

ÜRÜN BÜLTENİ

TSplus Advanced Security - Ürün Bülteni

Türkiye pazarına özel Türkçe sürüm · 2026

Sunucunuzu güvenle koruyun.



TSPLUS TÜRKİYE · RESMÎ DİJİTAL DOKÜMAN

tsplus.com.tr · sales@tsplus.com.tr

RESMÎ KAYNAK GÖRSELİ



TÜRKÇE İÇERİK

Kaynak sayfa 1/2

gelişmiş

Uzak Masaüstü bağlantılarını ve Uzaktan Erişim ortamlarını koruyun.

GÜVENLİK

Çalışma Saatlerini Kısıtlama Çalışma saatlerine uzaktan erişimi sınırlandırın. - Gün ve Saat Kısıtları: günlük ve zaman dilimi. - Belirli bir saat dilimi seçmek mümkündür. - Kullanıcı ve Gruplar İzin - Otomatik bağlantı kesme - Bildirimler

Uzaktan erişim için tasarlanmış hepsi bir arada siber güvenlik yazılımı TSplus Advanced Security, hem küçük hem de büyük işletmelerin gereksinimlerini karşılayan bir teknolojidir. Uzak sunucu yöneticilerinin ihtiyaç duyduğu temel korumaları sağlar. Ağ için doğru güvenlik seviyesini ayarlamak için etkinleştirilebilen yedi farklı önlem sunar. İki koruma seviyesi sunar: Essentials ve Ultimate.

Coğrafi Koruma İhtiyacı olan kişilere uzaktan erişimi kısıtlar: - Ülke Kısıtlaması: İstenmeyen ülkeleri engeller ve belirli ülkelerden erişime izin verir. - İnternet ve IP Erişim Kısıtlamaları: İnternette erişimi kısıtlar. - İzlenen Süreçler: İç Güvenlik özelliği tarafından izlenen işlemleri ekleyin veya kaldırın.

Brute Force Protection Sistemleri Hacker ve botlardan korur. Brute Force Defender, genel sunucunuzu Yönetici girişinizi ve şifrenizi tahmin etmeye çalışan bilgisayar korsanlarından, ağ tarayıcılarından ve kaba kuvvet robotlarından korumanızı sağlar. Başarısız Windows oturum açma girişimlerini izleyin ve önceden belirlenmiş bir hata sayısından sonra rahatsız edici IP adreslerini otomatik olarak engelleyin.

Ransomware Koruması Ransombus saldırılarını etkin bir şekilde tespit eder, engeller ve önler. TSplus Advanced Security sunucunuzdaki ransomware'i algılar algılamaz tepki verir. Hem statik hem de davranışsal analize sahiptir: - Statik analiz, yazılımın bir uzantı adı değiştiğinde hemen tepki vermesini sağlar. - Davranışsal analiz, bir programın dosyalarla nasıl etkileşime gireceğini ve yeni fidye yazılımları nasıl algılayacağını inceler.

- Kesintisiz Öğrenme Süresi - Saldırıcı otomatik olarak durdurur ve etkilenen programları ve dosyaları karantinaya alır. Yöneticiler karantinaya alınan öğelerin listesini gözden geçirebilir ve belirli girdileri beyaz listeye almaya karar verebilir. - Raporlar: Saldırıların kaynağını belirleyerek tehditleri tahmin etmeyi öğrenin ve raporlarda listelenen çalışma süreçlerini analiz edin. - E-posta Uyarıları: Otomatik uyarılar hızlı yanıt sağlar - Snapshots:

Saldırıdan sonra etkilenen dosyaları hızlı bir şekilde tanımlayın ve kurtarın. Yöneticiler ayrıca anlık görüntülerin tutma süresini de düzenleyebilirler. - Görmezden gelinen dosya uzantıları: Ransomware Protection analizlerinden hariç tutulması gereken dosya uzantılarını kolayca tanımlar.

Global IP Yönetimi IP adreslerini birleşik bir izin/blok listesinden kolayca yönetin. - Kolay Yönetim: Engellenen ve beyaz listeye alınanlar için tek liste - Arama Çubuğu ve çok adresli düzenleme - IP Adresi Açıklaması -.csv formatında dışa aktarma yetenekleri

<https://tsplus.com.tr/advanced-security>



RESMÎ KAYNAK GÖRSELİ

<https://tsplus.net/advanced-security>TS
PLUS

TÜRKÇE İÇERİK

Kaynak sayfa 2/2

Hacker IP Protection Bilinen tehditlerin dünya çapındaki topluluk kara listesinden yararlanın: on-line saldırılar, on-line hizmet kötüye kullanımı, kötü amaçlı yazılımlar, botnetler ve diğer siber suç faaliyetleri. Hacker IP Protection, Gelişmiş Güvenlik kullanıcıları topluluğu tarafından sağlanan bilgileri günlük olarak 564 milyondan fazla tanımlanmış tehdidi otomatik olarak kara listeye almak için kullanır.

Firewall Supercharged firewall, Windows Firewall'ı geride bırakıyor ve daha güçlü koruma sağlıyor.

Admin Tool Tüm güvenlik özelliklerini kolayca yönetin ve yapılandırın. - Kullanıcı dostu ve sezgisel gösterge paneli - Son 100 başarısız girişimle Etkileşimli Dünya Haritası - Görsel Veri ve etkileşim ile Özellikler durumu - Olaylara Erişim günlüğü birkaç saniyede bir yenilenir - Sistem Denetimi (işlemleri ve güvenliği izleme)

İzinler Yönetimi Kullanıcılar, gruplar ve dosyalar için uzaktan erişim iznini yönetin. - Yan yana İzin Panosu: Bu öğeleri yan yana listeleyen bir gösterge panelindeki kullanıcıların, grupların, dosyaların, klasörlerin ve yazıcıların izinlerini kolayca denetleyin ve düzenleyin. - Dört izin arasından seçim yapın: Reddetme, Okuma, Değiştirme veya Sahiplik. - İzinleri İnceleyin: Bir klasöre, alt klasöre veya ağaç görünümünde görüntülenen dosyaya tıklayın.

Olay görüntüleyicisindeki izinleri izlemek için belirli dosyaları denetleyin.

Güvenli Oturumlar Her kullanıcı veya grup için güvenlik seviyesini yapılandırın. - Standart Güvenlik Seviyeleri (endüstrinin en iyi uygulamalarına göre): Windows Modu - varsayılan Windows oturumuna erişim, Güvenli Masaüstü Modu - belgelere, yazıcılara, Windows anahtarına ve oturum bağlantısının kesilmesine erişim ve Kiosk Modu - bağlı bir kullanıcının yasak eylemleri çalıştırmasını önler. - Özelleştirme aracı - Sağ Tıklama ve Bağlam Menü Kısıtlamaları

Ön Talepler: 1) Donanım TSplus Advanced Security 32-bit ve 64-bit mimarileri destekler. 2) İşletim sistemi Sunucunuz aşağıdaki işletim sistemlerinden birini kullanmalıdır:

- Microsoft Windows sürüm 7 Pro, 8/ 8.1 Pro, 10 Pro, 11 Pro - Windows 2008 R2, Service Pack 1 (yapı 6.1.7601) veya 2008 SP2/Small Business Server SP2 - Server 2012 veya 2012 R2 - Server 2016, 2022, 2025 Gerekli çerçeve.NET v 4.7.2 veya üstüdür. Microsoft Windows 7 SP1 ve Windows 2008 R3 SP1, SHA2 Çapraz İmzalamayı desteklemek için ek bir güncelleme gerektirir (KB44719).

Bu güncelleme, TSplus Advanced Security yerleşik güvenlik duvarı ve fide yazılımı korumasının düzgün çalışmasını sağlar.

Advanced Security'nin deneme sürümü tam özellikli Ultimate Edition'dır. Sunucu başına lisanslıdır.

Güvenilen Aygıt Kontrol Bloğu tehlikeye giren kimlik bilgileri ve istenmeyen aygıtlar. - Cihaz Kontrolü: Yöneticiler, bir kullanıcının herhangi bir cihazdan veya yalnızca belirli cihaz adlarından bağlanıp bağlanamayacağına karar verebilir. Bir cihaz bağlanmaya çalışıldığında otomatik olarak bir liste oluşturulur. - Uç Nokta Koruması: Cihazları kullanıcı hesaplarına eşleştirerek Endpoint Protection, tehlikeye atılan kimlik bilgilerinin ağınıza erişmek için kullanılmasını önler.

Uyarılar, Bildirimler ve Raporlama Takvimi e-postaları tüm temel güvenlik istatistiklerine sahiptir ve uyarıları e-posta, SMS veya Microsoft Teams bildirimleri ile alır.

İletişim Adı: Adres: Tel: E-posta:

<https://tsplus.com.tr/advanced-security>

