



# Singularity™ EPP+EDR

Birleşik Önleme, Tespit, Araştırma, Müdahale

Tehditlerin hızı, karmaşıklığı ve ölçeği gelişerek birinci nesil önleme ve EDR çözümlerini geride bıraktı

Saldırganlar önleme tedbirlerini aştığında, ağ bağlantısı olsun veya olmasın uç nokta tespit ve müdahalesinin, uç noktada otonom bir şekilde, gerçek zamanlı olarak uygulanması gerekir. SentinelOne Singularity EPP+EDR, makine hızında otonom EPP elde etmek için yeni nesil önleme ve EDR yeteneklerini tek bir Sentinel aracısında bir araya getirir.

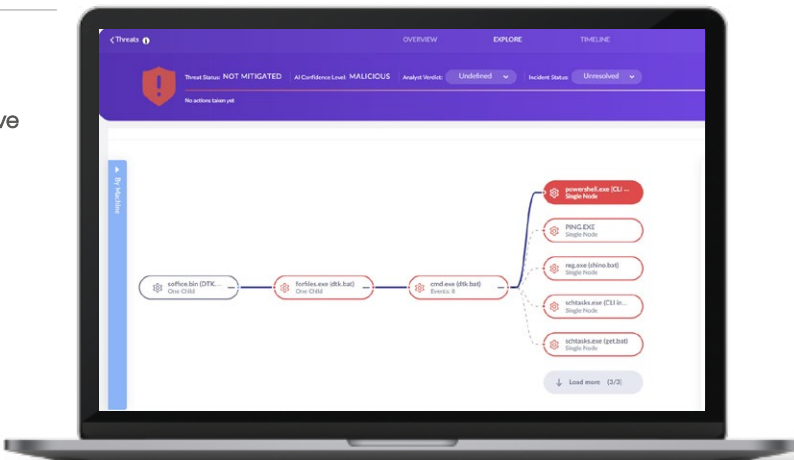
## Deep Visibility™ ve ActiveEDR™ ile çalışır™

ActiveEDR, kötü niyetli süreçler meydana geldikçe, onları tanımlamak için davranışsal yapay zeka kullanır, ilişkili olayları etiketler, araştırmayı görselleştirmek ve hızlandırmak amacıyla saldırıya dair otomatik bir zaman çizelgesi oluşturur. Koruma Modundayken, Sentinel yalnızca saldırıyı tanımlamakla kalmaz, aynı zamanda bulaşmayı da otomatik olarak engeller. Ardından, patentli Tek Tıkla Düzeltme moduyla analist, meydana gelmiş olabilecek tüm yetkisiz değişiklikleri geri alabilir. Bunun için de komut dosyası gerekmez.

## Güçlü Araştırma, Sezgisel Basitlik

MTR'yi (Ortalama Onarım Süresi) azaltmak ve üretkenliği en üst düzeye çıkarmak için EDR 2.0, tespit ve müdahaleyi basitleştirmelidir. Veri merkezi, bulut hizmeti sağlayıcısı, ofis veya uzak çalışma konumu olsun, yapay zeka, her işletim sisteminde ve her ortamda her olayı sürekli olarak izler. Deep Visibility, sıfır öğrenme eğrisi ile avlanma ve araştırmaya güç katarak IR ve avı, daha geniş bir güvenlik yeteneği havuzu ile buluşturur.

Automatic Storyline™, sınıflandırma ve araştırmayı hızlandırır



## SINGULARITY EPP+EDR

Makine hızında otonom, yapay zeka odaklı Önleme ve EDR

## ANA ÖZELLİKLER

- + Konsolide, otonom EPP/EDR
- + Yalnızca EPP, yalnızca EDR. Kombine modlar. Aynı ürün.
- + Linux, macOS, Windows, Kubernetes ve Docker
- + Çevrimiçi/ofis koruması, algılama & yanıt
- + Zaman çizelgeleri için otomatik olay korelasyonu
- + Patentli Tek Tıkla İyileştirme & Geri Dönüş
- + MITRE ATT&CK® çerçevesi ile tam uyum
- + Esnek EDR veri saklama, 14-365+ günlük seçenekler
- + Her işletim sistemi için uzaktan araştırma



“Mükemmel müşteri hizmeti ve daha da iyi ürün.”



KIDEMLİ DİREKTÖR, BT Sağlık Hizmetleri

## Temel Yetenekler

- ✓ İnsan müdahalesine gerek kalmadan, karmaşık tehditlerin **otonom, gerçek zamanlı** tespiti ve düzeltilmesi.
- ✓ Windows, Linux ve macOS genelinde **tavizsiz koruma**  
- fiziksel, sanal, container, bulut, veri merkezi... Her yerde.
- ✓ MDR'li veya MDR'siz, piyasadaki en iyi MITRE ATT&CK® uyumuyla ve olay öngörülerıyla, **hızlandırılmış sınıflandırma ve temel neden analizi**. Otomatik korelasyonlar ve zaman çizelgeleri ile saniyeler içinde araştırma yapın.
- ✓ **Tek Tıkla Düzeltme ve Geri Dönüş**, yanıtı basitleştirir ve MTTR'yi (Ortalama Onarım Süresi) azaltır.
- ✓ Deep Visibility, SIQL ve STARTM (Storyline Active Response)'ın **sezgisel kullanıcı deneyimi**, güvenlik operasyonlarınıza tehdit avını dahil etmek için gereken becerileri azaltır.
- ✓ 14'ten 365+ güne kadar, her ihtiyaca uygun **veri saklama** seçenekleri.
- ✓ **Hızlı dağıtım** ile birlikte çalışabilirlik özellikleri, hızlı ve sorunsuz bir sunum sağlar.
- ✓ Önde gelen 3. taraf yayınlarından ve ayrıca kendi tescilli kaynaklarımızdan algılama ve zenginleştirme için **entegre tehdit istihbaratı**.

## ÖDÜLLER VE ONAYLAR

**ATT&CK®**

**2020 MITRE ATT&CK**

- En az GÖZDEN kaçırma
- En Yüksek Teknik + Taktik Korelasyonları
- En İyi Veri Zenginleştirme Kapsamı

**FORRESTER®**

**2020 FORRESTER WAVE™ EDR**

"Güçlü Performans"

**kuppingercoie**  
ANALYSTS

**2020 KUPPINGERCOLE MARKET COMPASS**

Öne Çıkan EPDR Yenilikçisi

## TEMEL AVANTAJLAR

- + Daha az bekleme süresi
- + Hızlandırılmış IR
- + Azaltılmış MTTR
- + Daha az uyarı yorgunluğu
- + Daha yüksek analist üretkenliği
- + Singularity Platformu bileşeni

## YÖNETİLEN TESPİT & MÜDAHALE

Vigilance MDR, müşterilerin yalnızca önemli olan olaylara odaklanmalarını sağlar ve bu da onu aşırı gerilmiş BT/SOC Ekipleri için mükemmel uç nokta eklenti çözümü haline getirir.

Daha fazla bilgi için:  
<https://s1.ai/s1mdr>

## DEMO İÇİN HAZIR MISINIZ?

Daha fazla bilgi için SentinelOne internet sitesini ziyaret ediniz.

## SentinelOne, Müşteriye Öncelik Veren bir Şirkettir

Sürekli ölçüm ve iyileştirme, müşteri beklentilerini aşmamızı sağlar.

**96%**

Gartner Peer Insights™  
'Voice of the Customer'  
Eleştirmenlerinin %96'sı  
SentinelOne'i öneriyor

**97%**

Müşteri Memnuniyeti  
(CSAT) ~%97'dir

"Harika" ile "mükemmel"  
aralığında  
Net Destekçi Puanı

## SentinelOne Hakkında

2013 yılında kurulan ve merkezi Mountain View, California'da bulunan SentinelOne, bir siber güvenlik yazılım şirkettir. SentinelOne Singularity, tüm kurumsal varlıklar bağlamında önlemek, tespit etmek, yanıt vermek ve avlanmak için kullanılan bir platformdur.



[sentinelone.com](https://sentinelone.com)

sales@sentinelone.com  
+1 855 868 3733

S1-PROD-SINGULARITY\_EPP\_EDR-180920