Web Erişim Güvenliği

Güvenlik, Bağlantılı İstihbarat ve Verim için

Kuruluşlar bugün web üzerinden her zamankinden daha fazlasını yapabilir. Günümüz web siteleri dinamik, gerçek zamanlı bir kullanıcı deneyimi sunuyor. Bununla birlikte, web, her gün artan karmaşık saldırılarla daha tehlikeli bir yer haline geldi.

İnternet kullanımı ve gelişmişlik arttıkça, gelişmiş web güvenliği ihtiyacı da artıyor. Görünüşe göre "güvenli" siteler bile kötü amaçlı yazılım dağıtımı için hedeflenebilir. Günümüz dünyasında sadece bilinen virüsleri engellemek veya bilinen kötü web sitelerine erişimi kısıtlamak yeterli değildir. İmza tabanlı anti virüs ve yalnızca kategoriye özel URL filtreleme gibi reaktif teknikler, gerekli olsa da bulut uygulamalarına erişimi korumak veya günümüzün istismarlarıyla mücadele etmek için yetersizdir.

Bu çözümler bilinen içeriğe ve kötü amaçlı nesnelere veya yürütülebilir dosyalara odaklandığından, görünüşte güvenilir HTTP veya HTTPS trafiği içinde kötü amaçlı kodu gizleyen veya bilinmeyen veya ortaya çıkan tehditlere karşı koruma sağlayan günümüzün saldırılarını engelleyemezler. Bilinmeyen ve bilinen tehditleri proaktif olarak engellerken bulut uygulamalarına güvenli, ayrıntılı erişim sağlama yeteneği çok önemlidir.

BBS bu konuyla ilgili müşterilerinde geliştirdiği projelerinde McAfee® Web Gateway çözümünü kullanmayı tercih etmektedir. Bu çözümle herhangi bir kuruluşun ortaya çıkan kötü amaçlı yazılım tehditlerine karşı koruma sağlaması için kritik bir savunma oluşturmaktadır. Güçlü, yerel niyet analizini McAfee Labs tarafından desteklenen bulut tabanlı korumayla birleştiren gelişmiş bir güvenlik yaklaşımıyla riski büyük ölçüde azaltırken, kuruluşlara güvenli internet erişimi sağlar.

Kapsamlı Gelen ve Giden Internet Erişim Koruması

McAfee Web Gateway, tek bir yüksek performanslı cihaz yazılımı mimarisinde web trafiğinin tüm yönleri için kapsamlı güvenlik sağlar. Kullanıcı tarafından başlatılan web istekleri için, McAfee Web Gateway önce bir kuruluşun internet kullanım politikasını uygular. İzin verilen tüm trafik için, istenen web sayfaları aracılığıyla ağa giren tüm içeriğin ve aktif kodun yapısını ve amacını analiz etmek için yerel ve küresel teknikleri kullanır ve kötü amaçlı yazılımlara ve diğer gizli tehditlere karşı anında koruma sağlar. Ayrıca, temel paket inceleme tekniklerinden farklı olarak, McAfee Web Gateway, şifreleme yoluyla gizlenmiş kötü amaçlı kodlara veya kontrol uygulamalarına karşı derinlemesine koruma sağlamak için SSL trafiğini inceleyebilir.

McAfee Web Gateway Sektörün En İyi Korumasını Sağlıyor

McAfee Gateway Kötü Amaçlı Yazılımdan Koruma Motoru ile imzasız amaç analizine yönelik patentli bir yaklaşım kullanır. Proaktif niyet analizi ile gerçek zamanlı olarak web trafiğinden daha önce bilinmeyen veya sıfırıncı gün kötü amaçlı içeriği filtreler kullanılır. McAfee Web Gateway, bir web sayfasının etkin içeriğini tarayarak, davranışını taklit ederek ve anlayarak ve amacını tahmin ederek, sıfırıncı gün kötü amaçlı yazılımlarının uç noktalara teslim edilmesini önleyerek sistem temizleme ve iyileştirme ile ilgili maliyetleri önemli ölçüde azaltır.

Gelişmiş Tehdit Analizi Entegrasyonu

McAfee Web Gateway, özelleştirilebilir korumalı alanı derinlemesine statik kod analiziyle birleştiren gelişmiş kötü amaçlı yazılım algılama teknolojimiz olan McAfee Advanced Threat Defense ile entegre olur. McAfee Advanced Threat Defense ve McAfee Web Gateway'deki Gateway Anti-Malware Engine'in satır içi tarama yetenekleri, internet üzerinden iletilen tehditler için mevcut en güçlü korumayı sağlar. Daha düşük maliyetli, basitleştirilmiş gelişmiş tehdit analizi seçeneği isteyen kuruluşlar, birden fazla ek tehdit analizi katmanına sahip bulut tabanlı bir sanal alan olan McAfee Cloud Threat Detection'ı entegre edebilir.

Tehdit İstihbaratı Paylaşımı

Anahtar istihbaratın uç noktada, ağda, güvenlik bilgileri ve olay yönetimi (SIEM) çözümünde, ağ geçidinde ve daha fazlasında mevcut olmasına rağmen tehdit istihbaratını paylaşmak için oluşturulmamıştır. Bu zeka paylaşıldığında, tehditlere karşı daha iyi koruma, mevcut ihlallerin tespiti ve güvenliği ihlal edilen sistemlerin verimli bir şekilde düzeltilmesi yoluyla olay müdahalesinin iyileştirilmesi için kullanılabilir. McAfee

Threat Intelligence Exchange aracılığıyla, McAfee Web Gateway dahil olmak üzere

McAfee Web Gateway, şifreli trafik denetimine kapsamlı bir yaklaşım için kötü amaçlı yazılım algılama, SSL denetimi ve sertifika doğrulamasını bir araya getirir.

SSL trafiği incelemelerinde daha derine inmek için inisiyatif almak isteyen kuruluşlar, McAfee Web Gateway içindeki SSL kontrol aracılığıyla şifrelenmemiş trafik akışının tamamını veya tek tek akışları ilkeye göre inceleyebilir. Bu etkin özellik, şifresi çözülmüş SSL trafiğinin tam veya kısmi aynasının izinsiz giriş önleme sistemleri (IPS) veya ağ tabanlı veri kaybı önleme (DLP) çözümleri gibi ek güvenlik çözümlerine gönderilmesine olanak tanır.

Veri kaybı önleme

McAfee Web Gateway, SSL dahil tüm önemli web protokolleri üzerinden giden içeriği tarayarak, kuruluşları gizli bilgilerin sızması gibi tehditlerden korur. Bu, onu fikri mülkiyet kaybını önlemek, mevzuata uygunluğu sağlamak ve belgelemek ve bir ihlal durumunda adli verileri sağlamak için güçlü bir araç haline getirir.

Bulut tabanlı depolama kullanan kuruluşlar için yerleşik dosya şifreleme, dosya paylaşım/iş birliği sitelerine yüklenen verileri yetkisiz erişime karşı korur. Kullanıcılar, McAfee Web Gateway'den geçmeden verileri alamaz ve görüntüleyemez.

Ağ dışı kullanıcılar için koruma

İş gücü daha dağınık ve mobil hale geldikçe, ofisten yola sorunsuz bir şekilde geçiş yaparken web filtreleme ve koruma ihtiyacı giderek daha önemli hale geliyor. McAfee Client Proxy, dolaşımdaki kullanıcıların sorunsuz bir şekilde kimlik doğrulaması yapmasına ve askerden arındırılmış bir bölgede (DMZ) bulunan şirket içi McAfee Web Gateway'e veya McAfee Web Gateway Bulut Hizmetine yeniden yönlendirmesine olanak tanır. Bu, internet erişimleri bir kafe, otel veya başka bir Wi-Fi erişim noktası gibi halka açık bir portal üzerinden olsa bile, dolaşımdaki veya uzak konumdaki kullanıcılara internet erişim politikası zorlaması ve tam güvenlik taramasının uygulanmasını sağlar.

Kuruluşların güvenlik politikalarını mobil cihazlarda genişletmesine ve uygulamasına da olanak tanır. Mobil cihaz yönetimi sağlayıcıları AirWatch ve MobileIron ile yaptığımız ortaklıklar aracılığıyla McAfee Web Gateway, Apple iOS ve Google Android mobil cihazlarının gelişmiş kötü amaçlı yazılımdan koruma ve kurumsal web filtreleme politikalarıyla güvenliğini sağlar.

McAfee Web Gateway ile Üstün Esneklik

McAfee Web Gateway, denetimi bulut uygulamalarına genişleterek web uygulamalarının nasıl kullanıldığı üzerinde ayrıntılı, proxy tabanlı denetim sağlar. Kuruluşlar, gerektiğinde belirli işlevleri etkinleştirerek veya devre dışı bırakarak, bir web uygulamasını kimin kullandığını ve nasıl kullanıldığını denetleyerek bulut uygulamalarına binlerce denetim uygulayabilir. Dropbox sistemine erişimi etkinleştirmek istiyor ancak yüklemelere izin vermiyor musunuz? Sorun yok.

Esneklik ve kontrol, kullanıcı kimlik doğrulamasını ve erişimini de kapsar. McAfee Web Gateway, NT LAN yöneticisi (NTLM), kullanıcı hizmetinde uzaktan kimlik doğrulama araması (RADIUS), Active Directory (AD)/hafif dizin erişim protokolü (LDAP), eDirectory, tanımlama bilgisi kimlik doğrulaması, Kerberos veya yerel kullanıcı veri tabanı McAfee Web Ağ Geçidi kimlik doğrulama motoru, yöneticilerin birden çok kimlik doğrulama yönteminin kullanımı da dahil olmak üzere esnek kurallar uygulamasına olanak tanır. Örneğin, McAfee Web Ağ Geçidi bir kullanıcının kimliğini şeffaf bir şekilde doğrulamayı deneyebilir ve sonuca göre kullanıcıdan kimlik bilgilerini isteyebilir, başka bir kimlik doğrulama yöntemi kullanabilir, kısıtlayıcı bir ilke uygulayabilir veya yalnızca erişimi reddedebilir.

McAfee Web Gateway Identity, yüzlerce popüler bulut tabanlı uygulama için çoklu oturum açma (SSO) bağlayıcıları içerir. McAfee Web Gateway Identity, kullanıcıların tek tıklamayla yetkili bulut uygulamalarına erişebildiği bir SSO başlatma paneli kullanarak güvenliği artırma ve parolayla ilgili yardım masası çağrılarını azaltma yeteneği sağlar. Hem HTTP açılışta kendi kendine sınama (POST) hem de güvenlik onayı biçimlendirme dili (SAML) bağlayıcıları için destek, çok çeşitli uygulamalar için kapsam sağlar. Sağlama bağlayıcıları, sistem yöneticilerinin belirli Hizmet Olarak Yazılım (SaaS) uygulamalarında kullanıcı hesapları oluşturmasına ve sonlandırmasına olanak tanır.

McAfee Web Gateway, yerel akış proxy desteği aracılığıyla da erişim kontrolünü akış içeriğine genişleterek bant genişliği tasarrufu sağlar ve gecikme süresini azaltır. Tanımlanmış trafik sınıfları için minimumları, maksimumları ve önceliklendirmeyi zorlamak için ek bant genişliği kontrolleri ayarlanabilir ve kuruluşların mevcut bant genişliğinin kullanımını optimize etmesine olanak tanır.

McAfee Web Gateway ile Çevik Altyapı ve Performans

Bütünleşmiş yüksek kullanılabilirlik, sanallaştırma seçenekleri ve McAfee Web Ağ Geçidi Bulut Hizmeti ile hibrit dağıtım ile ölçeklenebilir bir cihaz modelleri ailesinde sunulan yüksek performanslı, kurumsal düzeyde bir proxy olacaktır. McAfee Web Gateway, tek bir ortamda yüz binlerce kullanıcıyı desteklemek için ölçeklenebilirliğin yanı sıra dağıtım esnekliği ve performansı sunar.

Dağıtım seçeneklerini de karıştırabilirsiniz. Örneğin, ağdaki kullanıcılar için tüm web trafiğini şirket içi cihaza yönlendirebilir ve tüm ağ dışı kullanıcıları bulut hizmetine yönlendirerek, trafiği çok protokollü etiket değiştirme (MPLS) hatları veya sanal üzerinden geri taşıma maliyetini önemli ölçüde azaltabilirsiniz. özel ağ (VPN). Hibrit şirket içi ve bulut dağıtımları için otomatikleştirilmiş ilke senkronizasyonu ve raporlama, yönetimi kolaylaştırmaya, tutarlı ilke uygulamasını sağlamaya ve raporlama, izleme ve araştırmayı basitleştirmeye yardımcı olur.

McAfee Web Gateway, ağ mimarinizin desteklendiğinden emin olmak için açık proxy sunucudan şeffaf köprü ve yönlendirici modlarına kadar çok sayıda uygulama seçeneği sunar.

Çok sayıda entegrasyon standardını destekleyen McAfee Web Gateway, benzersiz ortamınızda çalışmak üzere tasarlanmıştır. Web önbellek iletişim protokolünden (WCCP), internet içeriği uyarlama protokolünden (ICAP/ICAPS) ve WebSocket protokolünden güvenli yuva (SOCKS) protokolüne kadar, McAfee Web Gateway diğer ağ cihazları ve güvenlik cihazlarıyla verimli bir şekilde iletişim kurar.

Ek olarak, McAfee Web Gateway IPv6 desteği sunarak daha büyük kuruluşların ve federal kurumların düzenlemelere uymasına yardımcı olur. McAfee Web Gateway, dahili IPv4 ve harici IPv6 ağları arasındaki boşluğu doldurur ve mevcut tüm güvenlik ve altyapı özelliklerini ve işlevlerini trafiğe uygular.

Güvenlik Risk Yönetimi ve Raporlama

Popüler ve saygın güvenlik yönetimi teknolojisi McAfee ePolicy Orchestrator ® (McAfee ePO ™) yazılımı, tüm güvenlik raporlamaları için tek bir kaynak olarak McAfee Web Gateway tarafından desteklenir.

McAfee ePO yazılımı, McAfee Content Security Reporter uzantısı aracılığıyla ayrıntılı web güvenliği raporlaması sağlar. McAfee Content Security Reporter, kuruluşunuzun Web sistemini nasıl kullandığını anlamanız, düzenlemelere uymanız, eğilimleri belirlemeniz, sorunları yalıtmanız ve web güvenlik ilkelerinizi uygulamak için filtreleme ayarlarınızı uyarlamanız için size bilgi ve adli araçlar sağlar. McAfee Content Security Reporter, mevcut McAfee ePO sunucusundan kaynak yoğun veri işleme ve depolama yükünü boşaltmak için tasarlanmış harici, bağımsız bir raporlama sunucusu sunarak, en büyük küresel kuruluşların bile raporlama ihtiyaçlarını karşılayacak şekilde ölçeklenmesini sağlar.

Bilgi Birikim Sistemleri, müşteriye “doğru çözüm” sunmanın en büyük değer olduğuna inanır. Belirlenen proje bütçesine sadık kalmayı ve zamanında teslim etmeyi amaçlayarak bu alanda yıllardır hizmet vermektedir. Bu kapsamda yetkin ve deneyimli personeli ile birçok başarılı projeler gerçekleştirmiştir. Yaptığımız işleri tanıtma ve size de doğru çözümü sunmamız için lütfen izin verin size ulaşalım.

İlginizi çekebileceğini düşündüğümüz ağ güvenliği ile ilgili diğer konular için lütfen web sitemizi ziyaret ediniz.

- Ağ Erişim Kontrolü (NAC)
- Saldırı Tespit ve Önleme Sistemi (IPS)
- Yeni Nesil Güvenlik Duvarı
- Firewall-Ağ Yapılandırma ve Değişim Kontrolü
- APT Güvenliği (Sandbox)
- Web Uygulama Güvenlik Duvarı
- DNS Güvenliği
- E-Posta Güvenliği
- Ağ Davranış Tabanlı Algılama Sistemi (NDR)