infoblox

ÖRNEK DURUM İNCELEMESİ

EMEA Merkezli İnternet ve İletişim Sağlayıcısı Okul Ağlarının Güvenliğini Infoblox ile Sağlıyor

MÜŞTERI: EMEA MERKEZLI İNTERNET VE İLETIŞIM SAĞLAYICISI

“Akademik kurumlar için internet güvenliğini sağlamaktan ve telekomünikasyon hizmetleri sunmaktan sorumlu EMEA merkezli bir internet ve iletişim sağlayıcısı, büyük ölçekli bir ulusal eğitim ağı kurmak için seçildi. Proje, 25.000 ilkokul ve ortaokulda 700.000 okul bilgisayarı kullanarak 4,5 milyon çocuğa güvenli internet bağlantısı sağlama temeline dayanıyor.”

ZORLUKLAR

Büyük Ölçekli Ağda Güvenli İnternet Erişimi Sağlamak

Telekom hizmet sağlayıcısı, özellikle kullanıcılar okul çocukları olduğu için ağ bağlantılarının ve kullanıcı deneyiminin yalnızca istikrarlı değil aynı zamanda güvenli olduğundan da emin olmak istiyordu. Buna ek olarak, bu çocukların uygunsuz web sitelerine girmelerini veya yanlışlıkla malware indirmelerini önlemeyi amaçladılar. Böylesine kapsamlı bir projede, içerik filtreleme için tek başına güvenli web ağ geçitlerinin (SWG’ler) uygulanması çok riskliydi. Daha önce hiç kimse SWG’lerin bu kadar büyük bir uygulamasını yapmamıştı. (Tahmini indirme trafiği 1Tbps’nin üzerindedir ve bu da başlıca SWG sağlayıcılarından yaklaşık 200 cihaz gerektirir). Bir şeylerin ters gitmesi durumunda, internet sağlayıcısı SWG’leri artırmanın bir yolu olmasını istiyordu. Ancak sağlayıcı SaaS tabanlı güvenlik çözümlerine güvenmek istemiyordu. Bunun yerine, kendi ağlarını, bulutunu ve veri merkezlerini inşa ettiği için güvenlik uygulamalarının şirket içinde olması gerekiyordu.

Sağlayıcının kurduğu devasa özel ağ, 25.000 okulun her biri için yönlendiricilerle 100 megabitlik bağlantılar gerektiriyordu. Proje üç aşamaya ayrıldı: bağlantıların teslimi, ağ ekipmanının teslimi ve güvenlik. Güvenlik iki aşamada gerçekleştirildi. İlkinde DNS uygulama dağıtım denetleyicileri (ADC’ler) ve güvenlik duvarları kullanılarak temel güvenlik sağlandı. İkincisi, web ağ geçitlerinin dağıtımını gerektirdi.

Müşteri: *Internet ve İletişim Sağlayıcısı*
Sektör: *Telekom Hizmet Sağlayıcıları*
Konum: *EMEA*

HEDEFLER:

- Büyük ölçekli eğitim sistemi için istikrarlı bir ağ oluşturmak
- Güvenli İnternet bağlantısı sağlamak
- Şirket içi çözüm uygulayın

SONUÇLAR:

- Güvenli ve temiz tarama deneyimi
- Kötü amaçlı yazılımları önleme
- DNS tabanlı içerik filtreleme
- Temel güvenlik hizmetleri
- Uygun maliyetli, ölçeklenebilir çözüm

ÜRÜNLER:

- NIOS DDI
- Tehdit İçgörüsü

ÇÖZÜM

Dahili Özel Ağda DNS Tabanlı Temel Güvenlik

Infoblox, okulun projesini değerlendirdi ve DNS tabanlı temel güvenliğin okul ağlarını korumak için ilk adım olarak düşünülmesini önerdi. SaaS sağlayıcıları da şirkete yaklaşmış olsa da, şirket okullar için kurduğu dahili özel ağ üzerinde dağıtılabilecek bir şey istediği için bunları hiç düşünmedi. Çoğu hizmet sağlayıcı kendi altyapısını kurar ve bu nedenle SaaS tabanlı bir hizmet kullanmaz.

Sağlayıcının diğer rakipleri yerine Infoblox'u seçmesine yol açan birkaç faktör daha vardı:

- Infoblox, Threat Insight gibi malware komutunu algılayabilen ve DNS sorgularında gizli trafiği kontrol edebilen **farklı laştırılmış işlevler** sundu. BU işlev ayrıca bazı öğrencilerin SWG güvenlik politikası sınırlamalarını atlamak için kullanabilecekleri yaygın bir yöntem olan DNS tünellerinin varlığını da algılayabilir.
- Sağlayıcı, Infoblox'un yerel teknik uzmanlığı sayesinde **daha iyi bir teknik ortak** olduğunu düşündü. Bu, diğer rakiplerin bölgede teknik uzmanları olmadığı için sunamadığı bir şeydi.
- Infoblox, Infoblox teknolojisini kullanan diğer birçok hizmet sağlayıcı ve benzer dağıtımların referanslarını sağladı.

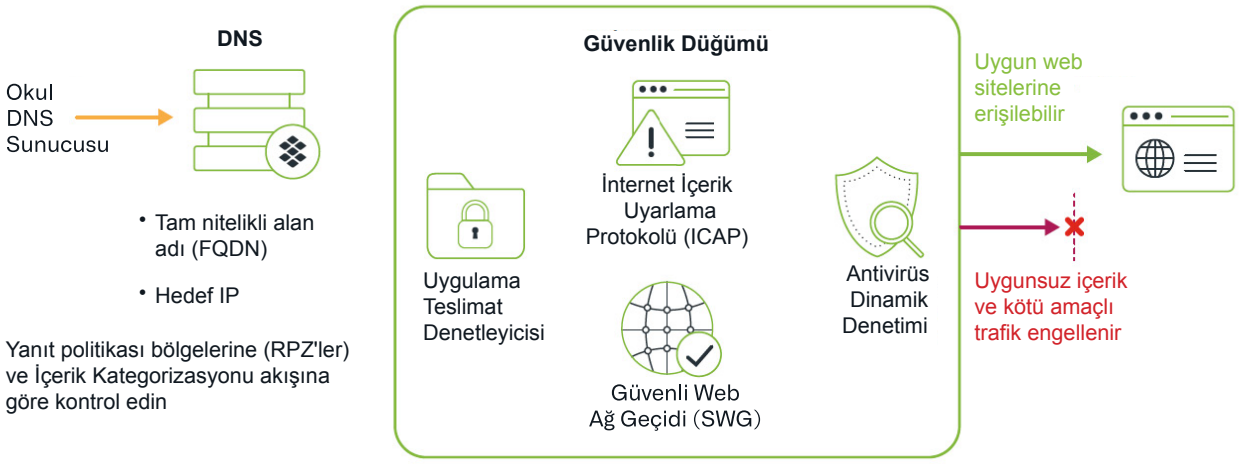
Tartışmalarının bir parçası olarak Infoblox, farklı malware örneklerini ve DNS'yi komut ve kontrol için nasıl kullandıklarını kapsayan derinlemesine bir güvenlik atölyesi düzenledi. Ek olarak, Infoblox ile yapılan temel bir malware önleme tartışması kısa sürede aşağıdakileri içeren daha geniş bir tartışma haline geldi:

- DNS kullanarak içerik kategorizasyonu, güvenli web ağ geçitlerinin performansını nasıl uygun maliyetli bir şekilde artırabilir?
- DNS düzeyinde trafik denetimi, SWG'ler için nasıl istikrarlı, ölçeklenebilir artırma sağlayabilir. Örneğin, Infoblox aracılığıyla, sağlayıcı artık DNS düzeyinde trafiği engelleyerek öğrencilerin yetişkin web siteleri gibi uygunsuz içeriklere erişmelerini önleyebilir. Daha belirsiz siteler, SWG'ler kullanılarak URL'lere göre filtrelenir (Şekil 1).
- Bu birleşik yaklaşım, SWG'lerin ele alması gereken kötü niyetli trafik miktarını nasıl sınırlar ve tehdit savunmasının toplam maliyetini nasıl düşürür?

SONUÇ

Anında Değer Sağlayan Kolay, İstikrarlı Bir Uygulama

İlk, sınırlı ölçekli dağıtım sırasında, bir Infoblox ortağı DNS çözümünü hizmet sağlayıcı konumlarından ikisi için sadece yedi gün içinde uyguladı. Bu dağıtım, Infoblox çözümünün **uygulanmasının kolay ve istikrarlı** olduğunu göstererek sağlayıcıya çözümün büyük ölçekli dağıtımlarda işe yarayacağına dair güven verdi. Kalan 16 konum için uygulama Haziran 2019 itibarıyla devam etmektedir. Sağlayıcı, DNS güvenlik duvarlarında merkezi güvenlik politikası yönetimi ve değerli bir güçlendirme ve boşaltma çözümü olduğu kanıtlanan Infoblox DNS sunucularındaki içerik filtreleme sayesinde ADC ve SWG'de trafik kontrolü ile ilgili geçici sorunların azaltılması gibi çeşitli avantajlar elde etti. Böylece sağlayıcı, Infoblox aracılığıyla **bölge genelindeki öğrenciler için güvenli, emniyetli ve sorunsuz bir gezinme deneyimi sunabildi.**



Şekil 1: Infoblox çözümü, içerik filtrelemede SWG'leri artırmak için DNS tabanlı içerik kategorizasyonu ve denetimi kullanır.

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: 20240304v1