



Websense®

## Web Güvenliđi Ađ Geçidi Çözümleri

Dinamik, etkileşimli Web 2.0 teknolojileri Web'i bir çekirdek faaliyet uygulaması platformuna dönüştürmüştür. Geleneksel müşteri ilişkileri ve bordro uygulamaları artık etkileşimli olarak Web üzerinden sağlanırken, toplumsal ağlar gibi uygulamalar günlük bazda işe alma, etkileşimli kılavuz oluşturma ve diğer faaliyet süreçlerinde kullanılmaktadır. Web 2.0 ile birlikte dinamik ve kullanıcı-oluşumlu içerik gibi oluşan yeni riskler virüs önleme ve URL filtreleri gibi geleneksel güvenlik teknolojilerinin yetersiz kalmasına yol açmaktadır. Bu teknolojiler Web 2.0 sitelerine gönderilen duyarlı veriler üzerinde yeterli kontrol sağlayamamaktadır.

Websense® Web Güvenliđi Ađ Geçidi Güvenli, modern Websense tehditlerine karşı en düşük edinme maliyetleri ile en iyi koruma sağlayan Ađ Geçidi piyasasını oluşturmuştur. Bunlar yüksek hız ve güvenilirlikte veri kaybı koruma ve birleştirilmiş hibrit ađ esaslı/tesis esaslı çözümler sağlayan tek yönetim kurulumlarıdır. Web Güvenliđi Ađ Geçidi çözümleri kuruluşları Websense gücü desteđini herhangi bir Web kötü niyetli yazılımlar, uygunsuz içerik veya duyarlı bilgilerin afişe edilmesi endişesi yaşamaksızın sağlamaktadırlar.

### Nasıl Çalışır

Web Güvenliđi Ađ Geçidi çözümleri kurumsal sınırlar içinden geçerken gelen ve giden içerikleri dinamik Web kötü niyetli yazılımlara karşı korur, duyarlı giden veri kayıplarını önler ve personel üretkenliğini artırır. Websense TruHybrid™ kurulumu kurum için aygıtlar yanı sıra aynı zamanda Hizmet olarak Güvenlik (SaaS) platformlarını desteklerken, tüm ortamı tek bir politika ve raporlama altyapısı üzerinden yönetir. Alternatif yaklaşımlardan farklı olarak, Websense müşterileri platformu tercih etmek veya birden fazla sistemleri yönetme maliyetine katlanmaksızın kendine özgün faaliyet gereksinimlerini en iyi karşılayacak platform karmasını seçme esnekliğine sahip olmaktadır.

Websense Web Güvenliđi Ađ Geçidi çözümleri şunları sağlar;

- **Giden Veri Kaybı Koruma ve Uyum Kontrolleri** – Bütünleşik yüksek hız ve güvenilirlikte veri kaybı koruma yazılım ve donanımı Web posta ve toplumsal ağlar gibi kurum dışı hedeflerle olan haberleşmelerin gerçekleştirilmesi için gerekli kontrolleri oluştururken, aynı zamanda duyarlı verilerin ifşa edilmesini denetleyen yasal uyumu da karşılar.
- **Kötü Niyetli Yazılım Koruma** – TRITON™ İleri Düzey Sınıflandırma Motoru (ACE) eski dosya esaslı saldırıların yanı sıra, geleneksel virüs önleyici çözümleri savuşturan kod esaslı saldırılara karşı da koruma sağlar.
- **Web 2.0 Çalışan Üretkenliđi** – TRITON İleri Düzey Sınıflandırma Motoru, geleneksel URL filtreleme çözümleri ile tam olarak sınıflandırılmayan karmaşık, dinamik ve şifre-korumalı Web sitelerinden gelen uygun olmayan içerikleri ayıklar.
- **En Düşük Toplam Sahip Olma Maliyeti** – Websense TRITON Konsolu ve TruHybrid kurulumu kuruluş bünyesinde desteklenmesi gereken cihaz, yönetim sistemleri ve müşteri çözümleri sayısını azaltır.
- **Tutarlı, Kurum-Çapında Güvenlik Kapsamı** – TruHybrid kurulumu tesis basında ve SaaS kurulumları politikalarını bir araya getirir. Kullanıcılar çalışmalarını ofis veya ev üzerinden yürüttüklerinde bu özgün politika sürekli devrede kalır.

“İlk 100 Web sitesinin yüzde 90'ı sosyal veya arama ağları olarak sınıflandırılmakta ve bunların yüzde 47'sinden fazlası kullanıcı-oluşumlu içerikleri desteklemektedir”

**Websense Security Labs™,  
2009**

“2009’un ilk yarısında, ilk 100 sitenin yüzde 80’inden fazlasında kötü niyetli içerik barındırmış veya yasal olmayan Web sitesi maskeli yönlendirmeleri bulaşmıştır.”

Websense Security Labs, 2009

### İleri Düzey Sınıflandırılmalı Motor

Websense Web Güvenliği Ağ Geçidi çözümleri içinde, gelen içerik incelemelerini giden veri kaybı koruma ile birleştiren en hassas\* iki yönlü güvenlik inceleme motoru olan, Websense TRITON İleri Düzey Sınıflandırma Motoru (ACE) yer alır. ACE geleneksel güvenlik uygulamalarını gelen ve giden içerik risklerini hassas biçimde sınıflandıran virüs önleme, URL filtreleme, itibarlı hizmetler ve parmak izi en son içerik sınıflandırma teknolojileri ile birleştirir. Websense ThreatSeeker® Ağ tarafından desteklenen İleri Düzey Sınıflandırma Motoru gerçek zamanlı tarama, gerçek zamanlı sınıflandırma ve hızlı ve güvenli veri kaybı koruma ile içerikleri ağ geçidinden geçerken inceler.

### Gerçek Zamanlı Güvenlik Tarama

Virüs önleme teknolojisi Web tehdit coğrafyasında hakim nitelikteki dinamik ve kod esaslı saldırılara tek başına karşı koyamaz. Websense için özel gerçek zamanlı güvenli tarama incelemeleri bu tür kötü niyetli içerikleri “sıfır gün” tehditlerini daha önceki saldırı veri tabanı başvurusu yapılmasına gerek kalmaksızın “anında” belirlemektedir.

### Gerçek Zamanlı İçerik Sınıflama

Çok yaygın olarak kullanılan sitelerin çoğunluğu geleneksel URL filtrelemeyi tam olarak sınıflayamaz. Örneğin, tek bir Google veya Facebook sayfası içine çok sayıda sınıflandırmaya özgü içerik elemanları karması yer alıyor olabilir ki, bu durum tek bir sınıf uygulamasını imkânsızlaştırır. Bunun sonucunda, çoğu kuruluşlar ayırım yapmaksızın değerli kaynakları engellemekte veya dinamik Websense hedeflerine tam erişime izin vererek kabul edilebilir kullanım politikası uygulamasını göz ardı etmektedirler.

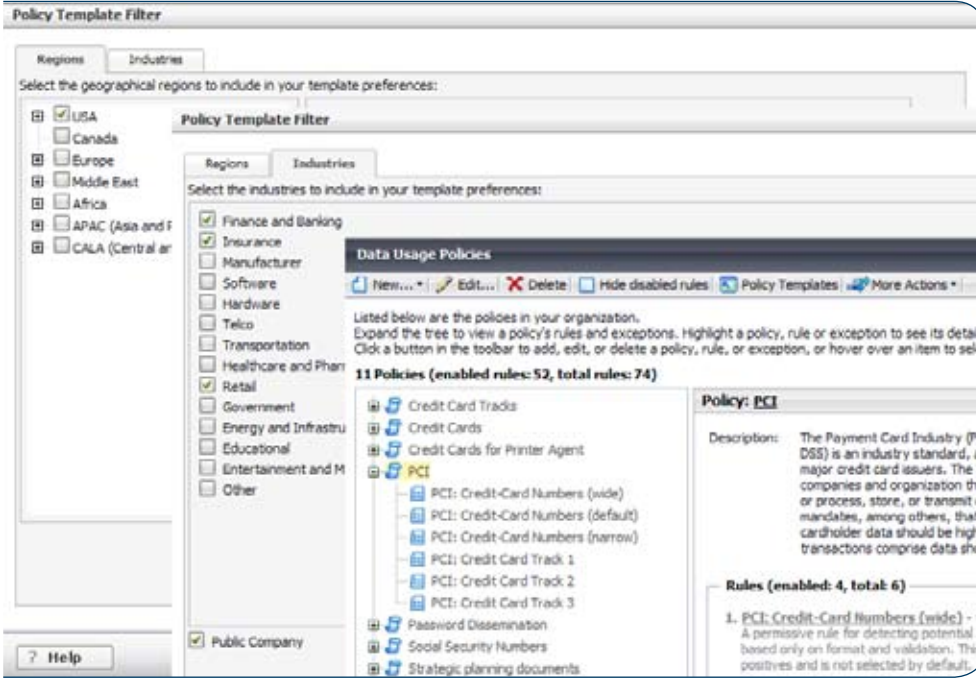
Web Güvenliği Ağ Geçidi çözümleri, her bir Web sayfası içindeki içerik elemanlarını anında sınıflayarak gerçek zamanlı içerik sınıflandırmayı dinamik Web 2.0 siteleri için kabul edilebilir kullanım politikalarını da içine alacak biçimde genişletebilmektedir. Bu politikaya aykırılık içinde olan herhangi bir içerik elemanı sayfadan ayıklanırken, uyumlu bilgilere izin verilmektedir. Bu özgün yetenek sayesinde üretkenlik sürdürülür ve kabul edilebilir kullanım politikası uyumu sağlanırken, Websense faaliyet hedeflerine geniş ölçekte erişim sağlanmaktadır.

### Yüksek Hız ve Güvenlikli Veri Kaybı Koruma Yazılım ve Donanımı

Bütünleşik yüksek hız ve güvenilirlikte veri kaybı koruma (DLP) yazılım ve donanımı Web posta ve toplumsal ağlar gibi kurum dışı hedeflerle olan faaliyet haberleşmelerin gerçekleştirilmesi için gerekli kontrolleri oluştururken, aynı zamanda duyarlı verilerin ifşa edilmesini denetleyen yasal uyumu da karşılar. DLP kapasitesi şifre inceleme ile sınırlı veya karmaşık üçüncü taraflar kurulumlarını gerektiren alternatif yaklaşımlardan farklı olarak Web Güvenliği Ağ Geçidi çözümleri http, https ve FTP ağ trafiği için piyasada öncü nitelikteki Websense DLP çözüm kapasitesini sağlamaktadır. Bunun içinde 800 ayrı yaratıcı politikalar, içerik inceleme için parmak izi uygulaması ve kapsamlı uyum raporlama yer almaktadır.

Web DLP ile Web Güvenliği Ağ Geçidi çözümlerinin bir araya getirilmesi özel, tek tek kurumların her birinde üçüncü taraflar için DLP donanımı gereksinimini ortadan kaldırarak toplam edinme maliyetini önemli ölçüde düşürür. Veri kaybı koruma için uzun vadeli planlara sahip kuruluşlar için Web DLP ayrıca kapsamlı yatırım koruma sağlamakta; bunun için basit bir yazılım güncelleme ile denetleme ölçeği içine Web ötesine geçerek diğer trafik tipleri (e-posta, IM, P2P) uç noktaları ve bekleyen veri (yani, veri tabanları, dosya paylaşımları, Alışveriş Paylaşım Noktası) katılmaktadır. Bu nedenle, kapsamın Web DLP’den diğer kanalları da içine alacak biçimde genişletilmesi ilave donanım gerektirmez. Mevcut politika ve altyapı yatırımlarına dokunulmaz.

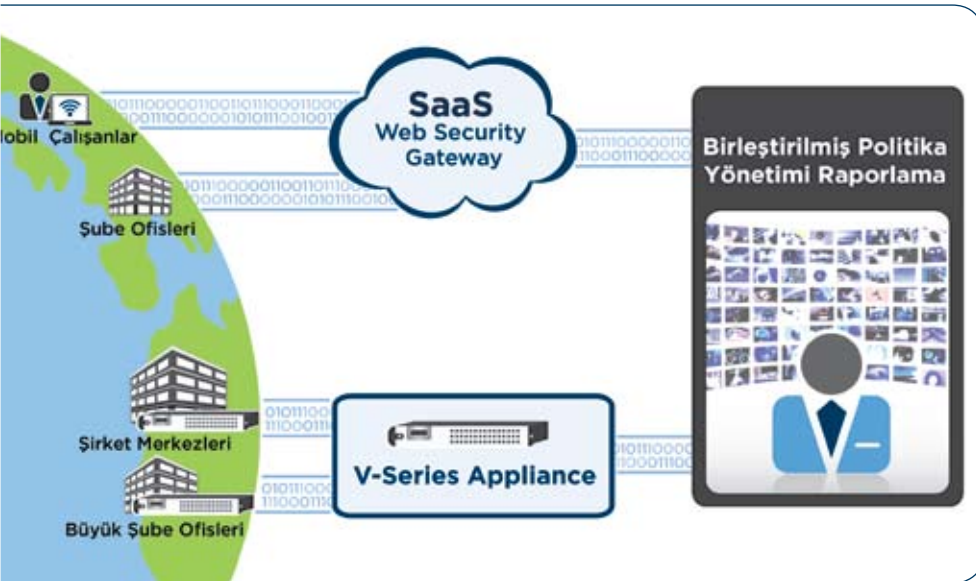
\* <http://www.websense.com/content/tolly-report-reg.aspx>



Basit DLP politika sihirbazları yöneticilere bölgesel ve sanayi-ölçeğinde yönetmelik gereksinimlerini karşılayan en iyi uygulama politikalarını çabucak tanımlama olanağı sağlar.

### TruHybrid Kurulumu

TruHybrid kurulumu, kuruluş içi ve SaaS kurulum platformları karması arasından bir seçim esnekliği sağlarken, aynı zamanda tüm çevre tek bir birleştirilmiş yönetim sistemi ile yönetilebilir. Böylelikle güvenlik SaaS platform desteği ile şube ofislerine veya mobil kullanıcılarını içine alacak biçimde genişletilebilir. Aynı zamanda kurumsal, büyük şube veya diğer veri merkezi yerleşimlerinde yüksek randımanlı aygıt konuşlandırılabilir. SaaS karması veya seçilen aygıt seçeneğine bağlı kalmaksızın, bir yerde tek bir kurumsal politika tanımlanabilir. Böylesi birleştirilmiş bir yaklaşım, sadece hibrit tesis-bazlı/SaaS kurulumları yönetim maliyetini azaltmakla kalmaz, aynı zamanda tüm ortam içinde tutarlı güvenlik kapsamı garanti eder.



TruHybrid kurulumu tesis-bazlı/SaaS kurulumları yönetimini tekleştirir.

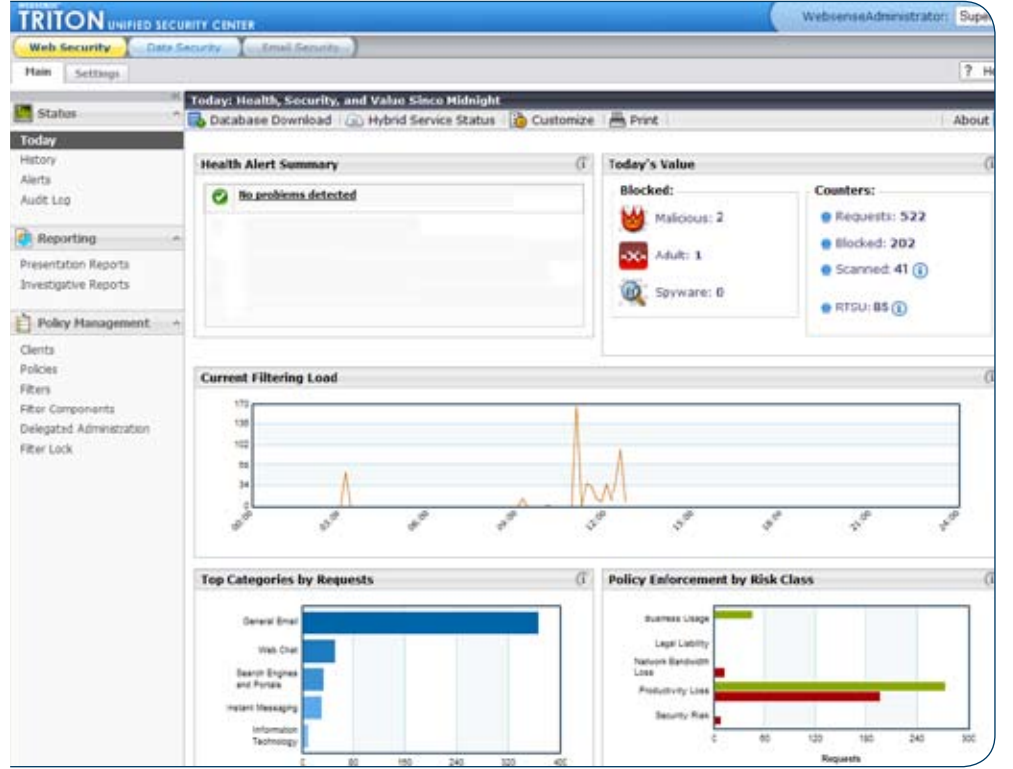
“Websense V10000 TM garantili Web ağ geçidi aygıtı sayesinde hemşirelerimiz gerek duyduğu bilgileri güvenle ve garantili nitelikte edinmelerini mümkün kılıyor. Gerçek zamanlı tarama ve Internet kullanımı doğrultusunda esnek politikalar oluşturma kapasitesi sayesinde saha hemşirelerimiz hakkında artık veri çalmaya yönelik kötü niyetli yazılımlarla yüklü Web sitesi ile yüz yüze gelme veya gizli hasta verilerinin yanlışlıkla hatalı yerlere gönderilmesi endişesi duymuyorum.”

### Larry Whiteside

Baş Güvenlik Sorumlusu  
Visiting Nurse Service  
of New York

“Kötü niyetli Web saldırılarının yüzde 57’si veri çalma yazılımlarından oluşur.”

Websense Security Labs, 2009



TRITON Konsolu etkileşimli paneli, tehdit ve politika ihlali faaliyetlerini anında belirleyebilmektedir.

### SSL Görsellik ve Kontrolü

Artan SSL trafik kullanımı esli URL filtreleri için kör noktalar oluşturmakta ve tehdit ve veri kaybı şifre baypas tekniklerini açığa çıkartmaktadır. Web Güvenliği Ağ Geçidi çözümleri SSL trafik üzerinde görsellik ve kontrol sağlayarak kuruluşlara bütün Web haberleşmelerinde politika uygulamalarına olanak vermektedir.

### İleri Düzey Uygulama Kontrolleri

IM ve P2P gibi ağ uygulamalarının artışı kırıclara faaliyetleri engelleme ve gizli verileri çalma olanakları verir. Web Güvenliği Ağ Geçidi çözümleri, risklerin azaltılması ve yetkisiz uygulamalardan kaynaklanan veri kaybı koruma için 125'in üzerinde ağ protokol ve binlerce uygulamayı kontrol eder. Politika uygulamaları basit uygulama engellemeden yüksek granüle bant genişliği kontrollerine uzanmaktadır.

### Birleştirilmiş İçerik Güvenlik Yönetimi ve Raporlama

Web Güvenliği Ağ Geçidi çözümleri ile birlikte temin edilen ve sadece Websense üzerinden elde edilebilir bir başka özellik ise TRITON Konsoludur. Bu bütün Websense Web, veri ve e-posta güvenlik çözümlerini tek bir Websense-esaslı arayüz içinde bir araya getirir. Yaratıcı paneli içinde 55'in üzerinde hazır raporlar ve kapsamlı özelleştirme özellikleri yer almakta ve böylelikle kullanıcı faaliyetlerinin açığa çıkartılması, arıza giderme uygulaması ve ilave risk azaltma olanakları sağlanmaktadır. Kapsamlı sondaj özellikleri, politika sihirbazları, yapılandırma şablonları, bir alt-sistem programlama ve otomatik içerik güncelleştirme gibi çeşitli kullanımı kolay özellikler sayesinde rakip çözümlere kıyasla idari iş yükü ve maliyet büyük ölçüde düşürülmektedir. İçerik güvenlik gereksinimleri zaman içinde Web güvenliğinin ötesine geçerken, TRITON konsolu birleşik yönetim özelliği, rahatlıkla e-posta ve komple DLP yönetimini merkezi olarak yürütülecek biçimde genişletilebilmektedir.

Özellikler	Yararlar
TruHybrid Kurulumu	Toplam edinme maliyetini azaltır ve tüm kuruluş bünyesinde ödünsüz birleşik yönetim ve SaaS kurulumları aracılığı ile tutarlı politika uygulamasını garanti eder.
Yüksek Hız ve Güvenlikli Veri Kaybı Koruma Yazılım ve Donanımı	Giden içerik veri kayıplarını önler ve gerekli yasal uyum kontrolleri gerçekleştirir. Karmaşık DLP kurulumlarından kaçınarak toplam edinme maliyetini düşürür.
Gerçek Zamanlı İçerik Sınıflama	Dinamik, şifre korumalı ve karma içerikli Web özellikleri kullanımını "anında" Web içerik filtreleme ile garanti eder.
Gerçek Zamanlı Güvenlik Tarama	Kuruluşları dinamik, kodlu ve bilinmeyen tehditleri "anında" teşhis ederek Web kötü niyetli yazılımlara karşı korur.
TRITON Konsolu	Birleştirilmiş Web, veri ve e-posta güvenlik çözümleri ile, toplam edinme maliyeti ve satıcı yönetim maliyetlerini düşürür.
Bütünleşik Virüs Önleme	Dosya esaslı virüs saldırılarını üçüncü taraflar ve ileri düzey Websense Web virüs önleyicileri kullanarak engeller.
İleri Düzey İtibarlı İnceleme ile Öncü Web Filtreleme	Asgari düzey kabul edilebilir kullanım politikasını etkinleştirir ve bilinen kötü niyetli siteleri engeller. Çok noktalı itibarlı inceleme bağlamında varlık tipi, sözcük itibarı, Web 2.0 postaları, URL sınıfı, en yakın komşu, arama itibarı, tarih, yaş ve coğrafya unsurları yer alır.
ThreatSeeker Ağı Gerçek Zamanlı Güncelleme	Her beş dakikada bir yapılan güvenlik güncellemeleri ile yeni ortaya çıkan tehditleri azaltır.
SSL Görşelliği	Şifreli Web trafiğinin SSL biçim ve bütünleşik sertifika yönetimi aracılığı ile incelenmesine olanak verir.
Uygulama Kontrol	Ağ protokolleri ve uygulamalarının yönetici kullanımı sayesinde riskleri azaltır, üretkenliği artırır ve bant genişliği maliyetinin düşürür.
Hızlı ve Güvenli Web Yardımcı/ Ön Bellek	Optimum trafik sağlayarak randımanı artırır ve bant genişliği maliyetini düşürür. Saydamlık ve açık yardımcı yapılandırmaları destekler.
Esnek Kullanıcı Yetkilendirme	Aktif Dizin, LDAP, RADIUS, Novell, NTLM v2. aracılığı ile esnek yetkilendirmeli kullanıcı ve grup-esaslı politikalara olanak sağlar.
Yüksek Bulundurma ve Yük Dengeleme	WCCP veya harici yük dengeleyicileri desteği ile sistem yedekleme ve büyük kuruluş ölçekleme imkânı verir.

Gartner tarafından en son Güvenli Ağ Geçidi için yapılan Sihirli Çeyrek sınıflamasında Websense öncü çeyrek sınıflaması içinde değerlendirilmiştir.

**Gartner, Inc.**

"Magic Quadrant for Secure Web Gateway"\* yazan Peter Firstbrook ve Lawrence Orans Ocak 8, 2010

**Websense, Inc.**  
San Diego, CA USA  
tel 800.723.1166  
tel 858.320.8000  
www.websense.com

**Websense UK, Ltd.**  
Reading, Berkshire UK  
tel 0118.938.8600  
fax 0118.938.8697  
www.websense.co.uk

<b>Australia</b> websense.com.au	<b>Italy</b> websense.it
<b>Brazil</b> websense.com/brasil	<b>Japan</b> websense.jp
<b>Colombia</b> websense.com/latam	<b>Malaysia</b> websense.com
<b>France</b> websense.fr	<b>Mexico</b> websense.com/latam
<b>Germany</b> websense.de	<b>PRC</b> prc.websense.com
<b>Hong Kong</b> websense.cn	<b>Singapore</b> websense.com
<b>India</b> websense.com	<b>Spain</b> websense.com.es
<b>Ireland</b> websense.co.uk	<b>Taiwan</b> websense.cn
<b>Israel</b> websense.com	<b>UAE</b> websense.com

## Kurulum Platformu Bulundurma

Tesis basında kurulumlar Websense V-Series™ aygıtları veya genel maksatlı servis sağlayıcılar üzerinde çalışan yazılım ile sağlanmaktadır. SaaS kurulumları Websense İçi Web Güvenliği Ağ Geçidi çözümü ile desteklenir.

- **V-Serisi Cihazlar** V-Serisi uygulamalar hızlı ve güvenli randıman, güvenilirlik ve tesis bazında kurulum için basit uygulama olanağı sağlarlar. Fortune 100 ortamı ile kanıtlanmış V-serisi cihazları, bileşen-düzeyinde bütünlük yedekleme yanı sıra, aynı zamanda yük dengeleme ve yüksek bulundurma özellikleri yanı sıra bir dizi kuruluş yapılandırma özelliklerini de destekler. V-serisi cihazlar ayrıca donanım yükseltme gerektirmeksizin, mevcut platform ömrü ve değerini yükselten gelecek Websense çözümlerini desteklemek için tasarlanmıştır.
- **Hosted Web Security Gateway** Websense Bütünlük Web Güvenliği Ağ Geçidi çözümleri güvenlik inceleme süreçlerini 10 ayrı "ağ içi" konuşlandırılmış küresel erişilebilir ve yedek veri merkezlerine kaydırmaktadır. Bu SaaS sağlama modeli sadece kurulumu hızlandırmakta kalmamakta, aynı zamanda her bir lokasyonda tesis bazlı donanımı destekleme gerekliliğini ortadan kaldırarak işletme maliyetlerini önemli ölçüde azaltmaktadır. Websense veri merkezleri ISO 27001 sertifikalıdır ve kuruluş bazlı ve özellikle uzak konumdaki ofisler gibi bireysel kuruluşlar için aşırı maliyetli olacak kesin güvenlik ve bulundurma standartlarını tek başına karşılamaktadır. Bağımsız ve salt SaaS içeren çözümler geliştirildiğinde, Websense Bütünlük Web Güvenliği Ağ Geçidi SaaS e-posta güvenliği bütünlükte ilave yarar sağlamaktadır.



Websense V10000™ Cihazı

## Websense Web Güvenliği Ağ Geçidi Çözümleri Seçenekleri

**Websense Web Security Gateway Anywhere** — TruHybrid tesis bazlı\*/SaaS yönetimi, hızlı ve güvenli veri kaybı koruma veya Websense Uzak Filtreleme müşterisi gerektiren kurulumlar için

**Websense Web Security Gateway** — Tesis bazlı\* kurulumlar için

**Websense Hosted Web Security Gateway** — SaaS kurulumlar için

Yazılım Kurulumları için Asgari Servis Sağlayıcı Gereksinimleri:

**İşletim Sistemi**  
Red Hat Linux v4,  
Sürüm 5\* veya Windows Server 2003/  
Server 2008†  
CPU: 2 x İki çekirdekli 2.8GHz işlemci  
**Bellek**  
4GB RAM

**Sabit Disk Sürücü**  
İki fiziki disk:  
\* 100GB, OS ve uygulama ve geçici veriler için,  
100GB ön bellek\* için  
\* 100GB (önerilen RAID 1)†  
**Ağ arayüzleri**  
İki x 10/100/1000 Ethernet arayüzleri

\* Tesis basında kurulumlar Websense V-Series™ cihazları veya genel maksatlı servis sağlayıcılar üzerinde çalışan yazılım ile sağlanmaktadır.

†Sihirli Çeyrek - The Magic Quadrant, özel bir dönem için piyasa grafik gösterimidir. Gartner tarafından tanımlanan bir piyasa içinde belli satıcılarla ilgili ölçütler bazındaki değerlendirmeler ile ilgili Gartner incelemelerini yansıtır. Gartner, sözü edilen Sihirli Çeyrek içinde yer alan herhangi bir satıcı, ürün veya hizmet ile ilgili herhangi bir garanti vermediği gibi, "Öncü" çeyrek içinde yer alan satıcılarla ilgili teknoloji kullanıcılarına herhangi bir öneride bulunmaz. Sihirli Çeyrek sadece bir araştırma aracıdır ve belli bir girişim için yol gösterici nitelik taşımaz. Gartner işbu çerçevede verdiği beyan doğrultusunda, bu araştırma ile ilgili hiçbir açık veya zımni garanti vermediğini ve buna belli bir ticari veya bir amaca uygunluk garantisinin dahil olduğunu ifade eder.

Websense Web Güvenliği özet ürün gösterimleri veya bedelsiz değerlendirme için, bkz: [www.websense.com/evaluations](http://www.websense.com/evaluations).