라우드 워크로드에서 제공되는 기본 네트워크 트래픽을 활용하여 McAfee® Global Threat Intelligence(McAfee® GTI) 데이터 피드의 인텔리전스를 보강하고 적용할 수 있습니다. 보강된 정보는 위험 점수, 위치정보 및 기타 중요한 네트워크 정보와 같은 속성을 표시할 수 있습니다. 이 정보는 워크로드를 보호하는 자동화된 교정 작업을 만드는 데 사용할 수 있습니다.

주요 혜택

- 탄력적인 워크로드 인스턴스에 대한 지속적 가시성은 예전에는 노동 집약적이었던 정책 배포를 자동화하는 동시에 운영상의 “사각 지대”를 없애줍니다.
- 중앙 집중식 관리 및 자동화된 워크로드는 하이브리드 및 다중 클라우드 환경의 복잡성을 대폭 감소시킵니다.
- 에이전트를 설치하지 않고 네트워크 위협을 시각화 및 검색할 수 있습니다.
- 가상 시스템 최적화 위협 방지는 다중 계층의 대책을 제공합니다.
- Chef 및 Puppet 등의 자동화 도구와의 통합으로 배포 시 공용 및 사설 클라우드 워크로드에 보안을 적용할 수 있습니다.

McAfee에 문의

배포 프레임워크로 통합

McAfee CWS는 클라우드 워크로드에 대한 McAfee® 에이전트의 자동 배포 및 관리를 허용하는 배포 스크립트를 작성합니다. 이러한 스크립트는 AWS 및 Microsoft Azure와 같이 클라우드 공급자에 의해 실행되는 워크로드에 McAfee 에이전트를 배포할 수 있도록 Chef, Puppet 및 기타 DevOps 프레임워크와 같은 도구에 통합할 수 있습니다.

이벤트 통합

McAfee CWS를 이용하면 조직은 단일 인터페이스로 사내 및 클라우드 환경 모두를 위한 수많은 대책 기술을 관리할 수 있습니다. 이는 또한 AWS GuardDuty, McAfee® Policy Auditor 및 McAfee® Network Security Platform과 같은 추가 기술로 통합되기도 합니다.

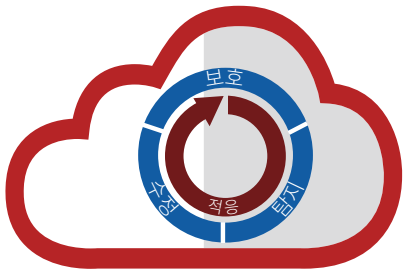
- 관리자는 지속적인 모니터링과 AWS GuardDuty에서 제공하는 무단 행동 식별 기능을 활용해 또 다른 수준의 위협 가시성을 제공할 수 있습니다. 이 통합을 통해 McAfee CWS 고객은 네트워크 연결, 포트 프로브, EC2 인스턴스에 대한 DNS 요청 등을 포함하는 GuardDuty 이벤트를 McAfee CWS 콘솔 내부에서 직접 확인할 수 있습니다.
- McAfee Policy Auditor는 HIPAA (Health Insurance Portability and Accountability Act), PCI-DSS (Payment Card Industry Data Security Standard), CIS Benchmark (Center for Internet Security Benchmark), 기타 산업 표준 등의 컴플라이언스를 위한 알려진 구성 감사 또는 사용자 정의 구성 감사에 대해 에이전트 기반 검사를 실시합니다. McAfee CWS는 클라우드에서 잘못 구성된 워크로드를 즉시 파악할 수 있도록 실패한 감사를 보고합니다.
- McAfee Network Security Platform은 하이브리드는 물론 AWS 및 Microsoft Azure 환경의 트래픽에 대한 네트워크 검사를 실시하는 또 다른 클라우드 보안 플랫폼입니다. 이 플랫폼은 네트워크 트래픽에 대해 심층적인 패킷 수준 검사를 실시하고 McAfee CWS를 통해 불일치 문제 또는 경보를 보고합니다. 교정을 위해 다중 클라우드 환경에 대한 단일 창 가시성을 제공합니다.

네트워크 보안 그룹 정책 시행

McAfee CWS를 통해 사용자 및 관리자는 기준 보안 그룹 정책을 만들고 이러한 기준에 따라 워크로드에서 실행되고 있는 정책을 감사할 수 있습니다. 기준에서 벗어나거나 변경된 경우 McAfee CWS 콘솔에서 교정을 위해 경보를 생성할 수 있습니다. 관리자는 McAfee CWS에서 클라우드 네이티브 보안 그룹 정책을 직접 제어할 수 있게 해주는 기본 네트워크 보안 그룹을 수동으로 구성할 수도 있습니다.

주요 혜택(계속)

- 고급 악성 프로그램 및 침입에 대한 다중 계층 보호를 쉽게 활용할 수 있습니다.
- Docker 컨테이너를 탐색 및 모니터링하고 마이크로 세분화를 통해 보호합니다.
- 솔루션 내부에서 직접 수정 조치를 취해 환경을 보호합니다.



Cloud Workload Security

포괄적인 **가시성** 및 **제어**

McAfee Cloud Workload Security의 차별화 요소: 주요 기능 및 기술

클라우드 네이티브 빌드 지원

고객은 McAfee CWS를 사용하여 AWS EC2, Microsoft Azure 가상 컴퓨터, OpenStack 및 VMware Vcenter를 비롯한 여러 공용 및 개인 클라우드의 관리 작업을 단일 관리 콘솔에 통합할 수 있습니다. McAfee CWS는 Amazon Elastic Container Service for Kubernetes(Amazon EKS) 및 Microsoft Azure Kubernetes Service(AKS)에 대한 새로운 클라우드 네이티브 빌드 지원을 통해 클라우드로 가져와 실행할 수 있습니다.

간편한 중앙 집중식 관리

단일 콘솔은 서버, 가상 서버 및 클라우드 워크로드 전반의 다중 클라우드 환경에 일관된 보안 정책과 중앙 집중식 관리를 제공합니다. 관리자는 또한 McAfee® ePolicy Orchestrator®(McAfee ePO™) 소프트웨어에서 더욱 구체적이고 적절하게 사용자 역할을 정의하는 데 사용할 수 있는 여러 역할 기반 권한을 만들 수도 있습니다.

마이크로 세분화와 네트워크 시각화

클라우드 네이티브 네트워크 시각화, 우선순위가 설정된 위험 경보 및 마이크로 세분화 기능은 가상화된 환경 및 외부의 악의적 소스로부터의 측면 공격을 방지할 수 있도록 인식 및 제어를 제공합니다. 단일 클릭 종료 또는 격리 기능은 구성 오류의 잠재성을 줄이고 교정 효율성을 향상하는 데 도움이 됩니다.

우수한 가상화 보안

McAfee CWS 제품군은 McAfee® Management for Optimized Virtual Environments AntiVirus(McAfee® MOVE AntiVirus)를 사용하여 악성 프로그램으로부터 개인 클라우드 가상 시스템을 보호합니다. 기본 리소스에 부담을 주거나 추가 운영 비용을 필요로 하지 않고 이러한 보호 기능을 제공합니다. McAfee MOVE AntiVirus를 사용하는 조직은 보안을 전용 가상 시스템으로 오프로드하여 가상화된 환경의 검색을 최적화할 수 있습니다.

사용자는 McAfee® Endpoint Security for Servers를 통해 안티맬웨어 보호 기능을 확보할 수 있습니다. 이 솔루션은 중요한 비즈니스 프로세스에 영향을 미치지 않도록 주문형 검색같은 리소스 집약적인 작업을 지능적으로 예약할 수 있습니다.

워크로드 보안 태그 지정 및 자동화

AWS 및 Microsoft Azure 태그 정보를 McAfee ePO 소프트웨어에 가져오고 그러한 태그를 기준으로 정책을 할당할 수 있는 기능을 통해 모든 워크로드에 적절한 정책을 자동으로 할당합니다. 기존 AWS 및 Microsoft Azure 태그는 McAfee ePO 소프트웨어 태그와 동기화되어 자동으로 관리됩니다.

자동 수정

사용자가 McAfee ePO 소프트웨어 정책을 정의합니다. McAfee CWS가 McAfee ePO 소프트웨어 보안 정책으로 보호되지 않는 시스템을 발견할 경우 악성 프로그램 또는 바이러스가 있는 것으로 검색된 시스템은 자동으로 격리됩니다.

적응형 위협 방지

McAfee CWS는 기계 학습, 응용프로그램 억제, 가상 시스템에 최적화된 안티맬웨어, 화이트리스트, 파일 무결성 모니터링, 마이크로 세분화 등을 아우르는 대책을 통합하며 이는 랜섬웨어 및 표적 공격 등의 위협으로부터 워크로드를 보호합니다. McAfee® Advanced Threat Protection 은 코드 속성과 동작을 바탕으로 악성 페이로드를 밝혀낼 수 있도록 기계 학습 기술을 적용하여 이전에는 감당할 수 없었던 정교한 공격을 막아냅니다.

응용프로그램 제어

응용프로그램 화이트리스트는 인증받지 못한 모든 페이로드를 차단하면서 신뢰할 수 있는 응용프로그램만 실행될 수 있도록 허용함으로써 알려진 공격과 알 수 없는 공격 모두를 방지합니다. McAfee® Application Control은 현지 및 전역적 위협 인텔리전스는 물론, 보안 기능을 비활성화하지 않고 시스템을 항상 최신 상태로 유지하는 능력을 바탕으로 동적인 보호를 제공합니다.

파일 무결성 모니터링(FIM)

McAfee® 파일 무결성 모니터링은 시스템 파일과 디렉터리가 악성 프로그램, 해커 또는 악의적인 내부자로 인해 손상되지 않도록 보장하기 위해 지속적으로 모니터링합니다. 포괄적인 감사 세부 정보는 서버 워크로드의 파일이 변화하는 방식에 대한 정보를 제공하고 사용자에게 공격 발생에 대해 경고합니다.

다중 클라우드 환경에 적합한 보안 범위

McAfee CWS는 클라우드를 활용하면서 최고 수준의 보안 품질을 유지할 수 있도록 보장합니다. 이 솔루션이 여러 보호 기술을 적용하고 보안 관리를 간소화하며 사이버 위협으로부터 비즈니스를 보호하므로, 고객은 비즈니스 성장에 전념할 수 있습니다. 아래 내용은 사용 가능한 패키지 옵션의 기능 비교입니다.

기능	McAfee Cloud Workload Security Basic	McAfee® Cloud Workload Security Essentials	McAfee® Cloud Workload Security Advanced
중앙 집중식 관리(McAfee ePO 플랫폼)	✓	✓	✓
여러 클라우드 지원(AWS, Microsoft Azure, VMware)	✓	✓	✓
마이크로 세분화를 사용하여 워크로드 및 컨테이너 격리	✓	✓	✓
McAfee MOVE(에이전트 없는 다중 플랫폼)	✓	✓	✓
McAfee Endpoint Security 서버 OS(Windows 및 Linux)용 위협 예방	✓	✓	✓
호스트 기반 방화벽	✓	✓	✓
AWS 및 Microsoft Azure용 기본 방화벽 관리(보안 그룹)	✓	✓	✓
호스트 침입 및 취약성 공격 방지	✓	✓	✓
McAfee ePO 소프트웨어로 AWS 및 Microsoft Azure 태그 정보 가져오기	✓	✓	✓
비-컴플라이언트 워크로드에 대한 자동 교정	✓	✓	✓
기계 학습을 통한 적응형 위협 방지		✓	✓
네트워크 트래픽 시각화와 마이크로 세분화		✓	✓
McAfee GTI 평판 점수와 결합된 클라우드 네이티브 네트워크 트래픽 분석		✓	✓
McAfee® Virtual Network Security Platform(McAfee® vNSP) 통합		✓	✓
McAfee Application Control을 통한 서버의 동적 화이트리스트			✓
McAfee 파일 무결성 모니터링을 통한 지속적인 감사 로깅			✓
McAfee® Change Control for Servers를 통한 파일 및 폴더 보호			✓

자세히 알아보기

자세한 내용을 보려면 다음 웹 사이트를 방문하십시오. **https://www.mcafee.com/ko-kr/products/cloud-workload-security.aspx**.

McAfee Together is power.

McAfee (Singapore) Pte Ltd
10 Kallang Avenue #08-10
Aperia Tower 2
Singapore 339510
www.mcafee.com/kr