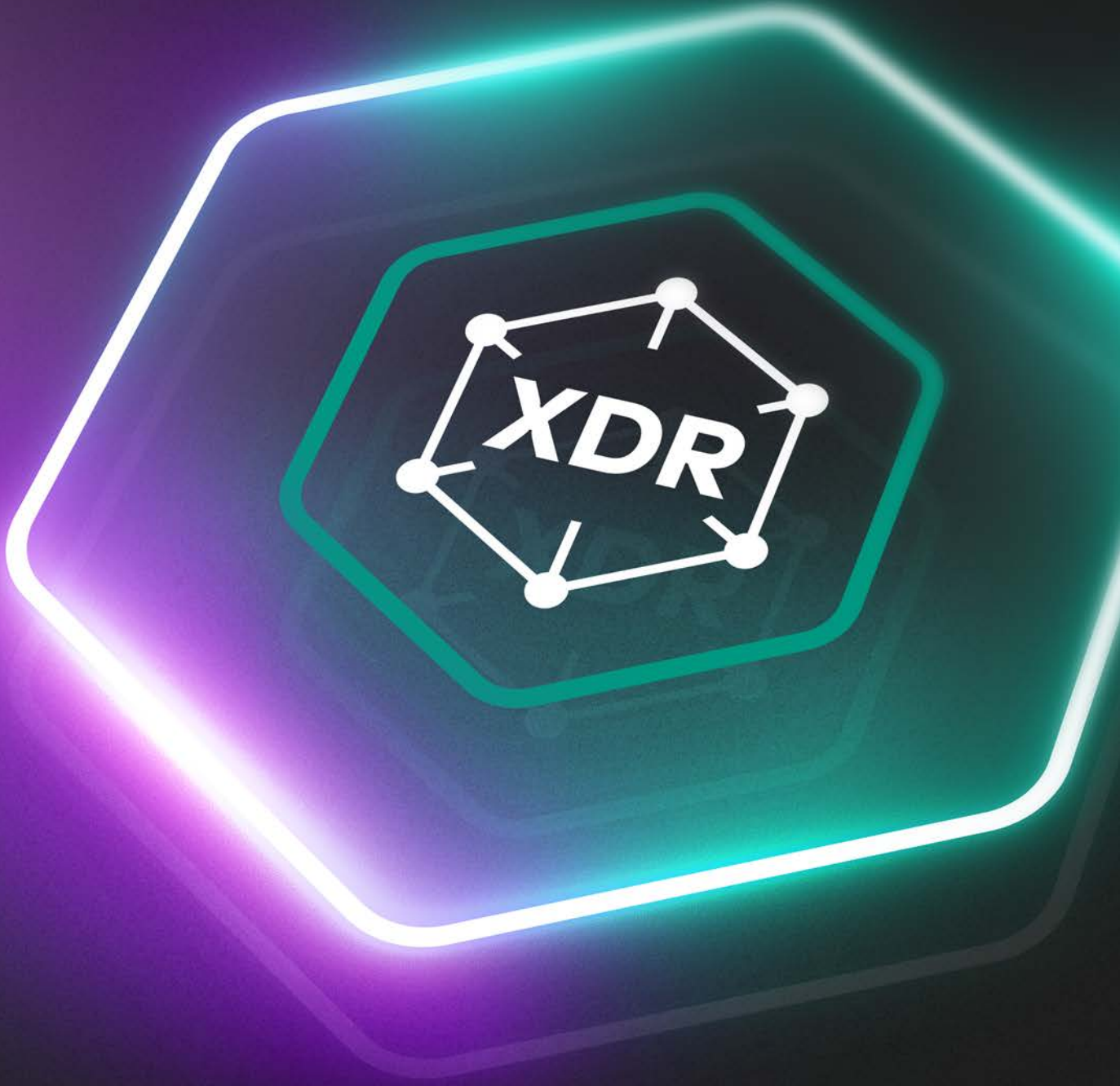




Benzersiz sezgi.
Tam koruma.

Kaspersky Geniřletilmiş Algılama ve Müdahale (XDR)

kaspersky

GELECEĐİ
YAKALAYIN



İşletmelerin siber güvenliğin karmaşıklığı

Siber tehdit dünyası, şirketler için bir yandan temel işletme faaliyetlerine odaklanırken diğer taraftan siber güvenliği en üst düzeyde tutmayı son derece zor hale getiriyor. Bu karmaşaya sürekli genişleyen saldırı alanları, yasal gereklilikler ve küresel kabiliyet açığı da eklenince, modern işletmelerin neden bu kadar baskı altında olduğunu ve neden bu kadar çok siber saldırının başarılı olduğunu anlamak hiç de zor değil.

%51

mevcut araçlarla gelişmiş tehditleri tespit etmekte ve araştırmakta zorlanan şirketlerin oranı

%68

ağlarına yönelik hedefli bir saldırı deneyimi olan ve bunun doğrudan bir sonucu olarak veri kaybına uğrayan şirketlerin oranı

6 trilyon dolar

yıllık olarak: siber suçların küresel yıllık maliyeti

4000000

her gün tespit edilen yeni zararlı yazılım sayısı

Kaynaklar: Kaspersky, PurpleSec, CybersecurityVentures

Kaspersky Genişletilmiş Algılama ve Müdahale

Tam görünürlük. Benzersiz koruma.

Kaspersky XDR, ileri derecede geliştirilmiş siber tehditlere karşı savunma sağlayan güçlü bir siber güvenlik çözümüdür. Uç nokta, ağ ve bulut verileri dahil olmak üzere çok çeşitli veri kaynaklarından yararlanarak tam görünürlük, korelasyon ve otomasyon sağlar.

2016'da Native XDR olarak ortaya çıkan Kaspersky Anti-Targeted Attack platformundan her şeyi kapsayan bir güvenlik görünümü sağlayarak 2023'te Open XDR'ye evrildi. Açık Tek Yönetim Platformu'ndan kolayca yönetilen Kaspersky XDR, veri bağımsızlığı gereksinimlerini karşılarken müşterilerin hassas verilerinin kendi altyapılarında kalmasını sağlayarak kapsamlı bir şirket içi güvenlik sunar.

Açık XDR

Açık XDR çözümleri, şirketlerin farklı tedarikçilerden çeşitli güvenlik ürünlerini entegre etmesine olanak tanıyarak ve daha fazla esneklik ve tedarikçiden bağımsız kabiliyetler sunarak çok çeşitli güvenlik ürünleriyle çalışacak şekilde tasarlanmıştır.

Yerel XDR

Yerel XDR çözümleri, daha birleşik ve uyumlu bir deneyim sağlayarak genellikle tedarikçinin kendi güvenlik araçları ekosistemiyle sorunsuz bir şekilde çalışır. Bu çözümler, tedarikçinin güvenlik ürün grubu içinde derin entegrasyon, otomasyon ve kolaylaştırılmış iş akışları sunarak birlikte çalışmak üzere özel olarak üretilmiştir.

Temel teknolojiler

Açık XDR'yi, birleşik siber güvenlik ekosistemi oluşturmaya yönelik evrensel bir araç olarak **tek bir açık platform** halinde sunuyoruz. Kaspersky XDR'nin temelinde lider çözümlerimiz olan Kaspersky Unified Monitoring and Analysis Platform, Kaspersky Endpoint Security for Business ve Kaspersky Endpoint Detection and Response yer alır. Gelişmiş ağ yönetimi için KATA da ek bir seçenektir.

İzleme ve Analiz

Günlük kayıtlarının merkezi olarak toplanmasını ve analiz edilmesini, güvenlik olaylarının gerçek zamanlı olarak korelasyonu ve vakaların zamanında bildirilmesini sağlar. Tehditleri, saldırıları ve IoC'leri tespit edip önceliklendirmek için hazır korelasyon kuralları seti ve zengin Kaspersky Threat Intelligence hizmetleri portföyüne erişim sağlar.

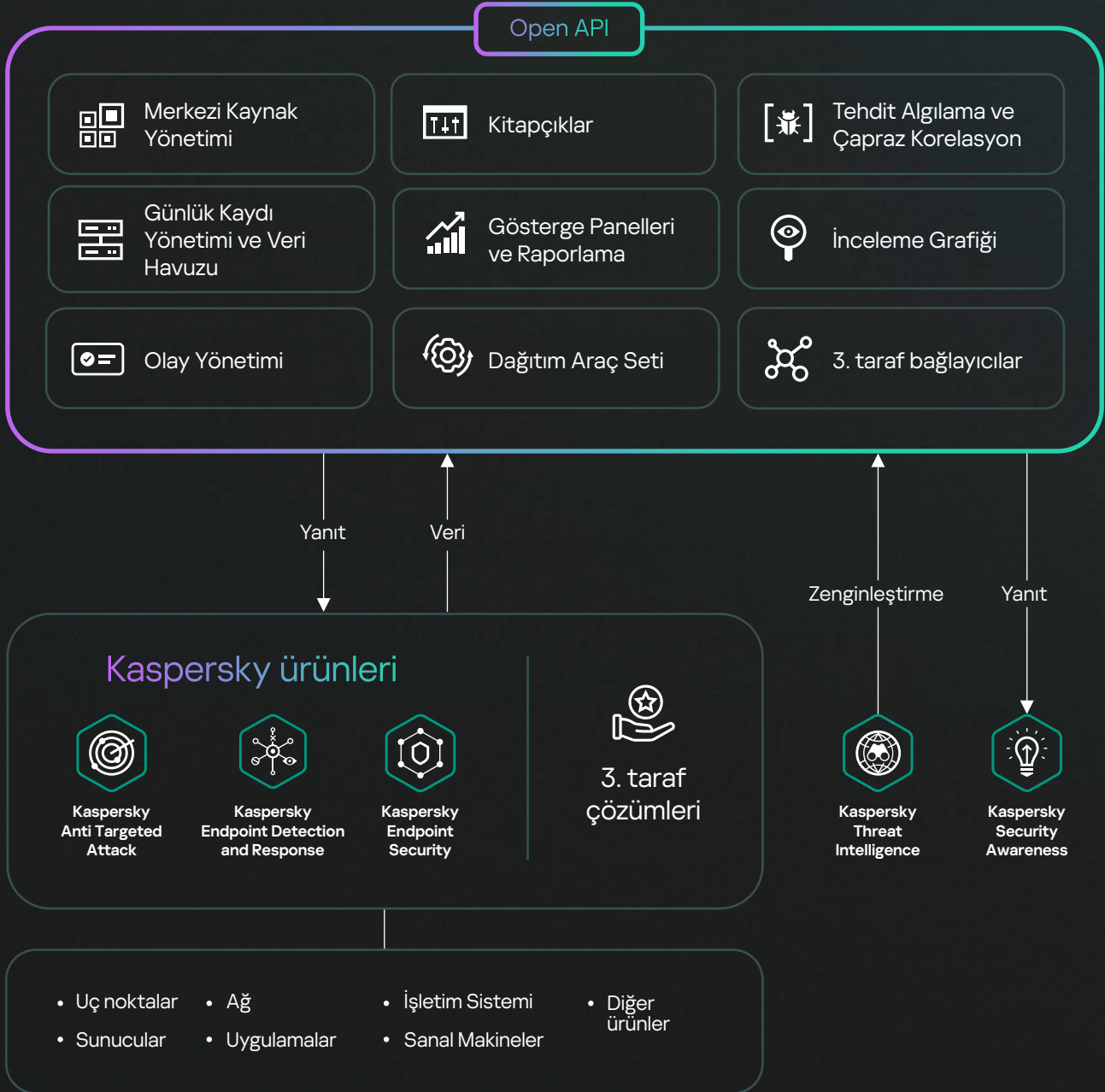
Uç Nokta Koruması

Fidye yazılımı, kötü amaçlı yazılım ve dosyasız saldırılara karşı koruma sağlayan güçlü uç nokta koruması sunar. Uç nokta korumamız, şirket içinde veya bulutta, herhangi bir ana işletim sistemini çalıştıran her tür uç noktayı korumak için makine öğrenimi ve davranış analizi kullanır.

Uç Nokta Algılama ve Müdahale

Şirketlerin tüm uç noktalarında kapsamlı görünürlük ve üstün koruma sağlar. Kaspersky'nin benzersiz, geniş kapsamlı tehdit istihbaratı sayesinde gelişmiş tehdit avı ve keşfi, ayrıca rutin görevlerin otomasyonu, yönlendirmeli inceleme süreçleri ve özelleştirilebilir algılamaların tümü hızlı vaka çözümünü destekler.

Açık Tek Yönetim Platformu



Güçlü özellikler, önemli avantajlar



Üçüncü taraflardan gerçek zamanlı veri kaynaştırma

Üçüncü taraf kaynaklardan gelen verileri entegre etme kabiliyeti, uç noktaların da ötesine geçerek gerçek zamanlı çapraz korelasyon ile geliştirilmiştir.



Rakipsiz ölçeklendirme

Tek seferde yüz binlerce uç noktayı kapsayan yükleri destekleme kabiliyeti olan Kaspersky XDR, yüksek kullanılabilirlik sağlarken tehditleri gerçek zamanlı olarak özenle takip eder.



MSSP senaryolarına olanak tanıyan çoklu kullanıcı özelliği

XDR'yi kullanıcılara tam teşekküllü bir hizmet olarak sunun - kullanıcılar birbirlerinin verilerini göremezken, ana yönetici (MSSP) tüm kullanıcılar için algılama ve yanıt süreçleri oluşturabilir.



Otomatik Müdahale ve Onarım

Güvenliği ihlal edilmiş uç noktaları karantinaya alın veya izole edin, kötü amaçlı işlemleri engelleyin ve güvenlik açıklarını düzeltin, böylece harcanan emek ve yanıt süresini azaltın.



Veri bağımsızlığı

Kaspersky XDR, kapsamlı bir şirket içi XDR çözümü sunan birkaç sağlayıcıdan biridir ve müşterilerin hassas verilerinin kendi altyapılarında kalmasını sağlayarak veri bağımsızlığı gereksinimlerini karşılar.



Gelişmiş güvenlik senaryolarını özelleştirme ve altyapı genelinde veri analizi

Tüm altyapılarındaki verileri analiz etme kabiliyeti ile kullanıcılara karmaşık güvenlik durumlarını ayarlama imkanı sunar.



EPP/EDR sınıfının en iyisi

Küresel lider olarak tanınan Kaspersky, dünya çapında EPP/EDR çözümleri için çitayı belirler. Kaspersky EDR, aldığı ödüller ve Interpol ve MAPP gibi uluslararası komitelere aktif katılımıyla küresel ölçekte üstünlük sağlamaktadır.



Kaspersky ürünleri arasında sorunsuz ve sıkı entegrasyon

Birleşik bir destek sistemi ve kusursuz bir şekilde entegre edilmiş bir tasarımı destekleyerek ürünler arasındaki bağlantı, üçüncü taraf çözümlerin erişemeyeceği bir seviyeye ulaşmaktadır.

Entegrasyon kabiliyetleri

Kaspersky XDR ile çalışan kapsamlı entegrasyonlar, potansiyel tehditlerin birleşik ve bağlamsallaştırılmış bir görünümünü sunarak güvenlik ekibinize şirketinizi siber suçluların her türlü saldırısına karşı korumak için ihtiyaç duydukları tüm araç ve bilgileri sağlamaktadır.

Ürünün entegrasyonu kabiliyetleri, diğer sistem ve cihazlardan veri (günlükler) alabilmenin yanı sıra diğer ürünlerde otomatik yanıtlar oluşturabilmeyi de kapsar. Kaspersky XDR, Kaspersky ve üçüncü taraf ürünlerle çok çeşitli kullanıma hazır entegrasyonlar sunar. Kaspersky Professional Services tarafından veya iş ortakları ya da müşterilerin kendileri tarafından da geliştirilebilecek (bağlanabilir ürünlerin API özelliklerini kullanmak dahil) ilave entegrasyonlar eklemek de mümkündür. Çeşitli alanlar ve farklı satıcılardan sistemlerle entegrasyon mümkündür ayrıca çok sayıda protokol ve veri formatı da desteklenmektedir.

Güvenlik alanına göre

Uç Nokta Güvenliği

- EPP & EDR çözümleri

Ağ & Web & E-posta Güvenliği

- E-posta Koruması
- Ağ Tespiti ve Müdahale (NDR)
- Güvenlik Duvarları (FW) ve Yeni Nesil Güvenlik Duvarları (NGFW)
- Birleştirilmiş tehdit yönetimi (UTM)
- Saldırı Tespit Sistemleri (IDS)

Bulut Güvenliği

- Bulut Erişim Güvenlik Aracısı (CASB)
- Bulut İş Yüğü Koruma Platformları (CWPP)

Tehdit İstihbaratı

- Siber Tehdit İstihbaratı (CTI)

Kimlik Güvenliği

- Kimlik ve Erişim Yönetimi (IAM)
- Ayrıcalıklı Erişim Yönetimi (PAM)

OT/IOT Güvenliği Farkındalığı

Aktarım türüne göre

- TCP
- UDP
- Netflow
- sflow
- nats-jetstream
- kafka
- HTTP
- SQL
- SQLite
- MSSQL
- MySQL
- PostgreSQL
- Cockroach
- Oracle
- Firebird
- Dosyası
- 1c-log and 1c-xml
- Diode
- FTP
- NFS
- WMI
- WEC
- SNMP
- SNMP-TRAP
- VmWare API

Veri türüne göre

- XML
- Syslog
- Csv
- JSON
- SQL
- IPFIX
- CEF
- Netflow 5
- Netflow 9
- KV

Tedarikçiye göre

- Kaspersky
- Absolute
- AhnLab
- Aruba
- Avigilo
- Ayehu
- Barracuda
- BeyondTrust
- Bloombase
- BMC
- Bricata
- Brinqa
- Broadcom
- CheckPoint
- Cisco
- Citrix
- Claroty
- CloudPassage
- Corvil
- Cribl
- CrowdStrike
- CyberArk
- DeepInstinct
- Delinea
- EclecticIQ
- Edge Technologies
- Eltex
- Eset
- F5 BigIP
- FireEye
- Forcepoint
- Fortinet
- Gigamon
- Huawei
- IBM
- Ideco
- Illumio
- Imperva
- Orion Soft
- Intralinks
- Juniper
- Kemptechnologies
- Kerio
- Lieberman
- MariaDB
- Microsoft
- MikroTik
- Minerva
- NetIQ
- NetScout
- Netskope
- Netwrix
- Nexthink
- NIKSUN
- Oracle
- PagerDuty
- Palo Alto
- Penta Security
- Proofpoint
- Radware
- Recorded
- ReversingLabs
- SailPoint
- SentinelOne
- Sonicwall
- Sophos
- ThreatConnect
- ThreatQuotient
- Trend Micro
- Trustwave
- VMWare
- Vormetric
- WatchGuard - Firebox
- Winchill Fracas
- Zettaset
- Zscaler & etc.

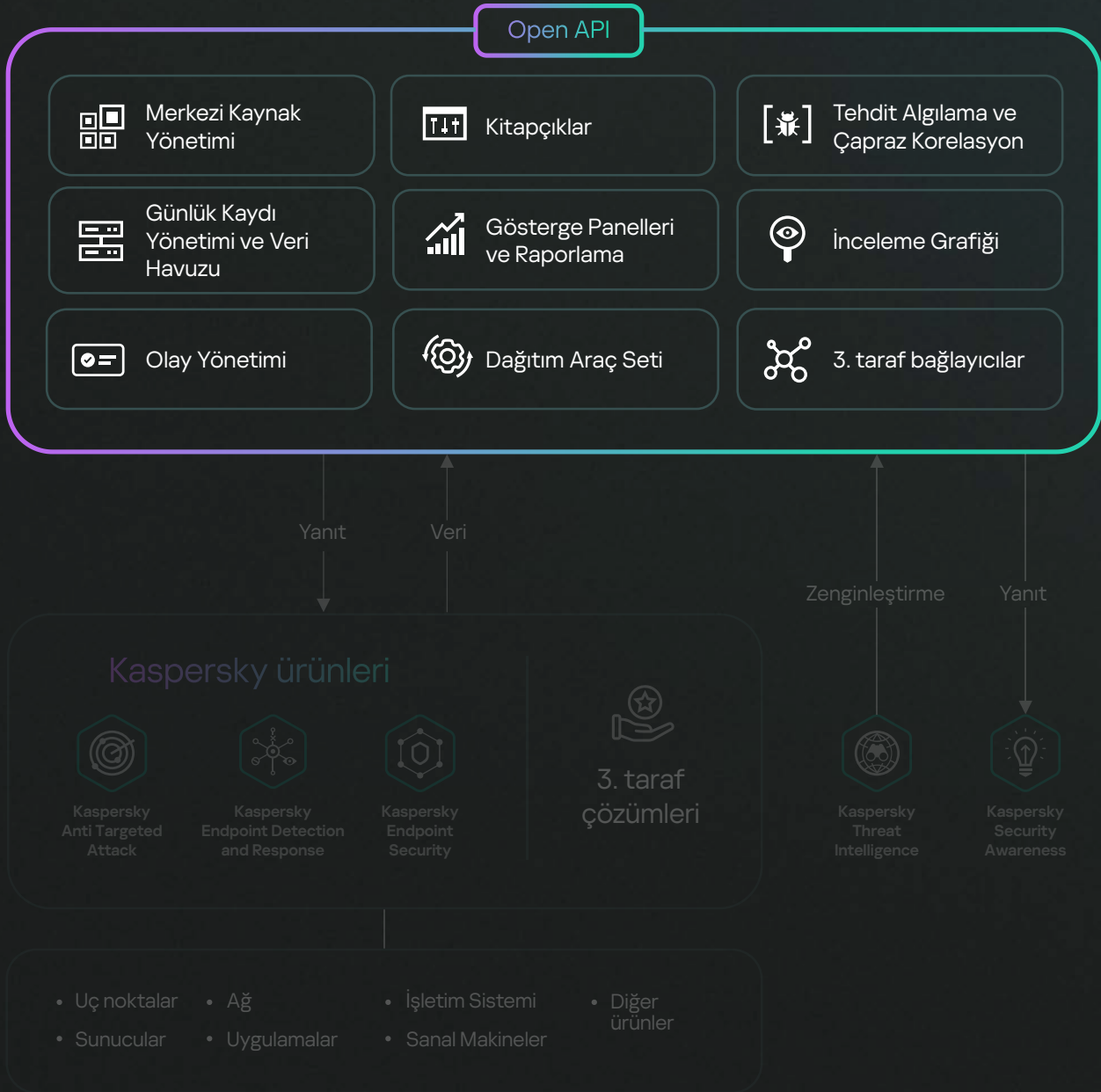
Sunduklarımız

Kaspersky XDR'nin iki seçenek olarak mevcuttur.

Kaspersky XDR Core

Kaspersky XDR Core, halihazırda uç nokta ve EDR çözümleri olan ve bunları değiştirmek istemeyen, ancak işlevselliği bir korelasyon motoru, otomatik yanıtlar ve üçüncü taraf bağlayıcılarla genişletmeyi tercih eden müşteriler içindir.

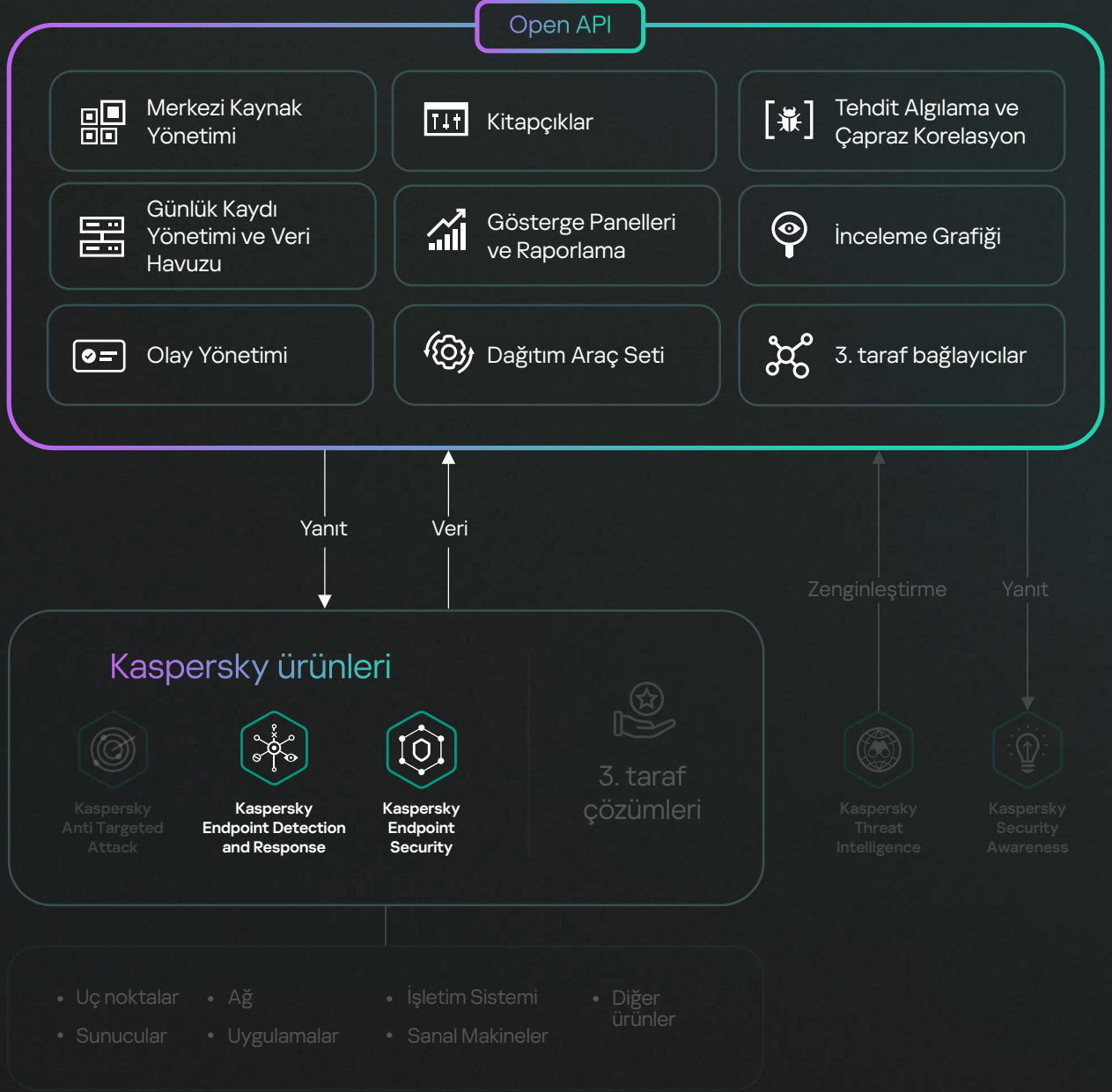
Açık Tek Yönetim Platformu



Kaspersky XDR Expert

Kaspersky XDR Expert, sunduğu üstün uç nokta korumasını Kaspersky EDR Expert'in gelişmiş algılama özellikleriyle birleştirerek korelasyon motoru ve otomatik yanıtlarla destekler. Tüm verileri bir araya getirmek için üçüncü taraf bağlantılar eklenebilir.

Açık Tek Yönetim Platformu



Tamamlayıcı sensörler ile ekstra değer

Kaspersky XDR, ek bir değer sağlamak için kusursuz bir entegrasyon sağlayarak ve XDR'yi analistlere tüm entegre çözümleri kapsayan merkezi bir çalışma alanı sunan uyumlu bir platforma dönüştürerek belirli kaynakları korumak için tasarlanan ek sensörlerin XDR'ye sorunsuz bir şekilde entegre edilmesini destekler.

Kaspersky XDR yalnızca EDR ile savunmanızı güçlendirmekle kalmaz, aynı zamanda esnek entegrasyon özellikleri sunar, böylece müşteriler herhangi bir noktada ekosisteme ürün ekleyebilir.

		Kaspersky XDR Core	Kaspersky XDR Expert
Açık Tek Yönetim Platformu ve bileşenleri	Çapraz korelasyon motoru (KUMA destekli)	•	•
	• 3. taraf bağlayıcılar • Günlük Kaydı Yönetimi ve Veri Havuzu • Tehdit Algılama ve Çapraz Korelasyon • Kaynak Yönetimi • Gösterge Panelleri ve Raporlama		
	XDR bileşenleri	•	•
	• Olay Yönetimi • Yanıt otomasyonu ve orkestrasyon (kitapçıkları) • Araştırma • Dağıtım Araç Seti • Open API		
Kaspersky EDR ve KESB fonksiyonelliği	Otomatik, yarı-otomatik ve manuel tespit		•
	Korunan uç noktaların izlenmesi		•
	Tehdit önleme		•
	Kurtarma seçenekleri		•

Kaspersky XDR Core



Kaspersky
Unified Monitoring
and Analysis Platform

XDR bileşenleri

Kaspersky XDR Expert



Kaspersky
Unified Monitoring
and Analysis Platform



Kaspersky
Endpoint Detection
and Response



Kaspersky
Endpoint Security
for Business

XDR bileşenleri

Neden Kaspersky XDR?

En çok test edilen. En çok ödül alan. Kaspersky koruması.

Kaspersky, güvenlik uzmanlığı konusunda güçlü bir kayıt sahibi olan küresel bir siber güvenlik şirkettir. Dünyanın dört bir yanındaki kuruluşları 25 yılı aşkın süredir koruyoruz ve bunun yanı sıra ürün ve hizmetlerimiz için sayısız ödül ve övgüye layık görüldük. 2013 ve 2022 yılları arasında Kaspersky ürünleri:

827

bağımsız test ve incelemeye katıldı

587

birincilik elde etti

685

kez ilk üçe girmeyi başardı

Kaspersky, 2023 yılında önde gelen küresel teknoloji araştırma ve danışmanlık firması ISG tarafından XDR çözümleri sektöründe Lider seçildi. ISG, 'liderleri' hem kapsamlı bir ürün ve hizmet yelpazesine sahip hem de yenilikçi güce ve rekabet istikrarına sahip şirketler olarak tanımlamaktadır.

Daha fazla bilgi edinin



Kaspersky Extended Detection and Response

Demo talep edin

www.kaspersky.com.tr

© 2023 AO Kaspersky Lab.
Tescilli ticari markalar ve hizmet markaları,
ilgili sahiplerine aittir.

#kaspersky
#geleceğiyakalayın