Kaspersky Next XDR Expert

Umfassende Transparenz.
Fortschrittlicher Schutz.

kaspersky

Die Komplexität der Cybersicherheit von Unternehmen

Die Cyberbedrohungslage macht es für Unternehmen extrem schwierig, ihre Cybersicherheit im Griff zu behalten und sich gleichzeitig auf das Kerngeschäft zu konzentrieren. Nimmt man die immer größer werdende Angriffsfläche, die gesetzlichen Vorschriften und den weltweiten Fachkräftemangel hinzu, wird klar, warum moderne Unternehmen unter so großem Druck stehen – und warum so viele Cyberangriffe erfolgreich sind.

51 %

der Unternehmen haben Schwierigkeiten, fortgeschrittene Bedrohungen mit den derzeitigen Tools zu erkennen und zu untersuchen

68 %

der Unternehmen waren von einem gezielten Angriff auf ihre Netzwerke betroffen und haben als direkte Folge einen Datenverlust erlitten

6 Billionen USD

pro Jahr: die weltweiten jährlichen Kosten von Cybercrime

Täglich werden 400.000

neue Schadprogramme entdeckt

Quellen: Kaspersky, PurpleSec, CybersecurityVentures

Kaspersky Extended Detection and Response

Umfassende Transparenz. Fortschrittlicher Schutz.

Wir haben die Produktlinie Kaspersky Next um Kaspersky Next XDR Expert erweitert. Diese Lösung folgt dem XDR-Ansatz von Kaspersky und bietet einen umfassenden Überblick über die Sicherheit eines Unternehmens.

Kaspersky XDR ist eine robuste Cybersicherheitslösung, die selbst die komplexesten Cyberbedrohungen wirksam abwehrt. Die Lösung bietet vollständige Transparenz, Korrelation und Automatisierung und nutzt eine Vielzahl von Datenquellen, einschließlich Endpoint-, Netzwerk- und Cloud-Daten.

Sie wurde von der Kaspersky Anti-Targeted Attack Plattform als Native XDR im Jahr 2016 zu Open XDR im Jahr 2023 weiterentwickelt und bietet unverzichtbaren 360-Grad-Blick auf Ihre Cybersicherheit. Kaspersky XDR lässt sich einfach über die Open Single Management Platform verwalten und bietet umfassenden On-Prem-Schutz, der sicherstellt, dass sensible Kundendaten in der eigenen Infrastruktur verbleiben und gleichzeitig die Anforderungen an den Datenschutz erfüllt werden.

Open XDR

Open XDR-Lösungen sind so konzipiert, dass sie mit einer breiten Palette von Sicherheitsprodukten zusammenarbeiten, so dass Unternehmen verschiedene Sicherheitsprodukte von unterschiedlichen Anbietern integrieren können. Dies bietet mehr Flexibilität und anbieterunabhängige Funktionen.

Native XDR

Native XDR-Lösungen arbeiten in der Regel nahtlos mit den Sicherheitstools des jeweiligen Anbieters zusammen und bieten so eine einheitliche Lösung. Diese Lösungen wurden speziell für die Zusammenarbeit entwickelt und bieten eine tiefgreifende Integration, Automatisierung und optimierte Arbeitsabläufe innerhalb der Sicherheitsproduktsuite des Anbieters.

Schlüsseltechnologien

Wir bieten Open XDR als zentrale offene Plattform an – ein universelles Tool, das ein einheitliches Ökosystem von Cybersicherheitsprodukten schafft. Den Grundstock von Kaspersky XDR bilden unsere führenden Lösungen – Kaspersky Unified Monitoring and Analysis Platform, Kaspersky Next EDR Foundations sowie Kaspersky Endpoint Detection and Response Expert. Für das erweiterte Netzwerkmanagement ist KATA eine zusätzliche Option.

Überwachung und Analyse

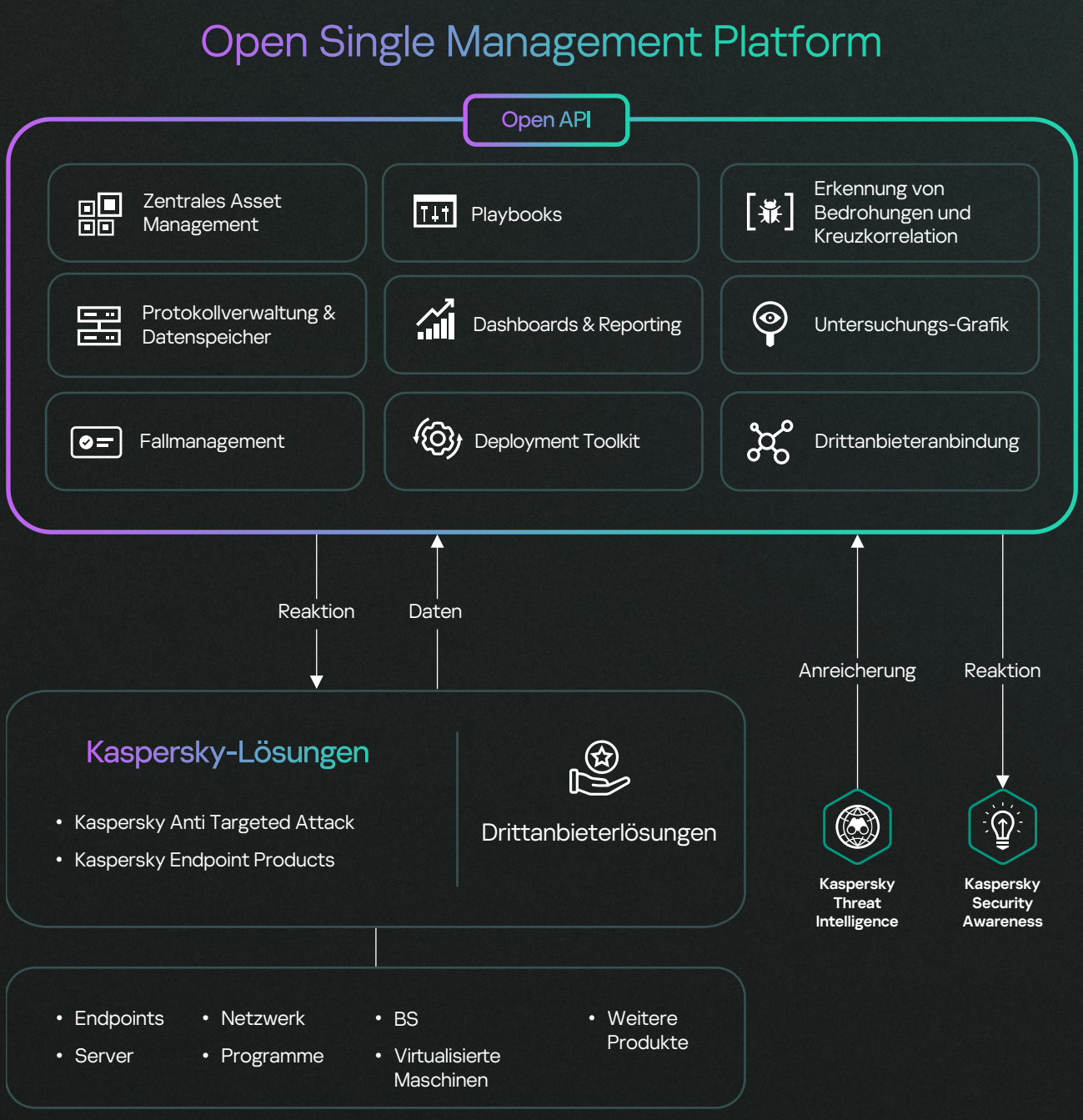
Ermöglicht die zentrale Erfassung und Analyse von Protokollen, die Korrelation von Sicherheitsereignissen in Echtzeit und die rechtzeitige Benachrichtigung über Vorfälle. Beinhaltet ein vorgefertigtes Set von Korrelationsregeln und den Zugriff auf das umfangreiche Portfolio von Kaspersky Threat Intelligence Services zur Identifizierung und Priorisierung von Bedrohungen, Angriffen und IoCs.

Endpoint-Schutz

Bietet zuverlässige Endpoint-Sicherheit und schützt zuverlässig vor Ransomware, Malware und dateilosen Angriffen. Ob On-Prem oder in der Cloud, unsere Endpoint-Lösung nutzt maschinelles Lernen und Verhaltensanalysen, um alle Arten von Endpoints mit allen gängigen Betriebssystemen zu schützen.

Endpoint Detection and Response

Bietet umfassende Transparenz und zuverlässigen Schutz für alle Endpoints eines Unternehmens. Verbesserte Bedrohungssuche und -erkennung dank der einzigartigen und umfassenden Bedrohungsdaten von Kaspersky sowie Automatisierung von Routineaufgaben, geführte Untersuchungsprozesse und anpassbare Erkennungsfunktionen für eine schnelle Lösung von Vorfällen.



Leistungsstarke Funktionen, bedeutende Vorteile

Datenfusion in Echtzeit von Drittanbietern

Die Fähigkeit zur Integration von Daten aus Drittquellen geht über die Endpoints hinaus und wird durch Echtzeit-Kreuzkorrelation verbessert.

Automatisierte Reaktion und Abhilfemaßnahmen

Quarantäne oder Isolierung gefährdeter Endpoints, Blockierung böswilliger Aktivitäten und Behebung von Schwachstellen, wodurch der manuelle Aufwand und die Reaktionszeit verringert werden.

Best-in-class EPP/EDR

Kaspersky ist als Weltmarktführer anerkannt und setzt weltweit Maßstäbe für EPP/EDR-Lösungen. Kaspersky EDR zeichnet sich weltweit aus. Zahlreiche Awards und die aktive Teilnahme an internationalen Gremien wie Interpol und Microsoft Active Protections Program (MAPP) bestätigen dies.

Umfassende Skalierbarkeit

Kaspersky XDR ist in der Lage, Hunderttausende von Endpoints auf einer einzigen Instanz zu unterstützen und verfolgt Bedrohungen in Echtzeit, während die Lösung gleichzeitig eine hohe Verfügbarkeit gewährleistet.

Datensouveränität

Kaspersky ist einer der wenigen Anbieter, der eine umfassende On-Prem-XDR-Lösung anbietet, die sicherstellt, dass die sensiblen Daten der Kunden in ihrer eigenen Infrastruktur verbleiben und gleichzeitig die Anforderungen an die Datensouveränität erfüllen.

Nahtlose und enge Integration in alle Kaspersky-Produkte

Die Interaktion zwischen den Produkten erreicht ein Niveau, das von Lösungen anderer Anbieter nicht erreicht wird, und zeichnet sich durch ein einheitliches Support-System und ein nahtlos integriertes Design aus.

Mehrmandantenfähigkeit, die MSSP-Szenarien ermöglicht

Bereitstellung von XDR als Dienst mit vollwertigen Mandanten – Benutzer eines Mandanten können die Daten anderer Mandanten nicht einsehen, während der Hauptadministrator (der MSSP) Erkennungs- und Reaktionsprozesse für alle Mandanten erstellen kann.

Erweiterte Anpassung von Sicherheitsszenarien und infrastrukturweite Datenanalyse

Die Benutzer können komplexe Sicherheitsszenarien konfigurieren und haben zusätzlich die Möglichkeit, Daten über ihre gesamte Infrastruktur zu analysieren.

Integrationsfunktionen

Das breite Spektrum an Integrationen, die mit Kaspersky XDR möglich sind, bietet eine einheitliche und kontextbezogene Sicht auf potenzielle Bedrohungen und gibt Ihrem Sicherheitsteam alle Werkzeuge und Informationen an die Hand, die es braucht, um Ihr Unternehmen vor allen Angriffen von Cyberkriminellen zu schützen.

Die Integrationsfähigkeiten des Produkts umfassen die Möglichkeit, Daten (Protokolle) von anderen Systemen und Geräten zu empfangen sowie automatische Reaktionen in anderen Produkten einzurichten. Kaspersky XDR verfügt über eine breite Palette an sofort einsetzbaren Integrationen mit Kaspersky- und Drittanbieterprodukten. Es ist auch möglich, zusätzliche Integrationen hinzuzufügen, die entweder im Rahmen der Kaspersky Professional Services oder von Partnern bzw. Kunden selbst entwickelt werden können (einschließlich der Nutzung von API-Funktionen verknüpfbarer Produkte). Die Integration ist mit Systemen aus verschiedenen Bereichen und von verschiedenen Anbietern möglich, und es werden zahlreiche Protokolle und Datenformate unterstützt.

Nach Security Domain

Endpoint Security

- EPP- und EDR-Lösungen

Netzwerk-, Web- und E-Mail-Sicherheit

- E-Mail-Schutz
- Network Detection and Response (NDR)
- Firewalls (FW) und Next-Gen Firewalls (NGFW)
- Unified Threat Management (UTM)
- Intrusion Detection Systeme (IDS)

Cloud Security

- Cloud Access Security Brokers (CASB)
- Cloud Workload Protection Platforms (CWPP)

Threat Intelligence

- Cyber Threat Intelligence (CTI)

Identitätssicherheit

- Identity and Access Management (IAM)
- Privileged Access Management (PAM)

OT / IoT Security / Security Awareness

Nach Transportart

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

Nach Datenart

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

Nach Anbieter

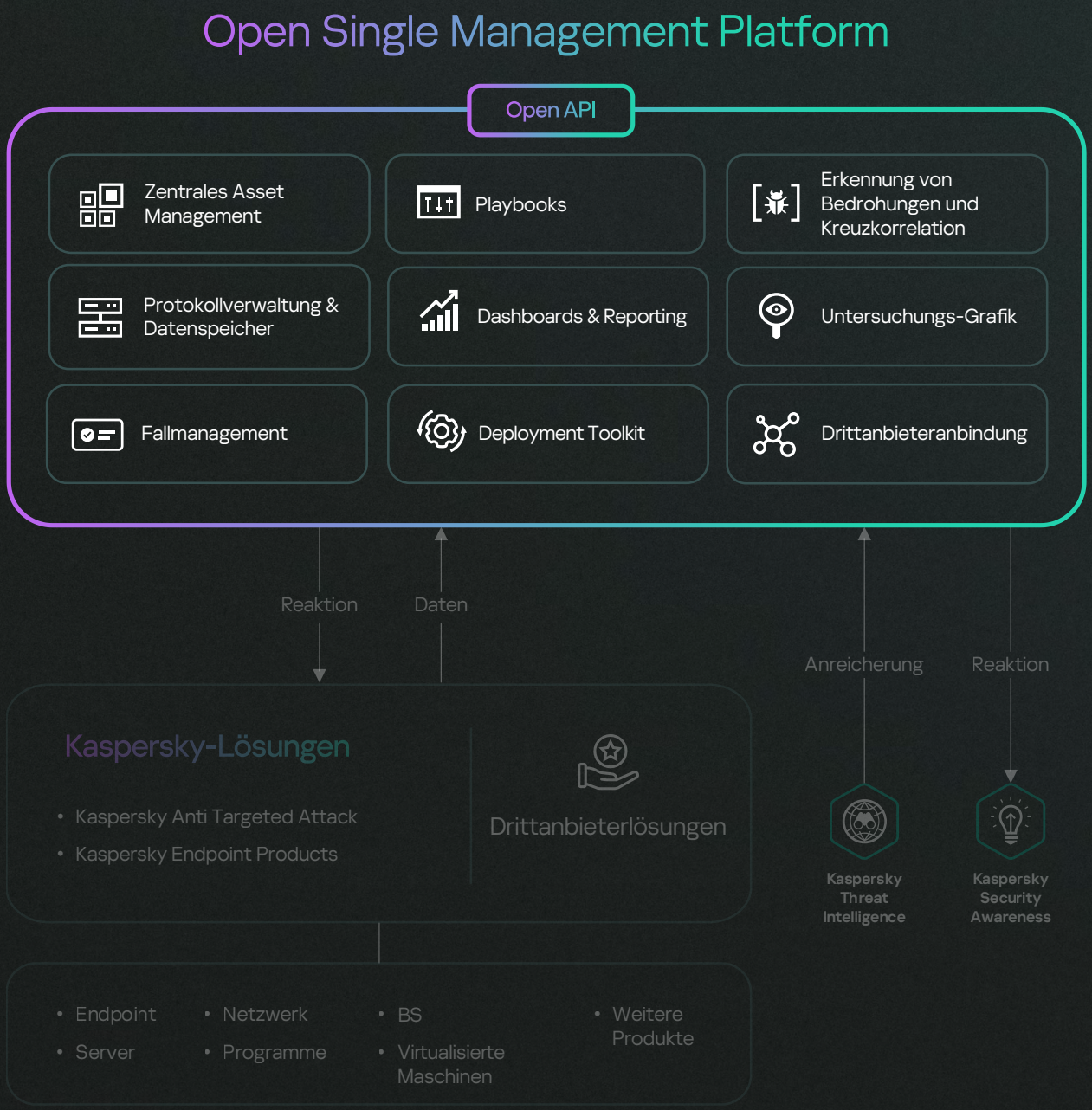
- Kaspersky
- Absolute
- AhnLab
- Aruba
- Avigilo
- Ayehu
- Barracuda
- BeyondTrust
- Bloombase
- BMC
- Bricata
- Brinqa
- Broadcom
- CheckPoint
- Cisco
- Citrix
- Claroty
- CloudPassage
- Corvil
- Cribl
- CrowdStrike
- CyberArk
- DeepInstinct
- Delinea
- EclecticIQ
- Edge Technologies
- Eltex
- Eset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

Unsere Lösung

Kaspersky XDR ist in zwei Varianten erhältlich.

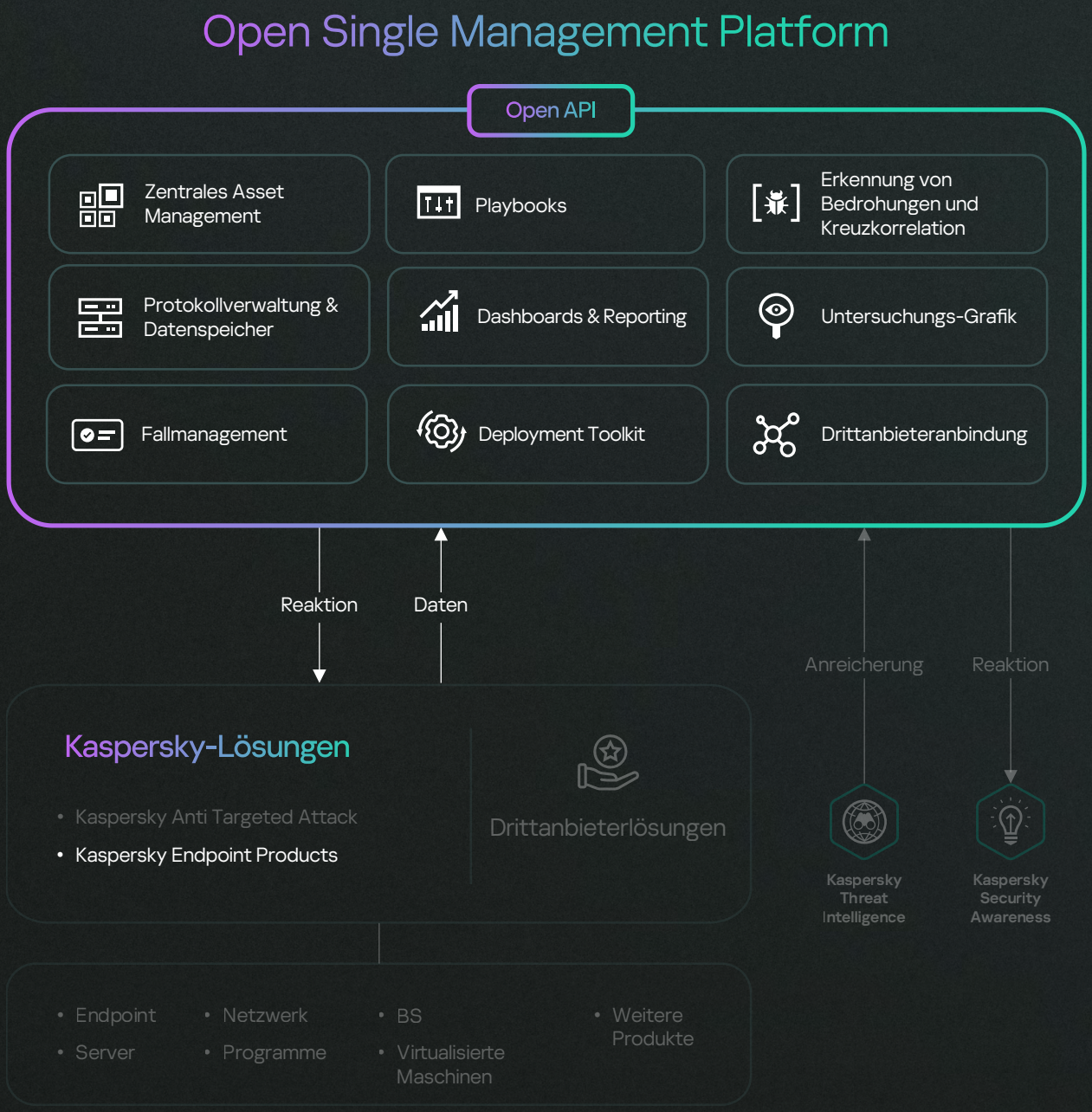
Kaspersky XDR Core

Kaspersky XDR Core richtet sich an Kunden, die bereits über Endpoint- und EDR-Lösungen verfügen und diese nicht ersetzen wollen, sondern die Funktionalität um eine Korrelations-Engine, automatische Reaktionen und die Anbindung von Drittanbietern erweitern möchten.



Kaspersky Next XDR Expert

Kaspersky Next XDR Expert kombiniert erstklassigen Endpoint-Schutz mit den fortschrittlichen Erkennungsfunktionen von Kaspersky EDR Expert, einer Korrelations-Engine und automatischen Reaktionsmaßnahmen. Drittanbieterlösungen können angebunden werden, um alle Daten zusammenzuführen.



Mehrwert mit zusätzlichen Sensoren

Kaspersky XDR unterstützt die nahtlose Integration zusätzlicher Sensoren zum Schutz spezifischer Objekte, die nahtlos in XDR integriert werden können. XDR wird damit zu einer umfassenden Plattform, die Analysten einen zentralen Arbeitsbereich bietet, der alle integrierten Lösungen umfasst.

Kaspersky XDR stärkt nicht nur Ihren Schutz durch EDR, sondern bietet auch flexible Integrationsmöglichkeiten. So können Kunden jederzeit Produkte zum Ökosystem hinzufügen.

		Kaspersky XDR Core	Kaspersky Next XDR Expert
Die Open Single Management Platform und ihre Komponenten	Kreuzkorrelations-Engine • Drittanbieter-Konnektoren • Protokollverwaltung & Datenspeicher • Erkennung von Bedrohungen und Kreuzkorrelation • Asset Management • Dashboards & Reporting	●	●
	XDR-Komponenten • Fallmanagement • Automatisierung von Reaktionsmaßnahmen und Orchestrierung (Playbooks) • Untersuchung • Toolkit für die Bereitstellung • Open API	●	●
Kaspersky Endpoint-Funktionalität*	Automatisierte, halbautomatische und manuelle Erkennung		●
	Überwachung über alle geschützten Endpoints hinweg		●
	Eindämmung von Bedrohungen		●
	Optionen zur Wiederherstellung		●
	Schutz und Verwaltung mobiler Geräte		●
	Cloud Discovery und Blockierung		●
	Sicherheit für MS O365, Datenerkennung		●
	Cybersicherheitstraining für IT-Administratoren		●

* Welche Funktionen verfügbar sind, hängt von der Implementierungsmethode ab

Kaspersky XDR Core

- Kaspersky Unified Monitoring and Analysis Platform
- XDR-Komponenten

Kaspersky Next XDR Expert

- Kaspersky Unified Monitoring and Analysis Platform
- Kaspersky Next EDR Foundations
- Kaspersky Endpoint Detection and Response Expert
- XDR-Komponenten

Wir präsentieren: Kaspersky Next

Kaspersky Next EDR Foundations

Robuste Sicherheit für alle

Schutz für alle Ihre Endpoints

Wenn Sie Folgendes brauchen:

- Starker Endpoint-Schutz
- Grundlegende Sicherheitskontrollen
- Maximale Automatisierung

Kaspersky Next EDR Optimum

Stärken Sie Ihre Abwehr

Erhöhen Sie Ihre Sicherheit durch wichtige Funktionen zur Untersuchung und Abwehr

Wenn Sie Folgendes brauchen:

- Verbesserte Sichtbarkeit und Reaktionsmöglichkeiten
- Hybrid Cloud Security
- Kontrollen auf dem Niveau von Großunternehmen

Kaspersky Next XDR Expert

Tools für Ihre Experten

Schutz gegen komplexe, raffinierte Bedrohungen

Wenn Sie Folgendes brauchen:

- Fortschrittliche Threat Detection
- Nahtlose Integration
- Leistungsstarke Threat Hunting-Tools

Warum Kaspersky XDR?

Häufig getestet. Vielfach ausgezeichnet. Schutz von Kaspersky

Kaspersky ist ein etabliertes, weltweit tätiges Cybersicherheitsunternehmen mit langjähriger Expertise. Wir schützen seit über 25 Jahren Organisationen auf der ganzen Welt und haben für unsere Produkte und Dienstleistungen zahlreiche Auszeichnungen erhalten. Lösungen von Kaspersky haben zwischen 2013 und 2022:

827

an 827 unabhängigen Tests teilgenommen

587

587 erste Plätze erreicht

685

685 Top-Drei-Platzierungen erreicht

Im Jahr 2023 wurde Kaspersky von dem weltweit führenden Technologieforschungs- und Beratungsunternehmen ISG zum Marktführer im Bereich XDR-Lösungen ernannt. ISG definiert „Leader“ als Unternehmen mit einem umfassenden Produkt- und Dienstleistungsangebot, das für Innovationskraft und Wettbewerbsstabilität steht.

Weitere Informationen

Kaspersky Extended Detection and Response

Demo anfordern

www.kaspersky.de

#kaspersky
#bringonthefuture