SentinelOne EXCLUSIVE NETWORKS

DATA SHEET

SentinelOne Uç Nokta Güvenliği

SingularityTM Platform Ürün Paketleri

SentinelOne Singularity güvenlik platformu, hassas bilgi içeren verileriniz için, günümüzün karmaşık tehditlerine karşı daha verimli koruma sağlayarak, SOC ve BT Operasyon Ekiplerini güçlendirir.

Singularity özelliği, farklılaştırılmış uç nokta koruması, uç nokta tespiti ve müdahalesi, IoT güvenliği, bulut güvenliği ve BT operasyon yetenekleri sunarak, birden fazla mevcut teknolojiyi tek bir çözümde birleştirir. SentinelOne, Windows, Mac, Linux ve Kubernetes için kaynak açısından verimli otonom ajanlar sunar ve fiziksel, sanal, VDI, müşteri veri merkezleri, hibrit veri merkezleri ve bulut hizmeti sağlayıcıları dahil olmak üzere çeşitli form faktörlerini destekler.

Sentinel'ler, kullanım kolaylığına ve gereksinimlerinizi karşılayan esnek yönetime yönelik olarak tasarlanmış, küresel olarak mevcut çok kiracılı SaaS aracılığıyla yönetilir. SentinelOne'ın Vigilance Yönetilebilir Tespit ve Müdahele (MDR) hizmetleri aboneliği, güvenlik organizasyonunuzu 7 gün 24 saat desteklemek için hazırdır.

Bu döküman, SentinelOne'ın Singularity Core, Control ve Complete olarak bilinen katmanlı ürün tekliflerini açıklamaktadır. Her ürün paketi, altındakinin üzerine kurulur.

Singularity Complete Güvenlik Operasyonları	Görünürlüğü, arama ve IR yeteneklerini iyileştirmek için EDR ekleyin / değiştirin
Singularity Control IT OPS Hygiene	Daha az uç nokta aracısıyla birleştirin
Singularity Core Uç Nokta Koruması	Etkisiz AV ve NGAV ürünlerini değiştirin
Singularity Platform	Küresel SaaS Platformu Uç nokta. Bulut. IoT.

NEDEN SENTINELONE'I SEÇMELİSİNİZ?

- SentinelOne, EPP+EDR'yle gerçek anlamda birleşir; böylece fazlalık uç nokta aracılarını ortadan kaldırabilir ve operasyon giderlerini düşürebilirsiniz.
- %97 müşteri desteği memnuniyeti
- Müşterilerin %97'si SentinelOne'ı öneriyor
- Zaman kazandıran iş akışlarına sahip özelleştirilebilir konsol
- Üstün davranışsal yapay zeka ile çözülen fidye yazılımı
- Anında tetiklenen otonom koruyucu müdahaleler
- Olaylara müdahale edenler ve tehdit avcıları için tasarlanmış ActiveEDR® ile zaman kazandıran, yorgunluğu azaltan Storyline™
- Tam geçmiş analizi için 365+ gün süreli, uygun fiyatlı EDR veri saklama
- Diğer üreticiler ile kolay XDR entegrasyonları

DEMO İÇİN HAZIR MISINIZ?

Daha fazla bilgi için SentinelOne web sitesini ziyaret edin

Singularity Platform Özellikleri ve Teklifleri

Tüm SentinelOne müşterileri, aşağıdaki SaaS yönetim konsolu özelliklerine erişebilirler:

- Global SaaS uygulaması. Yüksek kullanılabilirlik. Konum seçimi (ABD, AB, Asya Pasifik).
- Esnek idari kimlik doğrulaması ve yetkilendirme: SSO, MFA, RBAC
- Kuruluş yapınıza uyacak şekilde özelleştirilebilir yönetim
- 365 gün tehdit olay geçmişi
- Entegre SentinelOne Tehdit İstihbaratı ve MITRE ATT&CK Tehdit Göstergeleri
- Veriye dayalı kontrol paneli güvenlik analitiği
- E-posta ve sistem günlüğü ile yapılandırılabilir bildirimler
- Tek tıklamalı uygulamalardan oluşan Singularity Marketplace ekosistemi
- 340+ işleve sahip tek API

Singularity™ Core

Tüm SentinelOne uç nokta güvenlik tekliflerinin temelinde Core bulunmaktadır. Eski AV veya NGAV'ı daha etkili ve yönetimi kolay bir EPP ile değiştirmek isteyen kuruluşlar için giriş seviyesi uç nokta güvenliği ürünüdür. Core ayrıca, EPP+EDR yeteneklerinin gerçek birleşimini gösteren temel EDR işlevlerini de sunar. Tehdit İstihbaratı, standart teklifimizin bir parçası olup, AI işlevlerimiz ve SentinelOne Cloud aracılığıyla entegre edilmiştir. Singularity Core'un özellikleri aşağıdaki gibidir:

- **Yerleşik Statik Yapay Zeka ve Davranışsal Yapay Zeka analizi,** çok çeşitli saldırıları hasara neden olmadan önce gerçek zamanlı olarak önler ve tespit eder. Core ise, bilinen ve bilinmeyen kötü amaçlı yazılımlara, Trojenlara, korsanlık araçlarına, fidye yazılımlarına, bellek istismarlarına, komut dosyasının kötüye kullanımına, kötü makrolara ve daha fazlasına karşı koruma sağlar.
- **Sentinel'ler otonomdur,** yani bulut bağlantısı olsun veya olmasın, önleme ve tespit teknolojisi uygular ve gerçek zamanlı olarak koruyucu yanıtları tetiklerler.
- **Kurtarma işlemi hızlıdır** ve kullanıcıların işletme sistemini ve tüm yazılımı kaldırıp sistemi tekrar kurmaksızın ve komut dosyası yazmaksızın, dakikalar içinde tekrar işlerinin başına dönmesini sağlar. Saldırı sırasında meydana gelen tüm yetkisiz değişiklikler, Windows için Tek Tıkla Düzeltme ve Tek Tıkla Geri Dönüş ile geri alınabilir.
- **Güvenli SaaS yönetimi erişimi.** ABD, AB, Asya Pasifik bölgeleri arasından seçim yapın. Veriye dayalı kontrol panelleri, site ve gruba göre politika yönetimi, MITRE ATT&CK entegrasyonu ile olay analizi ve daha fazlası.

Singularity™ Control

Control, uç nokta yönetimi için "güvenlik paketi" özelliklerinin eklenmesiyle Singularity Core'da bulunan türünün en iyisi güvenliği arayan kuruluşlar için yapılmıştır. Control, **Core'un tüm özelliklerinin** yanı sıra aşağıdakileri içerir:

- Konum farkındalığı dahil olmak üzere cihazlara ve cihazlardan ağ bağlantısının kontrolü için **Güvenlik Duvarı Kontrolü**
- USB cihazlarının ve Bluetooth/BLE çevre birimlerinin kontrolü için **Cihaz Kontrolü**
- Sentinel ajan korumasına ihtiyaç duyan ağ üzerindeki cihazları ortaya çıkarmak için **rogue görünürlüğü**
- MITRE CVE veri tabanına eşlenen bilinen güvenlik açıklarına sahip 3. taraf uygulamalarına ilişkin içgörü için Uygulama Envanterine ek olarak **Güvenlik Açığı Yönetimi**

SENTINELONE, DAVRANIŞSAL YAPAY ZEKA VE GÜÇLÜ OTOMATİK İYİLEŞTİRME FONKSİYONLARI İLE FİDYE YAZILIMI VE DİĞER DOSYASIZ SALDIRILARI DURDURUR

Singularity Complete

Complete, modern uç nokta koruması ve kontrolüne ek olarak ActiveEDR® adını verdiğimiz gelişmiş EDR özelliklerine ihtiyaç duyan kuruluşlar için üretilmiştir. Complete ayrıca, her gün her saniye tüm işletim sistemi süreç ilişkilerini [yeniden başlatmalarda bile] otomatik olarak belirli bir bağlama oturtan ve bunları gelecekteki araştırmalarınız için depolayan patentli Storyline™ teknolojisine sahiptir. Storyline™, analistleri sıkıcı olay korelasyon görevlerinden kurtarır ve onları kök nedene hızlı bir şekilde ulaştırır. Singularity Complete, telemetriyi otomatik olarak ilişkilendirerek ve MITRE ATT&CK® çerçevesiyle eşleştirerek; güvenlik yöneticileri, SOC analistleri, tehdit avcıları ve olay müdahale ekipleri üzerindeki yükü hafifletmek için tasarlanmıştır. En zeki küresel kuruluşlar, boyun eğmeyen siber güvenlik talepleri için Singularity Complete'i kullanıyor. Complete, tüm Core ve Control özelliklerinin yanı sıra **aşağıdakileri** içerir:

- Hızlı RCA ve kolay pivotlar için **Patentli Storyline TM**
- Hem iyi niyetli hem de kötü niyetli verilere entegre **Active EDR®** görünürlüğü
- 14 günden 365+ güne kadar, **her ihtiyaca uygun veri saklama seçenekleri**
- **MITRE ATT&CK® Tekniği ile avlanın**
- EPP işlevleri tarafından uygulanması için **İyi niyetli Storyline'ları tehdit olarak işaretleyin**
- **Storyline Active Response (STAR™)** ile özel tespitler ve otomatik avlanma kuralları
- Zaman çizelgeleri, uzak kabuk, dosya getirme, korumalı alan entegrasyonları ve daha fazlası

Gartner peerinsights™

"

Etkileyici özellikler. Dağıtımı ve EDR kullanımı kolay.

Siber Güvenlik Direktörü – Sağlık Hizmetleri
1 Milyar – 3 Milyar USD

Gartner peerinsights™

"

SOC'nin güvenebileceği tek platform.

Güvenlik & Risk Yönetimi - Finans
50 Milyon – 250 Milyon USD

IT Central Station
Unbiased reviews from the tech community

"

Verimliliğimiz arttı. Kesinlikle yatırımımızın getirisini gördük.

Küresel InfoSec Direktörü – Üretim
10 Milyar – 25 Milyar USD

Vigilance MDR Hizmetleri Aboneliği

SentinelOne Vigilance Yönetilebilir Tespit ve Müdahele (MDR), müşteri güvenliği kuruluşlarını artırmak üzere tasarlanmış bir hizmet aboneliğidir. Vigilance MDR, her tehdidin incelenmesini, tehdide göre harekete geçilmesini, tehdidin belgelenmesini ve gerektiğinde bildirilmesini sağlayarak değer katar. Çoğu durumda, tehditleri yaklaşık 20 dakika içinde yorumlar ve çözer ve yalnızca acil konular için sizinle iletişime geçer. Vigilance MDR, müşterilerin yalnızca önemli olan olaylara odaklanmalarını sağlar; bu da onu aşırı gerilmiş BT/SOC Ekipleri için mükemmel uç nokta eklenti çözümü haline getirir.

Daha fazla bilgi için:
www.sentinelone.com/global-services/services-overview/

SentinelOne Readiness Hizmetleri Aboneliği

SentinelOne Readiness, hızlı bir şekilde çalışmaya başlamanızı ve kurulumunuzun zaman içinde sağlıklı kalmasını sağlayan, yapılandırılmış bir metodoloji ile ürün kurulumu öncesinde, sırasında ve sonrasında ekibinize rehberlik etmek üzere tasarlanmış bir danışma abonelik hizmetidir. Readiness müşterilerine en iyi dağıtım uygulamaları konusunda rehberlik edilir, periyodik ajan bilgilendirme yardımı sağlanır ve SentinelOne ürünlerinin optimize edilmesini sağlamak için üç ayda bir ONEscoreTM sağlık kontrollerinden faydalanır.

Daha fazla bilgi için:
www.sentinelone.com/global-services/readiness/

Birlikte Sunulan Özellikler

	Singularity Complete	Singularity Control	Singularity Core
Küresel SaaS Platformu: Güvenli Erişim, Yüksek Kullanılabilirlik, Hiyerarşik Politika Yönetimi, EDR Olay Müdahalesi ve Tehdit Tespiti, Analitik, IoT Kontrolü (Ranger seçeneğiyle), CWS	✓	✓	✓
Güvenlik Operasyonları EDR Özellikleri			
Storyline™ bağlamıyla Deep Visibility ActiveEDR®	✓		
MITRE ATT&CK® Entegrasyonu	✓		
Storyline Active Response (STAR) Özel Algılama Kuralları	✓		
Storyline Active Response (STAR) Pro Özel Algılama Kuralları	+		
İkili Kasa Canlı Kötü Amaçlı Yazılım Yükleme Havuzu	+		
Dosya Bütünlüğü İzleme	✓		
14 günlük EDR Avlama Verilerini Saklama	✓		
365 güne kadar Genişletilmiş EDR Avcılık Verilerini Saklama	+		
Bulut Data Lake Akışı	+		
Güvenli Uzaktan Kabuk	✓	✓	
BT OPS / Güvenlik Hijyeni ve Ürün Özellikleri			
Konum farkındalığına sahip işletim sistemi	✓	✓	
Güvenlik Duvarı kontrolü (Win, Mac, Linux) USB cihaz kontrolü (Win, Mac)	✓	✓	
Bluetooth®/Bluetooth Low Energy® kontrolü (Win, Mac)	✓	✓	
Rogue Cihaz Bulma	✓	✓	
Uygulama Güvenlik Açığı (Win, Mac)	✓	✓	
Temel Uç Nokta Koruması Özellikleri			
Otonom Sentinel ajanı StorylineTM motoru	✓	✓	✓
Statik AI ve SentinelOne Bulut dosya tabanlı saldırı önleme	✓	✓	✓
Davranışsal AI dosyasız saldırı algılama	✓	✓	✓
Otonom Tehdit Müdahalesi/Öldürme, Karantina (Win, Mac, Linux)	✓	✓	✓
Otonom Düzeltme Müdahelesi/ Tek tıkla, komut yazmadan (Win, Mac)	✓	✓	✓
Otonom Geri Dönüş Müdahelesi/ Tek tıkla, komut yazmadan (Win)	✓	✓	✓
Cihazı ağdan karantinaya alma	✓	✓	✓
Olay Analizi (MITRE ATT&CK®, zaman çizelgesi, explorer, ekip ek açıklamaları)	✓	✓	✓
Ajan kurcalama önleme	✓	✓	✓
Uygulama Envanteri	✓	✓	✓

Opsiyonel Paketler

	Singularity Complete	Singularity Control	Singularity Core
Singularity RANGER			
Ağ Varlık Envanteri	+	+	
Ağ Saldırısı Yüzey Kontrolü	+	+	
Ajan Otomatik Dağıtımı (Çok Yakında)	+	+	
Tespit Araçları - Tehdit Temelli	+		
Singularity Cloud			
Kubernetes ve VM'ler için Bulut İş Yükü Güvenliği	+	+	+
Bulut Sağlayıcı Meta Veri Entegrasyonu	+	+	+
Kubernetes için Otomatik Uygulama Kontrolü Linux	+	+	
VM'ler için Otomatik Uygulama Kontrolü	+		
İş Yükleri için CIS Karşılaştırmaları (Çok Yakında	+		

Küresel Destek ve Hizmet Teklifleri

Telefon, web ve e-posta yoluyla teknik destek	**Dahil**
Ürün içi kaynak merkezi / Destek portalı erişimi	**Dahil**
Standart 9x5 Destek	**Dahil**
Kurumsal Destek 24x7x365, Sev 1 & 2 için Follow-the-Sun	**Mevcut**
Atanmış Teknik Hesap Yöneticisi + Kurumsal Destek	**Mevcut**
Vigilance Yönetimli Algılama & Yanıt (MDR) Aboneliği	**Mevcut**
Vigilance PRO MDR + DFIR Aboneliği	**Mevcut**
SentinelOne Readiness Dağıtım ve Devam Eden Sağlık Aboneliği	**Mevcut**

SENTINELONE KONUMLARI
Mountain View, CA (HQ)
Tel Aviv, Boston, Amsterdam, Tokyo, Oregon ABD

GLOBAL VERİ MERKEZLERİ
ABD, Frankfurt, Tokyo, AWS GovCloud
Yüksek Kullanılabilirlik

İŞLETİM SİSTEMİ DESTEĞİ

SentinelOne, çok çeşitli Windows, Mac ve Linux dağıtımlarının yanı sıra sanallaştırma işletim sistemlerini de destekler. Yaygın yazılım istisnaları, destek portalımızda belgelenmiştir.

Windows Sentinel ajanı
7 SP1'den Windows 10'a kadar tüm Windows iş istasyonları
2008 R2 SP1'den Server/Core 2019'a kadar tüm Windows Sunucuları

Mac Sentinel ajanı
macOS Big Sur, Catalina, Mojave

Linux Sentinel ajanı
Ubuntu, Redhat (RHEL), CentOS, Oracle, Amazon AMI, SUSE Linux Enterprise Server, Fedora, Debian, Virtuozzo, Scientific Linux

Eski Windows ajanı
XP, Server 2003 & 2008, POS2009

Desteklenen Kap Platformları
Kendi kendine yönetilen ve Yönetilen Kubernetes Hizmetleri (EKS, AKS, GKE), OpenShift

Sanallaştırma ve VDI
Citrix XenApp, Citrix XenDesktop, Oracle VirtualBox, VMware vSphere, VMware Workstation, VMware Fusion, VMware Horizon, Microsoft Hyper-V

Singularity™ Platform

DEMO İÇİN HAZIR MISINIZ?

Daha fazla bilgi için SentinelOne web sitesini ziyaret edin veya +1-855-868-3733 numaralı telefondan bizi arayın.

ATT&CK®

2020 MITRE ATT&CK

- **En Az Kaçırma**
- **En Fazla Korelasyon**
- **En İyi Veri Zenginleştirme Kapsamı**

FORRESTER®

2020 FORRESTER WAVE™ EDR

"Güçlü Performans"

kuppingercole ANALYSTS

2020 KUPPINGERCOLE MARKET COMPASS

Öne Çıkan EPDR Yenilikçisi

SentinelOne, Müşteriye Öncelik Veren bir Şirkettir

Sürekli ölçüm ve iyileştirme, müşteri beklentilerini aşmamızı sağlar.

Gartner peerinsights customers' choice™

97%

Gartner Peer Insights™ 'Voice of the Customer' Eleştirmenlerinin %97'si SentinelOne Çözümlerini Önderdi,

97%

Müşteri Memnuniyeti

FR FedRAMP

ISO 27001 CERTIFIED by schellman

EU GDPR COMPLIANT

SE Labs AAA

TEVORA

PCI DSS Attestation
HIPAA Attestation

Gartner peerinsights™ 4.9 ★★★★★

SentinelOne Hakkında

Daha Fazla Yetenek Daha Az Karmaşıklık SentinelOne, güvenlik yığınını kurumsal yeteneklerden vazgeçmeden basitleştirmeyi amaçlayan otonom, dağıtılmış uç nokta istihbaratıyla siber güvenliğin geleceğine öncülük ediyor. Teknolojimiz, insanları otomasyon ve sorunsuz tehdit çözümü ile ölçeklendirmek üzere tasarlanmıştır. Hazır mısınız?

Exclusive Networks Hakkında

Exclusive Networks olarak, firmaların dijital dönüşüm yolculuklarında, altyapı sistemlerinin güvenliğini ve sürekliliğini sağlamak en önemli görevimiz.

Benzersiz stratejilerimiz ile, iş ortaklarımıza daha çok fırsat sağlıyor ve müşteri ilişkilerini güçlendirmelerine yardımcı oluyoruz. Bizim uzmanlığımız, onların gücü – sürekli gelişen teknolojileri ve değişen iş modellerini yönetebilmeleri için, onlara uçtan uca eğitimler ve profesyonel hizmetlerimiz ile, destek veriyoruz.Exclusive Networks'ün hikayesi, tüm Dünya'ya yayılmış, 'önce hizmet' anlayışı ile, yeniliği ve özgünlüğü birleştirmiş sektörün büyüme hızının da önüne geçmiştir. 100 ülkede, 50'den fazla ofisimizle, eşsiz 'Global vizyon, yerel çözümler' modelini benimsiyoruz.

sentinelone.com
sales@sentinelone.com
+ 1 855 868 3733
S1-PROD-CCC-03312021
exclusive-networks.com/tr
info_tr@exclusive-networks.com