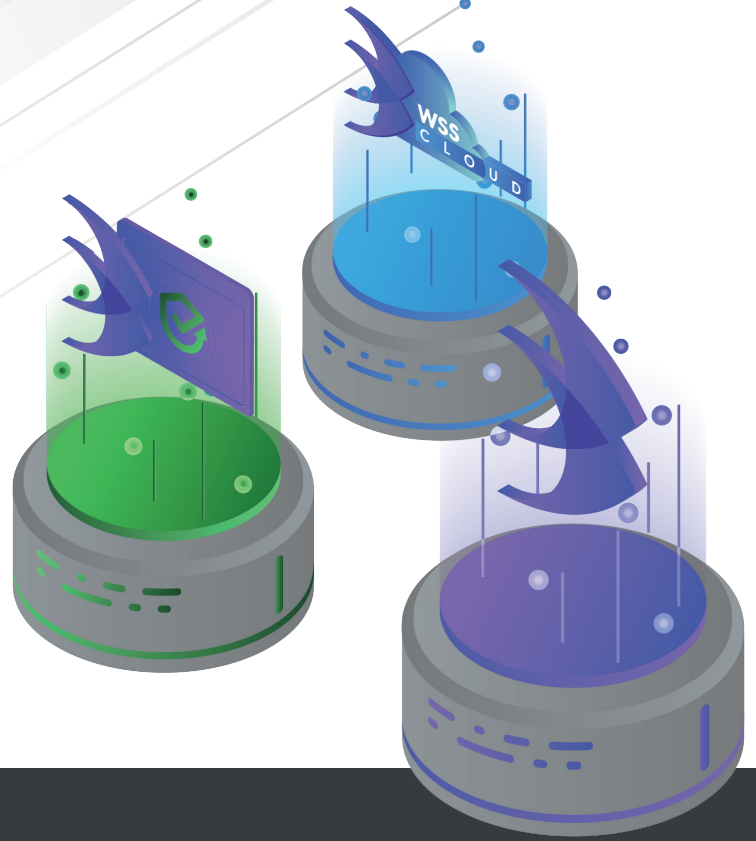


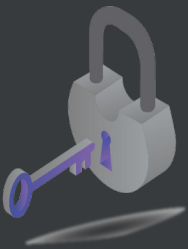


## WEB SUNUCULARI VE VM KULLANICILARI İÇİN KAPSAMLI GÜVENLİK ÇÖZÜMLERİ



**KESİNTİSİZ HİZMET VE KAPSAMLI GÜVENLİK İÇİN WEB GÜVENLİĞİNİZİ WSS İLE GÜÇLENDİRİN**

Gerçek Zamanlı Tespit - Bildirim - Karantina - Restorasyon Eylemleri



- ✓ APT Saldırılarına Karşı Savunma
- ✓ Web Kabuğu ve Kötü Amaçlı Yazılım Yükleme Saldırılarına Karşı Savunma
- ✓ Kişisel Bilgi Tespiti (KVKK)
- ✓ Dosya Değişikliği Önleme
- ✓ Web Sitesi Sahteciliği Anında Tespit & Restorasyon



## Gerçek Zamanlı Web Sunucusu Güvenliğinin Önemi

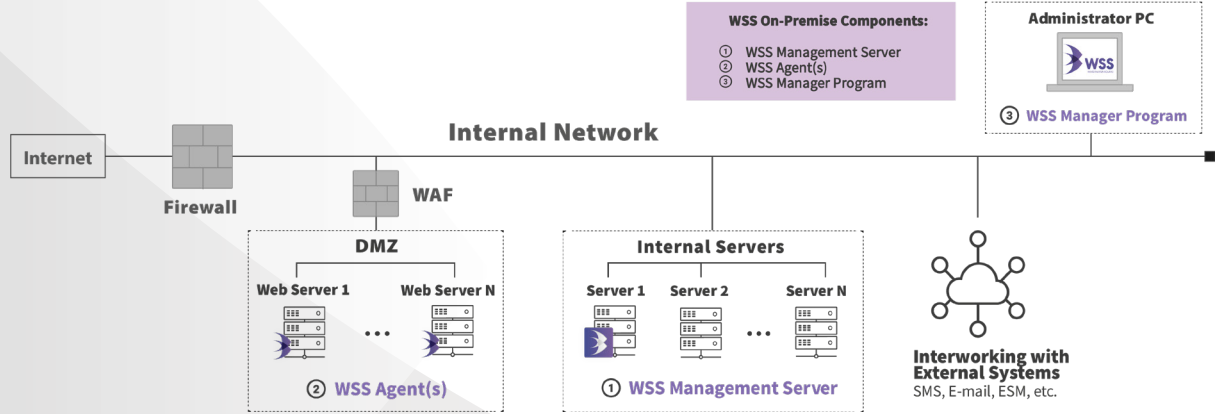
Her geçen gün çeşitlenen saldırı yöntemlerine karşı sadece ağ güvenlik çözümleri, ağızdan sızan web shell (web kabuğu) yüklemeleri ve kötü amaçlı kod/URL kullanılan saldırılara karşı savunmada yetersizdir.

- İzinsiz giriş yöntemlerinin çeşitlenmesi nedeniyle ağ savunmasının yetersiz kalması (sistem içerisindeki web sunucuna yüklenen web kabukları veya kötü amaçlı kodları gerçek zamanlı olarak tespit etme/karantinaya alma ihtiyacı oluşturmaktadır)
- Çeşitli ve farklı biçimlerde web kabuğu yükleme yöntemlerine karşı savunma (yetersiz kalıp eşleştirme ve filtreleme) sadece ağ güvenlik cihazları ile mümkün değildir
  - Bilinmeyen/kodlanmış/şifrelenmiş/gizlenmiş/dönüştürülmüş/parçalara bölünmüş web kabukları veya kötü amaçlı kodlar
- Sistemi yavaşlatan ağ güvenlik cihazlarının uyguladığı filtreleme, kalıp eşleştirmedeki zorluk
- Güncelleme, tam denetimde aşırı yük
- Sadece dışarıdan gelen saldırılar değil, dahili çalışanların da neden olduğu güvenlik riskleri
- Ağ atlama (bypass) yöntemleri ile artan penetrasyon

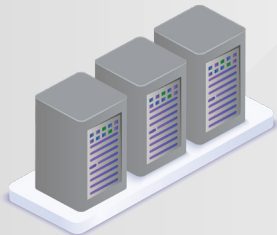
## Gerçek Zamanlı Güvenlik Çözümü WSS İle Web Tabanlı Verilerinizi Kapsamlı Koruyun

Entegre ve arttırıcı çözüm olan WSS, ağın zayıf noktalarından geçen ve saldırılara zemin oluşturmaya hazırlanan kötü amaçlı URL/kodlar veya web kabuklarını sisteminizde tespit ederek, saldırı anında bile henüz hiçbir saldırı hasarı veya veri hırsızlığı gerçekleşmeden önlem almanızı sağlar. Böylelikle WSS, güvenlik önlemlerinizi tam olarak kapsayarak, web sunucunuz ve web tabanlı verilerinizi korurken web hizmetlerinizi kesintiye uğratmaz.

### WSS On-Premise Configuration:



### WSS, 3 Katmanlı Yapıdan Oluşur;



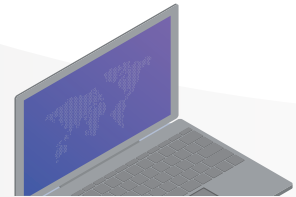
#### WSS SUNUCUSU

- Web kabuğu tespit bilgileri depolama
- Uzaktan yönetim kontrolü
- Web kabuğu kalıp güncelleme
- Aracı dağıtım işlevleri
- VM veya donanıma yüklenerek çalışma



#### WSS TESPİT ARACISI

- Web kabuğu ve kötü amaçlı URL tespiti
- Kişisel bilgi tespiti
- Tespit ve filtreleme sonuçlarını sunucuya iletme
- JDK 1.5 tarafından desteklenen tüm işletim sistemleriyle uyumluluk



#### WSS YÖNETİCİSİ

- Tespit işlevi ve çalıştırma
- İzleme, uzaktan eylem, ortam ayarı işlevleri
- Kullanıcı yönetimi, istatistik ve raporlama
- Güvenlik kontrol ve işletim bilgisayarı üzerine kurulum

# ÜRÜNLERİMİZ

## WSS On-Premise

Şirket içi ortamlarda web sunucularındaki web tabanlı verileri korumak ve kesintisiz hizmet sağlayabilmeniz için saldırıları gerçek zamanlı olarak tespit ederek anında yanıt veren kapsamlı web güvenlik çözümü

## WSS Cloud

Bulut bilişim (VM) kullanıcılarının web tabanlı verilerini korumak ve kesintisiz hizmet sağlayabilmeniz için saldırıları gerçek zamanlı olarak tespit eden ve anında yanıt veren kapsamlı sanal ortam güvenlik çözümü

## WARSS

Web sitelerine yapılan tahrifat, kaynak kodu ve içerik sahteciliği gibi saldırılara karşı itibar kaybı veya hasara uğramadan önce saldırıları tespit ederek değiştirilen web sunucusu orijinal kaynaklarını gerçek zamanlı olarak geri yükleyen web sitesi güvenlik çözümü



## WSS GERÇEK ZAMANLI KAPSAMLI GÜVENLİK PAKETİ

### Web Shell (Web Kabuğu) Saldırı Savunması

Güvenlik açıklarını geçtikten sonra sisteme yüklenmeye çalışılan tehlikeli web kabuklarını (ASP, JSP, PHP, CGI, Python vb. oluşan komut dosyası) tam algılama ve gerçek zamanlı algılama yöntemleriyle izleme, tespit, karantina, istisna işleme, yetkili bilgilendirme vb. gibi işlevleri sağlar ve istatistik raporu oluşturur.

### İzinsiz Önemli Dosya Değişikliği Önleme

Bir bilgisayar korsanı web sunucusu ayarlarındaki dosya kurcalama yoluyla sistemde yeni bir güvenlik açığı oluşturarak bir sonraki saldırısı için zemin hazırlayabilir. WSS, web sunucusu içerisindeki yapılan bir değişikliği gerçek zamanlı olarak tespit eder, değiştirilen dosyaları orijinaline anında geri yükleyerek kapsamlı savunma sağlar.

### Kişisel Bilgi Tespiti (KVKK)

Web sunucularındaki dosya içeriklerini gerçek zamanlı olarak izleyerek, kişisel bilgileri dosyalarda veya veritabanında (PDF, HWP, DOC, PPT, EXCEL, TXT vb.) tespit eder ve anında yetkiliye raporlar.

### Web Sitesi Sahtecilik Çözümü

Web sitesi tahrif saldırıları, web sunucusu kaynak kodu ve veri hırsızlığı, dijital içerik (videolar, resimler vb.) değiştirme/sahteciliği gibi itibara zarar veren saldırılara karşı, kurum ve kuruluşları henüz maddi/manevi zarara uğramadan savunma sağlamak için web sitesinin orijinal kaynaklarını (kaynak kodu, veri, içerik) gerçek zamanlı olarak izler, saldırıları tespit ettikten sonra anında orijinal haline geri yükleyerek restorasyon ve rapor işlevi sağlar.

### Kötü Amaçlı URL Yükleme Saldırı Savunması

Kötü amaçlı kod/URL'leri tespit etmek ve raporlamak için tam algılama ve gerçek zamanlı algılama teknikleri kullanılır. Tespit edilen karantina, kısmi karantina, istisna işleme işlevleri sağlarken tespitleri siyah/beyaz/gri liste halinde sınıflandırır ve raporlar.

### Yapılandırma Ayarları Değişikliği Önleme

Bilgisayar korsanının rastgele veya kötü amaçlı olarak web sunucusu yapılandırma dosyalarına yapılan değişiklikleri tespit eder ve anında yöneticiye bildirir. Web sunucusu/WAS günlüğü (log) analiz ederek tespit edilen saldırgan IP'sini yöneticiye raporlar.

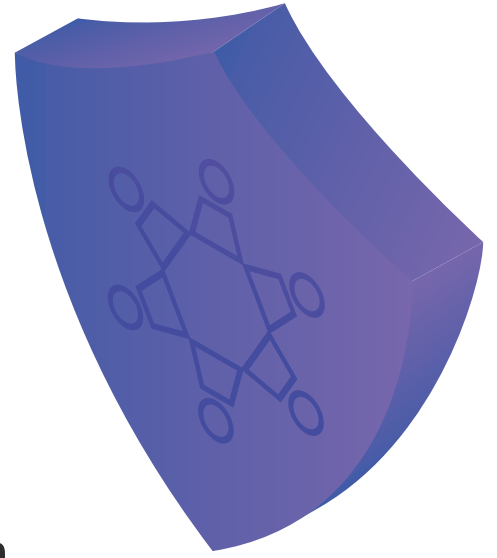
### Bulut Bilişim (VM) Güvenliği

WEB/WAS hizmeti Scale IN/OUT ölçeği, tespit/değişiklik/silme, otomatik kayıt işlemleri, Docker konteyner desteği, ana dizin otomatik tespit, olay çoğaltma yönetimi, geçmiş yönetimi, güvenlik yönetimi ve dahasını destekler.

### WSS Yönetim Özellikleri

Kolay güncelleme, yetki yönetimi, harici sistem ile birlikte çalışma (SYSLOG, SMTP, API/ ESM/SIEM/SMS/EMAIL vb. gibi), hedef dizin otomatik tespit ve yedekleme, yetkisiz uzantı filtreleme, kaynak kullanım ayarlama (CPU/bellek), çift yönlü kullanma desteği (aktif/aktif), uzaktan kimlik doğrulama gibi çeşitli yönetim işlevleri ve dahasını sağlar.

# Güvenlik Zinciri Ancak En Zayıf Halkası Kadar Güçlüdür



WSS ile Web Güvenliğinizi Tamamlayın

## Bizi Tercih Eden Müşterilerimiz

UMV ürünleri, işletmeler, medikal şirketler, devlet kurumları, telekomikasyon şirketleri, finans kurumları, güvenlik kontrol şirketleri, internet veri merkezleri gibi kurum içi veya bulut bilişim ortamlarında kullanıma uygundur.

AhnLab

HYUNDAI  
MOTOR GROUP

amazon  
web services

SAMSUNG  
ELECTRONICS

TOYOTA

LOTTECARD

STARBUCKS

BC CARD

SAMSUNG CARD

Hyundai Capital

Seoul Metro

KDB Bank

SEOUL METROPOLITAN  
GOVERNMENT

CHEONG WA DAE  
THE REPUBLIC OF KOREA

Ministry of Foreign Affairs  
Republic of Korea

SAMSUNG  
SAMSUNG SDS

gabia.

SK securities

SK telecom

K data  
Korea Data Agency

Seoul Design  
서울디자인재단

S-OIL Corporation

Hi Seoul  
SOUL OF ASIA

SUPREME COURT  
OF KOREA

cafe24

LOTTE  
DUTY FREE

ROBOTS

NH Bank

SK infosec

kt

iMBC

YTN

PANTECH

AMOREPACIFIC

JOSUN  
HOTELS & RESORTS

BOANNEWS

KORAIL

Prudential

KBS Media

dun & bradstreet

daiso  
다이소

GS

DAEWOO E&C

SHINSEGAE

Hansol

Hanwha

Gmarket

Ministry of National Defense  
Republic of Korea

CJ CHEILJEDANG

AUCTION.

umv

www.umvwebsecurity.com

Polat İş Merkezi, Mecidiyeköy Mahallesi Cemal Sahir Sokak

No:29/32, Şişli/İstanbul, Turkey

+90 212 266 21 88