VERİ SAYFASI

Infoblox gelişmiş DNS koruması

DNS tabanlı saldırıların neden olduğu kesintileri en aza indirin

ZORLUK: HİZMET KESİNTİLERİ

DNS, bir işletmeyi yürütmek için görev açısından kritik derecede gerekli ağ bağlantısını sağladığından her kuruluş için hayati öneme sahiptir. Dış DNS sunucunuz çökerse ağınızın tamamının internet bağlantısı kesilir. DNS kesintileri e-posta, web siteleri, VoIP ve SaaS gibi kritik BT uygulamalarını engeller veya kapatır. 2020'de işgücünün önemli bir kısmının uzaktan çalışmaya başlamasıyla DDoS saldırılarında büyük bir artış yaşandı. DNS, bir işletmeyi çevrimiçi tutmak için kritik öneme sahip olduğundan DDoS için başlıca bir hedef olmaya devam ediyor. Müşteri güveni ve repütasyon kaybına ek olarak, başarılı DDoS saldırıları bir kuruluş için ayda yüz binlerce dolar gelir kaybına yol açabilir.

Infoblox, hayati önem taşıyan DNS hizmetlerinizi saldırılara karşı korumak için piyasadaki en geniş koruma yelpazesini sunar. Tehditlere karşı hızlı yanıt verilmesini sağlamak için ağı kimin kullandığına, hangi cihazla bağlandığına ve saldırıyla ilgili ayrıntılara ilişkin merkezi görünürlük elde edebilirsiniz.

ÇÖZÜM: İŞLETMENİNİZİ DNS TABANLI SALDIRILARDAN KAYNAKLANAN KESİNTİLERDEN KORUYUN

Infoblox Gelişmiş DNS Koruması (ADP) ile işletmeniz DNS tabanlı bir saldırı altındayken bile her zaman çalışır durumdadır. Infoblox, volumetrik ataklar, NXDOMAIN, exploit ve DNS hijaking gibi her türden saldırıları engeller. Gelişmiş DNS Koruması, basit yanıt hızı sınırlamasına dayanan yaklaşımların aksine, aşağıdakileri akıllıca algılar ve güvenlik yamaları dağıtmaya gerek kalmadan, sürekli güncellenen tehdit istihbaratını kullanarak yalnızca meşru sorgulara yanıt vererek DNS saldırılarını azaltır. Infoblox sayesinde, kritik altyapınızın ve işinizin her zaman çalışmaya devam etmesini sağlayarak ağ güvenilirliğini bir üst seviyeyetaşıyabilirsiniz.

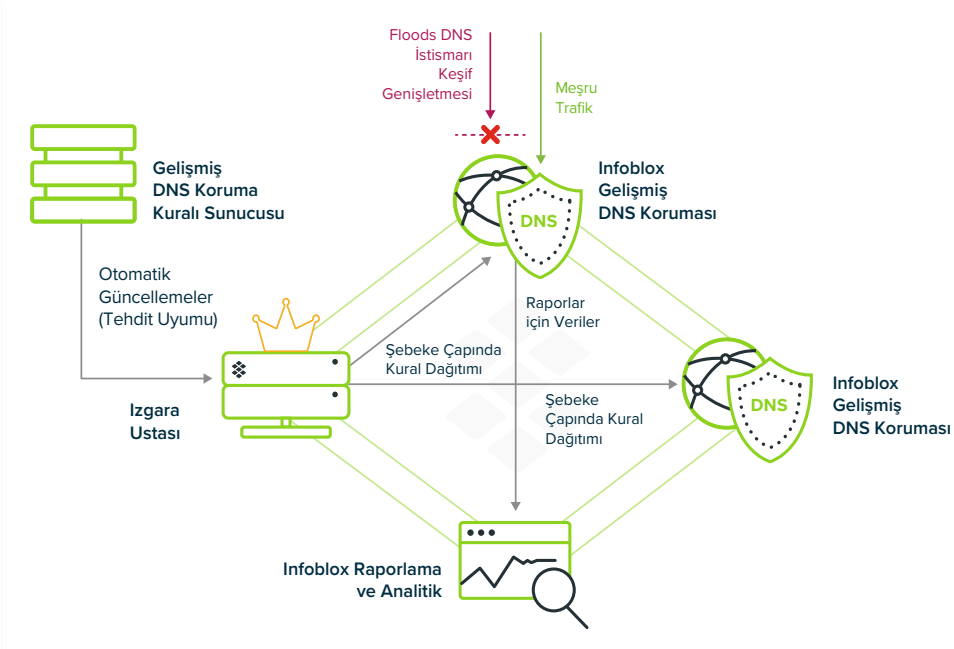
TEMEL ÖZELLIKLER

İş Kesintilerini Azaltın:
Infoblox Gelişmiş DNS Koruması (ADP), meşru sorgulara yanıt verirken volumetrik saldırılar, DNS açıkları ve DNS ele geçirme gibi volumetrik olmayan saldırılar dahil olmak üzere her türlü DNS saldırısını sürekli olarak izler, algılar ve durdurur. Ayrıca, DNS hijacking saldırılarının tehlikeye atabileceği DNS bütünlüğünü de korur. Infoblox güvenlik için sağlam bir temel oluşturarak ağınız için %99 kullanılabilirlik sağlar.

Gelişen Tehditlere Uyum Sağlayın:
Infoblox ADP, ortaya çıktıkça yeni ve gelişen tehditlere karşı korumayı otomatik olarak güncellemek için Infoblox Threat Adapt™ teknolojisini kullanır. Threat Adapt korumayı güncellemek için tehdit uzmanlarının müşteri ağlarında gördükleri de dahil olmak üzere, gelişen saldırı tekniklerine bağımsız analiz ve araştırma uygular.Bu sayede korumayı DNS yapılandırma değişikliklerini yansıtacak şekilde otomatik olarak uyarlar.

DOT VE DOH'U ETKİNLEŞTİRME

DNS istemcisi ile yerel DNS sunucusu arasındaki iletişim şifrelenmez. Şifrelenmemiş iletişimler, DNS'in "son mil" güvenlik sorunu olarak da bilinen veri snooping, veri yakalama ve veri sızdırmaya maruz kalır. Buna karşılık olarak sektör, DNS istemcileri ile harici internet DNS sunucuları arasında gizlilik ve şifreleme sağlamak için TLS üzerinden DNS (DoT) ve HTTPS üzerinden DNS (DoH) uygulamalarını başlattı. Ağınızdaki DNS çözümleyicisi aracılığıyla şifreleme uygulamak, güvenlik politikanıza göre güvenlik ve içerik filtreleme sağlarken kullanıcınızın ağ deneyimini denetlemenize olanak tanır. ADP, Fast Path adlı yüksek performanslı paket motorumuz için DNS şifrelemesini optimize eder. Böylece ağınızdaki şifreli DoT ve DoH bağlantılarını sonlandırabilirsiniz.



Şekil 1: Infoblox Gelişmiş DNS Koruması, DNS tabanlı saldırılara karşı benzersiz bir savunma sağlar.

TEMEL ÖZELLİKLER (DEVAMI)

Tek Arayüz Görünürlüğü Kazanın:
Infoblox ile, kuruluşunuz önceki veya mevcut DNS saldırılarını kolayca görüntüleyebilir ve hızlı tehdit iyileştirmemiz sayesinde operasyonel verimliliği artırabilir. Infoblox Gelişmiş DNS Koruması ayrıca ağdaki saldırı noktalarının ve saldırı kaynaklarının tek bir görünümü ile tehdit yönetimi için gerekli istihbaratı sağlar. DNS çözümümüz ile entegre edilmiştir.

Esnek Bir Şekilde Dağıtın:
Infoblox ile, sanal ve fiziksel Trinzic cihazlarına abonelik eklentisi olarak dağıtma seçeneğine sahipsiniz.

MÜŞTERİLERİMİZ NE DÜŞÜNÜYOR?

"DDoS saldırılarından kaynaklanan hizmet kesintileri yarıya indirildi ve uzun sayfa yükleme süreleriyle ilgili müşteri şikayetleri önemli ölçüde azaldı"

—VP of Customer Support, Large Service Provider

"Infoblox'u DNS, DHCP ve IP adresi yönetimi için dört yıldır kullanıyorum. Harika bir ürün. Ürün çok iyi çalıştığı için kaynakları başka yere taşıdık. Küresel ayak izimiz 1,5 FTE ile yönetiliyor ve bu da 65 cihaz anlamına geliyor."

—Küresel Altyapı Yöneticisi, Adobe

TABLO 1:
GELİŞMİŞ DNS KORUMASI (ADP) İLE ENGELLENEBİLEN SALDIRI TÜRLERİNİN ÖZETİ

Saldırı Adı	Tür	İşleyiş Şekli
DNS yansıması/DDoS saldırıları	Volumetrik	DoS veya DDoS saldırısını yaymak için üçüncü taraf DNS sunucular kullanma
DNS amplifikasyonu	Volumetrik	Kurbanı trafikle doldurmak için güçlendirilmiş bir yanıt oluşturmak üzere özel olarak hazırlanmış bir sorgu kullanma
TCP/UDP/ICMP floods	Volumetrik	Bir ağı veya hizmeti büyük miktarda trafikle doldurup çökmesini sağlayarak 3. katmanda hizmet reddi
NXDOMAIN	Volumetrik	DNS sunucusunun var olmayan alan adlarına yönelik isteklerle doldurulması, önbellek doygunluğuna ve yanıt süresinin yavaşlamasına neden olur
Random sub-domain (slow drip ataklar), alan lock-up saldırılar, hayalet alan saldırıları	Düşük hacimli gizlilik	DNS sunucusunu, saldırının bir parçası olarak kurulan hayali veya yanlış davranan alan adlarına yönelik taleplerle doldurarak kaynak tükenmesine, önbellek doygunluğuna, giden sorgu sınırının tükenmesine ve performansın düşmesine neden olmak
DNS tabanlı exploit ataklar	Exploits	DNS yazılımındaki güvenlik açıklarından yararlanan saldırılar
DNS önbellek zehirlenmesi	Exploits	Sahte bir adresle DNS önbellek verilerinin bozulması
Protokol anormallikleri	Exploits	Hatalı biçimlendirilmiş paketler ve sorgular göndererek sunucunun çökmesine neden olmak
Keşif	Exploits	Bilgisayar korsanlarının büyük bir DDoS veya başka tür bir saldırı başlatmadan önce ağ ortamı hakkında bilgi edinme girişimleri
DNS ele geçirme	Exploits	Sahte bir DNS sunucusuna yönlendirmek için alan adı kayıt bilgilerini geçersiz kılan saldırılar
Veri sızması (bilinen tünelleri kullanarak)	Exploits	Saldırı, güvenlik duvarı DNS dışı trafiği taşıyacak şekilde yapılandırılmışsa izin verilen DNS bağlantı noktası 53 üzerinden başka bir protokolün (veri sızıntısı amacıyla) tünellenmesini içerir

CİHAZ SEÇENEKLERİ

ADP Yazılımı: Fiziksel ve Sanal Platformlarda Kullanılabilir

ADP Yazılımı, Trinzic TE-815/825/1415/1425/ 2215/2225/4015/4025 cihazları için bir yazılım eklentisidir.

TE - 4015/4025

TE - 1415/1425

TE - 2215/2225

TE - 815/TE 825

Denemek için başlayın

Müşteriler için geçici lisansa sahip 60 günlük ücretsiz ADP yazılımı değerlendirmesi Hesap Yöneticileriniz/ SE'leriniz aracılığıyla sunulacaktır.

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