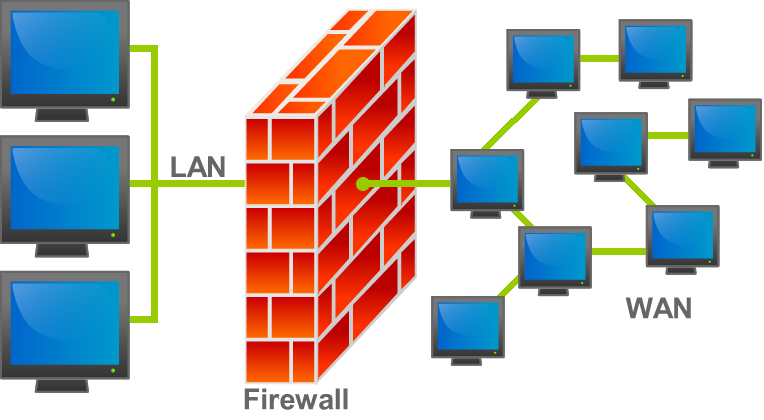
|  |
| --- |
| ***Savunma Mekanizmaları*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| -FIREWALL  -IDS/IPS  -WAF(Web App. Firewall)  -SIEM  -SOAR  -laaS  -SaaS  -PaaS |

***FIREWALL***

**20.08.2021**



- Güvenlik duvarları yani firewall sistemleri, gelen ve giden tüm ağ trafiğini kontrol ederek belirli filtrelerden geçirip, ağ trafiği içerisindeki zararlı eylemleri durdurmayı amaçlar

-Firewall ne kadar iyi yapılandırılırsa o kadar çok fayda sağlar.

-Yapılandırma dediğimiz;Tanımlanan kuralların mevcut altyapıda ki işlevselliği ve gerekliliğidir.

-Temel olarak firewall,network üzerinde kendisine gelen paketlerin ulaşması gereken yerlere önceden tanımlanmış kurallara uymayanların trafiğini engelleyerek koruma sağlar.

-Firewall sistemleri donanım ve yazılım tabanlı olmak üzere ikiye ayrılırlar.

-Yazılım tabanlı olan Firewall uygulamaları genelde istemci veya sunucular üzerindeki işletim sistemlerine kurulur. Donanım tabanlı firewall cihazları ise özel donanımlar üzerinde çalışan sistemlerdir.

-Firewall abartıldığı kadar işe yaramamaktadır.Çeşitli Bypass yöntemleri ile çok rahat bir şekilde atlatılabilir.

***IPS(SALDIRI ÖNLEME SİSTEMİ)***

-Güvenlik açığı ihlallerini tespit etmek ve önlemek için ağ trafiği akışlarını inceleyen bir ağ güvenliği-tehdit önleme teknolojisidir.

-IPS genellikle güvenlik duvarının hemen arkasında bulunur ve tehlikeli içeriği olumsuz , güvenilir içeriği olumlu olarak seçen tamamlayıcı bir analiz katmanı sağlar.

-IPS, kaynak ve hedef arasındaki doğrudan iletişim yoluna yerleştirilir, paketler aktif olarak analiz edilir ve otomatik eylemler gerçekleştirilir.

Başlıca eylemleri şunlardır:

-Yöneticiye saldırı anında uyarı gönderme.

-Kötü amaçlı paketlerin bırakılması.

-Kaynak adreste trafiği engelleme.

-Bağlantının sıfırlanması.

-CRC hatalarını düzeltme.

-Paket akışını birleştirme.

***IDS(SALDIRI TESPİT ETME SİSTEMİ)***

-Güvenlik analistleri için adli araç olarak tasarlanmış yazılımsal veya donanımsal ögedir.

-IDS ,temel olarak ağ trafiği etkinliğini izlemek, analiz etmek ve bir kullanıcı/kurumu olası güvenlik açıkları ve saldırılara karşı uyarmak üzere yapılandırılmış bir sistemdir.

-IPS gibi IDS de genellikle güvenlik duvarının hemen arkasında bulunur.

Başlıca eylemleri şunlardır:

-Bir program veya bir kişiden kaynaklanan saldırıları tespit eder.

-Algılama mantığını sürekli iyileştirmek için saldırı kalıplarını kaydeder.

-Güçlü bir kontrol paneli ve yükseltme mekanizması kullanarak uyarı ve rapor verir.

-Gelecekteki adli kanıtlar için tüm olası ve olmuş saldırıları veritabanına kaydeder ve etkinleştirir.

-Zarar görmüş sistemi karantinaya alır.

-Veri bütünlüğünü ,erişilebilirliğini ve gizliliğini sağlar.

***SIGNATURE(İMZA)***

-IDS ve IPS gibi bilinen saldırıları tespit etmek ve önceden tanımlanmış eylemlerle yanıt vermek için kullandığı bir dizi kuraldır.

***SİGNATURE ALARMS(İMZA ALARMLARI)***

-False-positive : Normal trafik veya olumlu bir hareket tarafından tetiklenen bir alarmdır.

-False-negative : Yanlış bir trafik vb. durum algılandığında ve buna karşı bir imza tetiklenmediğinde oluşan alarmdır.

-True-positive : Saldırıya karşı imza doğru şekilde tetiklendiğinde ve rahatsız edici trafik tespit edildiğinde oluşan alarmdır.

-True-negative : Gerçek olmayan bir saldırı yakalandığında ve analiz edildiğinde bir imza atılmadığında oluşan alarmdır.

***IDS VE IPS FARKLARI***

-Her iki IDS / IPS, ağ paketlerini okur ve içeriği, bilinen tehditlerin bir veritabanıyla karşılaştırır. Aralarındaki temel fark, daha sonra olanlar.

-IDS, kendi başlarına hareket etmeyen algılama ve izleme araçlarıdır. IPS, kuralları temel alan bir paketi kabul eden veya reddeden bir kontrol sistemidir.

-Aralarındaki temel fark, IDS bir izleme sistemi, IPS ise bir kontrol sistemidir.

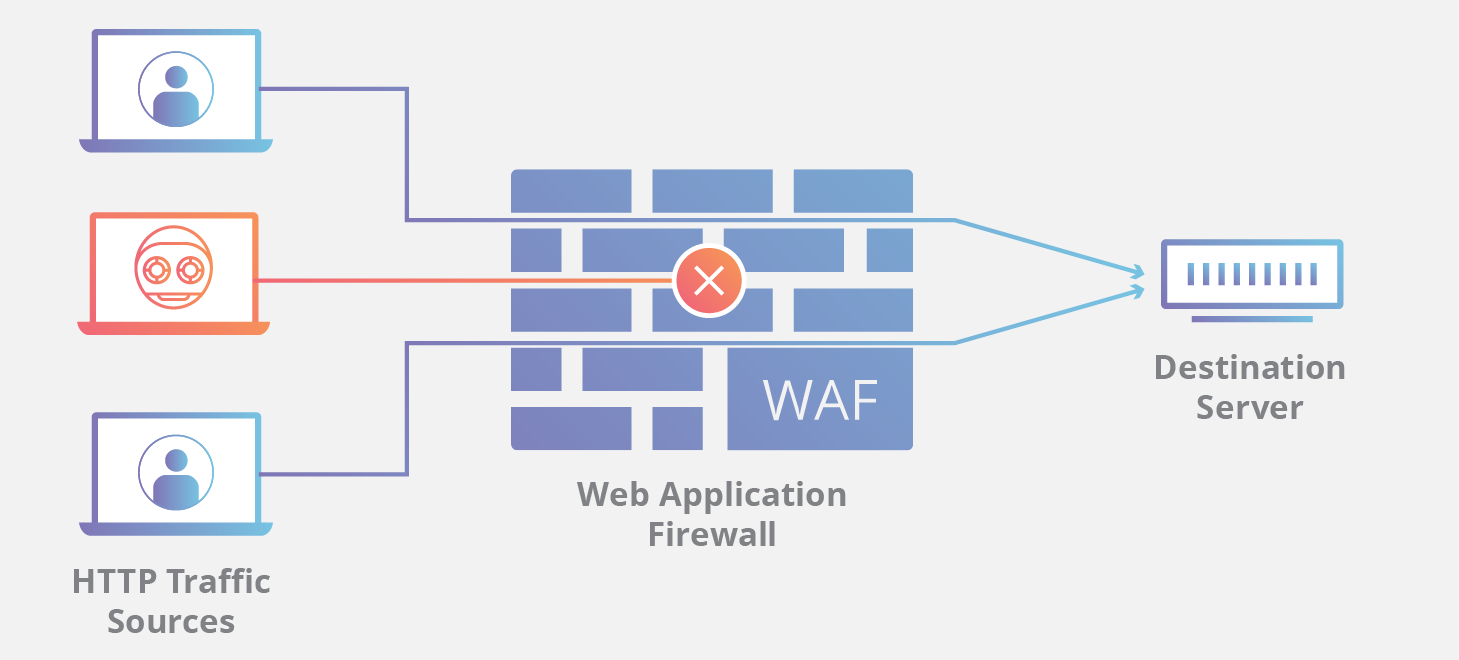
***IPS/IDS NASIL ÇALIŞIR ?***

**-Saldırı Tespit Sistemleri (IDS):** Saldırganların ağınızdan veri sızması veya çalması için bilinen bir siber tehdit kullandığını belirten işaretler için ağ trafiğini analiz eder ve izler. IDS sistemleri, güvenlik politikası ihlalleri, kötü amaçlı yazılımlar ve bağlantı noktası tarayıcıları gibi çeşitli davranış türlerini tespit etmek için mevcut ağ etkinliğini bilinen bir tehdit veri tabanıyla karşılaştırır.

**İzinsiz Girişi Önleme Sistemleri (IPS):** Ağın güvenlik duvarıyla aynı alanda, dış dünya ile iç ağ arasında yaşar. IPS bu paket bilinen bir güvenlik tehdidi oluşturuyorsa, güvenlik profiline dayalı ağ trafiğini proaktif olarak reddeder.

-IDS, ağ paketlerini hiçbir şekilde değiştirmez, IPS ise paketin, içeriğini IP adreslerine göre trafiğini önleme biçimine göre paketin içeriğine dayalı olarak teslim edilmesini önler.

***WAF (Web App. Firewall)***

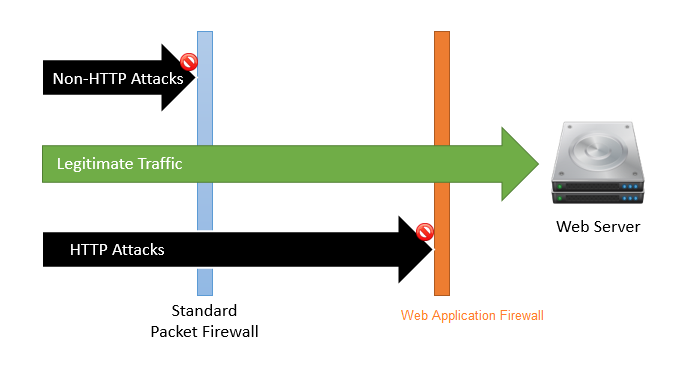


- WAF; OSI'nin 7. katmanı olan uygulama katmanında görev alır ve adından da anlaşılabileceği gibi web uygulamalarını olası saldırılara karşı korumayı hedefler. Son kullanıcı ile sunucu arasında oluşan iletişimi dinleyerek tanımlanan kurallara göre filtreleme, düzeltme veya engelleme uygular.

- Bir WAF, özelleştirilmiş denetimler yoluyla, geleneksel ağ güvenlik duvarlarının ve diğer saldırı tespit sistemlerinin (IDS'ler) ve izinsiz giriş önleme sistemlerinin (IPS'ler) yapamayacağı en tehlikeli web uygulama güvenlik açıklarından bazılarını tespit edebilir ve anında önleyebilme yeteneğine sahiptir.

-WAF’lar özellikle e-ticaret alışverişi,çevrimiçi bankacılık kısacası internet üzerinden ürün veya hizmetler sağlayan şirketler için yararlıdır ve kullanması güvenlik standartları tarafından tavsiye edilmektedir.

***WAF Nasıl Çalışır?***



-WAF,HTTP isteklerini analiz eder.

-İstemci tarafından gönderilen isteğin zararsız veya kötü niyetli olduğunu tanımlamak için bir dizi kural uygular.Bir WAF’ın analiz ettiği HTTP konuşmalarının ana bölümleri GET ve POST istekleridir.

-GET : Sunucudan veri almak için kullanılır.

-POST : Sunucuya veri göndermek için kullanılır.

***WAF’ın kullandığı güvenlik modelleri***

*Positive Security Model (Beyaz Liste Modeli) :* WAF’ın varsayılan olarak tüm istekleri reddedeceği ve yalnızca güvenilir olduğu bilinen isteklere izin vereceği anlamına gelir.

-Güvenli olduğu bilinen IP adreslerinin bir listesini sağlar ve bu liste doğrultusunda işlem yapar.

*Negative Security Model (Kara Liste Modeli) :* Varsayılan olarak paketlerin geçmesine izin verir.

-Kötü amaçlı web trafiğini engellemek ve web uygulamalarının mevcut güvenlik açıklarından korumak için önceden belirlenmiş imzaları kullanır.Yasaklanmış belirli işlemler hariç her şeye izin verilir.

-Kara liste,genel web siteleri ve web uygulamaları için daha uygundur.

*Karma Güvenlik :* Hem Positive Security Model hem de Negative Security Model’den yararlanır.

*Learning-based Firewall :* Gelen ve giden istekleri inceleyerek web sayfalarının haritasını çıkarmaya çalışır.Burada web adminlerinin katkısı WAF’a yönlendirilir ve öğrendikleri onaylanır veya reddedilir.

***WAF Türleri***

*Ağ Tabanlı WAF :* Genellikle donanım tabanlıdır ve uygulamaya olabildiğince yakın bir yerde,özel bir cihaz aracılığıyla şirket içinde yerel olarak konumlandırılırlar.

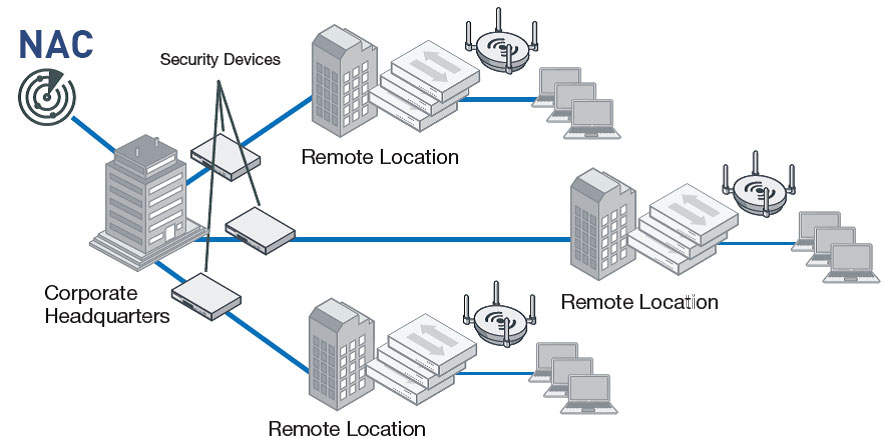
Ana Bilgisayar Tabanlı WAF : Uygulama kodunun kendisine tam olarak entegre edilebilir.Ana bilgisayar tabanlı WAF’lar,sunucu kaynaklarına bağlı oldukları için yönetilmesi zor olabilir.

-Yönetim için sistem analistleri ve DevOps dahil daha fazla personel kaynağı gerekebilir.

*Bulut Tabanlı WAF :* Uygulama ve yönetim için minimum kaynak gerektiren anahtar teslimi bir ürün isteyen kuruluşlar için düşük maliyetli bir çözüm sunar.

-Bulut tabanlı WAF'ların dağıtımı kolaydır, abonelik temelinde sunulur ve uygulama trafiğini yeniden yönlendirmek için yalnızca basit bir alan adı sistemi (DNS) veya proxy değişikliği gerektirir.

***NAC(Network Access Control)***



- Yerel ağa giren veya girmeye çalışan makinelerin erişiminin olup olmadığını kontrol eden, erişime izin veren veya engelleyen sistem ise Network Access Control yani Ağ Erişim Kontrolüdür.

-Ağa giren kişileri kendi güvenlik politikasına göre yetkilendirir.Politikaya uygun olmayanın yetkilerini kısıtlar.Kabul sonrası şüpheli bir etkinlik tespit edilirse sistemden kişi düşürülebilir.(IPS gibi)

-Örneğin,Ağ üzerinde yetkili ağ ve misafir ağı bulunmaktadır.Ağ’a Linux Sistemi kullanan bir cihaz bağlanmak istedi.Bunu tespit eder ve sadece misafir ağa erişim yapmasını sağlar.

*Eleman Algılama :* Ağa tanıtılan yeni elemanların tespiti.

*Kimlik Doğrulama :* Ağa erişen her kullanıcının kimliğini doğrulama ve hangi cihazı kullandıkları kayıt edilir.

*Uç Nokta Güvenlik Değerlendirmesi :* Yeni tanıtılan bir ağ öğesinin,kuruluşun güvenlik politikasına uygunluğu.Bu kontroller;bir öğenin işletim sistemi, yüklü yamaların listesi,antivirüs yazılımın varlığı ve virüs imza tarihi vb. denetlenir.

-Çoğu durumda,istemci yazılımının uç sisteme yüklenmesini içerir.

Düzeltme : Tanımlanan güvenlik politikasına uymayan bir unsuru karantinaya alır.

-Öğe karantinaya alındığında(Misafir ağa çekilir) tanımlanmış bir kümeye erişebilir.

Zorlama : Bir eleman ağ erişimine uygun değilse kısıtlanır.

Yetkilendirme : İçinde tanımlanan bir yetkilendirme şemasına göre kullanıcıların ağ kaynaklarına erişim doğruma Active Directory,RADIUS sunucuları vb. gibi mevcut bir yetkilendirme sistemidir.

Kabul Sonrası Koruma : IPS gibi çalışmaktadır.Sunucu üzerinde şüpheli bir etkinli saptanır ise NAC oturumunu düşürür.

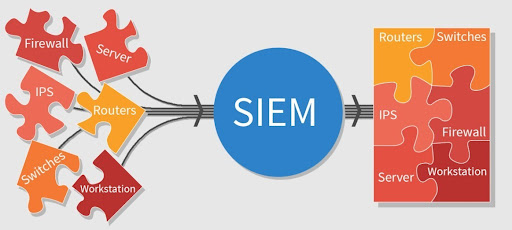
***Loglama***

-Log izleme, tüm kritik ağlar ve cihazları kapsayan bilişim sistemlerinin ürettiği olay kayıtlarının(loglarının) belirlenen kurallara göre analiz edilmesi olarak tanımlanmaktadır.

-Logların kapsamlı bir şekilde toplanması, birleştirilmesi, orijinal haliyle saklanması, metin olarak analizi ve sunumu gibi adımlardan oluşan log yönetimi ise saldırının göstergelerini ve delillerini elde etmeye olanak sağlamaktadır.

- Aynı zamanda saldırıların adli olarak incelenmesine de yardımcı olarak saldırının hangi kanallardan ne zaman gerçekleştirildiği, hangi protokollerin kullanıldığı ve atağın nereden start aldığı gibi önemli bilgileri elde etmeye yardımcı olmaktadır.

***SIEM(Security Information Event Management)***



-Bir kurumda farklı yöntemlerle onlarca log kayıdı toplanmaktadır.Bu kayıtların tek bir merkez üzerinde toplanmasına ve bu toplanan loğlar üzerinden güvenlik analizleri yapılması işlemini SIEM olarak nitelendirebiliriz.

*Çalışma Mekanizması*

-Toplanan logların global bir formata dönüştürülür ve olayların saldırı tipine göre sınıflandırılması yöntemlerini kullanarak normalleştirme ve kategorilendirme adımlarını uygulanır.

-Bağımsız gibi görünen olayları birbiriyle bağlantılandırılır ya da olaylar datayla ilişkilendirilir.

-Yöneticilere mail, SMS veya SNMP mesajları ile bildirim veya alarm sağlanır.

-Toplanan veri ve korelasyon sonuçlarını gerçek zamana yakın bir ölçüde güvenlik uzmanlarına sunan izleme paneli sağlanır.Buradan takip edilir.

-SIEM ürünü tarafından toplanan verinin analiz aşamalarını kapsayan rapor üretilir.

***SIEM’in Önemi***

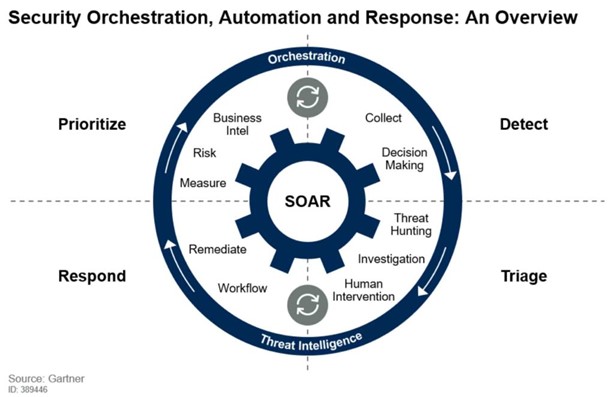
- SIEM ürünleri gerçek zamanlı raporlama ve güvenlik olayları analizi sağlayarak ağlara yönelik en son tehditleri tespit edebilme imkânını sunarlar.

- Uzaktan erişim noktalarının ve ağlara bağlanan cihazların sayısındaki artış ağlara sızma noktalarının da çoğalmasına neden olmaktadır. Bilişimciler ağın karşı karşıya kaldığı tehditleri algılayabilmek için birden fazla kaynaktan toplanan veriyi analiz etmek ve bunların sonucunda atılacak adımları kararlaştırmak durumundadırlar.

- SIEM ürünleri ağ geçidi, sunucular, güvenlik duvarları ve diğer kritik BT bileşenlerinin nasıl bir saldırı ile karşı karşıya kaldığı konusunda ayrıntılı rapor üretirler.

-Bu sayede sunucu çok rahat bir şekilde izlenip güvenliği sağlanabilir.

***SOAR(Security Orchestration,Automation and Response)***



-Sürekli artan tehditlere karşı ağda toplanan verilerin artması sonucunda elde edilen farklı ve büyük verilerin düzenlenmesi ve raporlanması zorlaşmaktadır.

-SOAR;veri çeşitliliğinin ve miktarının artması karşısında tehdit müdahele yeteneklerinin artmasını sağlamakta ve iş süreçlerini kolaylaştırmaktadır.Ayıca şüpheli davranışların algılanmasını kolaylaştırmakta ve cevap verme süresini azaltmaktadır.

-10 ve daha fazla elemanı çalıştığı NOC ve SOC ekiplerinin SIEM yanında SOAR da kullanma gerekliliği ortaya çıkmaktadır.

!!! SIEM olayların analizini yapıp sonuçları söylerken SOAR olayları anlayıp karşı hamle yapmaktadır.

***Cloud Computing (Bulut Bilişim)***

-Kullanıcıların yerel konumlarında yazılım,veri erişimi veya servis altyapısı gerekmeksizin alınacak ihtiyacın hizmet olarak sağlanmasıdır.

Bulut Bilişim hizmeti 3 şekilde sunulmaktadır.

-Infrastructure as a Service(IaaS)

-Platform as a Service (PaaS)

-Software as a Service(SaaS)

***Infrastructure as a Service(IaaS)***

-Bulut Bilişim’in e temel hizmetidir.IaaS ile sanal sunucu oluşturulup kullanıcılara bulut sunucu hizmeti sunulmaktadır.

-Bulut altyapısı ile sanal sunucu kaynakları size özel olarak tahsis edilir.Daha esnek altyapıya sahip olunur.

Örneğin;

-Tatil organize eden web sitelerinde tatil sezonlarının başlangıcına yakın sunucu kaynak ihtiyacı artar.Kullanılan kaynaklar,Bulut Bilişim’in esnek yapısından faydalanılarak istendiği zaman arttırılıp,azaltılabilir.

***Platform as a Service (PaaS)***

-Uygulama geliştiricilere donanım ve yazılım katmanları sunarak proje geliştirme imkanı sağlar.

-Bu hizmet sistem yönetimi,işletim sistemi,programlama dili ortamı,veri tabanı vs. gibi platformlar sunar.

-Sistem yönetimi hizmet sağlayıcı tarafından gerçekleştirildiği için siz sadece uygulamaları ve verileri yönetirsiniz.

Örneğin;

-PHP ile bir yazılım kodladınız.Kodladığınız yazılımın SQL ve Web sunucu altyapısı ile uğraşmak zorunda kalmazsınız.

-PaaS,sadece yazılımınızın çalışması gereken platformları sağlar.

***Software as a Service(SaaS)***

-Kullanıcıların ihtiyaç duyduğu finans,muhasebe vb. yazılımları gibi programları bulut üzerinde sağlar.

-Farklı lokasyonlarda faaliyet gösteren firmalar için SaaS ekstra yazılım maliyeti oluşturmayarak ciddi ekonomik avantaj sağlar.

-SaaS için en uygun örnek Gmail’dir.Google’ın sunduğu bu hizmet ile mail gönderebilir,dökümanlarınızı düzenyebilir ve dosyalarınızı yedekleyebilirsiniz.

-Yazılım bilginiz olmasa daha tüm işlemlerinizi gerçekleştirebilirsiniz.