FUMA
Bilgi Teknolojileri

FORTINET

Forti EDR

FortiEDR (Endpoint Detection and Response) Fortinet tarafından geliştirilen bir uç nokta güvenliği çözümüdür. FortiEDR, şirketlerin ve kurumların uç noktalarını (bilgisayarlar, dizüstü bilgisayarlar, sunucular ve mobil cihazlar gibi) siber tehditlere, kötü amaçlı yazılımlara ve saldırılara karşı korumalarına yardımcı olur. FortiEDR, aşağıdaki ana bileşenlere sahiptir:

- Tehdit algılama: FortiEDR, uç noktalarında kötü amaçlı veya şüpheli faaliyetleri tespit etmek için gerçek zamanlı davranış analizi kullanır. Bu, geleneksel imza tabanlı antivirüs çözümlerinin yakalayamayabileceği sıfırıncı gün saldırıları ve yeni tehditleri tespit etme yeteneğini artırır.
- Olaya müdahale: FortiEDR, kötü amaçlı faaliyetleri durdurmak ve saldırıları engellemek için otomatik müdahale mekanizmaları sağlar. Bu, kötü amaçlı yazılımın yayılmasını önlemeye ve sistemlerin daha fazla zarar görmesini engellemeye yardımcı olur.
- Olay sonrası analiz ve uyum: FortiEDR, siber olaylar ve tehditlerle ilgili verileri toplar ve analiz eder. Bu, olaylara yönelik kapsamlı bir anlayış sağlar ve şirketlerin güvenlik duruşlarını iyileştirmelerine, uyumluluk gereksinimlerini karşılamalarına ve gelecekteki saldırılara karşı daha iyi hazırlanmalarına yardımcı olur.
- Uç nokta risk değerlendirmesi: FortiEDR, uç noktaların güvenlik durumunu değerlendirmek ve potansiyel riskleri belirlemek için sürekli izleme ve analiz sağlar. Bu, şirketlerin güvenlik açıklarını tespit etmelerine ve bu açıkları proaktif bir şekilde ele almalarına yardımcı olur.

FortiEDR, Fortinet'in geniş güvenlik ekosistemi içinde çalışır ve FortiGate güvenlik duvarları, FortiSandbox ileri tehdit analizi ve FortiAnalyzer güvenlik olaylarını analiz etme ve raporlama gibi diğer Fortinet ürünleriyle entegre olur. Bu, şirketlerin uçtan uca güvenlik koruması sağlamalarına ve siber tehditlere karşı daha etkili bir şekilde savunmalarına yardımcı olur.

FortiEDR (Endpoint Detection and Response), çok çeşitli sektörlerde ve organizasyon tiplerinde kullanılabilir. Uç nokta güvenliği her türlü işletme ve kurum için kritik bir öneme sahip olduğundan, FortiEDR'nin uygulanabileceği alanlar geniştir. İşte FortiEDR'nin kullanılabileceği bazı örnekler:

- **Küçük ve orta ölçekli işletmeler (KOBİ'ler):** FortiEDR, KOBİ'lerin uç noktalarını kötü amaçlı yazılımlara, sıfırıncı gün saldırılarına ve gelişmiş sürekli tehditlere (APT) karşı korumalarına yardımcı olur.
- Büyük kuruluşlar ve şirketler: Büyük işletmeler genellikle daha karmaşık ağ yapılarına ve daha fazla sayıda uç noktaya sahip olduğu için, FortiEDR bu tür organizasyonların güvenlik duruşlarını güçlendirmeye ve geniş kapsamlı uç nokta koruması sağlamaya yardımcı olur.
- **Kamu sektörü ve hükümet kurumları:** FortiEDR, kamu sektöründeki hassas verilerin ve altyapının güvende tutulmasına yardımcı olarak, hükümet kurumlarının siber güvenlik gereksinimlerini karşılar.
- **Eğitim kurumları:** Okullar, üniversiteler ve diğer eğitim kurumları, öğrenci ve personel bilgilerini korumak ve fikri mülkiyeti güvende tutmak için FortiEDR kullanabilir.
- **Sağlık hizmetleri:** Hastaneler ve sağlık hizmeti sağlayıcıları, hasta verilerini ve tıbbi kayıtları korumak için FortiEDR kullanarak siber güvenliklerini güçlendirebilir.
- **Finansal hizmetler:** Bankalar, finans kurumları ve sigorta şirketleri, hassas müşteri verilerini ve finansal işlemleri korumak için FortiEDR kullanarak uç nokta güvenliğini artırabilir.
- **Perakende ve e-ticaret:** Perakende ve e-ticaret şirketleri, müşteri verilerini ve ödeme işlemlerini korumak için FortiEDR kullanarak siber güvenliklerini güçlendirebilir.

FortiEDR, uç nokta güvenliğini iyileştirmeye yardımcı olarak, bu ve diğer sektörlerdeki şirketlerin ve organizasyonların siber tehditlere karşı daha iyi savunmalarını sağlar.

EDR ve Antivirüs Arasındaki Farklar

EDR:
1. EDR, standart antivirüs tarafından kolayca tanınamayan veya tanımlanamayan tehditler de dahil olmak üzere tehditlerin gerçek zamanlı izlenmesini ve tespit edilmesini içerir. Ayrıca EDR davranış tabanlıdır, dolayısıyla normal olmayan bir davranışa dayalı olarak bilinmeyen tehditleri tespit edebilir.
2. Veri toplama ve analiz, tehdit modellerini belirler ve kuruluşları tehditlere karşı uyarır
3. Adli tıp yetenekleri, bir güvenlik olayı sırasında ne olduğunun belirlenmesine yardımcı olabilir
4. EDR, şüpheli veya virüslü öğeleri izole edebilir ve karantinaya alabilir. Kullanıcının sistemini bozmadan bir dosyanın güvenliğini sağlamak için genellikle korumalı alan oluşturmayı kullanır.
5. EDR, belirli tehditlerin otomatik olarak iyileştirilmesini veya kaldırılmasını içerebilir

Antivirüs:
1. Antivirüs imza tabanlı olduğundan yalnızca bilinen tehditleri tanır.
2. AV, bilinen tehditleri tespit etmek için korunan cihazların planlı veya düzenli taramasını içerebilir
3. Daha temel virüslerin (solucanlar, truva atları, kötü amaçlı yazılımlar, reklam yazılımları, casus yazılımlar vb.) kaldırılmasına yardımcı olur
4. Olası kötü amaçlı siteler hakkında uyarılar

Bazı örtüşmeler var EDR ile geleneksel antivirüs arasında bir fark vardır ancak genel olarak antivirüs tek başına daha az kapsamlı bir çözümdür.

Fuma Bilgi Teknolojileri Yorumu:

Hem EDR'ye hem de Antivirüs'e ihtiyacım var mı ?

Fuma'nın önerisi hayır. EDR ve antivirüs karşılaştırmasını değerlendirirken, uç nokta tespit ve müdahalesinin en iyi antivirüs çözümlerinin ve daha fazlasının yaptığını dikkate almak önemlidir. FUMA genellikle bir EDR çözümü yüklendiğinde diğer antivirüs araçlarının kaldırılmasını önerir. Her ikisinin de çalıştırılması, sistemlerde ve cihazlarda yavaşlamaya veya diğer teknik sorunlara neden olabilir. Karmaşık ve gelişen tehditlere karşı savunma yapmak için tercih açıktır; uç nokta tespiti ve müdahalesi size daha gelişmiş güvenlik sağlayacaktır.