VERİ SAYFASI

BloxOne® Threat Defense Advanced

Güvenlik seviyenizi temelden güçlendirin ve optimize edin

GENIŞ ÖLÇEKTE TEMEL GÜVENLIK İHTIYACI

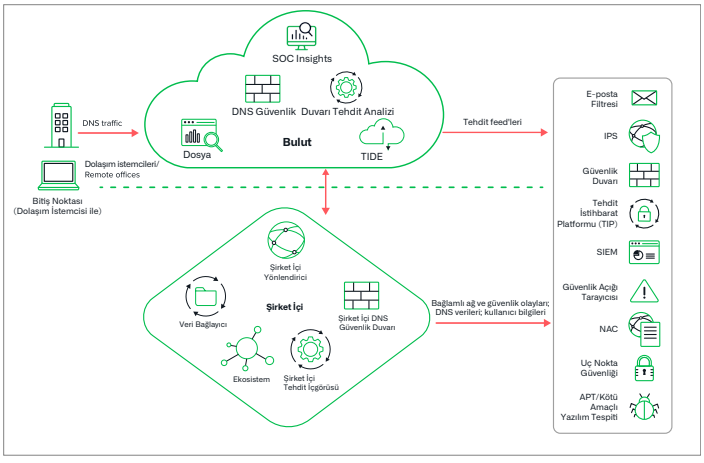
Geleneksel güvenlik modeli, dijital dönüşümlerin yaşandığı günümüz dünyasında yetersiz kalmaktadır.

- Ortam tümüyle değişti ve kullanıcılarınız bulut tabanlı uygulamalara her yerde doğrudan erişiyor.
- IoT, koruma için geleneksel uç nokta teknolojilerini kabul etmeyen cihazlarda büyük bir artışa yol açıyor.
- Çoğu güvenlik sistemi karmaşıktır ve bu dinamik ortamları korumak için gereken seviyeye kolayca ölçeklenemez.

Kuruluşların ihtiyacı olan şey, ek altyapı kurmaya veya yönetmeye gerek kalmadan tüm ağı koruyan ölçeklenebilir, basit ve otomatik bir güvenlik çözümüdür.

INFOBLOX, MEVCUT TEHDIT SAVUNMA YATIRIMINIZI EN ÜST DÜZEYE ÇIKARAN ÖLÇEKLENEBILIR BIR PLATFORM SAĞLAR

Kapsamlı bir DNS Algılama ve Yanıt (DNSDR) çözümü olan Infoblox BloxOne Threat Defense Advanced, diğer çözümlerin gözden kaçırdığı tehditleri tespit eder ve saldırganların tedarik zincirlerini bozma hedefli kampanya öncesi DNS tehdit istihbaratı ile saldırıları gerçekleşmeden önce durdurur. Akıllı ekosistem entegrasyonları ve otomasyon manuel çabayı azaltırken, Infoblox'un benzersiz yapay zeka odaklı analizleri, analistlerin en önemli konulara odaklanmasını sağlayarak MTTR'yi azaltan, mevcut güvenlik araçlarının yatırım getirisini artıran ve genel SecOps verimliliğini yükselten içgörüler sağlar.



Şekil 1: Infoblox hibrit mimarisi her yerde koruma ve dağıtım sağlar

TEMEL ÖZELLİKLER

- Diğer çözümlerin gözden kaçırdığı açıkları, kimlik avcılığını, fidye yazılımlarını ve diğer modern kötü amaçlı yazılımları algılayın ve engelleyin
- BYOD, IoT ve ICS dahil olmak üzere DNS katmanında tüm platform veya işletim sistemlerinde kullanıcıları ve cihazları koruyun
- Yüksek riskli uygulamaları keşfedin ve Shadow IT, Insider, Compliance ve diğer risklerinizi yönetin
- DNS tabanlı veri sızıntısı, DGA ve DNSMessenger dahil olmak üzere makine öğrenimi/yapay zeka analizleri ile veri sızma tekniklerini önleyin
- Uygunsuz veya istenmeyen web içeriğine kullanıcı erişimini kısıtlayın ve etkinliği izleyin
- En değerli internet mülkleriniz için Lookalike Domain Monitoring ile markanızı koruyun
- Soruşturmaları 3 kat hızlandırın, tehdit yanıtlama ve tehdit avlama faaliyetlerini kolaylaştırın
- Görünürlüğü artırın: Olayları optimum derecede anlama ve korelasyon için IPAM varlık meta verileriyle entegre olarak hassas görünürlük "ve zengin ağ bağlamı" elde edin
- SOC Insights, en önemli tehditleri hızlı bir şekilde araştırmanıza ve yanıtlamanıza ve Yapay Zeka Odaklı İçgörüler ile MTTR'yi azaltmanıza olanak tanır

GÜVENLIK OPERASYON MERKEZI VERIMLILIĞINI EN ÜST DÜZEYE ÇIKARIN

Olaylara Müdahale Süresini Azaltın

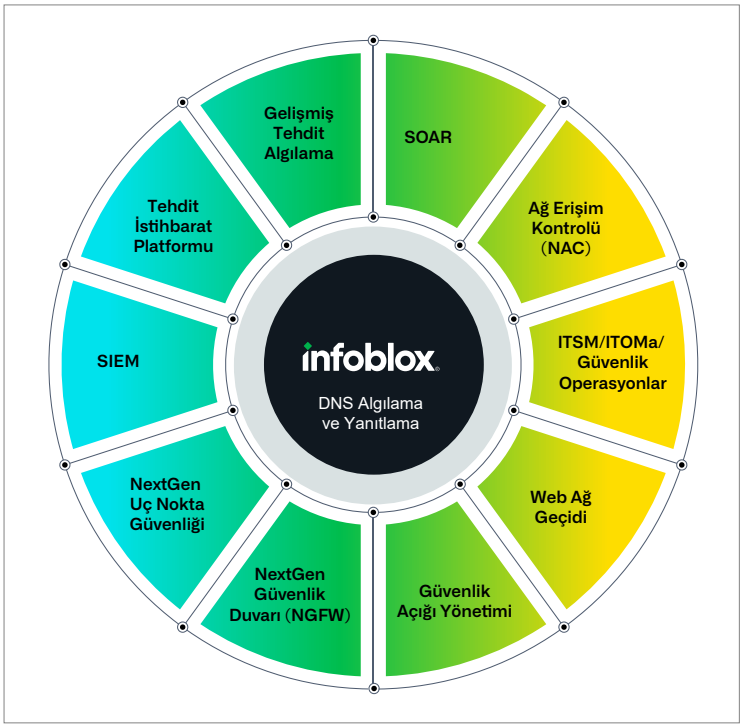
- Kötü amaçlı etkinlikleri otomatik olarak engelleyin ve tehdit verilerini araştırma, karantinaya alma ve düzeltme için güvenlik ekosisteminizin geri kalanına sağlayın
- SOAR çözümünü, bağlamsal ağ ve tehdit istihbaratı verilerini ve Infoblox ekosistem entegrasyonlarını (SOAR'ın kritik bir etkinleştiricisi) kullanarak optimize edin (tehdit yanıt süresini ve OPEX'i azaltın)
- Basit kötü amaçlı yazılım risk sıralamalı gösterge tablolarının ötesine geçen yapay zeka odaklı analizlerle hangi olayların en önemli olduğunu öğrenmek için Infoblox SOC Insights özelliklerinden yararlanın

Güvenlik Politikasını Tehdit Intel Taşınabilirliğiyle Birleştirin

- Dahili ve harici kaynaklardan tehdit istihbaratı verilerini toplayıp yönetmek ve mevcut güvenlik sistemlerine dağıtın
- Tüm güvenlik portföyünde tehdit istihbaratının etkinliğini artırırken tehdit feed'lerinin maliyetini azaltın

Daha Hızlı Tehdit Araştırması ve Avcılığı

- Basit kötü amaçlı yazılım risk sıralamalı gösterge tablolarının ötesine geçen yapay zeka odaklı içgörülerle en önemli tehditler üzerinde hızlı araştırma ve müdahale başlatarak MTTR'yi azaltın
- Güvenlik analistlerini otomatik tehdit araştırması, ilgili tehditler hakkında içgörüler ve tehditler hakkında hızlı ve doğru kararlar almaları için uzman siber kaynaklardan ek araştırma perspektifleri ile güçlendirerek tehdit analistleri ekibinizin **3 kat daha üretken** olmasını sağlar



Şekil 2: BloxOne Threat Defense, tüm siber güvenlik ekosistemiyle entegre olur

> *"Günümüzde ve çağımızda internet kullanıcıları tarafından açılan bağlantılar üzerinden gelen çok sayıda fidye yazılımı, casus yazılım ve reklam yazılımları var. Infoblox bulut güvenlik çözümü, kullanıcıları kötü sitelere gönderen yönlendirmeleri engellemeye yardımcı olur, makinelere virüs bulaşmasını önler ve kullanıcıları daha güvende tutar."*
>
> **Kıdemli Sistem Yöneticisi ve Ağ Mühendisi, Seattle Şehir Üniversitesi**

HİBRİT YAKLAŞIM, ÇALIŞTIĞINIZ HER YERDE KORUR

Bulutta Analitik

- Makine öğrenimi tabanlı analitiği kullanarak veri sızması, alan oluşturma algoritması (DGA), hızlı akış, dosyasız kötü amaçlı yazılım, Sözlük DGA gibi diğer tehditleri algılamak için bulutun daha fazla işleme kapasitesinden yararlanın
- Buluttaki tehditleri tespit edin ve genel merkezi, veri merkezini, uzak ofisleri veya dolaşım cihazlarını korumak için her yerde engelleyin

Tehdit İstihbaratı Ölçeklendirmesi

- Şirket içinde veya bulutta politikaları uygulamak için Infoblox araştırmalarından ve üçüncü taraf sağlayıcılardan edinilen kapsamlı istihbarata göre hareket edin ve bu bilgileri otomatik olarak güvenlik altyapısının geri kalanına dağıtın
- Her site için daha fazla güvenlik cihazına büyük yatırımlar yapmadan bulutta daha fazla tehdit istihbaratından yararlanın

Güvenlik ekosisteminizle güçlü entegrasyonlar

- Şirket içi Infoblox ve üçüncü taraf güvenlik teknolojileri ile tam entegrasyon sayesinde ağ genelinde iyileştirme sağlar ve bu teknolojilerin yatırım getirisini artırır

Uzaktan sürdürülebilirlik/dirençlilik

- İnternet bağlantınızda bir kesinti olursa, şirket içi Infoblox ağın güvenliğini sağlamaya devam edebilir

BloxOne Threat Defense'in verilerinizi ve altyapınızı nasıl güvence altına aldığı hakkında daha fazla bilgi edinmek için lütfen şu adresi ziyaret edin: https://www.infoblox.com/products/bloxone-threat-defense

INFOBLOX GÜVENLİĞİNİN YATIRIM GETİRİSİ

Gergin güvenlik cihazlarını boşaltın

- Zaten mevcut olan DNS sunucularınızı ilk savunma hattı olarak kullanarak, güvenlik duvarları, IPS ve web proxy'leri gibi aşırı yüklenen çevre güvenlik cihazlarının üzerindeki yükü azaltın
- **NGFW'lere gönderilen trafikte** 60 kata kadar azalma*

Mevcut yatırımların getirisini artırın

- Tehdit ve saldırgan bilgilerinin çift yönlü olarak paylaşılması ile bitişik/tamamlayıcı ürünlerden daha fazla değer elde edin
- DNS verilerini SIEM'e gönderiyorsanız, yalnızca şüpheli DNS verilerini bu platformlara gönderdiğinizden emin olarak SIEM çözümlerinin maliyetini azaltın

Otomasyon

- Otomasyonu kullanarak insan müdahalesini/hata maliyetini azaltın
- Nitelikli kaynak eksikliğinin üstesinden gelin - Ekibinizin uygulaması (aylar yerine saatler içinde yapılandırması) ve hem beceri hem de maliyet açısından çalışması için %60 daha az talep
- Derin tehdit istihbaratı için kullanımı kolay, tek bir konsol ile tehdit analistlerinizin 3 kat daha üretken olmasını sağlayın

Gerçek müşteri verilerini temel alır

infoblox.

Infoblox, benzersiz performans ve koruma sağlamak için ağ ve güvenliği birleştirir. Fortune 100 şirketleri ve gelişmekte olan yenilikçiler tarafından güvenilen firmamız, ağınıza kimin ve neyin bağlandığı üzerinde gerçek zamanlı görünürlük ve kontrol sağlıyor. Böylece kuruluşunuz daha hızlı harekete geçerek tehditleri daha çabuk durdurabilir.

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

+1.408.986.4000
www.infoblox.com

Sürüm: 20240122v1