데이터 시트

Infoblox Threat Defense™ Advanced

영향이 발생하기 전에 어디에서나 모든 요소를 보호하는 예측적 위협 인텔리전스 기반의 보호 DNS

DNS는 모든 사이버 공격을 가장 빠르게 방지할 수 있는 지점입니다.

DNS는 모든 사이버 공격을 탐지하고 예방할 수 있는 첫 번째 지점입니다. 피싱 이메일, 스미싱 문자 메시지, 악용된 취약점 중 무엇으로 시작되든 거의 모든 공격은 악성 도메인에 대한 DNS 쿼리를 생성합니다. 결과적으로 DNS는 온프레미스, 클라우드 또는 엣지에 있는 사용자, 장치, IoT/OT 및 워크로드를 포함하여 전체 기업을 보호하기 위한 강력하고 중앙 집중화된 가시성과 제어 지점을 제공합니다.

모든 커뮤니케이션의 첫 단계에서 DNS 계층에서 위협 활동을 탐지하고 차단하면, 악성 트래픽이 이후 도구에 도달하여 경고를 트리거하기 전에 이를 멈출 수 있습니다. DNS 데이터를 디바이스 및 자산 정보와 연계하면 NetOps 및 SecOps 팀은 환경 전체에서 일어나는 일에 대한 가시성을 높여 운영 효율성과 보안 수준을 모두 강화할 수 있습니다.

더 이상 효과가 없는 기존의 '탐지 및 대응' 솔루션

점점 더 많은 위협 행위자가 AI를 활용하여 더욱 성공적이고 정교하며 은밀하게 활동하고 있습니다. 이들은 고유한 설계의 일회용 멀웨어를 생성하여 '최초' 감염을 기다리는 기존의 '탐지 및 대응' 도구를 무력화합니다. 모든 공격은 시그니처나 알려진 동작이 없는 '최초 감염' 시나리오가 됩니다. '탐지 및 대응' 도구는 종종 킬 체인에서 너무 늦게 작동하여 피해를 방지하지 못합니다. 따라서 이와는 다른 선제적 접근 방식, 즉 위협이 환경에 침투하거나 수평 이동하기 전에 이를 차단하는 솔루션이 필요합니다. 이를 통해 공격을 조기에 차단할 수 있을 뿐만 아니라 기존의 '탐지 및 대응' 도구의 부담도 줄일 수 있습니다.

DNS는 상위 제어 지점으로 작동하여 위협이 사용자, 워크로드 또는 엔드포인트에 도달하기 전에 보안 팀이 이를 조기에 탐지하고 차단할 수 있는 선제적 기회를 제공합니다.

DNS를 통한 선제적 보안

Infoblox Threat Defense™ Advanced는 고유한 **선제적 방식**의 위협 탐지를 가능하게 합니다. 이러한 위협 탐지는 '최초 감염'에 의존하지 않으며, 위협 행위자의 인프라가 무기로 진화하기 전에 차단하는 **예측적 위협 인텔리전스 및** 고객 네트워크의 DNS 쿼리에 대한 알고리즘/ML 기반 분석을 함께 활용하여 영향이 발생하기 전에 보호합니다. 보안 사고에 연관된 자산의 신속한 식별, 에코시스템 통합 및 직관적인 작업 공간을 통해 더 빠른 탐지, 더욱 신속한 대응 및 기존의 보안 투자에 대한 더 큰 투자 수익(ROI)을 실현합니다.

사실 및 수치

- **20만 4천 개** 이상의 증가 중인 실시간 위협 행위자 클러스터 모니터링
- 오탐률을 **0.0002%로 감소**
- 첫 번째 쿼리 전에 **82%**의 위협 차단
- 평균적으로 공격 발생 **68.4**일 전에 보호 시작
- 알려진 악성 행위만을 찾는 도구에 비해 고위험/중위험 도메인을 **5배 더 많이** 차단
- 월 평균 **500시간의 SOC 분석가 시간** 절약*
- 연간 **40만 달러**의 생산성 절감 실현 지원*
- 경고 알림을 수만 건에서 몇 건 수준으로 축소*

SANS의 2025년 SOC 설문조사 결과에 따르면, SOC의 완전한 활용을 가로막는 주요 장애 요인 10가지 중 7가지는 과도한 경고, 보안 도구 간 통합 부족, 그리고 인력 및 기술 부족 문제와 관련이 있었습니다.

*실제 고객 데이터 기반.

영향이 발생하기 전에 위협 차단

Infoblox Threat Defense는 실시간 DNS 트래픽에 예측적 DNS 위협 인텔리전스와 함께 알고리즘/머신 러닝 분석을 적용하여 위협 활동이 네트워크에 영향을 미치기 전에 이를 차단하며, 많은 경우 다른 도구가 탐지하지 못하는 위협을 탐지합니다. Infoblox는 DNS 계층에서 위협을 차단하여 이후 보안 도구의 경고 수와 워크로드를 줄이는 데 기여합니다. 실제로 고객들은 차세대 방화벽(NGFW) 및 엔드포인트 탐지 및 대응(EDR) 시스템에서 경고가 최대 50% 감소했다고 보고했습니다.

> *"보안 DNS는 네트워크 내 악성코드를 성공적으로 배포하는 악성코드 공격의 약 92%를 줄일 수 있습니다."*
>
> **Anne Neuberger,**
> **미국 국가안보국(NSA)**
> **사이버보안국**
> **국장**

핵심 기능	설명	Infoblox Threat Defense	NGFW	SASE	EDR
전사적 Secure Resolver 및 DNS 쿼리 로깅	DNS 쿼리 데이터를 사용하여 도메인을 찾아 차단합니다.	●	◑	◑	◑
전체 DNS 동작 모니터링	모든 DNS 레코드 유형을 모니터링하여 악성 활동을 감지합니다.	●	●	◔	○
유사/도플갱어 도메인 탐지 및 도메인 삭제	유사 도메인 및 도플갱어 공격 노출 영역 감소	●	○	◑	○
Zero Day DNS 보호	조직에 위협이 될 수 있는 신규 또는 새로운 도메인을 식별합니다.	●	◑	◑	○
행동 기반 DNS 터널링 탐지	데이터 유출/침입, C2 통신 등에 사용되는 DNS 터널을 탐지합니다.	●	◑	◑	○
사전 예방적 의심/고위험 도메인 보호	향후 악성 캠페인에 사용될 가능성이 있는 의심스러운 도메인을 사전에 식별하고 차단합니다.	●	◑	◑	◑
자동화된 네이티브 컨텍스트 강화	클라이언트나 싱크홀링 없이도 네트워크 컨텍스트(사용자, 디바이스, 소스 IP, 위치, MAC 주소, VLAN)를 연관시킵니다.	●	◑	◑	◑
위협 배포 시스템(TDS) 사전 탐지 및 차단	탐지 회피를 위해 다수의 도메인을 순환 사용하는 위협 행위자에 대응하기 위해, 개별 도메인뿐만 아니라 위협 행위자의 TDS(트래픽 유도 시스템) 인프라 전체를 식별합니다.	●	◔	○	○

그림 1. 다른 보안 솔루션이 완전히 해결하지 못하는 위협까지 대응하는Threat Defense만의 독보적인 기능

위협 방어의 주요 기능

- **'영향 발생 전 보호' 모니터링.** CISO와 보안팀이 선제적 보안 전략을 실행하고, 영향을 받기 전에 무력화된 위협에 관한 명확하고 정량화 가능한 지표를 이사회에 자신 있게 보고할 수 있도록 하여 크나큰 시간적 이점을 확보하고 보안 운영 센터(SOC)의 부담을 줄입니다.
- **자산 탐지 및 인벤토리 통합.** 보안 사고와 관련된 자산을 신속하게 식별하여 사고 평가 및 대응 속도를 높입니다.
- **보안 작업 공간.** 보안팀이 환경에서 발생하는 상황을 이해하고 보안 위험을 줄이는 방법을 제안할 수 있도록 하는 간소화되고 직관적인 UI입니다.
- **탐지 모드.** 기존의 IT 또는 네트워크 인프라를 바꾸지 않고도 쉽게 배포하고 개념 증명을 제공하기 위한 것입니다.

예측적 인텔리전스를 활용한 선제적 보안성 강화

Infoblox는 독자적인 DNS 기반 위협 인텔리전스를 선도적으로 개발하는 기업입니다. 단순히 방어를 넘어, 자체적인 인사이트를 바탕으로 위협 행위자의 인프라를 구축되는 순간부터 추적하고 공격이 시작되기도 전에 사이버 범죄를 근본적으로 저지합니다.

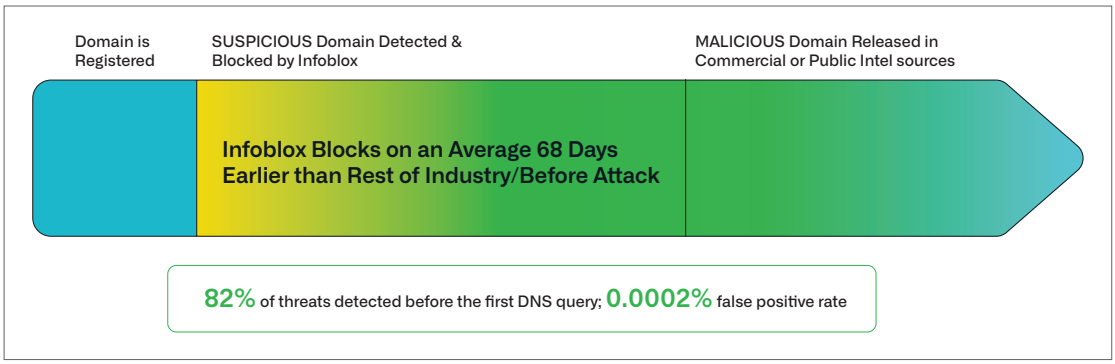

그림 2. Infoblox Threat Intel은 다른 보안 업계보다 앞서 위협으로부터 보호할 수 있습니다.

Infoblox가 독창적인 DNS 위협 인텔리전스를 생성하는 방법

DNS 전문가: Infoblox는 어디를 살펴야 할지 알기에 DNS에 숨어 있는 위협 행위자를 찾아냅니다. 고위험 또는 의심스러운 도메인에서 시작해 단서를 연결하고, 공격자의 인프라를 식별한 뒤 그 변화와 새로운 위협을 그 누구보다도 먼저 인식하여 지속적으로 추적합니다.

위협 인텔리전스 전문성: Infoblox는 악의적인 공격자의 활동 방식과 멀웨어, 랜섬웨어, 피싱 및 DNS 기반 악용과 같은 위협이 어떻게 나타나는지 잘 알고 있습니다. 이러한 전문성을 바탕으로 유사 도메인, DNS 명령 및 제어(C2) 활동, RDGA(등록 도메인 생성 알고리즘) 및 기타 의심스러운 행동을 탐지하는 예측 시스템을 운영합니다.

데이터 사이언스: Infoblox는 방대한 DNS 쿼리 데이터에 머신 러닝과 고급 데이터 사이언스를 적용하며, 이를 통해 데이터 유출, 도메인 생성 알고리즘(DGA) 및 여러 교묘한 위협에 대해 거의 실시간으로 보호를 제공합니다.

SOC 인사이트를 활용하여 더 스마트하게 일하기

Infoblox Threat Defense는 추가적인 SOC Insights 패키지를 통해 SOC 팀의 끝없는 경고 알림, 분석가의 피로, 장시간의 조사 및 대응과 같은 부담을 효과적으로 줄여줍니다.

- AI 기반 분석을 통해 수십만 개의 알림을 소수의 인사이트로 압축하여 분석가가 가장 중요한 것을 파악할 수 있도록 돕습니다.
- 로그, 위협 인텔리전스 및 기타 데이터 수집 및 상관관계를 자동화하여 분석가들이 조사 및 대응을 신속하게 시작할 수 있도록 합니다.
- 자산 탐색 및 인벤토리 통합을 통해 사고 대응을 가속화하여 분석가들이 영향을 받는 디바이스를 더 빠르게 식별할 수 있도록 지원합니다.

그림 3: Infoblox Threat Intel은 점점 증가하는 유사 도메인(Lookalike domain)의 위험성에 대해 주목할 만한 연구 데이터를 보여줍니다.

고가치 DNS 로그 대규모로 내보내기

Infoblox를 사용하면 충실도 높은 DNS 쿼리 및 이벤트 데이터를 SIEM, SOAR 또는 데이터 레이크로 쉽게 전송하여 중앙 집중식 가시성과 빠른 위협 상관관계를 확보할 수 있습니다.

- 고가치 DNS 이벤트만 필터링하고 전달하여 SIEM 수집 비용과 경고로 인한 노이즈를 줄이세요.
- Infoblox 클라우드 데이터 커넥터를 사용하여 실시간으로 강화된 DNS 로그를 스트리밍하세요.
- 모든 도구에 필요한 컨텍스트를 제공하여 에코시스템 전반에서 탐지 및 대응을 개선하세요.
- 인증된 양방향 통합을 통해 다른 도구와 데이터를 원활하게 공유하여 엔드투엔드 탐지, 분류 및 대응을 개선하세요.

DOSSIER로 더 빠르게 조사

Dossier는 분석가에게 강력하고 통합된 연구 도구를 제공하여 서로 다른 플랫폼 간 전환할 필요 없이 위협을 검증하고, 침해 지표(IOC)를 중심으로 분석하며, 조사 속도를 높입니다.

- 내부, Infoblox 및 타사 위협 인텔리전스를 하나의 직관적인 인터페이스로 통합하세요.
- 기본 제공되는 보강 및 링크 분석을 통해 IOC를 신속하게 조사하고 관련 위협을 발견하세요.
- 수동 데이터 수집과 컨텍스트 전환을 제거하여 조사 시간을 최대 67% 단축할 수 있습니다.

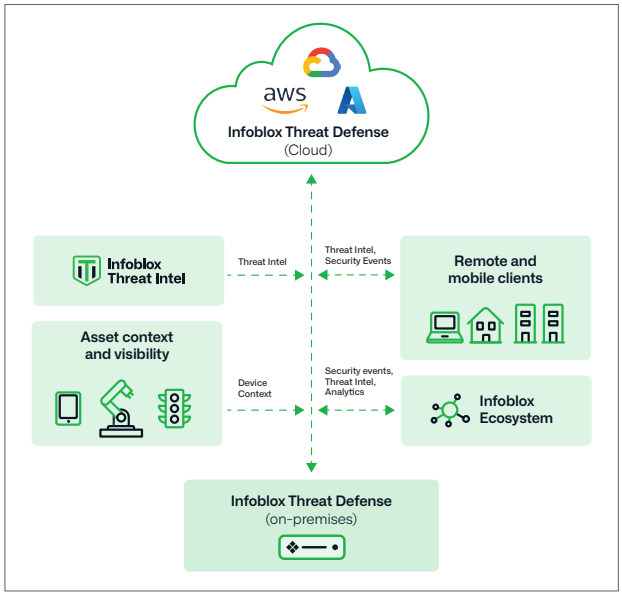

그림 4. Infoblox의 하이브리드 아키텍처는 오늘날 AI 기반 위협 환경에 대응하기 위해 어디서든 배포 가능하고, 전방위적인 보호를 제공합니다.

브랜드를 표적 디셉션으로부터 보호하세요

Infoblox는 유사 도메인 모니터링 및 도메인 완화 서비스라는 두 가지 통합 기능을 제공하여 디셉션 기반의 사이버 공격으로부터 브랜드, 고객 및 직원을 보호합니다. 이러한 기능을 함께 사용하면 새로운 위협에 대한 가시성을 확보하고, 악성 도메인이 비즈니스에 영향을 미치기 전에 빠르고 효과적으로 조치를 취할 수 있습니다.

유사 도메인 모니터링

브랜드나 신뢰할 수 있는 서드 파티를 악용하는 사칭 공격에 미리 대응하세요.

- 회사, 공급망 또는 고객을 상대로 한 자산을 사칭할 목적으로 등록된 도메인을 탐지하세요.
- 귀하의 직원 또는 고객을 대상으로 하는 피싱 및 사기 캠페인에 사용된 도메인을 식별하세요.
- 우선순위가 높은 도메인을 모니터링하여 위험 태세 변화를 감지하고 실시간 경보를 받으세요.

도메인 완화 서비스

활동 중인 악성 도메인을 신속하게 검증 및 제거

- 사람이 주도하는 사고 검증 및 요약 보고를 통해 악성 활동을 확인하고 문서화하세요.
- 글로벌 ISP, 호스팅 제공업체 및 규제 기관과 협력하여 신속한 삭제를 진행하세요(대개 24시간 이내).
- 제거 후 30일 동안 완화된 위협을 모니터링하여 추가 비용 없이 재활성화 시도를 감지하고 제거하세요.
- 피싱, 멀웨어 호스팅, C2 인프라 및 도난당한 데이터 등 다양한 위협 유형에 대응하세요.

Infoblox Threat Defense가 데이터와 인프라를 보호하는 방법에 대해 자세히 알아보려면 https://www.infoblox.com/products/threat-defense/를 참조하세요.

Infoblox는 네트워킹과 보안을 통합하여 비교할 수 없는 성능과 보호를 제공합니다. 포춘지 선정 100대 기업과 신생 혁신 기업에서 신뢰를 받으며, 사용자의 디바이스에 대한 실시간 가시성과 제어 기능을 제공하여 조직 내부에서 발생하는 위협을 조기에 차단할 수 있습니다.

본사
2390 Mission College Blvd, Ste.501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

버전: 20250121v1