

— WEB GÜVENLİĞİ VE BARINDIRMA YÖNETİMİ

DocMon – WAF Korumalı Barındırma Paneli

Tüm siteleriniz tek panelde, WAF kalkanının arkasında

DocMon, CloudPanel ve Docker üzerinde çalışan çok siteli barındırma ortamını ModSecurity v3 + OWASP CRS 4 WAF ile korur. Site ekleme, SSL, yedekleme, IP erişim kuralları, otomatik IP yasaklama ve insan doğrulamasını tek bir web panelinden yönetirsiniz.

ÖNE ÇIKANLAR

01

Katmanlı WAF

OWASP CRS 4 üzerine Log4Shell, webshell, PHP-CGI ve güncel WordPress açıklarına karşı 18 özel kural.

02

Otomatik IP Yasaklama

WAF kayıtlarında eşiği aşan IP'ler güvenlik duvarında engellenir; tekrar edenlerde süre artar.

03

İnsan Doğrulaması

Cloudflare Turnstile ile site veya yönetim yolu bazında bot filtresi; güvenilir IP'ler muaf tutulabilir.

04

Yapay Zekâ Destekli İnceleme

Siteleri tarar, öncelikli öneriler sunar; uygun bulgular tek tıkla ve geri alma güvencesiyle uygulanır.

KİMLER İÇİN

Onlarca müşteri sitesini tek sunucuda barındıran ajans ve barındırma firmaları

WordPress sitelerini brute-force, xmlrpc ve güncel exploit saldırılarından korumak

Kurum içi API ve SOAP servislerini reverse proxy arkasında WAF ve IP listesiyle yayınlamak

Yönetim panellerini insan doğrulaması ve ülke bazlı IP kısıtıyla kapatmak

Özellikler 89 ÖZELLİK

Aşağıdaki liste ürünün mevcut sürümünde çalışan özellikleri modül modül gösterir.

WAF Motoru ve Kural Seti 13

- ModSecurity v3 web uygulama güvenlik duvarı, sunucudaki tüm sitelerin önünde global çalışır
- OWASP CRS 4.x ve 18 Marta özel kuralı: SQL enjeksiyonu, XSS, izin geçişi, uzaktan kod çalıştırma koruması
- .git, .env, .svn, .ssh gibi gizli dosya ve dizinlere erişimi engeller
- Yedek/geçici dosyalar (.bak, .sql, .swp) ve yapılandırma sızıntıları (wp-config, web.config) engellenir
- sqlmap, Nikto, Nmap, WPScan, Nuclei gibi bilinen tarama araçlarını engeller
- Log4j/JNDI (CVE-2021-44228) ve PHP-CGI argüman enjeksiyonu (CVE-2024-4577) denemelerini engeller
- WordPress wp2shell açığına (CVE-2026-63030) karşı uç nokta, imza ve işaretçi kuralları
- Webshell uzantıları ve /shell.php, /cmd.php gibi webshell yolu taramalarını engeller
- TRACE, DEBUG, CONNECT, PROPFIND gibi tehlikeli HTTP metodlarını reddeder
- Boş User-Agent, hatalı Host başlığı ve aşırı parametre içeren istekleri reddeder
- WordPress xmlrpc.php kapatılır, referer'sız wp-login denemeleri işaretlenir
- Sunucuyu yoran agresif web örümceklerini engeller
- Engellenen ziyaretçiye markalı WAF engelleme sayfası gösterilir

WAF Yönetimi 7

- Site başına üç mod: Korum (engelle), İzle (yalnız kayıt), Kapat
- Seçili sitelerde WAF'ı toplu açma, kapatma veya izleme moduna alma
- Yanlış pozitifler için site bazlı veya global kural ID istisnası
- Belirli URL'leri WAF denetiminden muaf tutma veya tamamen engelleme
- CRS kural kataloğu: kategoriler, kategori başına kural sayısı ve paranoya seviyesi
- API modu: servisler arası sitelerde yanıt bloklaması kapanır; yanıt bloğu görülünce panel tek tıkla önerir
- Her değişiklikte yapılandırma testi; hata olursa ayar otomatik geri alınır

Saldırı Olayları, Oto-Ban ve IP Yasakları 10

- Ataklar / Olaylar ekranı: site bazında engellenen ve izlenen istekler, kural, IP ve istek ayrıntısı
- Olaydan tek tıkla IP yasaklama veya bir kuralı tetikleyen tüm IP'leri toplu yasaklama
- Oto-ban: ayarlanabilir pencerede WAF eşliğini aşan IP'ler güvenlik duvarında otomatik engellenir
- Hız limitine (429) sürekli takılan IP'ler de otomatik yasaklanır
- Artan ban süresi: 2 sa, 6 sa, 12 sa, 24 sa, ardından kalıcı
- Cloudflare ve iç ağı IP aralıkları hiçbir zaman otomatik yasaklanmaz
- Elle IP yasaklama ve kaldırma; yasak geçmiş kaynağı ve tarihle tutulur
- URL'den IP listesi besleme; kaynaklar her 3 günde bir otomatik yenilenir
- 15 günü geçen geçici yasaklar ayda iki kez otomatik temizlenir; kalıcılar korunur
- fail2ban ile SSH ve panel girişine brute-force koruması, artan ban süresi

Trafik Koruması ve İnsan Doğrulaması 9

- Site başına hız limiti: saniyedeki istek ve burst değeri
- Cloudflare arkasındaki sitelerde hız limiti gerçek ziyaretçi IP'sine göre uygulanır
- Arka uç aşırı yüklendiğinde markalı "yoğunluk" sayfası (flood guard)
- Tüm siteler için markalı 403, 404 ve 429 hata sayfaları
- Cloudflare Turnstile ile tüm siteyi insan doğrulamasının arkasına alma
- Yalnızca belirli yolları (ör. yönetim girişi) doğrulamayla koruma
- Doğrulan ziyaretçi imzalı çerezle bir süre tekrar sorulmadan geçer
- Güvenilir IP/CIDR listesi (IPv4 ve IPv6) doğrulamadan muaf tutulur
- Toplu taramada bulunan korumasız giriş panellerine tek tıkla Turnstile

IP Erişim Listeleri 5

- Site başına izin listesi (yalnız izinliler girer) veya engel listesi modu

- Tekil IP veya CIDR kuralı ekleme, açıklama ile; toplu yapıştırarak ekleme
- Hazır listeler: Cloudflare, Türkiye, Googlebot, Bingbot, arama motorları
- Özel URL'den IP listesi çekme ve yenileme
- Yol bazlı ACL: yalnızca belirli dizinler için ayrı izin/engel kuralları

Güvenlik Taraması ve AI Asistan 9

- Detaylı site taraması: canlı XSS, SQLi, izin geçişi ve RCE testleriyle WAF'ın gerçekten engellediği doğrulanır
- Taramada hassas dosya, izin listeleme, açık yönetim paneli, çerez bayrağı ve TLS kontrolü
- Tüm siteleri paralel tarayan toplu güvenlik raporu
- Bulgulara tek tıkla düzeltme: HSTS ve diğer güvenlik başlıkları, CSP, Secure/HttpOnly çerez, WAF koruması
- Hazır CSP profilleri: temel, WordPress, tek sayfa uygulama
- AI güvenlik incelemesi: tüm siteler için öncelikli öneriler ve tek tıkla "Fixle"
- AI asistan: doğal dilde WAF komutu verilir, işlem onaydan sonra çalışır
- Günün WAF olaylarının AI ile Türkçe özeti
- AI sağlayıcısı seçimi: Anthropic Claude veya yerel Ollama modelleri

Site Yönetimi ve SSL 11

- Gösterge paneli: CPU, RAM, disk, WAF durumu, engellenen istek ve yasaklı IP sayısı
- Sihirbazla yeni site: Docker ile izole uygulama, isteğe bağlı MariaDB veritabanı
- Tek adımda WordPress, Laravel, Drupal, Joomla, Symfony, Codelgniter, PrestaShop, Moodle kurulumu
- Kendi docker-compose dosyanızla site veya harici sunucuya reverse proxy olarak yayın
- Site arama, durum, HTTP yanıtı, disk kullanımı ve DNS (A/NS) bilgisi tek listede
- Site özet ekranı: günlük trafik, durum kodları, en çok istek alan yol ve IP'ler
- Siteyi bakım moduna alma (konteynerler durur) ve tek tıkla geri açma
- Konteynerleri yeniden başlatma ve site çalışma ortamı sürümünü değiştirme
- Reverse proxy ayarları: upstream http/https, Host başlığı, http→https yönlendirme
- Başarısız veya taşınmış siteyi tüm bileşenleriyle silme; kritik hostlar korunur

- Let's Encrypt ile ücretsiz SSL, kendi sertifikanızı yükleme, geçerlilik takibi ve toplu Let's Encrypt

Dosyalar, Konsol ve Yedekleme 9

- Tarayıcıdan dosya yöneticisi: yükleme, indirme, arşiv açma, klasör oluşturma, silme
- Dosya işlemleri sitenin kendi dizinine kilitlidir
- Konteyner içine tarayıcıdan tek kullanımlık terminal
- Site başına kalıcı geliştirici terminali; 3 gün kullanılmazsa kapanır
- Yöneticiler için adlandırılabilir sunucu konsolu oturumları
- Konteyner günlüklerini panelden görüntüleme
- Anlık site yedeği: dosyalar, veritabanı dökümü ve Docker yapılandırması tek pakette
- Site başına veya toplu zamanlanmış yedek: saat aralığı ve saklanacak kopya sayısı
- Yedeği indirme veya geri yükleme; geri yükleme öncesi mevcut sürüm saklanır

İzleme, Uyarılar ve Kullanıcılar 10

- Sunucu ve site durumu 15 saniyede bir otomatik güncellenir
- E-posta uyarıları: site CPU, bellek, disk ve HTTP erişilebilirliği
- Sunucu bellek ve disk doluluk uyarıları
- Ani sıçrama filtresi ve bekleme süresiyle gereksiz uyarı engellenir
- SMTP ayarları ve test e-postası panelden
- Kullanıcı yönetimi ve roller: admin, operatör, salt okunur; kullanıcıya yalnızca seçili siteler atanabilir
- TOTP tabanlı iki adımlı doğrulama; admin tarafından sıfırlanabilir
- Panel girişi Cloudflare Turnstile ile korunabilir
- Hatalı girişte IP kilidi, 2 saat boşta oturum kapanması ve CSRF korumalı formlar
- Panel içi kullanım kılavuzu

Kurulum ve Sistem Bakımı 6

- Tek komutla kurulum: CloudPanel, Docker, ModSecurity + OWASP CRS, panel ve zamanlanmış görevler
- WAF modülü sunucudaki web sunucusu sürümüne göre otomatik derlenir
- Güvenlik duvarında web portları açılır, panel için isteğe bağlı Let's Encrypt sertifikası
- İlk yönetici hesabı kurulumda oluşturulur

- Tekrar çalıştırılabilir kurulum; güncellemede mevcut ayar ve veriler korunur
- Gece günlük döndürmesinin sunucuyu kilitlemesini önleyen otomatik koruma

Teknik özellikler

WAF motoru	ModSecurity v3 (libmodsecurity) + nginx bağlayıcı modülü
Kural seti	OWASP CRS 4.x (v4.7.0) + 18 Marta özel kuralı
Barındırma altyapısı	CloudPanel + nginx + Docker Engine / Compose
Bot / insan doğrulaması	Cloudflare Turnstile, nginx auth_request, HMAC imzalı çerez
Brute-force ve yasaklama	fail2ban (SSH + panel girişi), UFW tabanlı WAF otomatik yasaklama
Panel güvenliği	CSRF token, CSP, HSTS, 2 saat boşta oturum kapatma, TOTP 2FA
Yetki modeli	Panel yalnızca belirli yönetim betiklerini sudo ile çağırabilir
Güvenli değişiklik	Her nginx değişikliğinde yapılandırma testi; hata olursa otomatik geri alma
AI sağlayıcısı	Anthropic Claude API veya yerel Ollama (isteğe bağlı)
Desteklenen işletim sistemi	Debian 12/13, Ubuntu 22.04/24.04

KURULUM VE TESLİM Tek komutluk kurulum betiği; CloudPanel, Docker, ModSecurity + OWASP CRS, panel ve zamanlayıcıları kurar, isteğe bağlı Let's Encrypt sertifikası alır. Tekrar çalıştırılabilir; mevcut ayarları korur. Kendi sunucunuzda (Debian/Ubuntu) çalışır.

Demo ve fiyat teklifi için

Ürünü kendi ortamınızda görmek, kapsamı ve fiyatı konuşmak için bize ulaşın.

TELEFON +90 850 441 3 441
E-POSTA bilgi@martateknoloji.com.tr
WEB martateknoloji.com.tr
ADRES Mersin Üniversitesi Teknopark İdari Binası 35C/B5, Yenişehir, Mersin
Mersin · İzmir · Londra

© 2026 Marta Teknoloji A.Ş. — Bu broşürdeki bilgiler bilgilendirme amaçlıdır; özellik kapsamı sürüme ve kurulumu göre değişebilir.