SOPHOS

EVOLVE

SOPHOS

Sophos XG Firewall

Dünyanın en iyi görünürlüğü, koruması ve müdahale.
Sophos XG Firewall, güvenlik duvarınızı nasıl yönettiğinize, tehditlere nasıl müdahale ettiğinize ve ağınızda olup bitenleri nasıl izlediğinize yeni bir yaklaşım getiriyor.

Öne Çıkan Noktalar

- Yeni nesil ağ koruması
- Security Heartbeat™ ve Senkronize Uygulama Kontrolü ile senkronize güvenlik
- Kullanıcı, uygulama ve ağ kontrolü bir arada
- Yanal Hareket Koruması
- Anında görünürlük
- Güçlü yönetim ve ölçeklenebilirlik
- Birçok aygıt için modüler bağlanırlık ve yedeklilik

Sophos XG Firewall

Sophos XG Firewall, gizli riskleri ortaya çıkaran, bilinmeyen tehditleri engelleyen ve olaylara otomatik olarak müdahale eden, kapsamlı bir yeni nesil güvenlik duvarı sağlamaktadır.

Gizli riskleri ortaya çıkarır

Sophos XG Firewall, riskli etkinlikler, şüpheli trafik ve gelişmiş tehditler konusunda benzersiz görünürlük sağlayarak ağınızın kontrolünü yeniden ele almanıza yardımcı olur. Ek ücrete tabi olmayan etkinlik odaklı kontrol merkezini ve kapsamlı cihaz üzerinde raporlamayı çok seveceksiniz. Başka hiçbir güvenlik duvarı, XG Firewall'dan daha iyi bilgi vermez.

Bilinmeyen tehditleri engeller

Sophos XG Firewall, ağınızı fidye yazılımları ve gelişmiş tehditlerden korumanız için en beğenilen IPS, Gelişmiş Tehdit Koruması, Deep Learning ile Bulut Korumalı Alan, Dual AV, Web ve Uygulama Kontrolü, E-posta Koruması ve tam kapsamlı bir Web Uygulaması Güvenlik Duvarı gibi ihtiyacınız olan en son ve en gelişmiş tüm teknolojileri sağlar. Üstelik kurulumu ve yönetmesi kolaydır.

Olaylara otomatik olarak müdahale eder

XG Firewall, ağınıza bulaşan bir tehdidin kaynağını tamamen tespit edebilen ve bunun karşısında diğer ağ kaynaklarına erişimi otomatik olarak sınırlandıran tek ağ güvenliği çözümüdür. Bu da korsanları ve saldırıların yayılmasını durdurmak için Sophos uç noktaları ve güvenlik duvarınız arasında telemetri ve sağlık durumunu paylaşarak Yanal Hareket Koruması sağlayan benzersiz Sophos Security Heartbeat™ teknolojimiz sayesinde mümkün olmaktadır.

Etkili, güçlü ... hızlı

Yatırımınızın karşılığını en iyi şekilde verecek, üstün performans ve güvenlik verimliliği sunacak XG Firewall'u geliştirdik. Aygıtlarımız Intel çok çekirdekli teknolojileri, katı hal diskleri ve hızlandırılmış bellekte içerik tarama kullanılarak yapılmıştır.

Birden fazla güvenlik duvarını kolayca yönetin

Sophos Central, tüm Sophos ürünleriniz için bulut yönetimini yürüteceğiniz nihai platformudur. XG Firewall'unuzun günlük kurulumunu, izlenmesini ve yönetimini kolaylaştırır. Uyarı verme, yedekleme yönetimi, tek tıkla aygıt yazılımı güncellemeleri ve yeni güvenlik duvarlarının hızlı tedariki gibi faydalı özellikler sunar.

Sophos XG Serisi Aygıtlara genel bakış

XG Serisi donanım aygıtlarımız, en son Intel çok çekirdekli teknolojileri, cömert RAM tedariki ve katı hal depolama teknolojileriyle amaca yönelik olarak üretilmektedir. İster küçük bir işletmeyi, ister büyük bir veri merkezini koruyor olun, sektörde öncü bir performans, esnek bağlanırlık ve en üst düzey güvenilirlik alırsınız.

Ürün Matrisi

Model			Tek. Özellikler			Veri hacmi[1]			
	Revizyon #	Biçim Katsayısı	Port/Yuva Sayısı (Maks Port Sayısı)	w-model 802.11 kablosuz	Değiştirilebilir Bileşenler	Güvenlik Duvarı (Mbps)	VPN (Mbps)	NGFW (Mbps)	AV vekil sunucusu (Mbps)
XG 86(w)	1	masaüstü	4	a/b/g/n/ac	mevcut değil	3.000	225	310	360
XG 106(w)	1	masaüstü	4	a/b/g/n/ac	ops. har. Güç	3.500	360	480	450
XG 115(w)	3	masaüstü	4	a/b/g/n/ac	ops. har. Güç	4.000	490	1.000	600
XG 125(w)	3	masaüstü	9/1 (9)	a/b/g/n/ac	ops. har. Güç, 3G/4G	6.500	700	1.100	700
XG 135(w)	3	masaüstü	9/1 (9)	a/b/g/n/ac	ops. har. Güç, 3G/4G, Wi-Fi*	8.000	1.180	1.200	1.580
XG 210	3	1U	8/1 (16)	mevcut değil	ops. har. Güç	16.000	1.450	2.900	2.300
XG 230	2	1U	8/1 (16)	mevcut değil	ops. har. Güç	20.000	1.700	3.500	2.800
XG 310	2	1U	12/1 (20)	mevcut değil	ops. har. Güç	28.000	2.750	4.500	3.300
XG 330	2	1U	12/1 (20)	mevcut değil	ops. har. Güç	33.000	3.200	6.200	6.000
XG 430	2	1U	10/2 (26)	mevcut değil	ops. har. Güç	41.000	4.800	7.000	6.500
XG 450	2	1U	10/2 (26)	mevcut değil	ops. dah. Güç	50.000	5.500	9.200	7.000
XG 550	2	2U	8/4 (32)	mevcut değil	Güç, SSD, Fan	65.000	8.400	11.700	10.000
XG 650	2	2U	8/6 (48)	mevcut değil	Güç, SSD, Fan	85.000	9.000	16.400	13.000
XG 750	2	2U	8/8 (64)	mevcut değil	Güç, SSD, Fan	100.000	11.000	18.550	17.000

* 2. Wi-Fi modülü seçeneği sadece 135w içindir (XG v17 MR6 veya üstü gerekir)

Sophos XG Firewall Avantaj Paketleri

Nihai koruma, değer, gönül rahatlığı için kullanışlı avantaj paketlerimizden birini alın.

Ne alıyorsunuz	EnterpriseProtect Plus Paketi	TotalProtect Plus Paketi
Temel Güvenlik Duvarı Güvenlik Duvarı, IPsec ve SSL VPN, Kablosuz Koruması (erişim noktaları ayrıca satılır)	✓	✓
Ağ Koruması IPS, RED, HTML5 VPN, ATP, Security Heartbeat	✓	✓
Web Koruması Kötü Amaçlı Yazılım Koruması, Web ve Uygulama görünürlüğü, kontrolü ve koruması	✓	✓
E-posta Koruması İstenmeyen E-posta, SPX E-Posta Şifreleme ve Veri Kaybı Koruması		✓
Web Sunucusu Koruması Web Uygulaması Güvenlik Duvarı ve ters vekil sunucu		✓
Sandstorm Koruması Next-Gen bulut tabanlı korumalı alan teknolojisi	✓	✓
Gelişmiş Destek 24x7 destek, güvenlik ve yazılım güncellemeleri, gel. değişim garantisi	✓	✓
XG Serisi Donanım Aygıtı Çok çekirdekli Intel işlemci, katı hal depolama, esnek bağlanırlık	✓	✓

Ücretsiz deneyin

30 günlük ücretsiz değerlendirme için **sophos.com/xgfirewall** adresine kaydolun

SOPHOS

Intercept X Advanced with EDR

Akıllı Uç Nokta Tespiti ve Müdahalesi

Sophos Intercept X Advanced with EDR, akıllı uç nokta tespiti ve müdahalesini (EDR) sektördeki en beğenilen kötü amaçlı yazılım tespiti, en beğenilen yetkisiz erişim koruması ve diğer benzersiz uç nokta koruma özellikleriyle bir araya getiriyor.

Öne Çıkan Noktalar

- EDR en güçlü uç nokta koruması ile birlikte
- Deep Learning Teknolojisi ile Kötü Amaçlı Yazılım analizi
- İstek üzerine SophosLabs tarafından düzenlenen tehdit istihbaratı
- Machine Learning ile şüpheli olay* tespiti ve önceliklendirme
- Kılavuz eşliğinde incelemeler, EDR'yi ulaşılabilir aynı zamanda güçlü bir hale getiriyor
- Tek tıkla olaylara müdahale

EDR En Güçlü Koruma ile Başlar

İhlalleri başlamadan durdurmak için önleme çok önemlidir. Intercept X, eşsiz korumayı, uç nokta tespitini ve müdahaleyi tek bir çözümde bir araya getiriyor. Bu da çoğu tehdidin henüz bir zarar veremeden durdurulması anlamına geliyor ve Intercept X Advanced with EDR olası güvenlik tehditlerini tespit etme, inceleme ve bunlara müdahale edebilme olanağıyla ilave siber güvenlik teminatı sağlıyor.

EDR'nin istikrarlı bir şekilde en beğenilen uç nokta koruma paketine dahil edilmesi, Intercept X'in EDR iş yükünü büyük ölçüde hafifletmesini sağlıyor. Tehditler ne kadar çok önlenirse güvenlik ekiplerinin incelemesi gereken o kadar az rahatsızlık ortaya çıkar. Bu da ekiplerin kilit kaynakları optimize ederek yalancı pozitiflerin ve bunaltıcı uyarı hacmiyle uğraşmak yerine IT işine odaklanabilmeleri anlamına geliyor.

Uzmanlığı artırın, kişi sayısını değil

Intercept X Advanced with EDR, normalde yetenekli analistlerin yerine getirdiği görevleri yapar ve böylece kuruluşlar personel sayısını artırmadan bünyelerindeki uzmanlığı artırabilir. Sorular soracak ve veriyi yorumlayacak yüksek becerilere sahip insan analistler gerektiren diğer EDR çözümlerinin aksine Intercept X Advanced with EDR, gücünü Machine Learning'den alır ve SophosLabs tarafından düzenlenen tehdit istihbaratıyla geliştirilir.

Güvenlik uzmanlığı*: Intercept X Advanced with EDR, olası tehditleri otomatik olarak tespit edip önceliklendirerek güvenlik uzmanlığını IT'ye teslim eder. Machine Learning kullanılarak şüpheli olaylar tespit edilir ve en önemli, derhal ilgilenilmesi gereken durumlar olarak belirlenir. Analistler hızlı bir şekilde neye odaklanmaları gerektiğini görebilir ve hangi makinelerin etkilenmiş olabileceğini anlarlar.

Kötü amaçlı yazılım uzmanlığı: Çoğu kuruluş, şüpheli dosyaları analiz etmek için ters mühendislik konusunda uzmanlaşmış kötü amaçlı yazılım uzmanlarına dayanır. Bu yaklaşım yalnızca zaman alıcı ve başarması zor olmakla kalmaz, aynı zamanda çoğu kuruluş sahip olmadığı bir siber güvenlik kapsamı gerektirir. Intercept X Advanced with EDR, kötü amaçlı yazılımları otomatik olarak aşırı ayrıntılı bir şekilde analiz eden, dosya öz niteliklerini ve kodu çözümleyen, bunları milyonlarca başka dosyayla karşılaştıran Deep Learning Teknolojisi ile Kötü Amaçlı Yazılım Analizinden yararlanarak daha iyi bir yaklaşım sunar. Analistler kolaylıkla hangi öz niteliklerin veya kodların "bilinen iyi" ve "bilinen kötü" dosyalara benzediğini görerek bir dosyanın engellenmesi mi, yoksa buna izin verilmesi mi gerektiğini belirleyebilir.

Tehdit istihbaratı uzmanlığı: Intercept X Advanced with EDR olası şüpheli bir dosyaya dikkat çektiğinde IT yöneticileri, SophosLabs tarafından düzenlenen ve her gün yaklaşık 400.000 tane daha önce görülmemiş kötü amaçlı yazılım örneği alan ve işleyen istek üzerine tehdit istihbaratına erişerek daha fazla bilgi toplayabilirler. Bu ve diğer tehdit istihbaratı toplanır, kümelenir ve kolay analiz edilebilmesi için özetlenir. Bu da sadece tehdit istihbaratı konusunda çalışan analistleri veya pahalı ve anlaşılması zor tehdit yayınlarına erişimi bulunmayan ekiplerin dünyadaki en iyi siber güvenlik araştırması ve veri bilimi ekiplerinden birinden yararlanabilmesi anlamına gelir.

Kılavuzlu tehdit müdahalesi

Intercept X Advanced with EDR, bir saldırının kapsamını, nasıl başladığını, nelerin etkilendiğini ve nasıl müdahale edilmesi gerektiğini göstererek yöneticilerin güvenlik olaylarıyla ilgili zor soruları yanıtlayabilmelerine olanak sağlar. Her türlü beceri düzeyindeki güvenlik ekipleri, atılacak sonraki adım önerileri, net görsel saldırı sunumları ve tümleşik uzmanlık sunan kılavuz eşliğinde incelemeler sayesinde güvenlik tutumlarını hızlıca anlayabilir.

Bir inceleme tamamlandığında analistler bir düğmeye tıklayarak müdahale edebilir. Hızlı müdahale seçenekleri arasında derhal iyileştirme sağlamak için uç noktalarını izole etme, dosyaları temizleme ve engelleme, adli anlık görüntüler oluşturma bulunur.

Akıllı EDR Kullanım Örnekleri

Akıllı uç nokta tespiti ve müdahalesi, güvenlik ekiplerinin bir olaya müdahale çalışması çerçevesinde sorulan zor soruları yanıtlayabilmek için ihtiyaç duydukları görünürlüğe ve uzmanlığa sahip olması anlamına gelir.

Bir olay hakkındaki zor soruları yanıtlama:

- Güvenlik olaylarının kapsamını ve etkisini anlama
- Fark edilmeyen olası saldırıları tespit etme
- Ağdaki tehdit belirtilerini arama
- İleri safhadaki araştırmalar için olayları önceliklendirme
- Dosyaları tehdit niteliğinde olmaları ya da istenmeme olasılıkları bakımından analiz etme
- Kuruluşunuzun güvenlik tutumu hakkında her an gizli raporlama

EDR'nin ötesinde

En geniş tehdit yelpazesini durdurmak için Intercept X Advanced with EDR, tek bir ana güvenlik tekniğine güvenmektense uç nokta koruması için kapsamlı bir derinlemesine savunma yaklaşımı getirir. İşte bu "artının gücüdür". Yani, önde gelen temel ve modern tekniklerin bir kombinasyonu. Intercept X Advanced with EDR, sektördeki en beğenilen kötü amaçlı yazılım tespiti, en beğenilen yetkisiz erişim koruması, akıllı uç nokta tespiti ve müdahalesini (EDR) bir araya getirir.

Modern teknikler, derin öğrenme teknolojili kötü amaçlı yazılım tespiti, erişim koruması ve fidye yazılımı korumasının belirli özelliklerini içerir. Temel teknikler arasında antivirüs, davranış analizi, kötü amaçlı trafik tespiti, veri kaybını önleme ve daha fazlası bulunur.

Intercept X Advanced with EDR, uç nokta tespiti ve müdahalesi becerilerini Intercept X'teki modern özellikler ve Sophos Merkezi Endpoint Protection dahilindeki temel teknikler ile birleştirir. Bu tek bir birimde tek bir çözüm olarak tedarik edilir.

	Sophos Intercept X Advanced with EDR	Sophos Intercept X Advanced	Sophos Intercept X	Sophos Endpoint Protection
Temel teknikler	✓	✓		✓
Deep learning	✓	✓	✓	
Yetkisiz erişimi önleme	✓	✓	✓	
CryptoGuard fidye yazılımı önleme	✓	✓	✓	
Uç nokta tespiti ve müdahalesi (EDR)	✓			

Ücretsiz deneyin

30 günlük ücretsiz değerlendirme için sophos.com/intercept-x adresine kaydolun

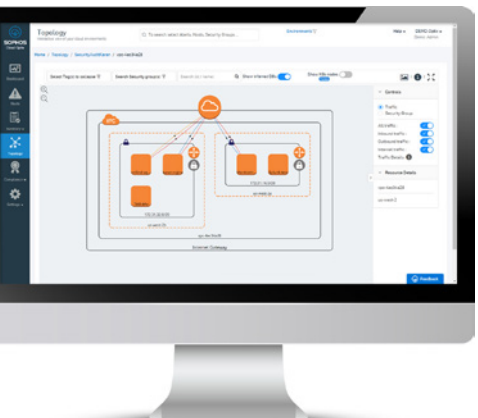
SOPHOS

Sophos Cloud Optix

Yapay zeka ve otomasyonun gücünü birleştirerek bulut güvenliğini basitleştirin
Aracısız, SaaS tabanlı Sophos Cloud Optix hizmeti, derin güvenlik uzmanlığını yapay zekanın gücüyle bir araya getiriyor. Kullanımı kolay tek bir arayüzle süreçleri verimli bir şekilde yöneterek bulut güvenliği izleme, analiz ve uyumluluk otomasyonu sağlıyor.

Öne Çıkan Noktalar

- Beş dakikada kurulan, aracısız, SaaS tabanlı hizmet
- Birden fazla bulut sağlayıcısı üzerinde envanter yönetimi
- Eksiksiz ağ topololojisi ve trafik akışı görselleştirme
- Yapay zeka tabanlı kullanıcı davranışı ve trafik anormalliği tespiti
- Sürekli uyumluluk değerlendirmeleri
- Bir dizi kullanıma hazır uyumluluk politikası
- Uyarı bağlantısı sayesinde daha hızlı iyileştirme
- Kritik öneme sahip ayarlardaki değişiklikleri tespit etme
- Kod halindeki altyapı şablonlarını sürekli tarama



Her şeyi görün, her şeyi güvence altına alın

Sürekli varlık izleme, ağ topolojisi, gelen, giden ve dahili trafik de dahil trafik görselleştirme ile kuruluşunuzun Amazon Web Services (AWS), Microsoft Azure ve Google Cloud Platform (GCP) ortamlarındaki varlıkları otomatik olarak keşfedilerek ekibinize dakikalar içinde müdahale ederek iyileştirme olanağı sağlanır.

Proaktif bulut uyumluluğu

İş yükleri buluta aktarılırken, hangi uyumluluk süreçlerinin uygulanacağını belirlemek giderek daha zor bir hal almaktadır; bunların nasıl hayata geçirileceğinden bahsetmiyoruz bile. Cloud Optix, kullanıma hazır şablonlar, özel politikalar ve iş birliği araçlarıyla yönetimin maliyetini ve karmaşıklığını, riski ve uyumluluğu düşürür.

Uyumluluk sürecini hızlandırın

CIS, GDPR, SOC2, HIPAA, ISO 27001 ve PCI DSS gibi standartlar için özel veya kullanıma hazır şablonlarla uyumluluğu sürekli izleyebilirsiniz.

İş birliği artık daha kolay

JIRA ve ServiceNow gibi araçlarla üçüncü taraf entegrasyonlar kullanarak piyasaya sürme sırasında dahi uyumluluğu yöneterek ve takip ederek önemli görevlerin asla kaybolmamasını sağlayın.

Yapay zeka güdümlü güvenlik analizi ve izleme

Cloud Optix, bulut varlık envanterinizi, konfigürasyonlarınızı ve ağ trafiğinizi sürekli izleyerek bunları öğrenir. Yapay zeka güdümlü akıllı uyarılar, bağlam bilgisiyle birlikte otomatik uyarı tasnifi sayesinde müdahale sürelerini düşürür ve güvenlik risklerini çözüme ulaştırmaya yardımcı olur.

- Bulut varlık envanterini (Amazon Simple Storage Service (S3), Güvenlik Grupları, kullanıcı erişim şifresi vb.), konfigürasyonları ve Güvenlik Grubu günlüklerini sürekli izleme
- Kullanıcı erişim şifrelerinin çalınması veya dolandırıcı çalışanlar nedeniyle gerçekleşen gelişmiş otomatik saldırıları tespit etmek için anormal kullanıcı davranışı örüntülerini belirleme
- Güvenlik ayarlarınız temelinde ağ trafiğinin nasıl akması gerektiğini tahmin ederek saldırılar başlamadan olası ihlal noktalarını önleme
- Ağ konfigürasyonunda kazayla veya kötü niyetli olarak yapılan değişiklikleri önlemek, tespit etmek ve gidermek için bariyerler oluşturma

Daha Akıllı DevSecOps

Sürekli yükleme sayesinde kod halindeki altyapıda gerçekleşen değişikliklerin hızlı olması ve DevOps uygulamaları günde birkaç kez piyasaya yeni yazılım sürülmesine olanak sağlar. Bu da güvenlik ekiplerinin üzerinde muazzam bir baskı oluşturarak tehlikelere maruz kalmanıza neden olabilir. Cloud Optix API güdümlü mimarisi, DevOps ekiplerinizin güvenliği kendi DevOps süreçlerine entegre etmeleri ve böylece hızlı ve güvenli tedarik sağlanması olanağı sunar.

Kayma tespiti ve bariyerler

Konfigürasyon standartlarındaki kaymayı sürekli izleyin ve tespit edin, kritik ayarlarda kuruluşunuzu güvenlik açıklarına maruz bırakabilecek değişiklikler olmasını önleyin.

Proaktif altyapı şablonu tarama

Terraform, Github veya Bitbucket gibi çözümler tarafından yüklenen kod halindeki altyapı şablonlarını sürekli tarayın. Altyapının savunmasız olmasına neden olabilecek hatalı konfigürasyonları belirleyin.

SIEM ve DevOps aracı entegrasyonu

Güvenlik operasyonlarını basitleştirmek için SIEM ve CI/CD için DevOps araçları gibi üçüncü taraf güvenlik araçlarını entegre edin.

Yönetimi ve yüklemeyi basitleştirin

Aracısız, SaaS tabanlı Cloud Optix hizmeti, mevcut iş araçlarınızla mükemmel bir şekilde çalışır.

Verilen talimatlar ve yerli bulut API'leri üzerinden Salt Okunur erişim oluşturan betikler sayesinde AWS, Azure veya GCP'deki bulut hesaplarına bağlanmak kolay bir işlemdir. Sadece dakikalar içinde bağlantılar kurulabilir ve Cloud Optix yüklendikten sonra derhal bulut ortamınızı değerlendirerek size değerli bilgiler sunmaya başlayabilir.

Bulut güvenliği karşılıklı bir sorumluluktur

Kamusal Bulut sağlayıcıları, büyük bir platform esnekliği sunuyor. Onlar veri merkezindeki fiziksel korumadan, verinin ve ortamların sanal tasnifinden sorumludur; ancak buluta koyduğunuz her şeyin güvenliğini sağlamak da sizin sorumluluğunuzdur.

Cloud Optix görünürlük, uyumluluk ve tehdit müdahalesi sağlıyor; Sophos'un kamusal bulut iş yükü koruması ve Next-Gen güvenlik duvarı çözümleri hakkında daha fazla bilgiyi ise sophos.com/public-cloud adresinde bulabilirsiniz.

Sophos Cloud Optix özellikleri	
Birden fazla bulut için tek ekran	✓
Topoloji görselleştirme	✓
Ağ trafiği görselleştirme grafiği	✓
Güvenlik Grubu görselleştirme grafiği	✓
Anormallik tespiti – ağ trafiği	✓
Anormallik tespiti – kullanıcı oturum açma davranışı	✓
Envanter – ana bilgisayarlar, ağlar, depolama, IAM	✓
Envanter – AWS CloudTrail	✓
Envanter – sunucusuz	✓
Sürekli uyumluluk değerlendirmeleri	✓
Uyumluluk politikaları (CIS, FEDRAMP, FFIEC, GDPR, HIPAA, ISO 27001, PCI DSS 3.2, SOC2, EBU R 143)	✓
CIS karşılaştırma politikaları	✓
Özel politikalar	✓
Uyumluluk/en iyi uygulama bildirimleri ve raporlama	✓
İyileştirme ve bariyerler	✓
DevSecOps betik değerlendirmesi	✓

Demo veya hemen ücretsiz deneyin

Tüm Cloud Optix özellikleri 30 gün boyunca ücretsiz Sophos.com/cloud-optix.

İstanbul
Tel: +90 216 663 61 61
Palladium Ofis ve Residence Binası, Barbaros Mahallesi
Halk Caddesi No:8/A Kat:2-3, Ataşehir, 34746 İstanbul

Orta Doğru ve Afrika
Tel: +971 (0)43754332
E-posta: salesmea@sophos.com

2019-12-16 DSTR (MP)

SOPHOS