McAfee
Together is power.

통합 보안을 위한 인포블록스와 McAfee 의 협력

보안 자동화, 오케스트레이션, 대응과 함께 실시간 가시성을 단일 창에서 제공하여 보안 운영 팀에 더 높은 수준의 효율성 제공

McAfee 와 인포블록스는 전체적인 가시성을 향상하고 포괄적인 보호를 제공하며 위협에 더 빠르게 대응하기 위해 협력하여 보안 운영팀에 더 높은 수준의 효율성을 제공하고 있습니다. 통합 솔루션은 의심스러운 DNS 트래픽을 McAfee® 웹 게이트웨이 클라우드 서비스로 리디렉션하고 악성 소프트웨어 검색 및 SSL 검사를 포함한 심층적 수준의 콘텐츠 검사를 수행합니다. 또한 조직은 ActiveTrust 와 데이터 교환 계층 (DXL) 간의 정보 공유를 통해 보안 도구 사일로를 극복하고 솔루션 간에 워크플로 오케스트레이션을 제공하여 네트워크와 웹에 바인딩된 엔드포인트를 모두 시기 적절하고 효과적인 방식으로 보호할 수 있습니다.

인포블록스는 2017 년에 가장 혁신적인 McAfee 보안 혁신 연합 파트너 상을 수상했습니다.

McAfee 호환 솔루션

- 인포블록스 ActiveTrust
- 인포블록스 ActiveTrust 클라우드
- 인포블록스 DDI
- McAfee 웹 게이트웨이
- McAfee 웹 게이트웨이 클라우드 서비스
- McAfee 엔터프라이즈 보안 관리자
- 데이터 교환 계층
- McAfee® ePolicy Orchestrator®

McAfee COMPATIBLE

Infoblox
NEXT LEVEL NETWORKING

인포블록스 연결

비즈니스 문제

기업은 다양한 보안 도구에 투자하고 있지만 악성 소프트웨어는 여전히 네트워크에 침입하고 데이터를 도용하며 기존 보안 인프라를 우회합니다. DNS 트래픽은 방화벽에서 검사되거나 필터링되지 않으므로 악의적인 작업자가 가장 일반적으로 악용하는 간극입니다. 오늘날 악성 소프트웨어의 91% 가 DNS 를 사용하여 주변에 침입한 후 작업을 수행합니다. 최근 *SC Magazine* 설문조사에서는 설문조사 응답자의 46% 가 DNS 기반 데이터 반출을 경험했다고 응답했습니다.

DNS 보호 플랫폼에서 발견되는 네트워크 이벤트와 위협을 실시간으로 감지하고 응답할 수 있으면 사고 대응을 대폭 가속화할 수 있습니다. 하지만 네트워크 데이터에 쉽게 액세스할 수 없으면 컨텍스트를 기반으로 적절한 조치를 취할 수 없습니다.

또한 오늘날 조직이 가지고 있는 다양한 보안 도구는 사일로에서 작동합니다. 상호 운용성이 없고 위협 정보를 공유할 수 없으면 조직은 계속 증가하는 공격에 효과적으로 대응할 수 없습니다.

위의 문제를 해결하려면 다음이 필요합니다.

- DNS 트래픽에 대한 가시성
- 위협 감지에 대한 다면적인 접근법으로 DNS 보안 간극 메우기
- DNS 보안과 생태계에 속한 기타 보안 도구 간의 통합

인포블록스와 McAfee 의 통합 솔루션은 DNS 및 웹 트래픽에 대한 가시성을 단일 창에서 제공하고 조직의 DNS 보안 간극을 메우며 인포블록스 DNS, DHCP, IPAM, DDI 와 McAfee 제품 간의 데이터 공유를 자동화합니다. 상호 운용성은 DNS 트래픽을 통한 공격에 대해 향상된 보호를 제공하며, 결합된 솔루션은 에이전트 배포의 관리 부담을 간소화하고 McAfee 가 관리하는 엔드포인트의 감염을 빠르게 해결하는 자동화된 워크플로를 지원하여 보안 운영 팀에 더 높은 수준의 효율성을 제공합니다.

McAfee 와 인포블록스의 공동 솔루션: DNS 및웹 보안, 데이터 공유, 오케스트레이션

인포블록스와 McAfee 는 어디서나 장치와 사용자를 보호하기 위해 온프레미스, 클라우드 기반 또는 이 두 가지의 조합이라는 솔루션 배포 선택을 고객에게 제공합니다.

McAfee 웹 게이트웨이 클라우드 서비스를 사용하는 인포블록스 ActiveTrust 클라우드

인포블록스 ActiveTrust 클라우드는 DNS 기반 데이터 반출과 C&C 서버 및 봇넷과 DNS 의 통신을 감지하고 방지합니다. 이 솔루션은 정책을 준수하지 않는 콘텐츠에 대한 액세스를 차단하고 더욱 빠른 해결을 위해 집계된 위협 정보 침해 지표 (IoC) 를 기존 보안 인프라와 공유합니다. 이 솔루션은 가시성 및 우선 순위 지정을 개선하기 위해 온프레미스 DDI 데이터를 사용하는 풍부한 네트워크 컨텍스트를 활용하며 하이브리드 배포에 대한 통합된 정책 관리 및 보고를 지원합니다. 서비스로 제공되는 ActiveTrust 클라우드는 전용 IT 리소스 없이 간편하게 구성하고 사용할 수 있습니다. 이 솔루션은

솔루션 개요

엔터프라이즈 네트워크, 로밍, 원격 사무실/지점 사무실 등 어디서나 장치를 보호합니다.

인포블록스 ActiveTrust 클라우드와 McAfee 웹 게이트웨이 클라우드 서비스의 통합은 도메인 차단 및 HTTP 보안을 단일화하여 양쪽 고객에게 더욱 광범위한 보호를 제공합니다. 다음과 같은 기능이 포함됩니다.

- 인포블록스 ActiveTrust 클라우드에서 식별된 의심스럽지만 아직 확정되지 않은 연결에 대해 McAfee 웹 게이트웨이의 웹 트래픽 검사를 더 많이 수행하여 다양한 계층의 연결 시도에 대한 사전 대비적 적응형 보호 제공
- 더욱 효과적인 보호를 위해 McAfee 와 인포블록스의 결합된 위협 정보 기능을 활용하여 더욱 광범위한 위협 정보 공유
- 모든 업로드에서 DLP 위반 가능성을 검색하여 클라우드 애플리케이션과 콘텐츠에 대한 액세스를 관리하는 향상된 콘텐츠 필터링 기술

이 통합을 통해 감염된 엔드포인트나 의심스러운 사용자에서 발생하는 악성 트래픽과 데이터 반출을 위치와 상관없이 더 빠르게 감지할 수 있습니다. ActiveTrust 클라우드에서 McAfee 웹 게이트웨이로 트래픽이 자동 리디렉션되므로 엔터프라이즈 데이터를 실시간으로 보호할 수 있습니다.

또한 인포블록스 ActiveTrust 클라우드는 프리미엄 McAfee 엔드포인트 관리 콘솔인 McAfee ePolicy Orchestrator (McAfee ePO™) 소프트웨어와 통합됩니다. McAfee ePO 소프트웨어는 엔드포인트 컴퓨터에서 실행하는 ActiveTrust 엔드포인트 에이전트를 중앙 집중식으로 배포하고 업데이트하고 관리하여 공동 솔루션의 워크플로를 향상하는 관리 작업을 간소화할 수 있습니다.

DXL 과 McAfee ePO 를 사용하는 인포블록스 DDI 및 ActiveTrust

인포블록스 DDI 는 장치 검색 기능과 장치 및 네트워크를 관리하는 단일 장소를 제공합니다. 새로운 장치가 네트워크에 조인하거나 가상 워크로드가 급등하거나 악의적인 활동이 DNS 보안 솔루션에서 감지되는 등의 네트워크 변경이 발생하면 즉시 알 수 있습니다.

인포블록스 DDI 와 ActiveTrust 는 아웃바운드 RESTful 애플리케이션 프로그래밍 인터페이스 (API) 를 사용하여 DXL 을 통해 보안 및 네트워킹 이벤트 주제를 컨텍스트와 함께 게시합니다. 데이터 교환 계층 (DXL) 은 전체 McAfee 제품 포트폴리오와 해당 기술 파트너 생태계에 대한 위협 정보 공유 패브릭입니다. SIEM, 사용자 행동 분석, 취약성 스캐닝, 모바일 관리 솔루션과 같은 애플리케이션은 보안 데이터 공유를 통해 고가치 정보를 고유의 컨텍스트로 가져오고 해결을 수행하여 잘 오케스트레이션된 보호 영역을 형성합니다. DXL 주제 구독자는 DDI 네트워크 변경과 식별된 DNS 위협을 솔루션 내에 통합하고 필요에 따라 이러한 이벤트에 대한 응답을 트리거할 수 있습니다. DXL 을 통해 이러한 네트워킹 및 보안 이벤트를 McAfee ePO 관리로 끌어와서 해결 및 정책 작업을 수행할 수 있습니다.

McAfee 및 인포블록스 공동 솔루션 참조 아키텍처

감지, 자동화 및 오케스트레이션

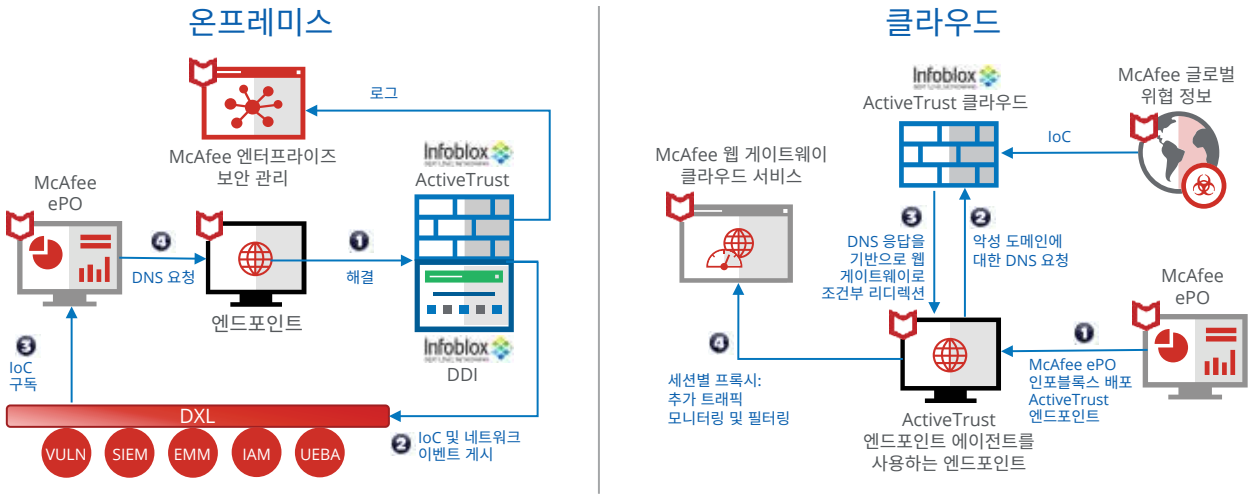

그림 1. 인포블록스 DDI, ActiveTrust, ActiveTrust 클라우드와 McAfee 보안 솔루션 간의 통합을 나타내는 솔루션 참조 아키텍처.

McAfee 엔터프라이즈 보안 관리자를 사용하는 인포블록스 DDI 및 ActiveTrust

인포블록스는 포괄적인 위협 데이터 상관 관계 및 감지를 수행할 수 있도록 네트워킹 이벤트 및 DNS 보안 이벤트/경보를 McAfee 엔터프라이즈 보안 관리자 (SIEM) 솔루션과 공유합니다. 또한 인포블록스는 위험 평가와 경보 우선 순위 지정을 지원하기 위해 가치 있는 네트워크 컨텍스트 및 실행 가능한 정보(IP 주소, DHCP 지문, 릴리스 기록 등)를 공유합니다. 이렇게 하면 실제 위험을 기반으로 사고에 더욱 효과적으로 대응하여 보안 운영팀에 더 높은 수준의 효율성을 제공할 수 있습니다.

McAfee 웹 게이트웨이 클라우드 서비스 정보

McAfee 웹 보호는 보안 게이트웨이 기술을 사용하여 모든 장치, 사용자 및 위치를 정교한 위협으로부터 보호합니다.

McAfee 웹 보호는 온프레미스 McAfee 웹 게이트웨이와 클라우드에서 제공하는 McAfee 웹 게이트웨이 클라우드 서비스를 결합한 통합 솔루션입니다. 온프레미스 솔루션과 클라우드 솔루션을 함께 배포하면 어디로 이동하든 상관없이 장치에 적용되는 단일 공유 정책을 사용하여 단일 콘솔에서 두 가지 솔루션을 모두 관리할 수 있습니다.

McAfee ePolicy Orchestrator 정보

McAfee ePolicy Orchestrator 는 엔드포인트 관리 콘솔이며 McAfee 관리 솔루션의 기초입니다. 30,000 명 이상의 고객이 6,000 만 개 이상의 노드에서 McAfee ePO 소프트웨어를 사용하여 보안을 관리하고 규정 준수 프로세스를 효율화 및 자동화하며 모든 보안 관리 활동에 대한 전체적인 가시성을 향상하고 있습니다. 확장 가능한 아키텍처, 빠른 배포 시간, 엔터프라이즈 시스템에 최적화된 기능을 갖춘 McAfee ePO 소프트웨어는 현재 사용 가능한 가장 발전된 보안 관리 소프트웨어입니다.

데이터 교환 계층 정보

데이터 교환 계층 (DXL) 통신 패브릭은 여러 공급업체 제품과 내부적으로 개발된 솔루션 전반에 걸쳐 보안 작업을 연결하고 최적화합니다. 기업은 새로운 데이터에 실시간으로 안전하게 액세스할 수 있으며 다른 제품과 가볍게 즉시 상호 작용할 수 있습니다.

McAfee 엔터프라이즈 보안 관리자 정보

McAfee 보안 정보 및 이벤트 관리 (SIEM) 솔루션 제품군의 기초인 McAfee 엔터프라이즈 보안 관리자는 보안 조직이 은밀한 위협을 식별하고 이해하며 대응하는 데 필요한 속도와 규모로 성능, 실행 가능한 정보, 실시간 상황 인식을 제공하면서 동시에 내장된 규정 준수 프레임워크를 통해 규정 준수를 간소화합니다.

인포블록스 ActiveTrust 클라우드 정보

인포블록스 ActiveTrust 클라우드는 SaaS 솔루션으로, DNS 기반 데이터 반출을 차단하고, C&C 서버와 악성 소프트웨어의 통신을 중단시키며, 정책을 준수하지 않는 콘텐츠에 대한 액세스를 자동으로 방지하고, 오케스트레이션과 더 빠른 해결을 위해 정보 및 IoC 를 기존 보안 인프라와 공유합니다. 이 솔루션은 자동화된 고품질 위협 정보 피드, 행동 분석, 기계 학습을 사용하여 이러한 이점을 제공하므로 제로데이 위협까지도 포착할 수 있습니다.

인포블록스 ActiveTrust 정보

인포블록스 ActiveTrust 는 DNS 를 통한 데이터 반출과 악성 소프트웨어 C&C 통신을 방지하고, 큐레이팅된 내부 및 외부 위협 정보를 중앙에서 집계하며, 해결을 위해 유효성 검사된 위협 데이터를 고객의 보안 생태계에 배포하고, 컨텍스트 확인 및 위협 우선 순위 지정을 위한 신속한 조사를 지원하는 온프레미스 DNS 보안 솔루션입니다.

인포블록스 DDI 정보

인포블록스는 보안 클라우드 관리 네트워크 서비스를 통해 더 높은 수준의 DDI 로 이행하는 방법을 선도하고 있습니다. 인포블록스는 클라우드 및 하이브리드 시스템에 더 높은 수준의 보안, 신뢰성, 자동화를 제공하여 고객에게 네트워크 관리를 위한 단일 창으로 이동하는 경로를 안내합니다. 인포블록스는 Fortune 지 선정 500 대 기업 중 350 개 기업을 비롯해 8,000 명의 고객을 보유하여 50% 의 시장 점유율을 차지하고 있는 널리 인정 받는 선두 기업입니다.
www.Infoblox.com 에서 자세히 알아보십시오.

McAfee
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com