Kaspersky Next XDR Expert

比類なき洞察力。総合的な保護。

kaspersky

ビジネスのサイバーセキュリティの複雑性

サイバー脅威の状況により、サイバーセキュリティのトップに立ち続ける一方で基幹ビジネスの運用に注力することは、組織にとって極端に困難なことになっています。攻撃対象領域、規制要件、世界各国にわたるスキル格差は広がる一方であることを加味すると、近代ビジネスに非常に大きなプレッシャーがかかる理由も、多くのサイバー攻撃が成功する理由も容易に理解できます。

51%

現在のツールでの高度な脅威の検知と調査に苦慮している企業の割合

68%

ネットワークへの標的型攻撃を経験し、その直接的な被害としてデータ損失が発生した企業の割合

6兆ドル

1年間で発生するサイバー犯罪のグローバル規模でのコスト

400000

毎日検知される新しいマルウェアの数

情報源：カスペルスキー、PurpleSec、CybersecurityVentures

Kaspersky Extended Detection and Response

完全な可視性。他の追随を許さない保護機能。

Kaspersky Next製品ラインの一部として、Kaspersky Next XDR Expertを導入しました。カスペルスキーのXDRアプローチを取り入れ、企業のセキュリティを全方位から俯瞰可能なソリューションです。

Kaspersky XDRは、巧妙なサイバー脅威から保護する強固なサイバーセキュリティソリューションです。エンドポイント、ネットワーク、クラウドデータなど多様なデータソースの活用により、データの完全な可視化、相互の関連付けと自動化を実現します。

2016年にネイティブXDRとして開発されたKaspersky Anti-Targeted Attackプラットフォームが2023年にオープンXDRへと進化した結果、セキュリティを全方位から俯瞰可能なソリューションとなりました。Kaspersky XDRは、Open Single Management Platformから簡単に管理できます。オンプレミス環境を包括的に保護し、顧客の機密情報を自身のインフラストラクチャ内に保有したままの状態でデータ主権の要件を満たせるようになります。

オープンXDR

オープンXDRのソリューションは幅広いセキュリティ製品との連携を目的に設計されており、複数のベンダーが提供する多様なセキュリティ製品の統合を可能とし、より柔軟かつベンダーに依存しない形式で機能を使用できるようにします。

ネイティブXDR

ネイティブXDRのソリューションは通常、ベンダー自身のセキュリティツールのエコシステムとシームレスに連携し、統一感と結束性がより高い使用感があります。これらのソリューションは連携の目的に応じて構築されており、深度が高い統合、自動化、および合理化されたワークフローを、ベンダ ーのセキュリティ製品スイートの中で実現します。

主要な技術

当社が提供するオープンXDRは単一のオープンプラットフォームであり、サイバーセキュリティ製品を1つに統合したエコシステムを構築するための汎用的なツールです。Kaspersky XDRの中核をなすのは、当社の代表的なソリューションであるKaspersky Unified Monitoring and Analysis Platform、Kaspersky Next EDR Foundations、およびKaspersky Endpoint Detection and Response Expertです。高度なネットワーク管理向けに、KATAを追加オプションとしています。

監視と分析

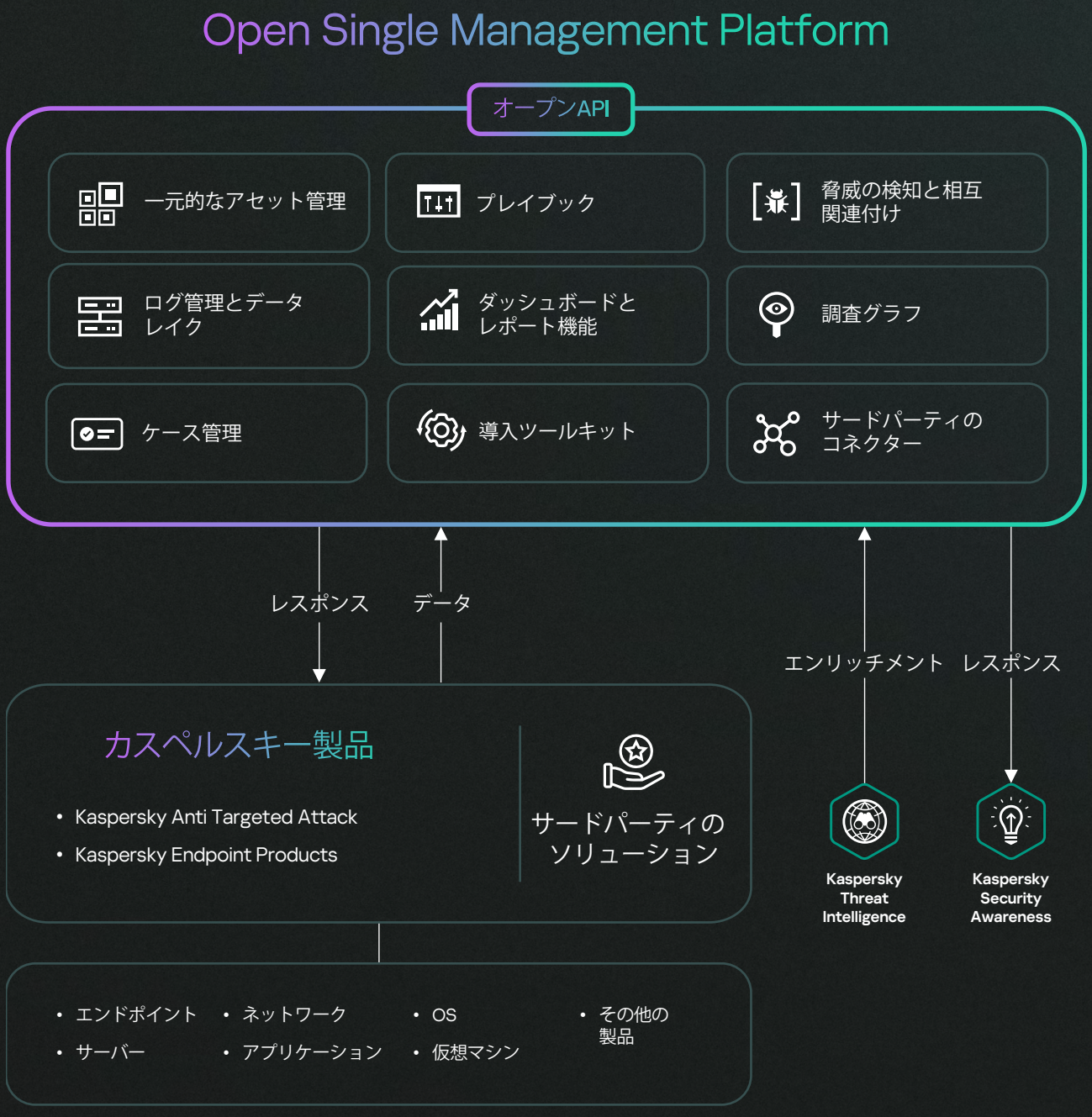
ログの集中的な収集と分析、セキュリティイベントのリアルタイムでの関連付け、インシデントのタイムリーな通知などが可能です。事前に定義された関連付けルールやKaspersky Threat Intelligenceサービスの豊富なポートフォリオへのアクセスが含まれており、脅威、攻撃、IoCの特定、優先順位付けができます。

Endpoint Protection

エンドポイント用の強力な保護機能が実装されており、ランサムウェア、マルウェア、ファイルレス攻撃から、エンドポイントを保護します。オンプレミス環境でもクラウド環境でも、当社のエンドポイント保護には機械学習とふるまい分析が使用されており、任意の主要なOSで稼働するすべての種類のエンドポイントを保護します。

Endpoint Detection and Response

企業のすべてのエンドポイントを包括的に可視化し、優れた保護機能で保護します。広範囲をカバーするカスペルスキー独自の脅威インテリジェンスによって強化された脅威ハンティングと探索に加えて、定期的なタスクの自動化、ガイダンスつきの調査プロセス、カスタマイズ可能な検知が実装されており、これらの機能のすべてがインシデントの早期解決を支援します。



強力な機能、大きなメリット

サードパーティからのデータをリアルタイムで融合

サードパーティのソースからのデータを統合する機能により、エンドポイントを超えた拡張性を実現します。また、この機能はリアルタイムの相互関連付けによって強化されます。

レスポンスと修正の自動化

攻撃されたエンドポイントの隔離と分離、悪意がある活動のブロック、脆弱性の修正、手動での作業やレスポンス時間の短縮。

最高クラスのEPP/EDR

グローバルリーダーとして認知されているカスペルスキーは、世界中のEPP/EDRソリューションのベンチマークとなっています。Kaspersky EDRのグローバルな優位性は、その受賞実績のほか、インターポ ールやMAPPなどの国際的な組織への積極的な参加によって実証されています。

他の追随を許さない拡張性

数十万のエンドポイントからの負荷を単 一インスタンスでサポートし、Kaspersky XDRはリアルタイムで脅威を追跡しながら高可用性を確保します。

データ主権

Kaspersky XDRは、包括的なオンプレミスのXDRソリューションを提供する数少ないベンダーによる製品です。顧客の機密情報を自身のインフラストラクチャに保有したままの状態で、データ主権の要件を満たすことができます。

カスペルスキー製品とのシームレスで堅固な統合

サードパーティソリューションが実現可能な範囲を超越したレベルでの製品間の対話が可能であり、統一されたサポートシステムとシームレスに統合されたデザインを誇ります。

MSSPシナリオを可能とするマルチテナンシー

XDRを本格的なテナントを実装したサービスとして提供します。あるテナントのユーザーが別のテナントのデータを見ることはできません。一方、メイン管理者（MSSP）は、検知とレスポンスのプロセスを全クライアント向けに構築できます 。

高度なセキュリティシナリオのカスタマイズと、インフラストラクチャ全体のデ ータ分析

インフラストラクチャ全体のデータ分析機能が追加され、ユーザーが複雑なセキュリティシナリオを構成することが可能です。

統合の機能

Kaspersky XDRと連携して動作する統合機能は広範囲におよび、潜在的な脅威を一元化し状況に合わせた形で表示することができます。これにより、どのようなサイバー脅威が発生しても、組織を保護するためにセキュリティチームが必要とするすべてのツールや情報が取得可能です。

本製品の統合機能は、他のシステムやデバイスからのデータ（ログ）の受信機能と、他の製品でレスポンスの自動化を設定する機能を網羅しています。Kaspersky XDRには、カスペルスキー製品またはサードパーティ製品とすぐに統合できる機能が数多くあります。Kaspersky Professional Servicesまたはパートナー、あるいは顧客自身が開発した追加の統合（接続可能な製品のAPI機能の使用を含む）を追加することもできます。多様なドメイン、様々なベンダーのシステムとの統合が可能であり、多くのプロトコルとデータ形式がサポートされています。

セキュリティ分野

エンドポイントセキュリティ

- EPP/EDRソリューション

ネットワーク/Web/メールセキュリティ

- メールの保護
- ネットワークの検知とレスポンス（NDR）
- ファイアウォール（FW）、次世代ファイアウォール（NGFW）
- 統合脅威管理（UTM）
- 侵入検知システム（IDS）

クラウドセキュリティ

- クラウドアクセスセキュリティブローカー（CASB）
- クラウドワークロード保護プラットフォーム（CWPP）

脅威インテリジェンス

- サイバー脅威インテリジェンス（CTI）

アイデンティティセキュリティ

- アイデンティティとアクセス管理（IAM）
- 特権アクセス管理（PAM）

OT / IoTセキュリティ / セキュリティアウェアネス

転送タイプ

- TCP
- UDP
- Netflow
- sflow
- nats-jetstream
- kafka
- HTTP
- SQL
  - SQLite
  - MSSQL
  - MySQL
  - PostgreSQL
  - Cockroach
  - Oracle
  - Firebird
- ファイル
- 1c-log、1c-xml
- Diode
- FTP
- NFS
- WMI
- WEC
- SNMP
- SNMP-TRAP
- VMWare API

データ種別

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

ベンダー

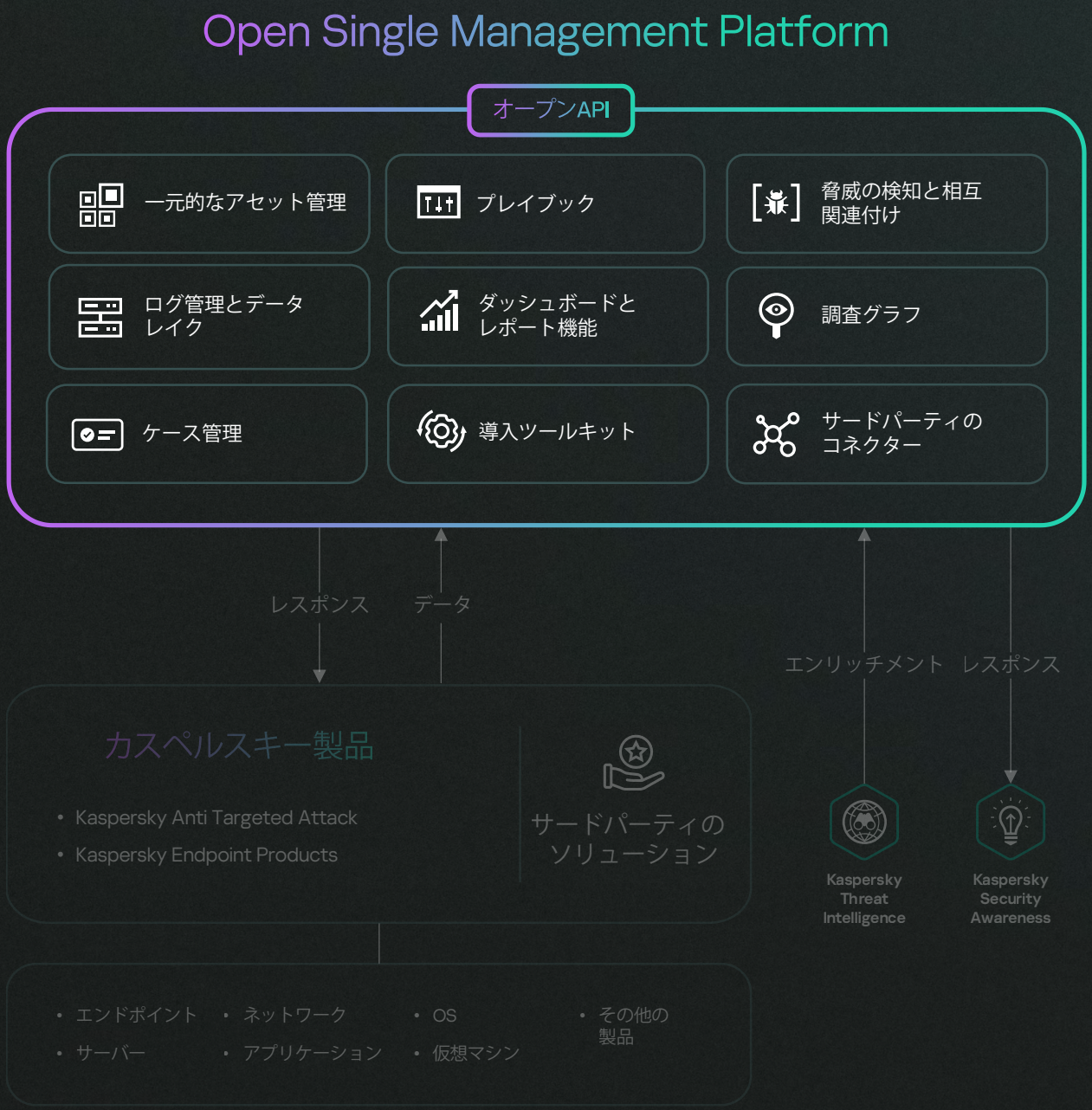
- カスペルスキー
- Absolute
- AhnLab
- Aruba
- Avigilo
- Ayehu
- Barracuda
- BeyondTrust
- Bloombase
- BMC
- Bricata
- Brinqa
- Broadcom
- CheckPoint
- Cisco
- Citrix
- Claroty
- CloudPassage
- Corvil
- Cribl
- CrowdStrike
- CyberArk
- DeepInstinct
- Delinea
- EclecticIQ
- Edge Technologies
- Eltex
- Eset
- 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.

製品とサービス

Kaspersky XDRは、2つのオプションから選んで使用できます。

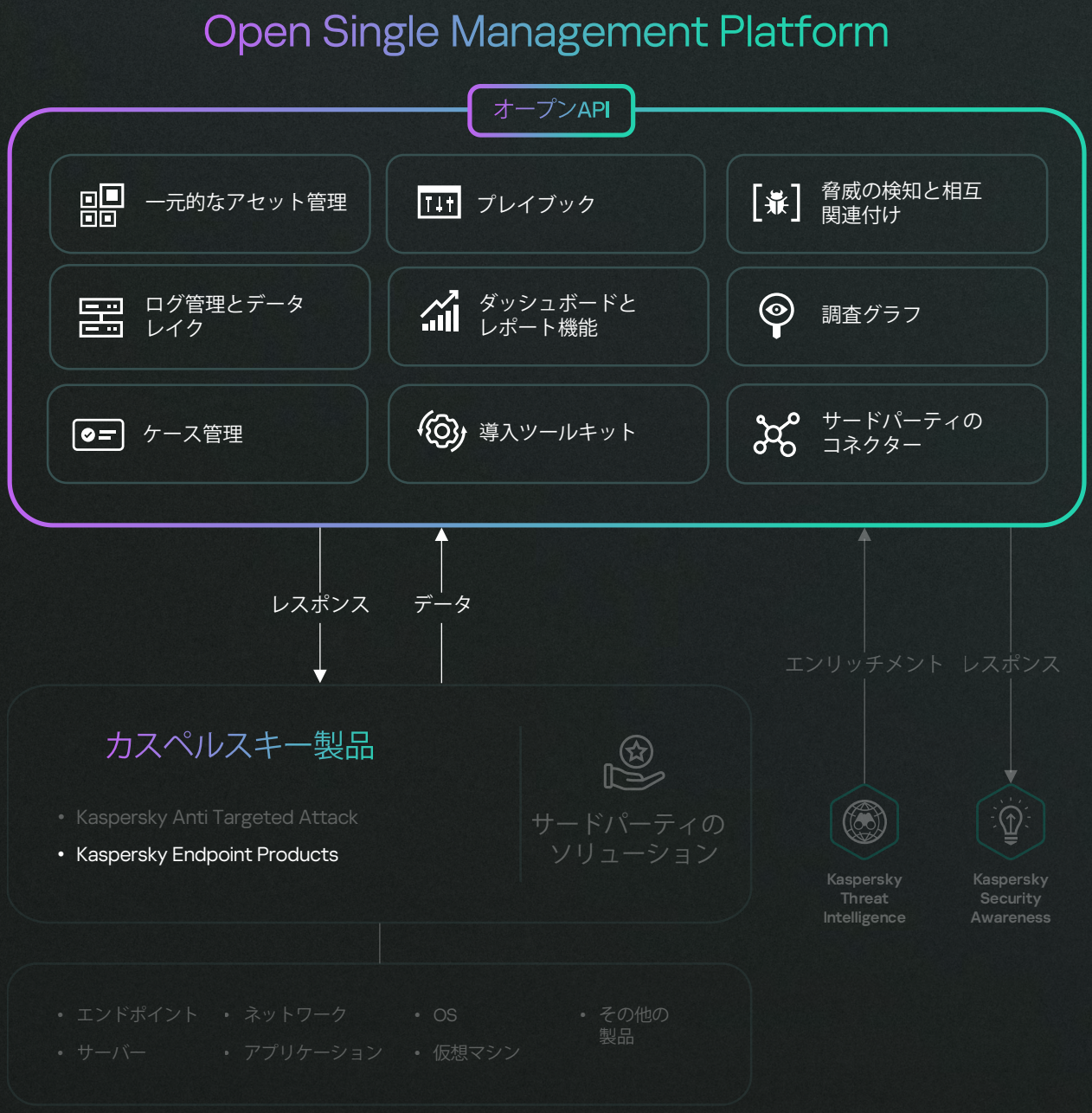
Kaspersky XDR Core

Kaspersky XDR Coreは、エンドポイントとEDRのソリューションを導入済みであり、それらをリプレースせずに相互関連付けエンジンやレスポンスの自動化、およびサードパーティのコネクターの機能を拡張したいお客様向けです。



Kaspersky Next XDR Expert

Kaspersky XDR Expertは、クラス最高のエンドポイント保護とKaspersky EDR Expertの高度な検知機能、および相互関連付けエンジンとレスポンスの自動化を組み合わせたソリューションです。サードパーティのコネクターを追加して、すべてのデータを収集することができます。



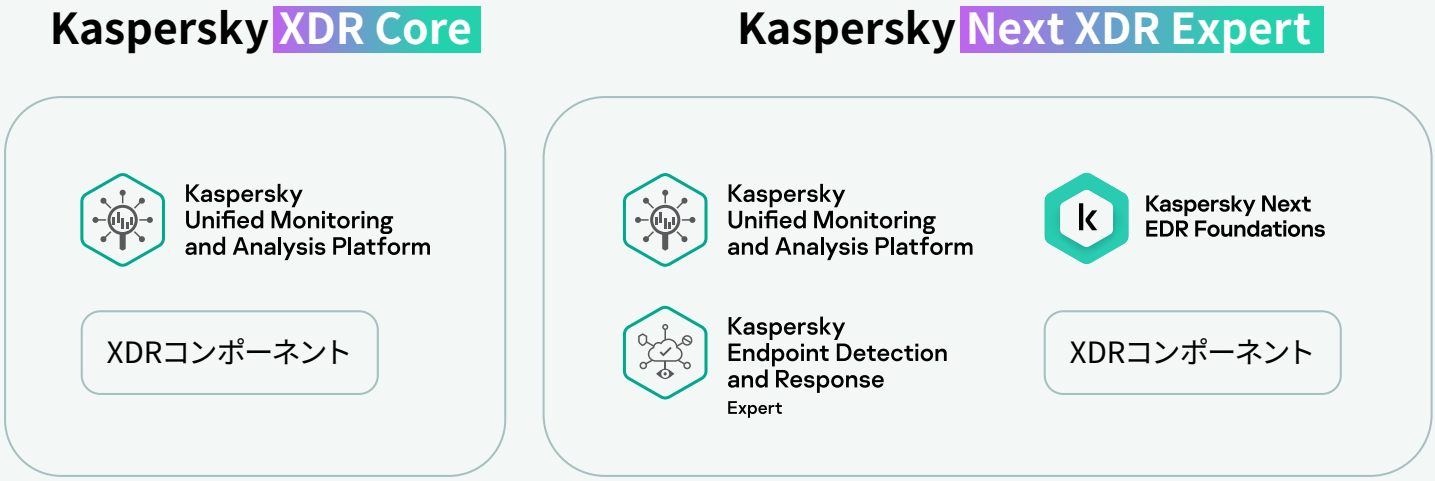
補助センサーによる付加価値

Kaspersky XDRは、特定のアセットを保護する目的で設計された補助センサーとのシームレスな統合をサポートしています。XDRとシームレスに統合して価値のレイヤーを追加し、XDRを結束性があるプラットフォームに変換することで、統合されたすべてのソリューションをカバーする一元化されたワークスペースをアナリストが使用できるようになります。

Kaspersky XDRによってEDRを使用した防御が強化されるだけでなく、柔軟な統合機能が使用できるようになり、任意の段階で製品をエコシステムへ追加できます。

		Kaspersky XDR Core	Kaspersky Next XDR Expert
Open Single Management Platformとそのコンポーネント	相互関連付けエンジン • サードパーティのコネクター • ログ管理とデータレイク • 脅威の検知と相互関連付け • アセット管理 • ダッシュボードとレポート機能	●	●
	XDRコンポーネント • ケース管理 • レスポンスの自動化とオーケストレーション（プレイブック） • 調査 • 導入ツールキット • オープンAPI	●	●
カスペルスキーのエンドポイント機能*	検知の自動化または半自動化、あるいは手動での実行		●
	保護対象エンドポイント全体の監視		●
	脅威の封じ込め		●
	回復オプション		●
	モバイル保護と管理		●
	クラウド利用の検出とブロック		●
	MS O365用セキュリティ、Data Discovery		●
	IT管理者向けのサイバーセキュリティトレーニング		●

* ご利用いただける機能は、実装方法によって異なります



Kaspersky Nextのご紹介

Kaspersky Next EDR Foundations

組織全体を保護する堅牢なセキュリティ

すべてのエンドポイントを保護

対応するニーズ

- 強力なエンドポイント保護
- 基本的なセキュリティコントロール
- 最大限の自動化

Kaspersky Next EDR Optimum

防御能力を強化

基本的な調査とレスポンスでセキュリティを強化

対応するニーズ

- 可視性とレスポンス能力の強化
- クラウドセキュリティの強化
- エンタープライズ水準のコントロール

Kaspersky Next XDR Expert

エキスパートにツールを提供

最も複雑で高度な脅威からビジネスを保護

対応するニーズ

- 高度な脅威の検知
- シームレスな統合
- 強力な脅威ハンティングツール

Kaspersky XDRを選ぶ理由

最多のテスト回数。最多のトップ評価獲得実績。それがカスペルスキーの保護です。

カスペルスキーは、セキュリティを専門分野として多くの実績を積み重ねてきたグローバルなサイバーセキュリティ企業です。世界各国の組織を保護してきた実績は25年以上におよび、当社の製品とサービスは数えきれないほどの受賞実績があり、称賛を受けています。2013年から2022年までに、カスペルスキー製品が達成した実績は次の通りです：

827
第三者評価機関が実施したテストやレビューに参加した回数

587
1位の獲得回数

685
トップ3の達成回数

2023年、世界有数のテクノロジーリサーチ&アドバイザリー企業であるISGにより、カスペルスキーはXDRソリューション市場のリーダーであるとされました。ISGの定義によると、「リーダー」とは、包括的な製品とサービスを提供し、力強いイノベーションと安定した競争力を示す存在です。

詳細

Kaspersky Extended Detection and Response

デモの依頼

www.kaspersky.co.jp

#kaspersky
#bringonthefuture