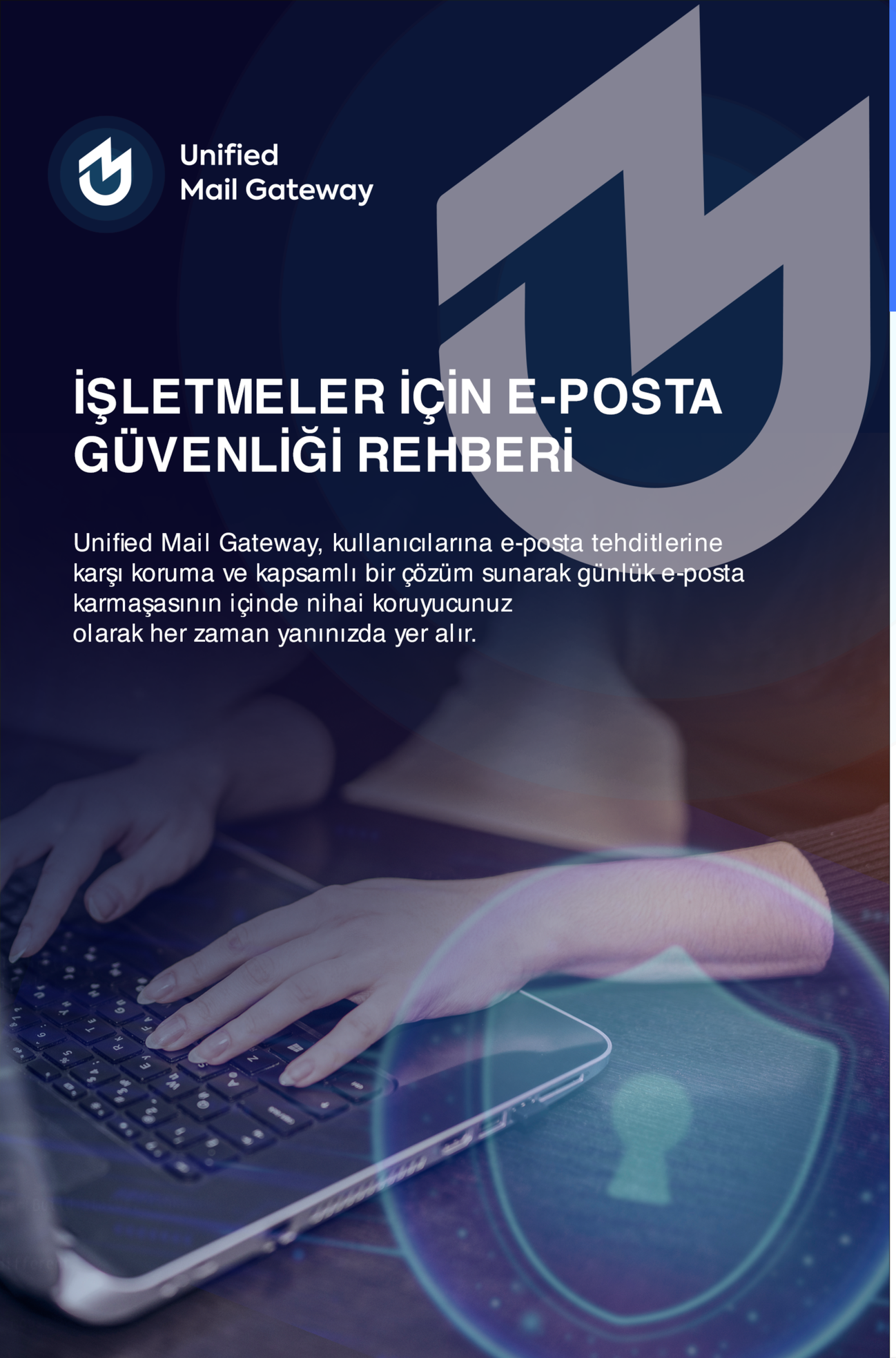
Unified
Mail Gateway

İŞLETMELER İÇİN E-POSTA GÜVENLİĞİ REHBERİ

Unified Mail Gateway, kullanıcılarına e-posta tehditlerine karşı koruma ve kapsamlı bir çözüm sunarak günlük e-posta karmaşasının içinde nihai koruyucunuz olarak her zaman yanınızda yer alır.



İÇERİKLER

E-posta Filtreleme Nedir? Nasıl Çalışır?

E-posta Filtreleme Nedir? Neden Önemlidir?

E-posta Filtreleme Nasıl Çalışır?

İşletmeler Neden E-posta Filtrelemeye İhtiyaç Duyar? Avantajları Nelerdir?

Yaygın E-posta Tehdit Türleri Nelerdir?

E-posta Filtreleme Yöntemleri Nelerdir?

Inbound ve Outbound Filtreleme Hakkında Bilmeniz Gerekenler

E-posta Filtreleme için Farklı Dağıtım Türleri Nelerdir?

Etkili E-posta Filtreleme için İpuçları

Üstün Koruma için Unified Mail Gateway'in E-posta Filtreleme Hizmetini Keşfedin

E-posta Filtreleme Nedir? Nasıl Çalışır?

Statista'ya göre, 2022 yılında günde tahmini 333.2 milyar e-posta gönderildi ve dünya çapındaki tüm e-posta'ların yaklaşık %49'u spam olarak tanımlandı.

Email Tool Tester tarafından 2022 yılında yapılan bir çalışmaya göre ise, tüm e-posta'ların sadece %15,8'i popüler spam filtreleri tarafından yakalandı.

Yapılan araştırmalardan da anlayacağınız gibi, gelen kutunuz her gün istenmeyen binlerce e-posta ile karşı karşıya… Bu yüzden işletmenizi ve kendinizi riske atmamak için kötü niyetli e-posta'lara karşı koruma sağlamanız gerekiyor.

Peki gelen kutunuzu istenmeyen e-posta'lardan korumak için ne yapmanız gerekli?

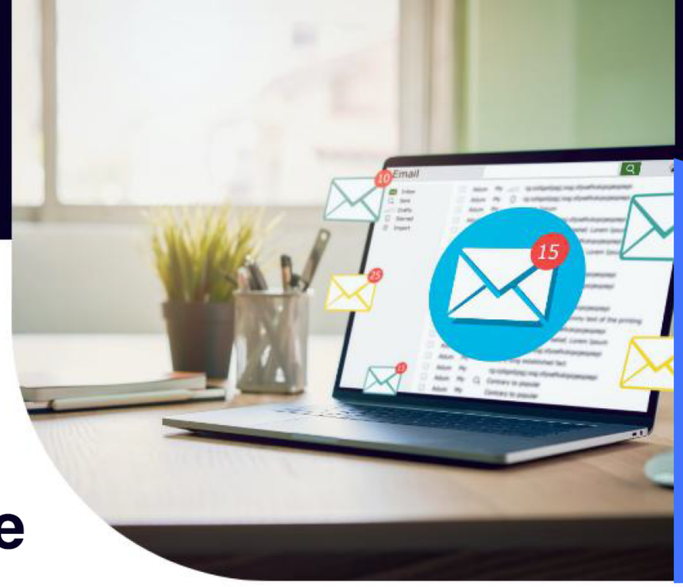
Tam da bu noktada e-posta güvenliğinizi üst düzeye çıkarmanızı için Unified Mail Gateway devreye girer. Unified Mail Gateway, kullanıcılarına e-posta tehditlerine karşı koruma ve kapsamlı bir çözüm sunarak günlük e-posta karmaşasının içinde nihai koruyucunuz olarak her zaman yanınızda yer alır.

E-posta Filtreleme Nedir? Neden Önemlidir?

E-posta iletişiminde yapılan tek bir kullanıcı hatası, hassas verilerin tehlikeye girmesine ve tüm ağınızın çökmesine neden olabilir. Bu noktada e-posta filtreleme, bu tehditlerle etkili bir şekilde mücadele eder ve spam ve kötü niyetli e-posta'ları ortadan kaldırma gibi amaçlara hizmet eder.

İşletmeleri ve bireyleri korur, zamandan tasarruf sağlar ve potansiyel güvenlik ihlallerine karşı son savunma hattı olarak hareket ederek temel bir güvenlik yüzeyi oluşturur. Ayrıca, gelen e-posta'ların ötesine geçerek spam benzeri davranışları tespit eder ve spam'ın e-posta sunucusunun IP adresinden çıkmasını engelleyen giden filtrelemeyi de kapsar.

Unified Mail Gateway



E-posta Filtreleme Nasıl Çalışır?

E-posta filtreleri, gelen e-posta'ları spam veya kimlik avı gibi siber tehlikelere karşı korur. Bu filtreler içeriği, gönderen ayrıntılarını ve tasarım öğelerini analiz ederek bir e-posta'nın gelen kutusuna mı teslim edileceğini yoksa "Spam" veya "Önemsiz" gibi alternatif klasörlere mi yönlendirileceğini belirler. E-posta, filtrenin belirlenen kriterlerini karşılıyorsa, alıcının gelen kutusuna teslim edilir.

Anahtar kelime analizi, gönderici itibar kontrolleri ve kimlik avı tespit teknikleri sayesinde kullanıcılar e-posta hesaplarını istenmeyen veya kötü niyetli içerikten etkili bir şekilde koruyabilir. Alıcıları hassas bilgileri ifşa etmeleri veya kötü amaçlı yazılım indirmeleri için kandırmayı amaçlayan oltalama e-posta'ları söz konusu olduğunda, ek filtreleme önlemleri devreye girer. Kimlik avı filtreleri, kötü amaçlı içerik içerebilecek şüpheli bağlantıları veya ekli belgeleri tespit eder.

Sonuç olarak, e-posta filtreleri bu teknikleri kullanarak meşru e-posta'lar ile spam veya kimlik avı girişimlerini etkili bir şekilde ayırt edebilir. Böylece kullanıcıların e-posta iletişimlerini daha verimli ve güvenli bir şekilde yönetmelerine yardımcı olur.

Tam da bu noktada Unified Mail Gateway'in gelen ve giden e-posta filtrelemesi, sağlam algoritmaları ve güçlü filtreleriyle, günlük e-posta karmaşasının içinde nihai koruyucunuz olarak her zaman yanınızda yer alır.

İşletmeler Neden E-posta Filtrelemeye İhtiyaç Duyar? Avantajları Nelerdir?

Getastra'nın 2023 Kimlik Avı Saldırısı İstatistiklerine göre, gönderilen e-posta'ların yaklaşık **%1,2**'si kötü niyetlidir ve bu da günlük **3,4 milyar** kimlik avı e-posta'sına denk gelir. Veriler ayrıca 2023 yılında **33** milyondan fazla kaydın fidye yazılımı veya kimlik avı saldırıları nedeniyle tehlikeye gireceğini öngörmektedir. Bu rakamlar, her 11 saniyede bir meydana gelen yüksek bir siber saldırı sıklığına işaret etmektedir.

Earthweb'e göre ise, siber saldırıların yaklaşık **%94**'ü e-posta'lar aracılığıyla gerçekleştirilir.

Tüm bu araştırmalar işletmelere e-posta filtrelemenin, güvenli ve verimli bir iletişim ortamı sağlamak için ne kadar önemli olduğunu gösterir.

Peki e-posta filtrelemenin avantajları nelerdir?

%1,2
Kötü Niyetli

33M
Kimlik avı e-postası

Unified Mail Gateway

İşletmeler Neden E-posta Filtrelemeye İhtiyaç Duyar? Avantajları Nelerdir?

01

Spam'ı Engeller

E-posta filtreleri spam mesajları etkin bir şekilde tespit edip ortadan kaldırarak kullanıcıların gelen kutularındaki karmaşayı önemli ölçüde azaltır. Sadece üretkenliği artırmakla kalmaz, aynı zamanda önemli e-posta'ları bulma sürecini de kolaylaştırır ve sonuçta değerli zaman tasarrufu sağlar.

02

DDoS Saldırı Riskini En Aza İndirir

E-posta filtreleri, bu tür siber saldırılarla ilişkili olabilecek şüpheli veya kötü niyetli e-posta trafiğini engelleyerek Dağıtılmış Hizmet Reddi (DDoS) saldırı riskini azaltmaya yardımcı olabilir. Bu önlemlerin uygulanması, e-posta sunucusunu korur ve kesintisiz e-posta iletişimi sağlar.

03

Graymail'i En Aza İndirir

E-posta filtreleri spam ve önemli e-posta'ları birbirinden ayırabilir. Ek olarak, spam olmayan ancak önemli de olmayan e-posta'ları ifade eden graymail'i tanımlar. Graymail'i en aza indiren bu filtreler, kullanıcıların öncelikli olarak ilgili ve önemli e-posta'lara odaklanmasını sağlar.

04

Geliştirilmiş Üretkenlik Sağlar

E-posta filtreleri, gelen kutusu karmaşasını azaltarak ve e-posta'ları etkili bir şekilde düzenleyerek üretkenliği artırır. Önemli e-posta'lara öncelik verir ve onları daha az önemli olanlardan ayırır. Bu sayede kullanıcılar gelen kutularını verimli bir şekilde yönetebilir ve zamandan tasarruf sağlayabilir.

05

Çevrimiçi Tehditlere Karşı Koruma Sunar

E-posta filtreleri, işletmeleri kimlik avı saldırıları ve kötü amaçlı yazılımlar da dahil olmak üzere çeşitli çevrimiçi tehditlerden korumada hayati bir rol oynar. Şüpheli e-posta'ları belirleyebilir, kötü amaçlı ekleri engelleyebilir ve kullanıcıların dolandırıcılık kurbanı olmasını veya yanlışlıkla kötü amaçlı yazılım indirmesini önleyebilir.

06

Bant Genişliği Tasarrufu Sağlar

E-posta filtreleri spam ve diğer istenmeyen e-posta'ların kullanıcının gelen kutusuna ulaşmasını engelleyerek önemli ölçüde bant genişliği tasarrufu sağlar. Bant genişliği tasarrufu özellikle sınırlı bant genişliği kaynaklarına sahip işletmeler için avantajlıdır. Değerli ağ kapasitesinin istenmeyen e-posta trafiği için harcanmamasını sağlar.

07

Sabit Disk Alanı Tasarrufu Sağlar

E-posta filtreleri, spam ve diğer istenmeyen e-posta'ları kullanıcının posta kutusuna ulaşmadan önce engelleyerek sabit disk alanından tasarruf edilmesine yardımcı olur. Alan tasarrufu, mevcut kaynakları mümkün olduğunca etkili bir şekilde kullanmalarını sağladığından, özellikle sınırlı depolama kapasitesine sahip birey ve işletmeler için avantajlıdır.

08

Kötü Amaçlı Bağlantı veya Eklere Tıklama Riskini Azaltır

E-posta filtreleri kötü niyetli bağlantıları veya ekleri tespit edip engelleyerek proaktif bir savunma mekanizması görevi görür ve kullanıcıları olası güvenlik ihlal ve siber saldırılara karşı korur.

Unified
Mail Gateway

Yaygın E-posta Tehdit Türleri Nelerdir?

E-posta tehditleri genellikle hassas bilgileri çalmak, kötü amaçlı yazılım yaymak, fidye yazılımı yoluyla şantaj yapmak, BEC dolandırıcılığı yapmak veya veri sızdırmak için aldatıcı e-posta'lar yoluyla iletilir. Bu yaygın e-posta tehdidi türlerini tespit etmek ve tanımak çok önemlidir, çünkü hemen tespit edilip azaltılmazlarsa, işletmenize önemli zararlar verebilir.

En yaygın e-posta tehdit türleri aşağıdaki şekildedir:

Kimlik Avı: Kimlik avı e-posta'ları alıcıları kandırarak parolalar, kredi kartı bilgileri veya kişisel veriler gibi hassas bilgileri ifşa etmelerini sağlar. Genellikle saygın işletmeleri veya kişileri taklit ederek aciliyet hissi yaratır. Kimlik avı e-posta'ları genellikle hedeflenen kişilerin bilmeden gizli bilgilerini verdikleri sahte web sitelerine veya formlara bağlantılar içerir. Örneğin, bir bankadan geldiğini iddia eden bir e-posta, alıcıdan bir bağlantıya tıklamasını ve hesap bilgilerini güncellemesini isteyebilir. Eğer bağlantıya tıklarsanız, yönlendirdiğiniz sahte web sitesi verilerinizin çalınmasına sebep olabilir.

Kötü Amaçlı Yazılım Ekleri: E-posta'lar bazen belge veya fatura gibi zararsız dosyalar gibi gizlenmiş eklerle gelebilir. Ancak bu ekler virüs, fidye yazılımı veya casus yazılım gibi zararlı kötü amaçlı yazılımlar taşıyabilir.

Alıcı bu ekleri açtığında, kötü amaçlı yazılım bilgisayarına veya ağına bulaşarak bilgisayar korsanlarına yetkisiz erişim veya dosyaları şifreleme olanağı sağlar. Açıldığında bir virüsü etkinleştiren ve alıcının bilgisayarına bulaşarak sistemini tehlikeye atan bir ek içeren e-posta, kötü amaçlı yazılım ekleri için önemli bir örnektir.

Spear Phishing: Spear phishing saldırıları, belirli kişi veya işletmeleri hedef alacak şekilde hazırlandıkları için ciddi bir tehdit oluşturur. Bu saldırı türünde bilgisayar korsanları, gerçek gibi görünen aldatıcı e-posta'lar oluşturmak için kişisel bilgileri toplamak için zaman harcar. Spear phishing, e-posta'yı kendi özel koşullarına göre özelleştirerek alıcının güvenini istismar etmeyi amaçlar. Bu özel siber saldırılar, hedeflenen kişinin bilmeden hassas bilgileri ifşa etme veya sahte bağlantılara tıklama riskini önemli ölçüde artırır.

Business Email Compromise (BEC): BEC saldırılarında, siber suçlular aldatıcı taktikler benimseyerek üst düzey yöneticiler, tedarikçiler veya iş ortakları gibi davranır ve şüphelenmeyen kurbanları zararlı eylemlere çeker. Bireyleri para transfer etmeye, hassas bilgileri ifşa etmeye veya bilgisayar korsanına finansal fayda sağlayacak görevleri yerine getirmeye ikna eder. BEC saldırıları, işletmelerdeki güven ve otoriteyi istismar ederek tehlikeli sonuçlara yol açabilir.

CEO'nuzdan gelmiş gibi görünen ve belirli bir hesaba önemli bir meblağ aktarmanızı isteyen bir e-posta en bilinen BEC örneklerinden biridir.

Tüm bu sebeplerden dolayı kendinizi ve işletmenizi korumak için tetikte olmak ve bu tür dolandırıcılık taleplerinin işaretlerini anlamak çok önemlidir.

Email Spoofing: Email spoofing, e-posta başlığının taklit edilerek e-posta'nın meşru bir kaynaktan veya güvenilir bir kişiden geliyormuş gibi gösterilmesiyle oluşur. Amaç, alıcıları e-posta'nın saygın bir göndericiden geldiğine inandırmak ve böylece bilgisayar korsanının komutlarına uyma olasılıklarını artırmaktır. Örneğin, iyi bilinen bir işletme veya hizmetten geliyormuş gibi görünen bir e-posta, gerçek kaynağını gizlemek için e-posta başlığı değiştirebilir.

Email Bombing: Bu kötü niyetli saldırı, alıcının gelen kutusunu çığ gibi büyüyen bir e-posta bombardımanına tutar. Bu e-posta bombardımanı iletişimi ciddi şekilde kesintiye uğratabilir, üretkenliği engelleyebilir ve hatta e-posta sunucularının çökmesine yol açarak ek rahatsızlıklara neden olabilir. Örneğin, bir kişi birden fazla kaynaktan gelen yoğun bir e-posta bombardımanına maruz kalarak e-posta hesabını kullanamayabilir. Bu da gerçekten önemli e-posta'ları kaçırmasına neden olabilir.

Spam ve İstenmeyen E-posta'lar: Temelde kötü niyetli olmasa da, spam ve istenmeyen e-posta'lar gelen kutularını reklamlar, dolandırıcılıklar veya şüpheli tekliflerle doldurarak değerli kaynakları tüketir ve daha zararlı tehditleri gizleyebilir. Örneğin, bir gelen kutusu çeşitli ürünleri, hizmetleri veya şüpheli teklifleri tanıtan istenmeyen e-posta'lar içerebilir.

E-posta Filtreleme Yöntemleri nelerdir?

E-posta yönetimini ve güvenliğini geliştiren e-posta filtreleme teknikleri; e-postaları sıralayarak, kategorize ederek ve önceliklendirerek spam, virüs ve istenmeyen içeriklere karşı koruma sağlar.

Peki bu filtreleme yöntemlerinden en önemlileri nelerdir? Aşağıda listede popüler e-posta filtreleme yöntemlerini bulabilirsiniz:

Unified Mail Gateway

1. İçerik Filtreleme

Anahtar kelimeleri, ifadeleri veya kalıpları belirlemek için e-posta'ların içeriğini analiz etmeyi içeren içerik filtreleme, e-posta yönetimi için önemli bir tekniktir.

Filtreler, içeriği inceleyerek e-posta'ları önceden tanımlanmış kategorilere ayırır veya potansiyel spam olarak işaretler. İçerik filtreleme, önemli e-posta'ların doğru şekilde yönlendirilmesi ve alakasız veya potansiyel olarak zararlı e-postaların filtrelenmesini sağlar.

2. Başlık Analizi

E-posta üstbilgileri gönderen, alıcı ve e-posta'nın gelen kutusuna ulaşma yolculuğu hakkında değerli ayrıntılar sağlar. Filtreler, e-posta üstbilgisini inceleyerek kaynağı değerlendirebilir ve e-posta'nın meşruiyetini doğrulayabilir. Gönderenin IP adresi, alan adı itibarı ve e-posta yönlendirme bilgileri gibi faktörler, bir e-posta'nın spam veya yasal olma olasılığını belirlemek için değerlendirilir.

3. Beyaz Liste ve Kara Liste

Beyaz ve kara liste hayati önem taşıyan e-posta filtreleme tekni̇kleridir. Beyaz liste, filtreleri atlayarak e-posta'ları doğrudan gelen kutusuna almak için güvenilir e-posta adresleri veya alan adları eklemeyi içerir. Diğer yandan kara listeye alma, belirli e-posta adreslerini veya alan adlarını gelen kutusundan hariç tutmak için engeller veya filtreler. Bu sayede istenmeyen veya şüpheli e-posta'ların alıcıya ulaşmasını önler.

4. 4. Sender Policy Framework (SPF)

Sender Policy Framework (SPF), bir alan adı için yetkili gönderen IP adreslerine karşı gönderenin IP adresini doğrulayan bir e-posta kimlik doğrulama yöntemidir. E-posta sahtekarlığı ile mücadele eder ve sahte veya yetkisiz e-postala'rı tespit etmek için bir filtreleme tekniği olarak hizmet eder. Filtreler, bir e-posta'nın gerçekliğini doğrulamak için gönderenin alan adlarının SPF kaydını kullanır ve SPF sonucuna göre uygun eylemleri etkinleştirir.

5. Bayesian Filtreleme

Bayesian filtreleme, e-posta özelliklerini analiz etmek için olasılık ve makine öğrenimi algoritmalarını kullanan istatistiksel bir tekniktir. Filtre, bilinen spam ve spam olmayan e-posta'larla eğitildikten sonra bir e-posta'nın spam olma olasılığını hesaplamayı öğrenir. Sürekli işleme ve kullanıcı geri bildirimi ile Bayesian filtresi zaman içinde uyum sağlar ve doğruluğunu artırır. Öğrenilen kalıp ve olasılıklara dayalı olarak spam e-postaları etkili bir şekilde tanımlar ve filtreler.

6. Greylisting

Greylisting, meşru sunucuların teslimatı yeniden deneyeceği beklentisinden yararlanarak bilinmeyen gönderenlerden gelen e-posta'ları geçici olarak reddeder. Spam göndericilerin genellikle yeniden denememesinden, meşru göndericilerin ise yeniden denemesinden faydalanır. Bu teknik, önemli miktarda spam'i etkili bir şekilde filtreleyerek yasal e-posta'ların yeniden denemede başarıyla teslim edilmesini sağlar.

7. DomainKeys Identified Mail (DKIM)

DomainKeys Identified Mail (DKIM), kriptografik imzalar kullanarak e-posta'nın gerçekliğini doğrulayan bir e-posta kimlik doğrulama yöntemidir. Filtreler, e-posta bütünlüğünü doğrulamak ve geçersiz veya eksik imzalı e-postaları filtrelemek için DKIM imzalarını kullanır. DKIM, e-postaların iletim sırasında kurcalanmamasını sağlayarak e-posta filtrelemenin güvenliğini ve güvenilirliğini artırır.

8. İşbirliğine Dayalı Filtreleme

İşbirliğine dayalı filtreleme, spam e-posta'ları tanımlamak ve filtrelemek için birden fazla kullanıcının paylaştığı bir spam veri tabanını kullanır. Kullanıcıların katkıda bulunduğu spam raporları kolektif bilgiyi geliştirerek filtreleme doğruluğunu sürekli iyileştirir.

Inbound ve Outbound Filtreleme Hakkında Bilmeniz Gerekenler

Inbound ve outbound e-posta filtreleme, modern e-posta güvenlik sistemlerinin ayrılmaz bileşenleridir. İşletmeler genellikle e-posta güvenliğini artırmak için inbound ve outbound filtreleme özelliklerini birleştiren kapsamlı e-posta filtreleme çözümleri kullanır.

Inbound e-posta filtreleme, kullanıcıları korumak için internetten gelen e-posta'ları taramaya odaklanır. Amacı, bu mesajlarla ilişkili potansiyel riskleri belirlemek ve azaltmaktır. Gelişmiş algoritmalar, gelen kutularını karıştırabilecek ve kötü niyetli içerik taşıyabilecek istenmeyen e-posta'ları (spam) tespit eder ve engeller. Inbound filtreler ayrıca kötü amaçlı yazılım veya virüs içeren e-posta'ları tespit edip izole ederek kullanıcıların zararlı yazılımları indirmesini önler. Ayrıca kimlik avı saldırılarına veya diğer güvenlik ihlallerine yol açabilecek şüpheli bağlantılar içeren e-posta'ların belirlenmesine de yardımcı olur.

Öte yandan, outbound e-posta filtreleme, yerel kullanıcılar tarafından gönderilen e-posta'ları internetteki alıcılara ulaşmadan önce tarar. Amacı, potansiyel olarak zararlı veya yetkisiz içeriğin iletilmesini önlemektir. Bu yaklaşım, gönderenin itibarının bozulmamasını ve e-posta iletişim güvenliğinin korunmasını sağlar.

Outbound filtreleri, güvenlik politikalarına uygunluğu sağlamak ve hassas bilgilerin kazara sızmasını önlemek için e-posta içeriğini ve eklerini analiz eder. Örneğin, veri ihlallerini önlemek ve gizliliği korumak için kredi kartı bilgileri veya fikri mülkiyet gibi gizli veriler içeren outbound e-posta'ları engelleyebilir. Ayrıca diğer işletmelerin filtreleri tarafından spam olarak işaretlenen e-posta'ların iletimini tespit eder ve durdurur.

E-posta Filtreleme için **Farklı Dağıtım Türleri** Nelerdir?

İşletmelerin bir e-posta filtreleme dağıtımı seçerken gereksinimlerini dikkatle değerlendirmeleri ve ölçeklenebilirlik, mevzuata uygunluk, veri gizliliği ve yönetim çabaları gibi faktörleri göz önünde bulundurmaları çok önemlidir. Doğru dağıtım türü, etkili ve verimli e-posta koruması sağlamak için işletmenin ihtiyaçları, kaynakları ve uzun vadeli hedefleriyle uyumlu olmalıdır.

Aşağıdaki listede her biri farklı avantajlar sunan birden fazla dağıtım yöntemini bulabilirsiniz:

1. Bulut Tabanlı Dağıtım

Bulut tabanlı e-posta filtrelemede, analiz ve filtreleme üçüncü taraf sağlayıcılar tarafından sağlanır. Gelen ve giden e-posta trafiği, spam algılama, kötü amaçlı yazılım taraması, içerik filtreleme ve gönderen itibar analizi gibi teknikler için bulut hizmetine güvenilir. Bulut tabanlı dağıtımın avantajları arasında kolay kurulum, ölçeklenebilirlik ve altyapı yönetiminin boşaltılması yer alır. Ayrıca sürekli güncellemeler ve gelişmiş tehdit istihbaratı sağlanır. Bu noktada işletmelerin e-posta verileri konusunda bulut sağlayıcısına güvenmesi gerekir.

2. Şirket İçi Dağıtım

Şirket içi e-posta filtreleme, belirli sektörlerde yasal uyumluluk için gereklidir ve verilerini şirket içinde tutmak isteyenler tarafından tercih edilir. Bu model, filtreleme yazılımının yüklü olduğu fiziksel bir cihazın sağlanmasını gerektirir. Cihaz tabanlı filtreleme, verileri kurum içinde ve kurumun BT personelinin kontrolü altında tutar. Ancak, dahili BT personeli tarafından altyapının zaman alıcı bakım, yönetim ve güncellemelerini gerektirir.

3. Hibrit Dağıtım

Hibrit dağıtım, şirket içi ve bulut e-posta kutularının birlikte kullanıldığı işletmeler için uygun bir alternatiftir. Örneğin, Microsoft'un Office 365 için Defender'ı, karma bir kurulumda posta yönlendirme ve korumanın yapılandırılmasını sağlar. Hibrit dağıtım, kapsamlı e-posta güvenliği için Exchange Online Protection gibi hem şirket içi hem de bulut tabanlı e-posta filtreleme çözümlerinden yararlanmaya olanak tanır.

Hibrit dağıtım, şirket içi ve bulut tabanlı filtrelemeyi birleştirerek özel gereksinimlere, uyumluluk ihtiyaçlarına veya altyapı sınırlamalarına göre özelleştirme esnekliği sunar. İşletmeler, gelişmiş tehdit algılama, e-posta sürekliliği veya diğer işlevler için bulut tabanlı filtreleme kullanırken belirli e-posta güvenliği bileşenlerini şirket içinde dağıtabilir.

4. Yönetilen Hizmet Sağlayıcı (MSP) Dağıtımı

Bazı işletmeler e-posta filtreleme gereksinimlerini Yönetilen Hizmet Sağlayıcılara (MSP'ler) yaptırmaktadır. MSP'ler filtreleme, tehdit algılama, şifreleme, arşivleme ve mevzuata uygunluk yönetimini kapsayan kapsamlı e-posta güvenlik hizmetleri sunma konusunda uzmanlaşmıştır.

İşletmeler bir MSP kullanarak e-posta güvenlik altyapılarının bakım ve güncellemelerini güvenilir bir üçüncü tarafa emanet edebilir. Bu strateji, daha küçük işletmeler veya sınırlı BT kaynaklarına sahip olanlar için daha avantajlıdır. Bununla birlikte, işletmeler e-posta iletişimlerinin güvenli bir şekilde ele alınmasını sağlamak için dikkatli olmalı ve güvenilir bir MSP seçmelidir.

Etkili E-posta Filtreleme için İpuçları

Gelen kutunuzda oluşan karmaşada kaybolduğunuzu hissettiyseniz ve e-posta filtrelemenizi geliştirmek istiyorsanız, Unified Mail Gateway, etkili e-posta filtreleme konusunda size tavsiyelerde bulunmak için tam da bu noktada devreye girer. Zaman içinde test edilmiş bu stratejileri uygulayarak gelen kutusu kontrolünü yeniden kazanabilir ve e-posta verimliliğinizi artırabilirsiniz.

1. Filtreler oluşturun

Önemli e-posta'ları işaretlemek veya belirlenen klasörlere taşımak için kurallar oluşturun. Bu noktada gelen kutunuzda belirgin bir şekilde görünmelerini sağlamak için belirli gönderenlere veya anahtar kelimelere öncelik verebilirsiniz.

2. Gönderen filtrelerini kullanın

Değerli veya önemsiz göndericileri belirleyin ve onlardan gelen e-posta'ları uygun klasörlere ayırın. Gönderen filtresinin, yüksek öncelikli e-posta'lara odaklanmanıza ve gelen kutunuzdaki dağınıklığı gidermenize yardımcı olacağını unutmayın.

3. Anahtar kelime filtrelerini kullanın

Spam ile ilgili anahtar kelimeleri belirleyin ve bu anahtar kelimeleri içeren iletileri yönlendirmek veya silmek için filtreler oluşturun. Bu noktada meşru e-posta'ları yanlışlıkla filtrelemekten kaçının.

4. Güvenilir göndericileri beyaz listeye alın

Güvenilir e-posta adreslerini veya alan adlarını onaylı kişiler listesine ekleyin. Beyaz liste oluşturmak, e-posta'larının spam filtrelerini atlamasını ve doğrudan gelen kutunuza ulaşmasını sağlar. Yasal e-postalar için spam klasörünüzü düzenli olarak kontrol edin ve gerekirse bunları beyaz listeye alın.

5. İstenmeyen göndericileri kara listeye alın veya engelleyin

Belirli gönderenlerden gelen spam veya alakasız e-posta'ları spam klasörünüze göndermek veya tamamen engellemek için filtreler oluşturun. Kara liste oluşturmak gelen kutusu karmaşasını azaltır ve dikkat dağıtıcı unsurları en aza indirir.

6. Gelişmiş spam filtrelerini etkinleştirin

E-posta hizmetiniz tarafından sağlanan yerleşik spam filtrelerini özelleştirin ve etkinleştirin. İstenmeyen e-posta'ları etkili bir şekilde yakalamak ve kaldırmak için bunları yapılandırın.

7. Spam filtrelerinizi eğitin

Belirli e-posta'ları spam olarak işaretlemenize veya işaretlememenize olanak tanıyan özelliklerden yararlanın. Spam filtrelerinizin doğruluğunu zaman içinde iyileştirmeye yardımcı olmak için sürekli olarak geri bildirim sağlayın.

8. Filtreleri düzenli olarak gözden geçirin ve güncelleyin

Filtrelerinizi sık sık gözden geçirin ve gerekli ayarlamaları yapın. Zaman içinde yeni göndericiler ortaya çıkabilir veya tercihleriniz değişebilir, bu nedenle filtreleme kurallarınızı buna göre uyarlayın.

9. Abonelikten çıkma seçeneklerini kullanın

Artık işinize yaramayan haber bültenleri veya pazarlama e-posta'larının aboneliğinden çıkın. Bunu yapmak, gelen e-posta'ların hacmini azaltmaya yardımcı olurken gelen kutusu karmaşasını da önler.

10. E-posta hesaplarınızı her yerde paylaşmayın

İstenmeyen veya spam e-posta'lar alma olasılığını en aza indirmek için e-posta adresinizi herkese açık olarak nerelerde paylaştığınıza dikkat edin. Gelen kutunuzu gereksiz e-posta'lardan korumak için bu ipucunu her zaman göz önünde bulundurun.

Üstün Koruma için Unified Mail Gateway'in E-posta Filtreleme Hizmetini Keşfedin

Siber suçlular, güvenlik açıklarından yararlanmak ve hassas bilgileri tehlikeye atmak için sürekli yeni taktikler geliştirir. Bu yeni yöntem ve teknikler, siber güvenlik konusunda bilgi sahibi olanları bile zaman zaman tuzağa düşürmeye yeter.

Siz de tüm bu siber tehlikelerden korunmak ve siber suçluların hedeflerinden biri olmak istemiyorsanız, bu noktada Unified Mail Gateway'in E-posta Filtreleme Hizmeti, e-posta tehditlerine karşı en üst düzeyde koruma için kapsamlı ve güvenilir bir çözüm sunarak işletmenizin güvenlikten ödün vermeden temel faaliyetlerine odaklanmasını sağlar.

Unified Mail Gateway'i e-posta iletişimlerinizi korumak için başvurulacak çözüm haline getiren temel özellikleri aşağıdaki şekildedir:

Unified Mail Gateway Kapsamlı Tehdit Koruması

Unified Mail Gateway'in E-posta Filtreleme Hizmeti kapsamlı tehdit koruması sunar. Spam, virüs, kimlik avı girişimleri ve kötü amaçlı yazılım saldırılarını etkili bir şekilde engelleyerek güvenli bir gelen kutusu sağlar. Gerçek zamanlı izleme, en son vspam ve kötü amaçlı yazılım salgınlarını tespit eder ve bunlara yanıt vererek sizi gelişen tehditlere karşı korur.

Kötü amaçlı ekler ve URL'ler ayrıntılı tarama ile etkisiz hale getirilerek işletmenizi ihlallere karşı korur. Gelişmiş antivirüs ve antispam koruması, birden fazla üçüncü taraf satıcı tarafından edinilen imzaları kullanarak güncel tehditlere karşı güncel kalır.

Son olarak, bilinmeyen tehditleri tespit eder ve bunlara karşı koruma sağlayarak sıfır gün saldırılarına karşı en üst düzeyde savunma sağlar.

Sorunsuz E-posta İşlemleri

Unified Mail Gateway, esnek bir filtreleme altyapısı ile sorunsuz e-posta işlemleri sağlar. Ağ kesintileri veya sunucu arızaları sırasında bile e-posta iletişiminiz kesintiye uğramaz, kesintileri en aza indirir ve işlemleri sorunsuz şekilde sürdürür. Otomatik veri yedekleme, kritik e-posta'ların ve eklerin güvenliğini garanti ederek değerli bilgiler için sürekli güvenlik sağlar.

Kazara silme veya veri kaybı durumlarında, hayati verileri sorunsuz bir şekilde hızlıca kurtarmak için kolay kurtarma seçenekleri sunar. Günlük izleme işlevi, e-posta altyapısının etkinliği ve trafiği hakkında değerli bilgiler sunarak günlük verilerini izler ve analiz eder. Bu optimizasyon, performansı artırmaya yardımcı olur ve bilinçli karar vermeyi kolaylaştırır.

Özelleştirilmiş Kontrol ve Uyumluluk

Unified Mail Gateway'in e-posta filtreleme hizmeti, işletmenizin ihtiyaçlarına göre özelleştirilmiş kontrol ve uyumluluk özellikleri sağlar. Gelişmiş içerik filtreleme, inbound ve outbound e-posta'lar için kişiselleştirilmiş filtreler oluşturmanıza olanak tanıyarak spam, kimlik avı girişimleri ve kötü amaçlı yazılımlara karşı kontrol ve koruma sağlar.

Veri sızıntısı önleme özelliği, işletme bilgilerinizin gizliliğini ve güvenliğini koruyarak outbound e-posta'lar yoluyla hassas verilerin iletimini tanımlar ve durdurur. İçerik uyumluluğu taraması, kurumsal politikaları ve sektör düzenlemelerini uygulayarak uygunsuz veya hassas içeriğin gönderilmesini engeller. Unified Mail Gateway, e-posta kimlik doğrulamasını geliştirmek ve sahte e-posta'lara karşı korumak için SPF, DKIM ve DMARC kayıtlarını aktif olarak yönetir.

Unified
Mail Gateway

Kullanıcı Hesaplarını ve Giden İletişimi Koruma

Unified Mail Gateway, kullanıcı hesaplarının ve outbound iletişimin güvenliğine öncelik verir. Hesap koruma özelliği, kullanıcı hesaplarıyla ilişkili şüpheli veya yetkisiz etkinlikleri engelleyerek güvenliği ihlal edilmiş hesapların outbound e-posta'lar göndermesini önler. Outbound filtreleme, işletmenizin itibarını korur ve hassas bilgilere yetkisiz erişimi önler. Abuse account blocking, güvenliği ihlal edilmiş veya kötüye kullanılmış kullanıcı hesaplarından gelen şüpheli veya yetkisiz etkinlikleri tanımlar ve engeller.

Unified Mail Gateway'in outbound e-posta filtrelemesi, işletmenizin ağlarını outbound spam, virüs ve kötü amaçlı yazılımlardan koruyarak kesintisiz e-posta iletişimi sağlar ve ağdan yararlanma riskini azaltır. DKIM imzalama, outbound e-posta'ların gerçekliğini ve bütünlüğünü artırır. Son olarak, giden hız limiti yönetimi, e-posta dağıtımını optimize etmenize ve kontrolleri ayarlayarak kötüye kullanımı önlemenize olanak tanır.

Unified
Mail Gateway

Unified
Mail Gateway

Bütünleşik E-posta Güvenlik Çözümü

Ücretsiz Dene

www.uzmanposta.com