ÇÖZÜM BRIEF'I

McAfee™
Together is power.

Logonuzun **burada görünmesini** ister misiniz?
iletisim@banasorun.net

Web Gateway için İleri Tehdit Savunma Analizi

Gizli yazılımları ağ sınırında durdurun

Sosyal ağlar, bulut uygulamaları, bloglar, wiki'ler, RSS akışları, ve içerik paylaşım siteleri kurumsal kullanıcılar için vazgeçilmez iş araçları haline gelmiştir - ve IT organizasyonları bu araçlara sağlanan kurum içi ve kurum dışı erişimi güvenli hale getirmek için çaba harcamaktadırlar. Secure Web Gateway bu çabanın önemli bir kilometre taşı olan ve gizli tehditleri bulup engellemek için gelen ve giden trafiği tarayan bir trafik denetleme çözümüdür. Ne yazık ki siber suçlularda giderek büyüyen kurumsal web trafik hacmini suistimal edebilmek için bir o kadar çok çalışmaktadırlar ve yaptıkları saldırılar her zamankinden daha sinsi, akıllıca, hedef odaklı ve maliyetli hale gelmiştir. Saldırılar kaçınılmaz olarak geleneksel gateway savunmalarından sızmaktadır.

Önemli avantajları

- McAfee® Web Gateway analizinden sonra şüpheli bulunan dosyalar, mümkün olan en ileri düzey denetim için otomatik olarak **McAfee Advanced Threat Defense**'e gönderilir.
- Derin statik kod analizi web güvenliğine eklenmiştir, gateway üzerinde ek iş yükü oluşturmamaktadır.
- Tak-çalıştır tehdit engelleme, insan müdahalesinin getirdiği gecikme olmaksızın anında devreye girer.
- Tek merkezli **sandbox** servisi, eş-zamanlı olarak diğer ağ ve uç nokta güvenlik sistemlerini destekler.
- Analiz esnasında dosyalar zaptedilerek kullanıcılarda sıfırıncı vaka engellenir.
- Analiz sonuçları otomatik olarak McAfee Web Gateway iş akışlarına entegre edilir.
- Esnek kurulum seçenekleri fiziksel, sanal ve bulut platformları destekler.

Sıkıca Entegre Edilmiş Web Gateway ve Sandbox Çözümü

McAfee, **McAfee® Web Protection** (on-premise McAfee Web Gateway ve Web Gateway Cloud Service) ve **McAfee ileri tehdit analiz çözümleri** (on-premise McAfee Advanced Threat Defense ve McAfee Cloud Threat Detection) entegrasyonu olan bir çözüm sunmaktadır. McAfee Web Gateway ve ileri tehdit analiz çözümleri için sunulan esnek kurulum seçenekleri fiziksel, sanal ve bulut ağlarının tamamını desteklemektedir.

McAfee Web Gateway, in-band trafik denetlemesi ve gerçek zamanlı çalışma için optimize edilmiş bir dizi zararlı zararlı yazılım tespit teknolojileri ile tehdit savunması sağlamaktadır. **McAfee ileri tehdit analiz** çözümleri, gelişmiş zararlı yazılım tespit teknikleriyle denetimi genişletmektedir. Sandbox becerilerini geliştiren ve yüksek kamuflajlı tehditler için, tespiti kolaylaştıran derin statik kod analizi ve makine öğrenimi, bu tekniklere bazılarıdır. Sağlanan sıkı entegrasyon sayesinde, ileri düzey tehditlerin tespit edilmesiyle etkisiz hale getirilmesi arasında geçen süre azaltılır, etkin bir uyarı mekaniği ile politika uygulamalarının devamlılığı sağlanır. **McAfee ileri analiz çözümleri** ve **McAfee Web Gateway** bünyesinde bulunan **Gateway Anti-Malware Engine**'in in-line tarama becerileri, internet tabanlı tehditlere karşı mevcut olan en güçlü korumayı sağlar.

Bütünsel uçtan uca çözüm için **McAfee Endpoint Protection**, **McAfee Threat Intelligence Exchange** ve **McAfee Active Response** ürünlerini ekleyin. Böylece güvenlik operasyon yanıtlarını ve verimliliğini hem görünürlük ile, hem de yeni konfigürasyonlar oluşturma, yeni politikalar uygulama, dosya silme ve proaktif şekilde risk azaltabilecek yazılım güncellemeleri yayınlama gibi aksiyonlarla optimize edebilirsiniz.

Bu uçtan uca çözümleri sıkı şekilde entegre ederek, sektörde eşsiz konumda bulunan operasyonel ve defansif avantajları elde edebilirsiniz.

Bu avantajlardan bazıları:

- **Tak çalıştır tehdit engelleme:** McAfee **ileri analiz çözümleri** tarafından tespit edilen saldırılar, insan müdahalesinin getirdiği gecikme olmaksızın McAfee Web Gateway tarafından otomatik olarak engellenir.
- **Merkezleştirilmiş sandbox hizmeti:** McAfee Advanced Threat Defense, ihlal engelleyici sistemler ve endpoint'ler dahil çalışan diğer ağ güvenliği sistemlerini de eş zamanlı olarak destekleyebilir. Böylece maliyetleri düşürebilir, güvenlik mimarisini daha basit hale getirebilir, ve yeni saldırı tespiti ile ağ genelinde engel sağlama arasındaki yanıt süresini azaltabilirsiniz
- **Hiper etkili tarama işlevi:** McAfee Web Gateway araçları ilk filtreleme ve zararlı yazılım analizi işlemlerini gerçekleştirir ve yalnızca gateway analizinden geçemeyen veya tanımlanamayan içerikleri sandbox'a yönlendirir.
- **Rapor ve iş akışı entegrasyonu:** McAfee ileri analiz çözümleri tarafından oluşturulan sonuçlar otomatik olarak McAfee Web Gateway iş akışlarına entegre edilir ve geri bildirim ve tarama sonuçları kullanıcılara sunulur.

- **Web-Only kurulum**

  - McAfee ePO™ Cloud ile tek konsoldan yönetim: McAfee bulut tabanlı yönetim platformu, hem web gateway hem de ileri analiz için tek bir kontrol paneli sunar.

  - Network dışı koruma: McAfee Endpoint Protection dahildir. Off-network endpoint trafiği McAfee Web Gateway koruması, politika uygulaması ve ileri analiz için kolayca buluta yönlendirilir.

  - Alt ağ trafiği yükünden kaçınma: Merkezi bir lokasyona veri yığmak yerine, tüm ortak internet trafiğini politika uygulaması ve analiz için buluta yönlendirerek ağ maliyetlerini düşürün.

McAfee Web Gateway

McAfee Web Gateway, evrim geçiren web kaynaklı tehditlere karşı bir şirketin ana savunma hattını oluşturmaktadır. Bir şirketin, web uygulamalarına ve kaynaklara esnek ve politika tabanlı kullanıcı erişimi sağlamasına olanak tanırken, dahili sistemlerin ve bilgilerin maruz kaldığı riski önemli ölçüde azaltır.

McAfee Web Gateway tüm web trafiğinin doğasını ve amacını gerçek zamanlı olarak tanımlayabilmek için tüm kullanıcı kaynaklı web istemleri üzerinde önce dahili bir erişim politikası, daha sonra da bir dizi lokal ve global denetim tekniği uygulayan bir proxy platformudur. Tespit analizi içeriğinde imza tabanlı antivirüs, itibar dosya ve kaynağı, kategorizasyon ve McAfee Global Threat Intelligence (McAfee GTI) tarafından sağlanan jeolokasyon bilgisi bulunmaktadır. Son olarak McAfee Web Gateway sıfırıncı gün zararlı yazılım önleme konusunda, dosya ve aktif web içeriğinin (HTML, JavaScript) davranışlarını öngörmek için makine öğrenimi zekası ve emülasyonu kullanan patentli proaktif bir yaklaşım uygulamaktadır. SSL şifreli içerikler dahi gizlenmiş saldırı ihtimaline karşı dekode edilmekte ve denetime tabi tutulmaktadır. Sonuç olarak, son derece yüksek yakalama oranı ve saldırıları gateway sınırında tamamen durduran anlık, öngörülü bir engelleme sistemi elde edilmektedir. Bağımsız testler, sıfır günlük zararlı yazılımların %95 ila %99'unun McAfee Web Gateway tarafından tanımlanıp engellendiğini onaylamıştır.

Iyi niyetli kullanıcı hatası veya bot bulaşmış bir host aracılığı ile gizlenmiş bir aksiyon nedeniyle gizli bilgilerin kaybolmasını önlemek için McAfee Web Gateway ayrıca, kullanıcılar tarafından oluşturulan içerikleri tüm önemli web protokolleri genelinde (HTTP, HTTPS ve FTP) tarayarak giden trafiği güvenlik altına alır. Veri kaybı önleme (DLP) politikaları için entegre destek sistemi, regüle edilen veya hassas olan verileri sızmalara karşı korur. Uygulama kontrolleri ise Box, Dropbox ve benzeri bulut dosya paylaşımı ve ortak çalışma siteleri için risk azaltımı sağlar.

McAfee Web Gateway'in sahip olduğu en güçlü özellik, diğer McAfee güvenlik çözümlerinin sağladığı bilgi ve becerilere erişim sağlayan entegrasyondur. Bu çözüme dair önemli bir nokta, aşağıdakiler ile sağlanan kusursuz entegrasyondur:

- Dünya genelinde 120 ülkede 100 milyondan fazla endpoint'ten gelen URL repütasyonlarını ve diğer dataları toplayan, analiz eden ve dağıtan, ve böylece zararlı yazılım içeren siteler hakkında dakika dakika güncel veri sağlayan **McAfee Global Threat Intelligence,** McAfee Web Gateway korumasını genişletir.

- **McAfee Threat Intelligence Exchange,** bilgi paylaşımı için güvenlik çözümleri sağlayarak korumayı güçlendirir ve olay yanıt sürelerini azaltır. McAfee Web Protection tarafından sağlanan tehdit bilgileri sayesinde, sıfır günlük bir tehdit keşfedildiği anda uç noktalar koruma altına alınır. Kaynak/hedef IP, dosya hash'leri ve URL gibi bağlamsal olay yanıt bilgileri, güvenlik bilgileri ve event yönetim (SIEM) çözümleri ile paylaşılır. McAfee Threat Intelligence Exchange yoluyla diğer kaynaklardan alınan bilgiler sayesinde McAfee Web Protection kendi koruma becerilerini geliştirebilmektedir.

- **McAfee Endpoint Security,** trafiği network dahilinde iken bir McAfee Web Gateway aracına, network dışında ise bulut tabanlı McAfee Web Gateway'e kolayca ve akıllıca yönlendirerek politika uygulaması ve analiz sağlar.

- Bu çözümün gelişmiş zararlı yazılım tespit bileşeni olan **McAfee Advanced Threat Defense**, Gateway Anti-Malware Engine tarafından yürütülen analiz sonucunda şüpheli bulunan dosyaları otomatik olarak teslim alır ve böylece azami tehdit tespit becerisi sağlanır.

Sandbox: McAfee Gelişmiş Tehdit Analiz Çözümleri

McAfee tarafından sunulan ileri tehdit tespit çözümleri, karmaşık zararlı yazılımları tanımlar ve tehdit bilgilerini aksiyona ve korumaya dönüştürür. Bu çözümler, gelişmiş malware tespit teknikleri ile denetim kapsamını genişleterek mevcut güvenlik yatırımlarını optimize etmektedir. Sandbox becerilerini geliştiren ve yüksek kamuflajlı tehditlerin tespitini kolaylaştıran derin statik kod analizi ve makine öğrenimi, bu tekniklere dahildir.

İleri tehdit tespit çözümlerimiz ve diğer McAfee ürünleri arasındaki sıkı entegrasyon, maliyetleri düşürür ve tespit ile düzeltme arasındaki süreyi azaltarak zararlı yazılım tanımlamalarını korumaya dönüştürür ve benzer saldırıları engeller. Esnek kurulum seçenekleri fiziksel, sanal ve bulut üzerindeki tüm ağları desteklemektedir.

Mcafee Advanced Threat Defense

Karmaşık yazılımları tespit edin ve koruma ile incelemeye dair iş akışlarını otomasyonlu hale getirerek saldırı sonrası düzeltim ve iyileşme sağlayın. McAfee Advanced Threat Defense, gizlenmiş tehditleri tespit etmek için davranışsal zararlı yazılım analizini genişleten derin statik kod analizi ve sandbox becerileri sunmaktadır. Bu eşsiz analiz hem bir saldırının kapsamını anlamanıza yardımcı olmak için özet raporlar sunar, hem de zararlı yazılımlarla ilgili analist düzeyinde verilerle aksiyonları ve yüksek detaylı raporları önceliklendirir.

McAfee Cloud Threat Detection

Bu etkin bulut hizmeti, mevcut McAfee çözümlerinize entegre olarak ileri düzey zararlı yazılımları tanımlar ve korumayı otomatikleştirir. Bulut tabanlı bir çözümün sunduğu kolaylıklar sayesinde, ciddi bir bilgisayar işlem gücünden faydalanabilir, en yeni analiz tekniklerini işleme koyabilir, tespit becerilerini genişletebilir ve mevcut güvenlik yatırımlarını optimize edebilirsiniz.

Gelişmiş, Kapalı Devre Tehdit Önleme Çözüm

McAfee Web Gateway ve McAfee ileri tehdit analiz çözümleri kombinasyonu, web kaynaklı ileri düzey zararlı yazılımlara karşı son derece etkili koruma sağlar. Bu otomasyonlu kapalı devre çözüm, yoğun çalışan IT personellerinin elle müdahalesine ihtiyaç duymaksızın karmaşık saldırıları bulur, bulundukları yerde onları dondurur ve etkilenen host sistemleri onarır