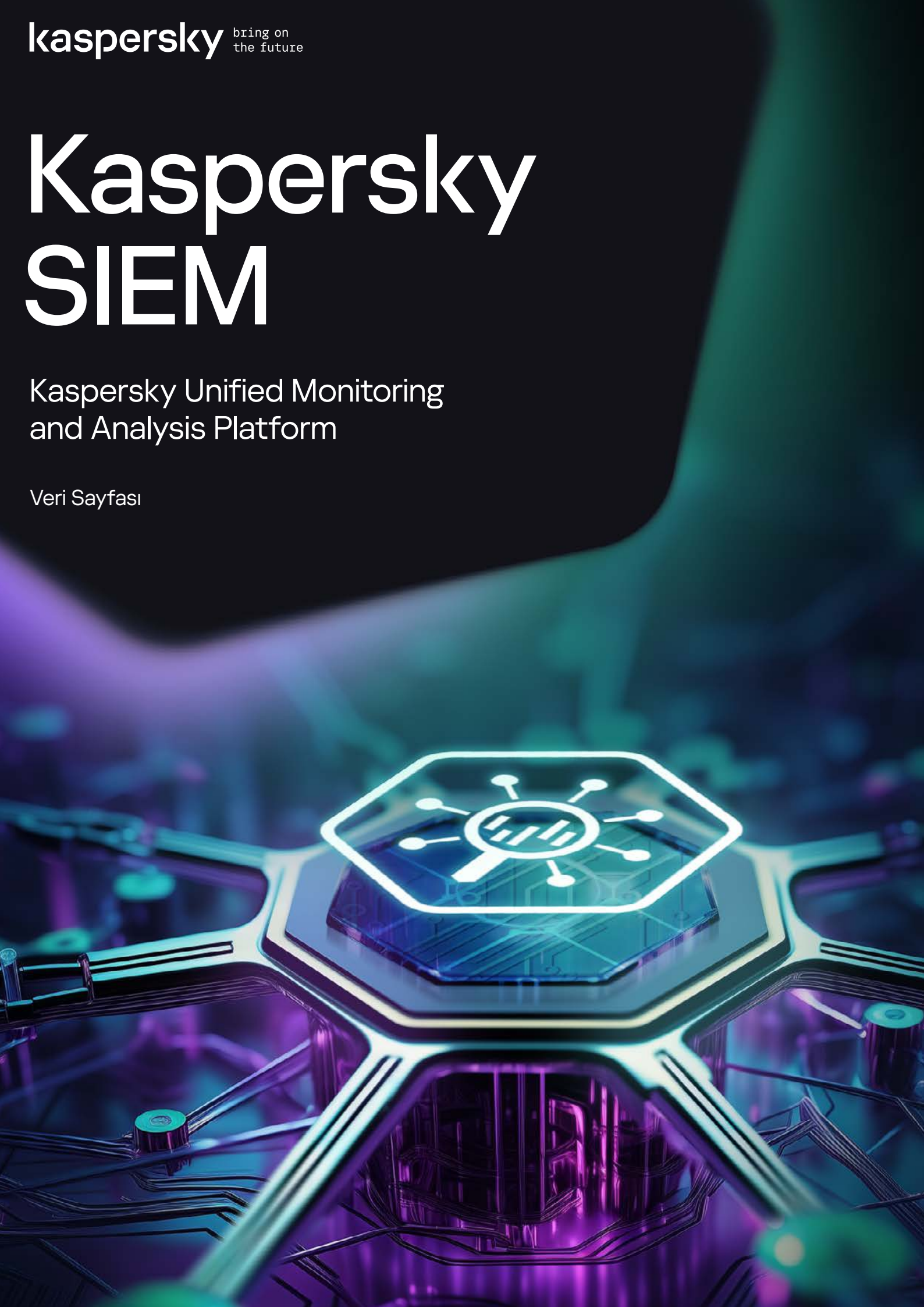
kaspersky bring on the future

Kaspersky SIEM

Kaspersky Unified Monitoring and Analysis Platform

Veri Sayfası



Kaspersky SIEM ve mimarisi hakkında

Kaspersky Unified Monitoring and Analysis Platform, güvenlik verilerini ve olaylarını yönetmek için entegre bir yeni nesil SIEM çözümüdür. Güvenlik bilgileri olaylarını alma, işleme ve depolama ve gelen verileri analiz etme ve ilişkilendirme konusunda mükemmeldir. Platform ayrıca bir arama özelliğine sahiptir, potansiyel tehditler tespit edildiğinde uyarılar oluşturur ve oluşturulan uyarılara otomatik yanıtları ve tehdit avcılığını destekler.

Yüksek performanslı modüler mimari, her örnekte saniyede yüz binlerce olayın (EPS) işlenmesine ve sistem gereksinimlerini optimize ederek toplam sahip olma maliyetinin (TCO) azaltılmasına olanak tanır.

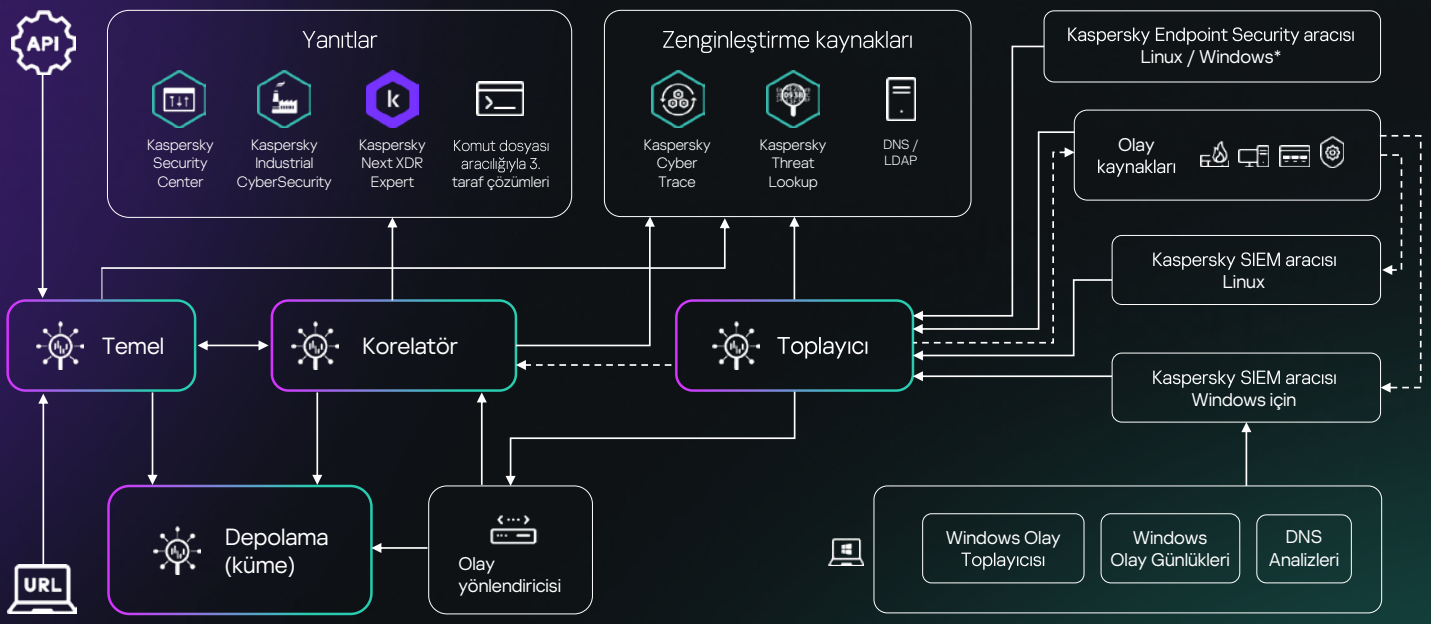
Üçüncü taraf ve Kaspersky ürünlerini merkezi bir bilgi güvenliği sistemine dahil eden Kaspersky SIEM, kurumsal ve endüstriyel ortamların güvenliğini sağlamanın yanı sıra BT'de başlayıp OT sistemlerine geçiş yapan siber saldırıları tespit edebilen kapsamlı bir savunma stratejisinin önemli bir parçasıdır.

Çözümün mikro hizmet mimarisi sayesinde yöneticiler, Kaspersky SIEM'i tam teşekküllü bir SIEM sistemi veya bir günlük yönetim sistemi olarak kullanmak için ihtiyaç duydukları mikro hizmetleri oluşturabilir ve yapılandırabilir.

Çözüm, Kaspersky ürünleri, işletim sistemleri, üçüncü taraf uygulamalar, güvenlik araçları ve çeşitli veritabanları dahil olmak üzere çeşitli kaynaklardan güvenlik olaylarını alır ve olayları birbiriyle ilişkilendirir ve kurumsal ağ altyapılarındaki şüpheli etkinlikleri belirlemek ve güvenlik olaylarının zamanında bildirilmesini sağlamak için bunları tehdit istihbaratı beslemelerinden gelen verilerle zenginleştirir.

Kaspersky SIEM, tüm güvenlik kontrollerinden günlükleri toplayarak ve verileri gerçek zamanlı olarak ilişkilendirerek olay inceleme ve müdahale için gereken tüm bilgileri bir araya getirir ve sağlar.

Ayrıca Kaspersky SIEM, operatörlerin geçmiş verileri analiz edip ilişkilendirmesine ve anormallikleri belirlemek için istatistiksel temeller oluşturmasına olanak tanıyarak tehdit avcılarının daha önce bilinmeyen tehditleri keşfetmesini sağlar.



Neden bizi seçmelisiniz?

Maliyet verimliliği açısından eski SIEM satıcılarından sürekli olarak daha iyi performans gösteren ve her örnekte yüz binlerce EPS'yi işleyebilen yüksek performanslı modüler bir çözümle donanım veya sanallaştırma kurulum gereksinimlerinden %50'ye kadar tasarruf edin ve sahip olma maliyetini azaltın.

Lisanslama seçeneklerimizle esnek kalın. Taşmaları sınırlamak için toplama ve filtrelemeden sonra günlük ortalama EPS akışını izliyoruz ve gerçekleşmeleri durumunda Kaspersky SIEM'e erişimi kısıtlamıyoruz.

Yerleşik yanıt seçenekleriyle hem Kaspersky hem de üçüncü taraf entegrasyonlarının geniş bir yelpazesinden yararlanın. Diğer satıcılar, Tehdit İstihbaratı entegrasyonu için tek bir arayüz, uç nokta sensörlerimizi SIEM aracıları olarak kullanma kapasitesi ve çok daha fazlasını içeren kendi ürünlerimizle sorunsuz entegrasyon düzeyimizle rekabet edemez.

ClickHouse ve Hadoop Dağıtılmış Dosya Sistemi (HDFS) veya yerel diskleri kullanarak sıcak ve soğuk depolama seçenekleriyle uzun bir süre bütçenizi aşmadan düşük maliyetli, tavizsiz bir şekilde yerel olarak veri depolayın ve aynı anda her iki alanda da hızlı bir şekilde arama yapın.

Dünya lideri araştırmacı ve analist ekibimiz tarafından Kaspersky Threat Intelligence Portal üzerinden sağlanan taktiksel, operasyonel ve stratejik Tehdit İstihbaratı ile zenginleştirme sayesinde veri alaka düzeyini artırın, saptama ve önceliklendirmeyi hızlandırın.

Kuruluşların ana altyapısında tek bir SIEM kurulumunun kendi olaylarını alan ve işleyen kullanıcılar için izole SIEM oluşturulmasını sağladığı yerel çoklu kullanım desteği sunan bir MSSP ve büyük kuruluşlara hazır çözümle yerleşik çoklu kullanımdan yararlanın.

Neden Kaspersky?

Kaspersky SIEM, 5 Uzmanlık Merkezinin yıllara dayanan bilgi birikimini ve rafine becerilerini bir araya getirir.

Daha fazla bilgi

27

27 yılı aşkın süredir en çok test edilen, en çok ödül alan teknolojilerimizle sizi güvende tutmak için araçlar geliştiriyor ve hizmetler sunuyoruz.

Daha fazla bilgi

Dünya çapında binlerce müşterisi ve iş ortağı olan, **şeffaflık ve bağımsızlık** ilkelerine bağlı küresel bir özel siber güvenlik şirketiyiz.

Daha fazla bilgi

Kaspersky Unified Monitoring and Analysis Platform

Daha fazla bilgi

www.kaspersky.com.tr

#kaspersky
#geleceğiyakalayın