Zero Trust Admission Control (ZTAC)

Gerçek zamanlı uyum sağlayan davranış bazlı erişim denetimi—ağınızı yavaşlatmadan

ZTAC, Corero Gözlemlenebilirlik ve Dayanıklılık Ekosistemi (CORE) içinde yer alır ve out-of-band (ağ dışı) davranış bazlı erişim kontrolü sağlar. Bu, kullanıcı trafiğini incelemeden veya yönlendirmeden, kuruluşunuzun iç kaynaklarına yapılan uzak erişimi kötü niyetli faaliyetlerden korur. CORE içinde lisanslı bir yetenek olarak ZTAC, Zero Trust yaklaşımını henüz ZTNA tarafından kapsanmayan internet trafiği ve servislerine genişleterek, korunmakta olan uygulamalara herhangi bir değişiklik yapmadan şeffaf erişim kontrolü sunar.

Hız, ölçeklenebilirlik ve basitlik için tasarlanan ZTAC, mevcut altyapınızdan elde edilen telemetriyi kullanarak network edge'de yetkisiz aktiviteleri durdurur; ek ajan, proxy veya yeni cihaz gerektirmez. Sistem, hem yeni hem de kimliği doğrulanmış kullanıcıları sürekli değerlendirir ve yalnızca güvenilen davranışlara izin verir.

Şu an önemli olan için tasarlanmış, uyarlanabilir ve maliyet etkin sıfır güven (Zero Trust) savunma:

İç altyapıya ve kritik kaynaklara erişimi koruyun

Edge'de sürekli doğrulama ile sıfır güven (Zero Trust) uygulayın

Karmaşıklığı ve gecikmeyi azaltın

ZTAC, servis sağlayıcılar ve kurumsal şirketlere, CORE'dan alınan canlı istihbarat ile gerçek zamanlı erişim kontrolü sunar; performansı veya operasyonları aksatmadan çalışır.

Temel Faydalar

Altyapıya güvenli erişimi sağlayın:
Gözlemlenen davranışlara dayanarak, giriş portalları, API'ler ve kontrol düzlemlerini hedef alan tehditleri engelleyin.

Dinamik erişim kontrolü uygulayın:
Kimlerin her seferinde erişebileceğini belirlemek için kimlik doğrulama verilerinden ve tehdit istihbaratından alınan canlı güven sinyallerini kullanın.

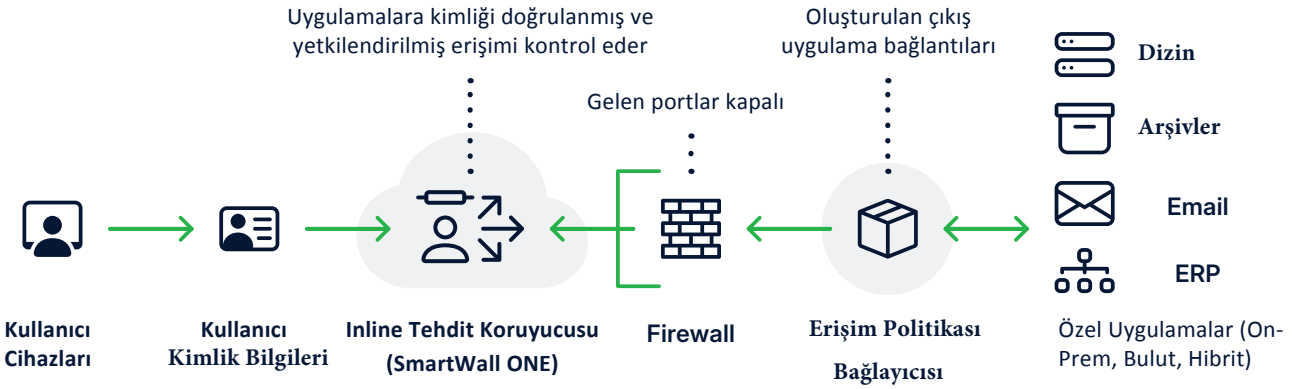
Trolling ve kesintiler:
Ağ dışı çalışır; ek gecikme yaratmaz ve kullanıcı trafiğini etkilemez.

Kesintisiz Ölçeklenebilirlik:
Milyonlarca bağlantıyı hiçbir yavaşlama olmadan ve uygulamalarda değişiklik yapmadan yönetin.

Şantaj (RDoS):
Politikaları uygulamak için SmartWall ONE™ veya uyumlu yönlendiriciler ve güvenlik duvarlarını kullanır — ek donanım gerekmez.

Uygulamayı Otomatikleştirin:
Kabul kararlarını SmartWall ONE veya uyumlu uygulama noktaları aracılığıyla otomatik olarak uygulayın, manuel inceleme gerektirmeden.

Zero Trust Admission Control (ZTAC) nedir?



Teknik Özellikler

Platform:	Corero CORE çözümü ile sunulur.
Kurulum:	SmartWall ONE gerektirir — uzaktan erişim ve kritik altyapılar için tam kapsamlı DDoS koruması sağlar.
Erişim:	Web tabanlı güvenli yönetim paneli
Sunum Modeli:	Bulut tabanlı abonelik hizmeti
Veri Kaynakları:	Kimlik doğrulama günlükleri, API telemetrisi, proxy ve altyapı günlükleri, botnet üyeliği bilgileri, itibar akışları, coğrafi konum verileri, kaynak profillemesi ile açık izin (allow) veya engelleme (block) listeleri.
Güvenlik:	Özel oturum açma, rol tabanlı erişim ve şifrelenmiş telemetri
Entegrasyon:	Uygulama noktası olarak SmartWall ONE ile entegre çalışır; etkinleştirilen ek uygulama seçeneklerini de destekler.
Otomasyon:	Canlı güven göstergelerine göre çalışır ve yapılandırılabilir izin verme veya engelleme politikalarını uygulama noktaları üzerinden uygular.
Ön Koşullar:	**SmartWall ONE™ gerektirir; daha kapsamlı savunma yeteneklerini etkinleştirir.**
Kullanım Senaryoları	İç kaynaklar ve hizmetler için bağımsız olarak veya daha geniş bir Zero Trust (ZTNA) mimarisinin parçası olarak uyarlanabilir erişim denetimi sağlar. VPN ağ geçitleri ve diğer ağ erişim noktaları için şeffaf, düşük gecikmeli erişim kontrolü sunar. Uzaktan erişim ağ geçitleri için uygulama katmanı tehdit tespiti sağlar. DDoS, brute force ve tarama saldırılarına karşı koruma sağlar. Kimlik doğrulama sonrasında sürekli doğrulama gerçekleştirir. IoT ve OT erişim kontrolü sağlar. VPN Ağ Geçidi / Güvenlik Duvarı zafiyetlerine yönelik istismar girişimlerine karşı koruma sağlar.

OTD BİLİŞİM GLOBAL VAD