데이터 시트

# BloxOne® Threat Defense Advanced

## 기초부터 보안 상태 강화 및 최적화

### 규모에 맞는 기초 보안의 필요성

기존 보안 모델은 오늘날의 디지털 트랜스포메이션에는 적합하지 않습니다.

- 경계가 변화했고 사용자는 어디서나 클라우드 기반 애플리케이션에 직접 액세스할 수 있습니다.
- IoT 덕분에 기존 엔드포인트 보안 기술을 수용하지 않는 디바이스가 대폭 증가했습니다.
- 대부분의 보안 시스템은 복잡하며 이러한 역동적인 환경을 보호하는 데 필요한 수준까지 확장하기 어렵습니다.

조직에 필요한 것은 추가 인프라를 구축하거나 관리할 필요없이 전체 네트워크를 보호하는 확장 가능하고 간편하며 자동화된 보안 솔루션입니다.

### INFOBLOX는 기존 위협 방어 투자를 극대화하는 확장 가능한 플랫폼을 제공합니다.

Infoblox BloxOne Threat Defense Advanced는 포괄적인 DNS 탐지 및 대응(DNSDR) 솔루션입니다. 다른 솔루션이 놓치고 있는 위협 활동을 탐지하고 공격자의 공급망을 방해하기 위해 추적된 사전 캠페인 DNS 위협 인텔리전스로 공격을 차단합니다. 지능형 에코시스템 통합 및 자동화는 수동 작업을 줄여주는 반면 Infoblox만의 독자적인 AI 기반 분석은 분석가들이 가장 중요한 것에 초점을 맞추도록 지원하며 MTTR을 단축하고 기존 보안 도구의 ROI를 높이며 전반적인 보안 운영 효율성을 높이는 인사이트를 제공합니다.

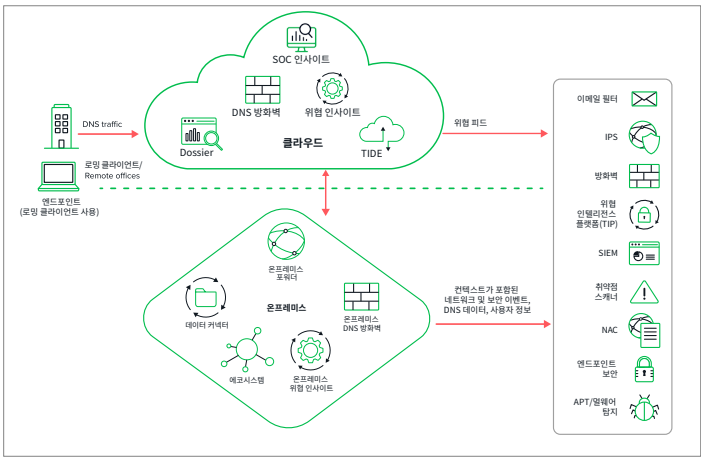



그림 *1: Infoblox* 하이브리드 아키텍처를 통해 언제 어디서나 보호 및 배치 가능

### 주요 기능

- 다른 솔루션이 놓치는 취약점 공격, 피싱, 랜섬웨어 및 기타 최신 악성 코드를 탐지하고 차단합니다.
- 플랫폼이나 OS 유형에 상관없이 BYOD, IoT, ICS 등 DNS 계층에서 사용자와 디바이스를 보호합니다.
- 위험도가 높은 애플리케이션을 발견하고 섀도우 IT, 내부자, 규정 준수 및 기타 위험을 관리합니다.
- AI 분석 및 머신 러닝을 사용하여 DNS 기반 데이터 유출, DGA 및 DNS Messenger를 포함한
- 데이터 유출 기법을 탐지해 차단합니다.
- 부적절하거나 원치 않는 웹 콘텐츠에 대한 사용자 액세스를 제한하고 활동을 추적합니다.
- 유사 도메인 모니터링을 통해 중요한 인터넷 자산을 보호합니다.
- 조사 속도를 3배 높이고 위협 대응 및 위협 추적 활동을 간소화합니다.
- 가시성 향상: 이벤트의 이해 및 상관 관계를 최적화 하기 위해 IPAM 자산 메타데이터를 통합하여 정확한 가시성과 '풍부한 네트워크 컨텍스트'를 제공합니다.
- SOC Insights를 사용하여 가장 중요한 위협에 대한 조사 및 대응을 신속하게 시작하고 AI 기반 인사이트를 통해 MTTR을 단축합니다.

## 보안 운영 센터 효율성 극대화

### 사고 대응 시간 단축

- 악성 활동을 자동으로 차단하고 위협 데이터를 나머지 보안 에코시스템에 제공하여 조사, 격리 및 복구를 지원합니다.
- 상황에 맞는 네트워크 및 위협 인텔리전스 데이터와 Infoblox 에코시스템 통합(SOAR의 핵심 지원 기술)으로 SOAR 솔루션을 최적화하고 위협 대응 시간 및 운영 비용을 절감합니다.
- Infoblox SOC Insights 기능을 사용하여 단순한 멀웨어 위험 순위 대시보드를 넘어서는 AI 기반 분석을 통해 가장 중요한 이벤트를 파악합니다.

### 위협 인텔리전스 수집을 통한 보안 정책 통합

- 내부 및 외부 소스로부터 만들어진 위협 인텔리전스 데이터를 수집 및 관리하여 기존 보안 시스템에 배포합니다.
- 위협 피드 비용을 절감하는 동시에 전체 보안 스택에서 위협 인텔리전스의 효율성을 개선합니다.

### 더 빠른 위협 조사 및 헌팅

- 단순한 맬웨어 위험 순위 대시보드를 뛰어넘는 AI 기반 통찰력으로 가장 중요한 위협에 대한 조사 및 대응을 신속하게 시작하고 MTTR을 단축합니다.
- 보안 분석가에게 자동화된 위협 조사, 관련 위협에 대한 인사이트 및 전문가의 추가 연구 관점을 제공하여 위협에 대응해 신속하고 정확한 결정을 내릴 수 있도록 지원함으로써 위협 분석가 팀의 **생산성을 3배 더 향상시킵니다**.

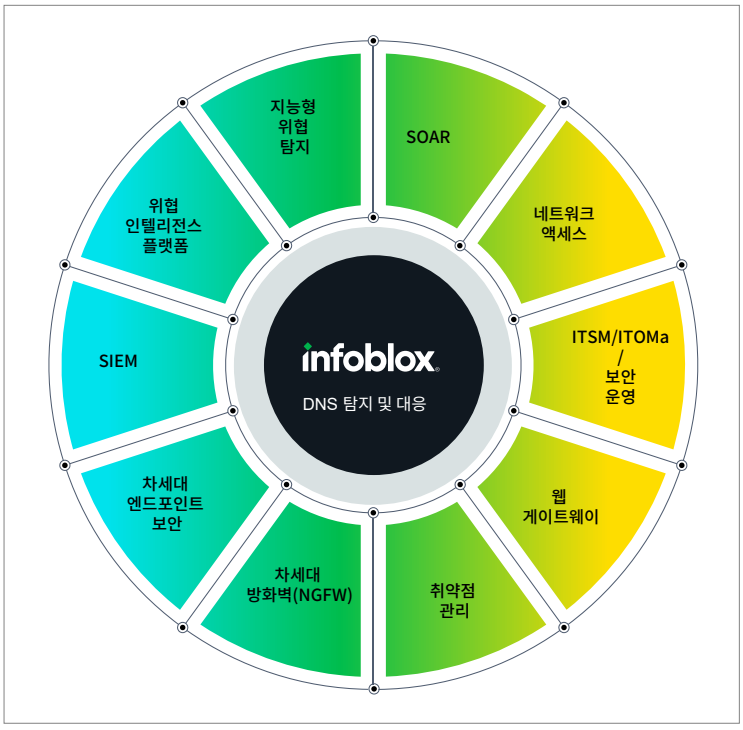
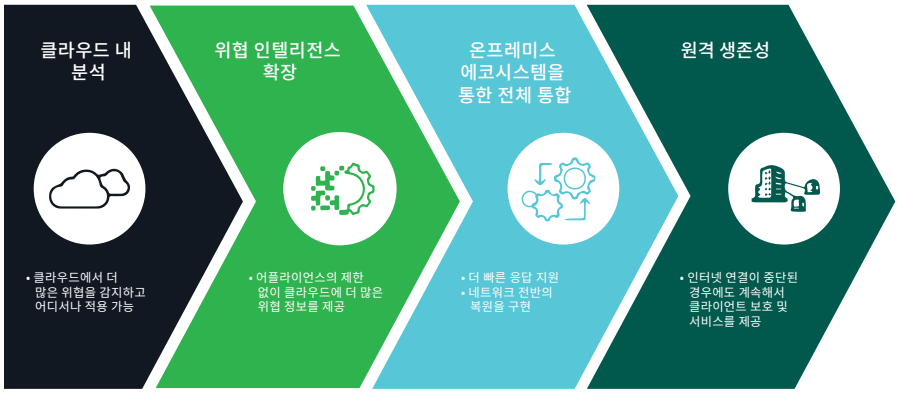



그림 2: 전체 사이버 보안 에코시스템과 통합된 *BloxOne Threat Defense*

> "오늘날에는 인터넷 사용자가 클릭한 링크를 통해 너무 많은 랜섬웨어, 스파이웨어 및 애드웨어가 유입되고 있습니다. "Infoblox 클라우드 보안 솔루션은 사용자를 악성 사이트로 이동시키는 리디렉션을 차단하고 시스템이 감염되지 않도록 보호하며 사용자의 안전을 보장해 줍니다."
>
> **수석 시스템 관리자 겸 네트워크 엔지니어, 시애틀 시립 대학교**

## 하이브리드 접근 방식으로 배포된 모든 곳에서 보호




### 클라우드 내 분석

- 클라우드의 우수한 처리 기능을 활용하여 데이터 유출, 도메인 생성 알고리즘(DGA), 패스트 플럭스 (fast flux), 파일리스 멀웨어(fileless malware),딕셔너리 DGA(Dictionary DGA) 등 다양한 위협을 머신 러닝 분석을 통해 더 광범위하게 탐지합니다.
- 클라우드에서 위협을 감지하고 어디서나 실행하여 본사, 데이터 센터, 원격 사무실 또는 로밍 디바이스를 보호합니다.

### 위협 인텔리전스 확장

- Infoblox 연구 및 타사 제공업체의 포괄적인 인텔리전스를 적용하여 온프레미스 또는 클라우드에서 정책을 시행하고 이를 나머지 보안 인프라에 자동으로 배포합니다.
- 모든 사이트의 추가 보안 어플라이언스에 대한 막대한 투자 없이 클라우드에서 더 많은 위협 인텔리전스를 적용합니다.

### 보안 에코시스템과의 강력한 통합

- 온프레미스 Infoblox 및 타사 보안 기술과의 완벽한 통합을 통해 네트워크 전반의 문제를 해결하고 해당 기술의 ROI를 향상시킵니다.

### 원격 지원/탄력성

- 인터넷 연결에 장애가 발생하더라도 온프레미스 Infoblox가 네트워크를 지속적으로 보호할 수 있습니다.

BloxOne Threat Defense가 데이터와 인프라를 보호하는 방법에 대해 자세히 알아보려면 다음 사이트를 방문하세요. https://www.infoblox.com/products/bloxone-threat-defense

## INFOBLOX 보안의 ROI

### 과부하가 걸린 보안 디바이스 부하 분산

- 이미 사용 중인 DNS 서버를 1차 방어선으로 사용하여 방화벽, IPS, 웹 프록시 등과 같은 주변 보안 장치에 대한 부담 완화
- **NGFW로 전송되는** 트래픽 최대 60배 감소*

### 기존 투자에 대한 ROI 개선

- 위협 및 공격자 정보를 양방향으로 공유하여 인접/보완 제품에서 더 많은 가치를 제공
- SIEM으로 DNS 데이터를 전송하는 경우 의심스러운 DNS 데이터만 전송하여 SIEM 솔루션 비용을 절감

### 자동화

- 자동화를 통해 인적 개입/오류로 인한 비용을 절감
- 숙련된 리소스 부족 극복 - 팀이 구현하고 (개월이 아닌 시간 단위로 구성) 운영하는데 필요한 기술과 비용이 60% 절감
- 심층적인 위협 인텔리전스를 위한 사용하기 쉬운 단일 콘솔을 통해 위협 분석가의 생산성을 3배 더 향상

*실제 고객 데이터를 기반으로

infoblox.

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

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

+1.408.986.4000
www.infoblox.com



버전: 20240122v1