Kaspersky B2B-Portfolio

kaspersky

Inhalt

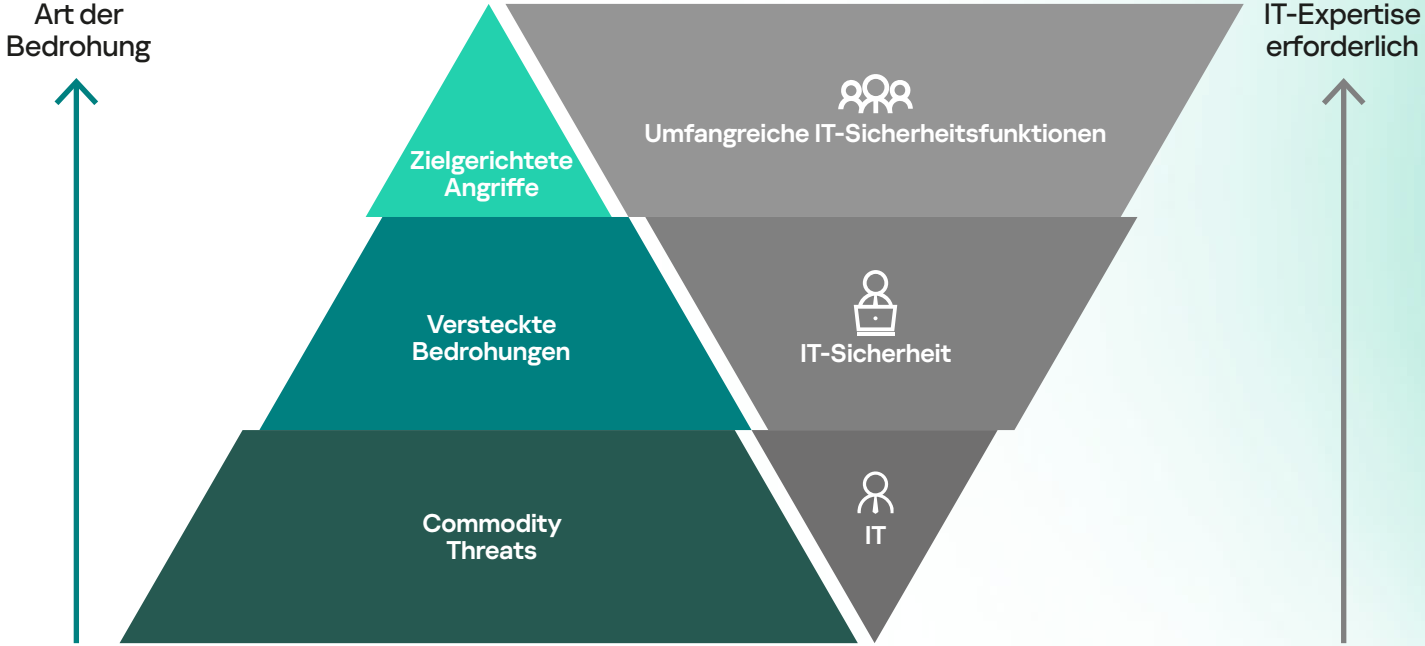
Über unser B2B-Portfolio

Der Aufbau einer Sicherheitsgrundlage für Ihr Unternehmen durch die Auswahl des richtigen Produkts oder Services ist der erste Schritt. Der Schlüssel für den langfristigen Erfolg liegt aber in der Entwicklung einer zukunftsorientierten Cybersicherheitsstrategie.

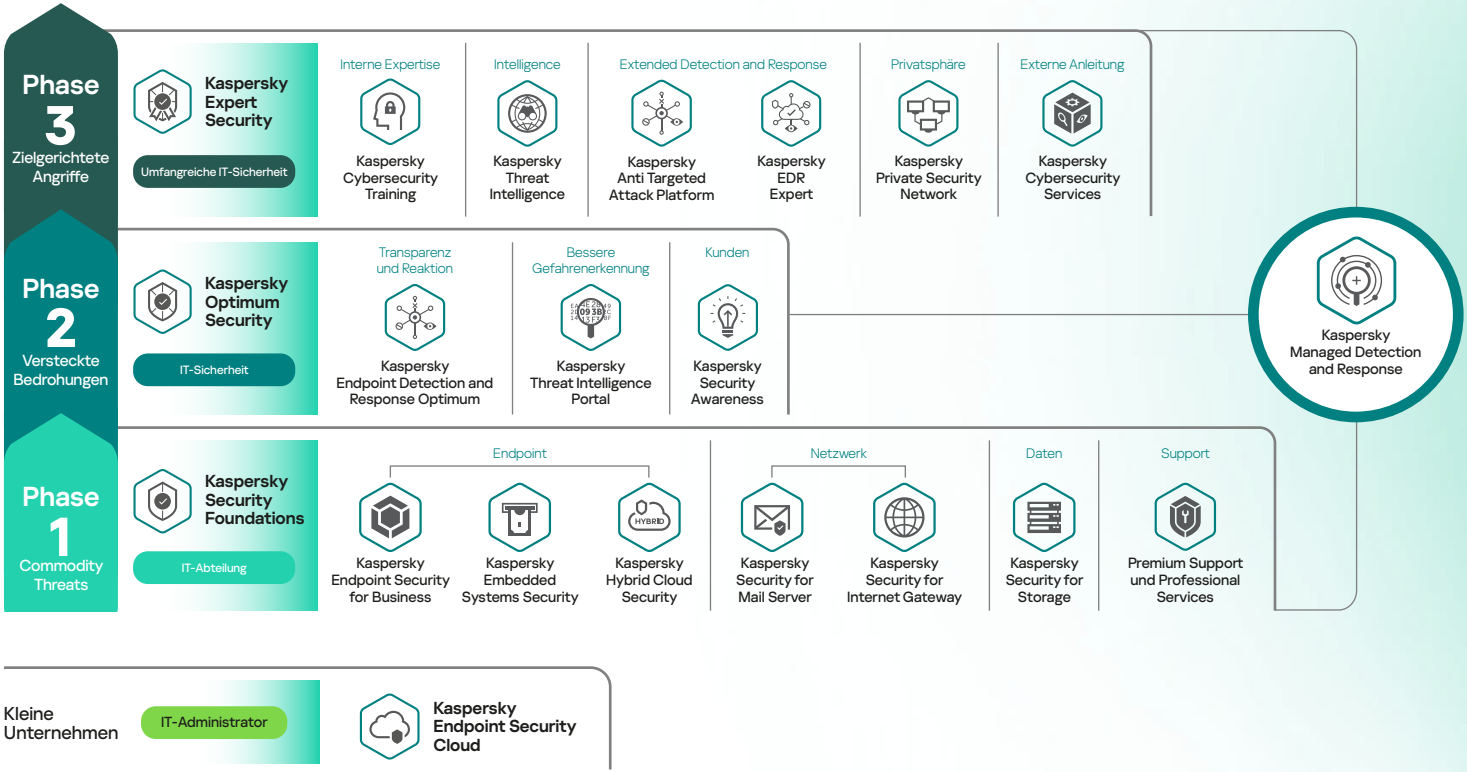
Das B2B-Portfolio von Kaspersky ist auf die Sicherheitsanforderungen von Unternehmen jeder Branche und Größe sowie jeden technischen Reifegrads abgestimmt. Dank unseres mehrdimensionalen Ansatzes sind Sie umfassend gegen alle Arten von IT- und OT-Cyberbedrohungen geschützt. Er unterstützt Unternehmen dabei, mehr als 90 % der Bedrohungen automatisiert zu neutralisieren. Zusätzlich können Unternehmen ihre Security-Strategie beliebig um weitere leistungsstarke Sicherheitstools erweitern.

Kaspersky ist Ihr Anbieter Nummer 1 in Sachen Cybersecurity.

Expertise zur Abwehr unterschiedlicher Bedrohungsarten



Kasperskys Cybersicherheitskonzept – Schritt für Schritt



Die Notwendigkeit langfristiger Sicherheitsplanung

Herkömmliche kurzfristige Sicherheitsplanung

Entscheidungsfindung:

- Markttrends
- Silo-Sicherheitslösung
- Feuerwehrstrategie
- Compliance-orientiert

Einsatz herkömmlicher Produkte:

- EPP
- Firewalls/NGFW
- Web Application Firewall
- Data Loss Prevention
- SIEM

Eigenschaften

- Kurzfristige Sicherheitsplanung
- Abhängigkeit von Technologien und Features
- Netzwerkschutz auf Perimeter-Grundlage

Gründe für den Misserfolg herkömmlicher Ansätze:

- Immer komplexere Bedrohungen
- Komplexität der zu sichernden IT-Infrastruktur
- Komplexität des Incident Response-Prozesses

Endpoints sind die gängigsten Eintrittspunkte in eine Unternehmensinfrastruktur, das Hauptziel für Cyberkriminelle und eine wichtige Quelle für die bei einer effektiven Untersuchung komplexer Vorfälle erforderlichen Daten.

der Vorfälle wurden erkannt, nachdem sie sich schon ausgewirkt hatten

der Unternehmen befassen sich mit der fehlenden IT-Sicherheitsexpertise

Quelle: Incident Response 2021 Analyst Report von Kaspersky, IT Security Economics 2021 Report von Kaspersky

Schutzlösungen für Unternehmen

Zurück zum Inhaltsverzeichnis

Phase
3
Zielgerichtete Angriffe

Kaspersky Expert Security

Zurück zum Inhaltsverzeichnis

Kaspersky Expert Security

Übersicht

Bei Kaspersky Expert Security handelt es sich um ein umfassendes Verteidigungsmodell, das den täglichen Anforderungen aller Unternehmen mit ausgereifter IT-Sicherheit bei der Bekämpfung der aktuell raffiniertesten Bedrohungen begegnet. Es bietet auch Schutz vor APTs (Advanced Persistent Threats, hochentwickelte und hartnäckige Bedrohungen) und zielgerichteten Angriffen.

Für wen ist diese Lösung geeignet?

- Erfahrenes und gut aufgestelltes IT-Sicherheitsteam oder ein Security Operations Center
- Unternehmen mit einer komplexen und verteilten IT-Umgebung
- Unternehmen, die im Hinblick auf kostspielige Sicherheitsvorfälle und Datenschutzverletzungen kein Risiko eingehen möchten

Vorteile

- Optimierung der Arbeitslast Ihrer Experten
- Erweiterung des Wissens und der Fertigkeiten
- Unterstützung Ihrer Experten

Herausforderungen

Warum haben Cybervorfälle Erfolg?

Zu wenig, zu spät

Ignorieren der Wahrscheinlichkeit eines komplexen Angriffs und Implementieren erweiterter Schutzmechanismen erst, nachdem ein schwerwiegender Vorfall aufgetreten ist

Ineffiziente Ansätze

Unsystematische oder ineffiziente Methoden für die Bearbeitung von Cybervorfällen aufgrund uneinheitlicher Tools, mangelnder Automatisierung und einer schwachen Bedrohungsanalyse

Kein Back-Up-Plan

Kein Drittanbieter, der im Falle einer Cyberkrise sofortige Unterstützung durch Experten bereitstellen kann

Kostspielige Konsequenzen

Umgang von Kaspersky Expert Security mit diesen Herausforderungen

Gut aufgestellt

Interne Experten werden richtig **ausgestattet**, damit sie komplexe Cybersicherheitsvorfälle abwehren und die Arbeitslast optimieren können.

Informiert

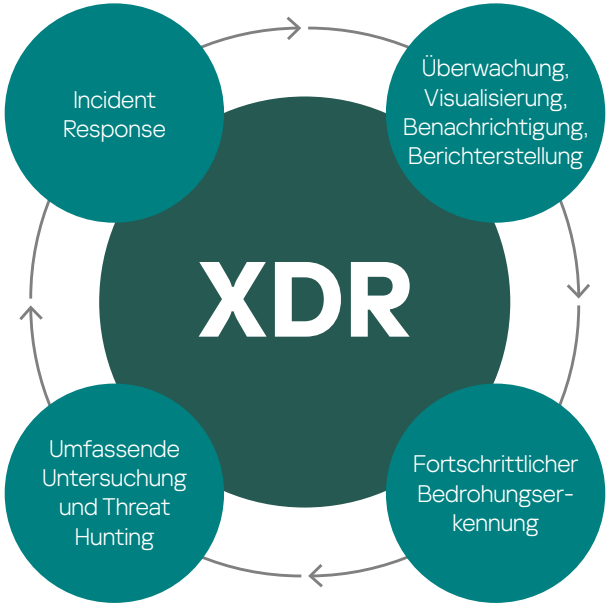
Wissen wird mit Bedrohungsanalysen **angereichert** und Experten im Umgang mit **komplexen** Vorfällen geschult.

Verstärkt

Ihre Experten **werden** mit Handlungsempfehlungen **unterstützt**.

Gut aufgestellt

Interne Experten werden ausgerüstet.



Die unternehmensweite Transparenz aller Angriffsphasen ermöglicht eine lückenlose Bedrohungsanalyse und eine zuverlässige Abwehr kompexer Angriffe.

Eine zentrale Plattform reduziert Warnstufen durch Bereitstellung von Threat Intelligence-basiertem Kontext und verhindert Alarmermüdung.

Die Automatisierung von Aufgaben bei Erkennung, Untersuchung und Vorfallsreaktion optimiert die Arbeitsbelastung von IT-Sicherheitsteams.

Die mögliche Integration in bestehende Sicherheitsprodukte verbessert die allgemeinen Sicherheitsniveaus und bietet Schutz für Ihre älteren Investitionen in die Sicherheit.

Wichtige Produkte:

Kaspersky Anti Targeted Attack
Weitere Informationen

Kaspersky EDR Expert
Weitere Informationen

Interne Experten bleiben informiert

Threat Intelligence

- **Security Operations** — Sie erhalten in verschiedenen Formaten einzigartige Einblicke in Ihre Gegner, um die Wirksamkeit von Sicherheitsoperationen zu verbessern.
- **Incident Response** — Globale historische Daten über Zusammenhänge von Bedrohungen und deren Zuordnung zu bestimmten Gegnern führt zu effektiveren Unsersuchungen durch Mitarbeiter.
- **Vulnerability Management** — Rechtzeitige und genaue Informationen zu Schwachstellen, die in der Praxis tatsächlich ausgenutzt wurden, tragen dazu dabei, Patching-Bemühungen anhand ihres Risiko-Levels zu priorisieren.
- **Security Leadership** — Dank des umfassenden Überblicks über Ihr Sicherheitsniveau erhalten Sie nötige Informationen für Ihre Verteidigungsstrategie und können Investitionen in Ihre IT-Sicherheit besser rechtfertigen.

Wichtige Produkte: **Kaspersky Threat Intelligence**

Weitere Informationen

Interne Experten werden weiter qualifiziert

Durch praxisorientierte Schulungen von branchenweit anerkannten Experten wird Ihr internes Team weiter qualifiziert und kann IT-Sicherheitsvorfällen noch effizienter begegnen.

Dies führt zu erheblichen Zeit- und Kostenersparnis, da in Zeiten der Ressourcenknappheit keine neuen Mitarbeiter eingestellt werden müssen.

Außerdem wird die Motivation Ihrer Mitarbeiter nachhaltig gesteigert.

Umfassende Schulungen lassen sich an Ihre Anforderungen anpassen und können vor Ort, remote oder auf Abruf bereitgestellt werden.

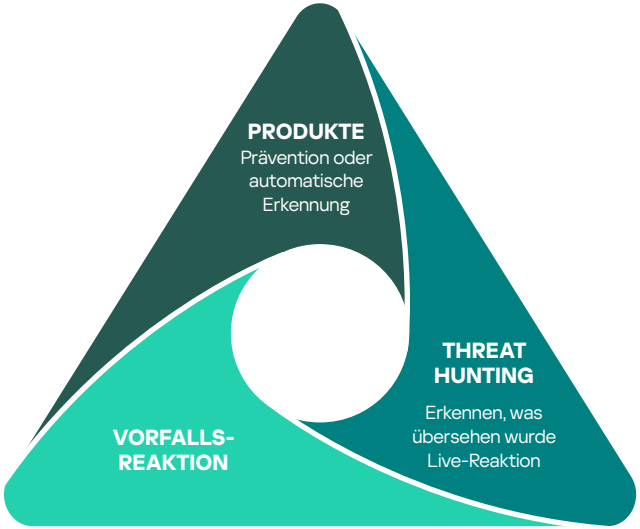
Wichtige Produkte:

Kaspersky Cybersecurity Training
Weitere Informationen

Kaspersky Tabletop Exercise

Verstärkt

Unterstützung Ihrer Experten



Eine umfassende Managed Protection-Lösung bedeutet, dass Sie Routineaufgaben auslagern können und sich interne Mitarbeiter auf Aufgaben konzentrieren können, die tatsächlich menschliches Eingreifen erfordern.

Dank der starken Kombination aus umfassenden Erkennungsfunktionen und umfassender Expertise rund um zielgerichtete Angriffe können False Positives und kostspielige False Negatives effektiv herausgefiltert werden.

Sofortiger Support von unseren Experten ermöglicht Ihnen die schnelle und effektive Behebung der komplexesten Vorfälle.

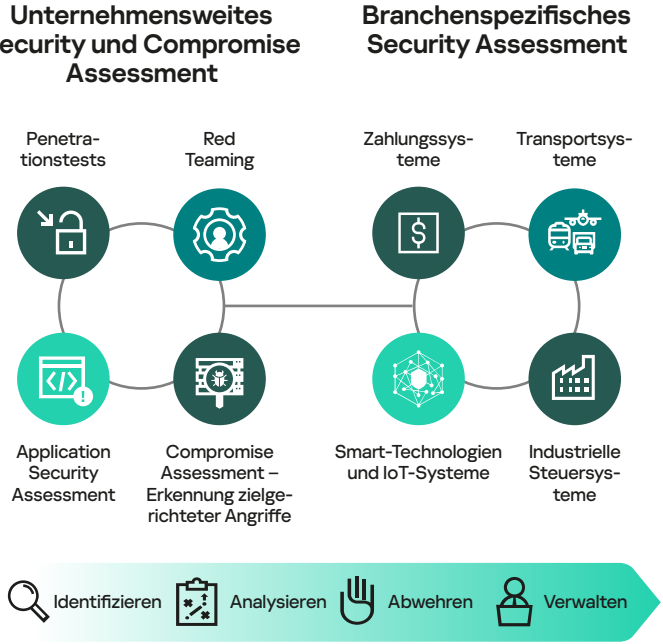
Wichtige Services:

Kaspersky Managed Detection and Response
Weitere Informationen

Kaspersky Incident Response
Weitere Informationen

Verstärkt

Ihre Experten werden mit Handlungsempfehlungen unterstützt



Auf Bedrohungsinformationen basierende Sicherheitsbewertungen bieten einen Überblick über Ihr Sicherheitsniveau. So können Sie Sicherheitslücken schließen bevor sie ausgenutzt werden.

Das Compromise Assessment ermöglicht die rechtzeitige Idenfikation von Sicherheitsvorfällen. So werden deren Auswirkungen eingedämmt, bevor sie offen zutage treten, und Schutz vor künftigen ähnlichen Angriffen wird aufgebaut.

Teams mit fundierten sowie aktuellen und praktischen Kenntnissen der branchenspezifischen Infrastruktur können zum verbesserten Schutz vor Bedrohungen, die bestimmte spezialisierte IT-Umgebungen betreffen, beitragen.

Wichtige Services:

Kaspersky Security Assessment
Weitere Informationen

Kaspersky for Security Operations Centers
Weitere Informationen

Kaspersky Targeted Attack Discovery
Weitere Informationen

Kaspersky Adversary Attack Emulation

Übersicht

Informiert | **Gut aufgestellt** | **Verstärkt**

Kaspersky Expert Security

Kaspersky Threat Intelligence

- Threat Data Feeds
- CyberTrace
- Threat Lookup
- Cloud Sandbox
- APT und Crimeware Intelligence Reporting
- Digital Footprint Intelligence
- Branchenspezifisches Intelligence Reporting (ICS, Transport)
- Ask the Analyst
- Takedown-Service

Kaspersky Cybersecurity Training

- Incident Response Training
- Digital Forensics Training
- Malware Analysis und Reverse Engineering Training
- Online YARA Training
- Tabletop Exercise

Kaspersky Extended Detection and Response Expert

Kaspersky Security und Compromise Assessment

- Targeted Attack Discovery
- Penetration Testing
- Red Teaming
- Application Security Assessment
- Branchenspezifisches Security Assessment (ICS, Zahlungssysteme, Transport, IoT)
- Adversary Attack Emulation
- SOC Consulting

Kaspersky MDR und Incident Response

- Managed Detection and Response (MDR) Expert
- Incident Response
- Malware-Analyse
- Digital Forensics

Wichtige Alleinstellungsmerkmale

Das umfassendste Verteidigungsmodell der Branche

Ein komplettes Arsenal an fortschrittlichen Technologien und -services, um die Effektivität Ihrer IT-Sicherheitstalente und des SOC-Teams zu stärken

Eine einzige zentralisierte Lösung zur Verwaltung von Multi-Vektor-Erkennung und -Reaktion

Spezialisierte Lösungen, die auf der Entdeckung von APT-Kampagnen durch das GReAT-Team von Kaspersky beruhen, mit umfassenden Abwehrmechanismen durch eine einzige Konsole

Bedarfsorientierter Support von weltweit führenden Threat Intelligence-Analysten

Branchenexperten bieten Ihnen Handlungsempfehlungen und Erkenntnisse zu spezifischen Bedrohungen, sodass es keiner zusätzlichen Spezialisten bedarf

Fortlaufender Zugang zu anerkannter IT-Sicherheitsexpertise

Erfahrene und branchenweit anerkannte Experten mit fundierten sowie aktuellen und praktischen Kenntnissen auf diesem Gebiet stehen Ihnen zur Verfügung

Kaspersky Optimum Security

Zurück zum Inhaltsverzeichnis

Kaspersky Optimum Security

Übersicht

- Kaspersky Optimum Security schützt Unternehmen vor neuen, unbekannten und versteckten Bedrohungen
- Bedrohungen erkennen und entsprechend auf sie reagieren – effektiv und ressourcenschonend zugleich
- Sicherheitsüberwachung rund um die Uhr, automatisiertes Threat Hunting und geführte und verwaltete Reaktionen, unterstützt von Kaspersky-Experten

Für wen ist diese Lösung geeignet?

- Kleines engagiertes IT-Sicherheitsteam, normalerweise bestehend aus ein bis drei Mitarbeitern
- Begrenzte Ressourcen für die Cybersicherheit
- Neu entstehendes Fachwissen im Bereich Cybersicherheit

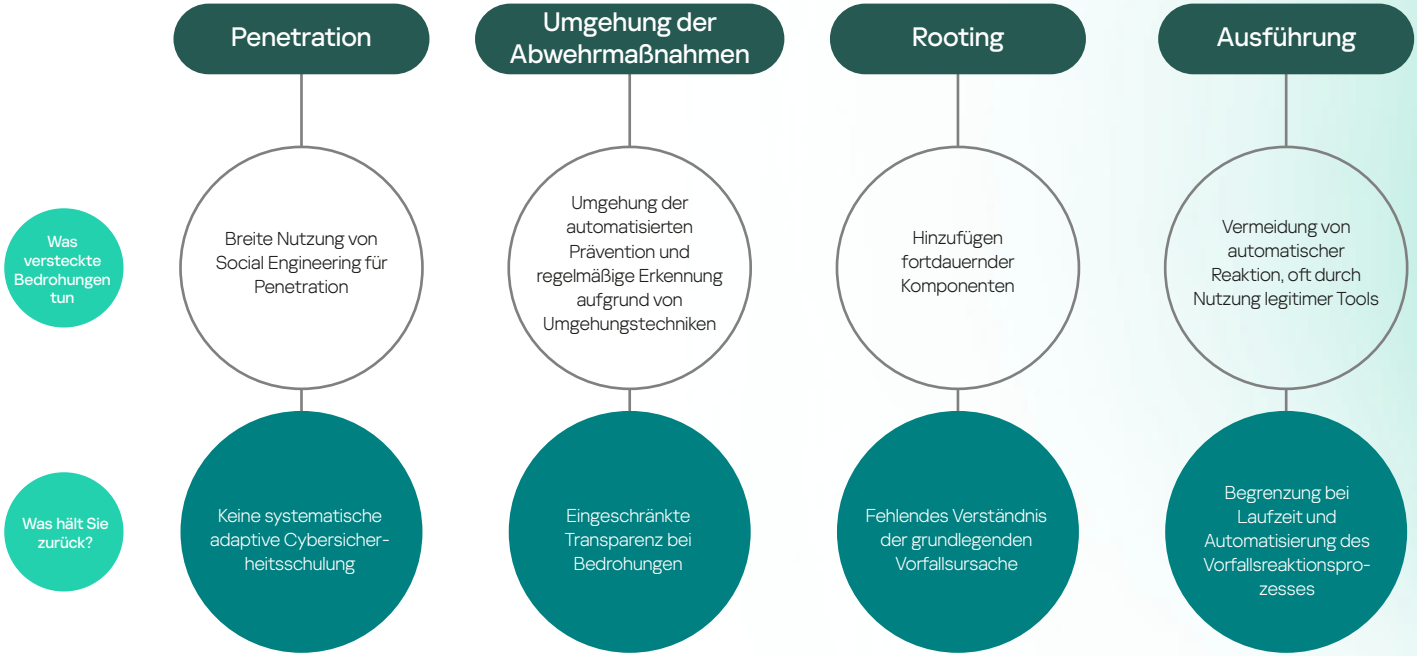
Vorteile

- Höherer Endpoint-Schutz gegen schwer aufzuspürende Bedrohungen
- Unterstützt den Aufbau wichtiger Vorfallsreaktionsprozesse
- Optimiert die Verwendung von Cybersicherheits-Ressourcen

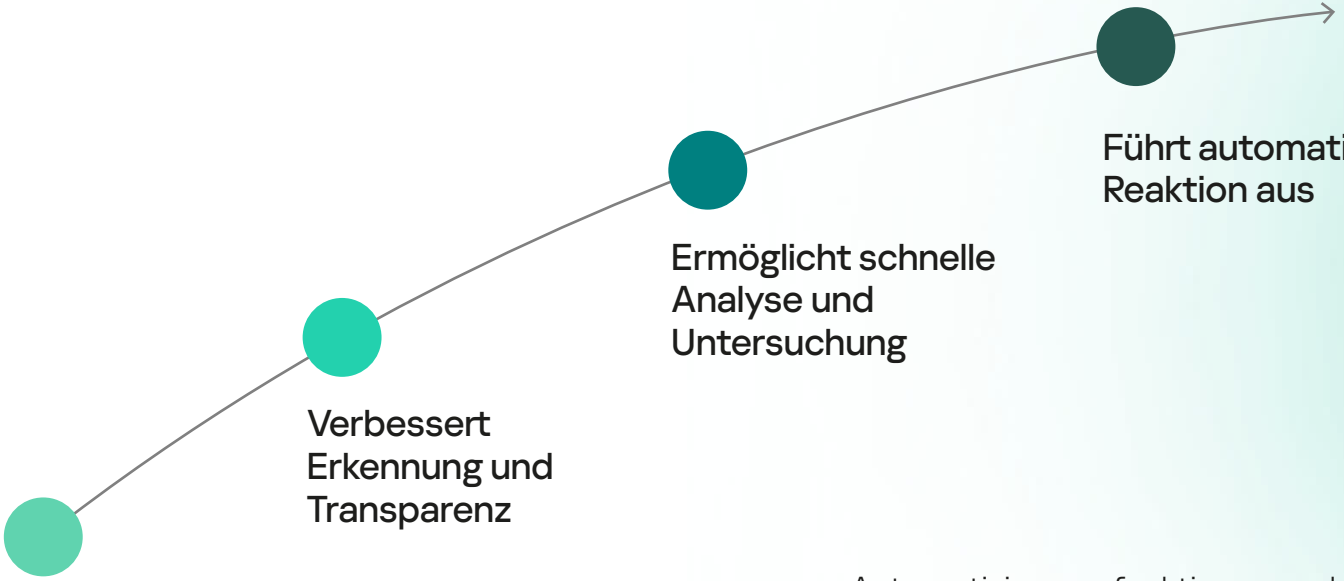
Herausforderungen

Neue, unbekannte und versteckte Bedrohungen
Hoch entwickelte Ransomware, Malware, Cyberdiebstahl usw.

Diese Bedrohungen können viel länger in Systemen vorhanden sein und mehr Schaden verursachen.



So adressiert Kaspersky Optimum Security diese Herausforderungen



+ Automatisierungsfunktionen und ein schlanker Workflow tragen dazu bei, das Beste aus begrenzten Ressourcen herauszuholen

Steigert das Sicherheitsbewusstsein unter den Mitarbeitern

Sie können innerhalb Ihres ganzen Unternehmens eine sichere Arbeitsumgebung aufbauen, indem Sie Mitarbeiter motivieren, spezifische Kenntnisse zu erlernen, Angewohnheiten zu ändern und sich cyber-sicher zu verhalten.

Fangen Sie bei der Führungsebene an.

Steigern Sie die Security Awareness auch für Vertreter der Führungsebene. Etablieren Sie das Thema in der Führungsebene, damit sie die gleiche Priorität für alle einführen können.

Rüsten Sie alle Mitarbeiter aus.

Erlangen Sie über 300 praktische Cybersicherheitskenntnisse von Experten auf diesem Gebiet. Nach einer allgemeinen Einstufung wird jeder Mitarbeiter so ausgebildet, dass er in puncto Sicherheitsbewusstsein ein Kompetenzniveau von 100 % erreicht.

Sprechen Sie spezialisierte Teams an.

IT-Generalisten erlernen praktische Fertigkeiten, z. B. wie sie einen möglichen Angriff erkennen oder Vorfallsdaten sammeln und an die Abteilung für IT-Sicherheit weitergeben.

Stellen Sie sicher, dass Kenntnisse auch angewendet werden.

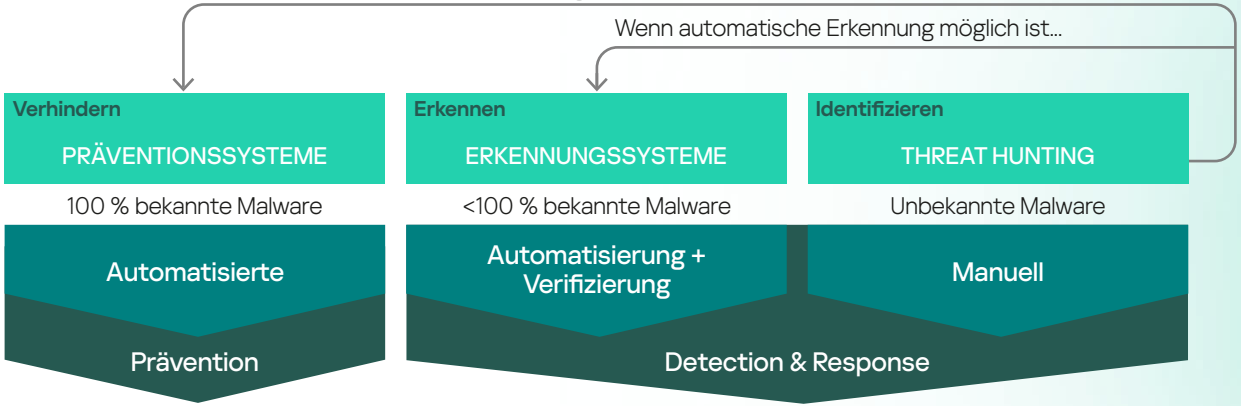
Nutzen Sie eine leicht zu verwaltende integrierte Lösung, die Wissen vermittelt und Mitarbeiter motiviert.

Wichtige Produkte: Kaspersky Security Awareness

Weitere Informationen

Verbessert Erkennung und Transparenz

Mehrere Erkennungsebenen erlauben die effektivste und rechtzeitige Erkennung von Bedrohungen.



Integrierter Emulator für die Erkennung vor der Ausführung von schädlichem Verhalten

Anti-Rootkit-Technologie und Firmware-Scanner

Durchgängige Nutzung von Threat Intelligence

Heuristik, smarte Datensätze, Machine-Learning-basierte Technologien und **Adaptive Anomaly Control**

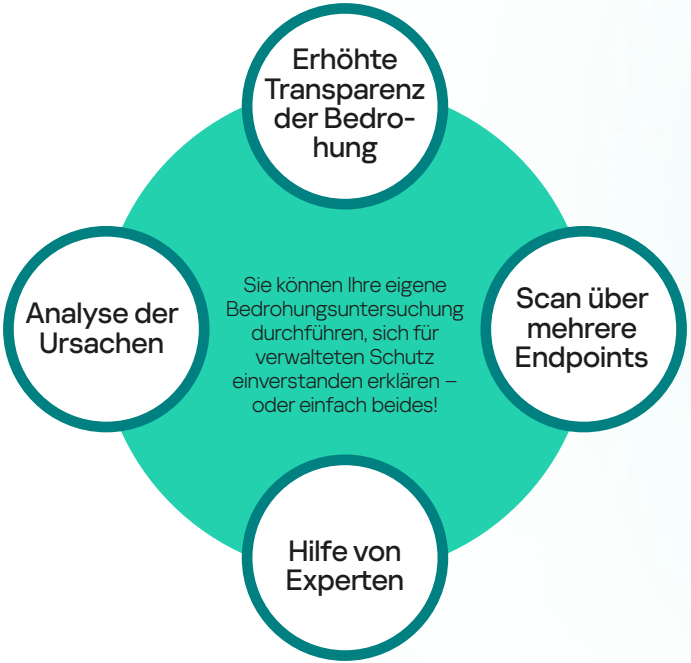
Sandbox für Verhaltensanalyse in einer sicheren Umgebung

Von Kaspersky-Experten eigens zusammengestellte Angriffsindikatoren (IoAs) heben Ihre Erkennungfunktionen auf ein neues Niveau.

Wichtige Produkte: Kaspersky Endpoint Detection and Response (EDR), Kaspersky Security Awareness

Ermöglicht schnelle Analyse und Untersuchung

Schnelle und effiziente Analyse mit allen verfügbaren Daten von einer Warnhinweiskarte



Schnelle Erkennung der grundlegenden Ursache einer Bedrohung mit detaillierter Übersicht

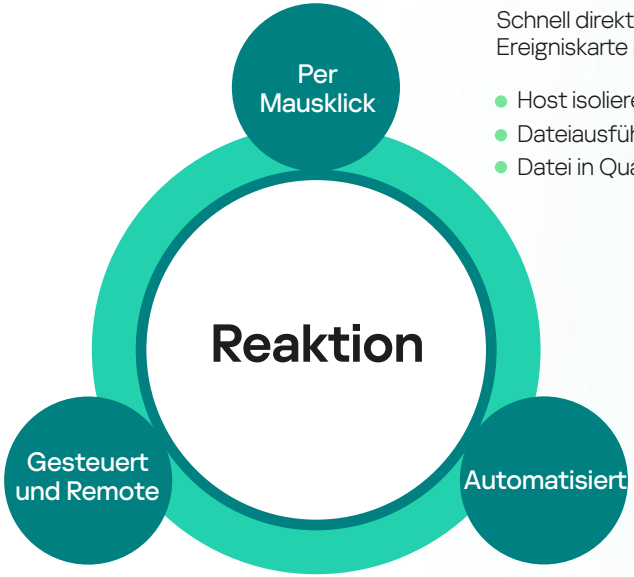
Import und Generierung von IoC[1] und Scan von Endpoints, um aktuelle Bedrohungen aufzudecken

Die Kaspersky-Experten nutzen führende TI[2]- und KI-fähige Tools, um Ihre Bedrohungsdaten umfassend zu analysieren

[1] Gefährdungsindikator
[2] Threat Intelligence

Wichtige Produkte: Kaspersky Endpoint Detection and Response (EDR) Optimum; Kaspersky Managed Detection and Response (MDR) Optimum

Führt automatisierte Reaktion aus



Schnell direkt von der Ereigniskarte reagieren:

- Host isolieren
- Dateiausführung verhindern
- Datei in Quarantäne setzen

Sie erhalten detaillierte Berichte und Handlungsempfehlungen – oder die Kaspersky-Experten leiten remote Reaktionsmaßnahmen ein

Sie können die Infrastruktur auf IoCs[1] für bekannte Bedrohungen scannen. Dabei wird sofort über ein Kontrollkästchen eine automatisierte Reaktion initiiert.

[1] Gefährdungsindikator

Wichtige Produkte: Kaspersky Endpoint Detection and Response (EDR) Optimum, Kaspersky Managed Detection and Response (MDR) Optimum

Bekämpft versteckte Bedrohungen auf verschiedenen Ebenen

Penetration

Der Nutzer erhält eine Phishing-Mail oder greift auf eine schädliche Webressource zu, die den Host infiziert.

Installation

In der ersten Phase der Infektion werden erforderliche Komponenten installiert, mit den C&C[1]-Servern kommuniziert und die Umgebung untersucht.

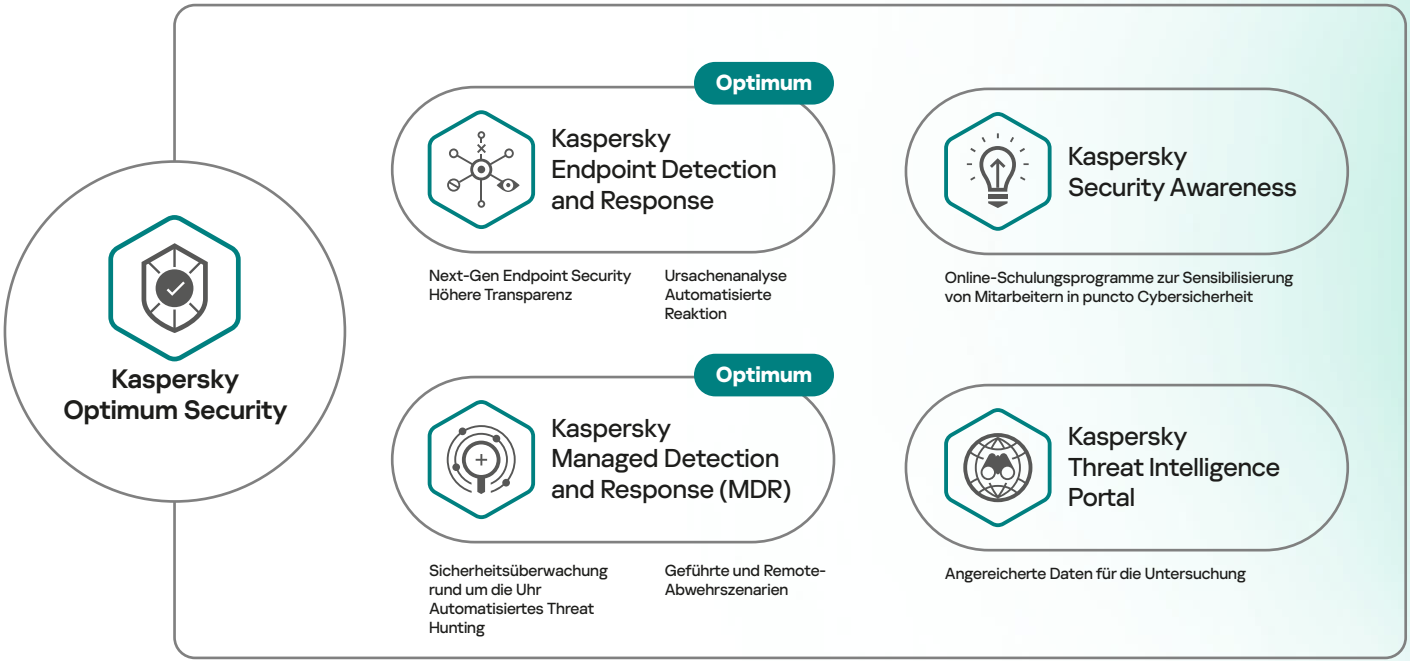
Rooting

Es folgt die Festsetzung im System über eine Reihe von Tools – auch seriösen und systemeigenen – und eventuell eine weitere horizontale Ausbreitung.

- Sicherheitsbewusstsein unter den Mitarbeitern
- Reduzierung der Angriffsfläche
- Automatische Gefahrenabwehr
- Erweiterte Erkennungsmechanismen, einschließlich ML-basierte Verhaltensanalyse und Sandbox
- Automatisiertes Threat Hunting mit IoAs[2]
- Ursachenanalyse und IoC[3]-Scans
- Automatisierte, gesteuerte und verwaltete Reaktionen

[1] Command and Control
[2] Indicators of Attack
[3] Gefährdungsindikator

Kaspersky Optimum Security – für ein Plus an Sicherheit vor komplexen Bedrohungen



Wichtige Alleinstellungsmerkmale

Unterstützt Hybrid-Umgebungen

Workstations, Server, virtuelle Maschinen, Public Clouds

Unkompliziert & effizient

Alle Produkte wurden für Unternehmen mit begrenzten Cybersicherheits-Ressourcen entwickelt. Somit haben optimierte Erkennung, Untersuchung und Reaktion Priorität.

Zentralisierte Verwaltung

Einheitliche Cloud- oder lokale Konsolen für Konfiguration, Analyse und Reaktion, alles von einem Ort.

Eine einzige Lösung

Grundlegende EDR- und verwaltete Schutzoptionen als Teil einer einzigen einheitlichen Lösung

Phase
1
Commodity
Threats

Kaspersky Security Foundations

Zurück zum Inhaltsverzeichnis

Kaspersky Security Foundations

Übersicht

Die Cloud-basierte Phase der Bedrohungsverhinderung ermöglicht jedem Unternehmen, Commodity Cyberbedrohungen auf jedem Gerät, in VDI- und Hybrid Server-Infrastrukturen automatisch zu stoppen. Aus der TEI-Kundenbefragung von Forrester geht hervor, dass so durchschnittlich ein ROI von 441 % erzielt werden konnte.

Für wen ist diese Lösung geeignet?

- IT-Teams in Unternehmen jeglicher Größe
- Entscheidungsträger, die jetzt einen soliden Basisschutz einrichten möchten, um kostspielige Probleme in der Zukunft zu vermeiden.

Vorteile

- Schützt jedes Gerät – einschließlich spezialisierter und älterer Endpoints
- Bietet Transparenz und Kontrolle über alle IT-Ressourcen
- Trägt zur Verhinderung oder Minimierung von Benutzerfehlern bei
- Bietet die nötige Automatisierung der Systemverwaltung ohne hohe Kosten
- Nimmt IT-Teams in Unternehmen mühsame Tätigkeiten und Wartungsaufgaben ab. Gleichzeitig sorgen die optimierten Konfigurationen für einen besseren ROI.

Herausforderungen

Hält meine Sicherheit Schritt mit meiner IT?

Wenn Ihre Infrastruktur groß oder komplex ist, müssen Sie sich möglicherweise mit einer Vielzahl von Endpoint-Arten, diversen Computerplattformen und verschiedenen Umgebungen auseinandersetzen.

Eine breite Palette an Geräten und IT-Netzwerkfunktionen muss zusammengebracht werden, um als ein Ganzes sicher zu funktionieren.

Das kann zur regelrechnten Mammutaufgabe werden.

Was hält Sie zurück?

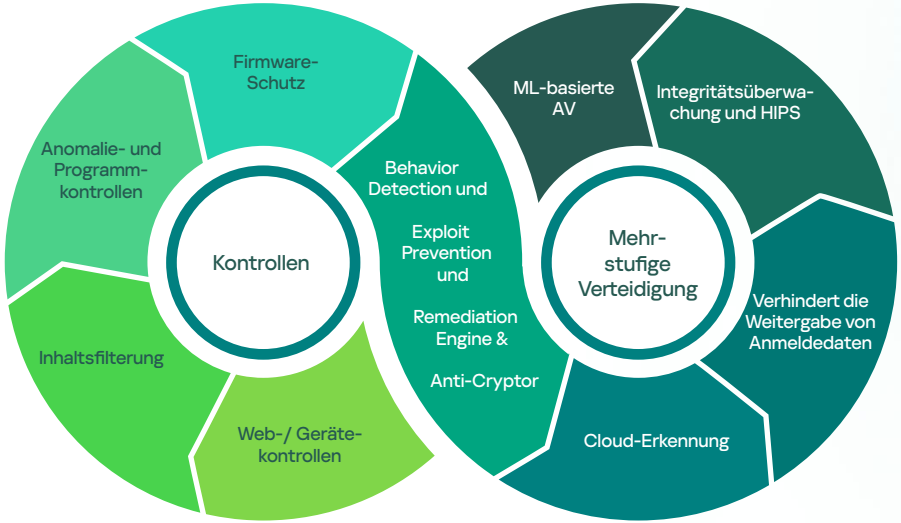
- Der Schutz von Unternehmens- und Kundendaten kann nicht gewährleistet werden
- Mangelnde Sicherheitskultur bei den Endnutzern
- Strikte Budget- und Ressourcenbeschränkungen
- Verlust von IT-Transparenz und Kontrolle
- Alte Systeme und lückenhafter Schutz, wodurch wichtige Teile der Infrastruktur gefährdet sind

So adressiert Kaspersky Security Foundations diese Herausforderungen

Unternehmens- und Kundendaten können nicht geschützt werden	Bewährter, umfangreicher Schutz, Beseitigung von Ausfällen und Datenverlusten
Mangelnde Sicherheitskultur bei den Endnutzern	Blockiert Angriffe, bevor sie Endbenutzer erreichen
Strikte Budget- und Ressourcenbeschränkungen	Optimierte Bandbreite an Technologien, die das Beste aus Ihrem Budget und Ressourcen holen
Verlust der IT-Transparenz und Kontrolle aufgrund der komplexen Infrastruktur	Transparenz, Kontrolle und Schutz Ihrer gesamten IT-Infrastruktur
Alte Systeme und lückenhafter Schutz, wodurch wichtige Teile der Infrastruktur gefährdet sind	Schutz für ältere Betriebssysteme und eigens entwickelte Sonderlösungen

Bewährter, umfangreicher Schutz, Beseitigung von Ausfällen und Datenverlusten

Mithilfe leistungsstarker Kontrollfunktionen können Sie den Zugriff auf wertvolle Daten beschränken sowie Aktivitäten von Apps, welche die Sicherheit dieser Daten bedrohen könnten, einschränken oder blockieren. Das Risiko, dass ein Vorfall zu Datenverlust/Datenlecks führt, ist durch mehrschichtige Verteidigungstechnologien erheblich reduziert.



Wichtiges Alleinstellungsmerkmal

Mit Kaspersky Security Foundations ist Ihr gesamter IT-Bestand dank eines mehrschichtigen Ansatzes, der effektive Abwehr auf jeder Ebene ohne Ausfallzeiten und Datenverlust bietet, umfassend geschützt.

Wichtige Produkte:

Kaspersky Endpoint Security for Business
Weitere Informationen

Kaspersky Hybrid Cloud Security
Weitere Informationen

Kaspersky Security for Mail Server
Weitere Informationen

Kaspersky Security for Internet Gateway
Weitere Informationen

Kaspersky Embedded Systems Security
Weitere Informationen

Blockiert Angriffe, bevor sie Endbenutzer erreichen

Mithilfe von Technologien und fein abgestuften Kontrollen können Sie den Zugriff auf Apps, Websites usw. anhand individueller Arbeitsrollen und Gruppen anpassen. So wird Ihre Sicherheit maximiert und das Risikio beseitigt.

Wichtiges Alleinstellungsmerkmal

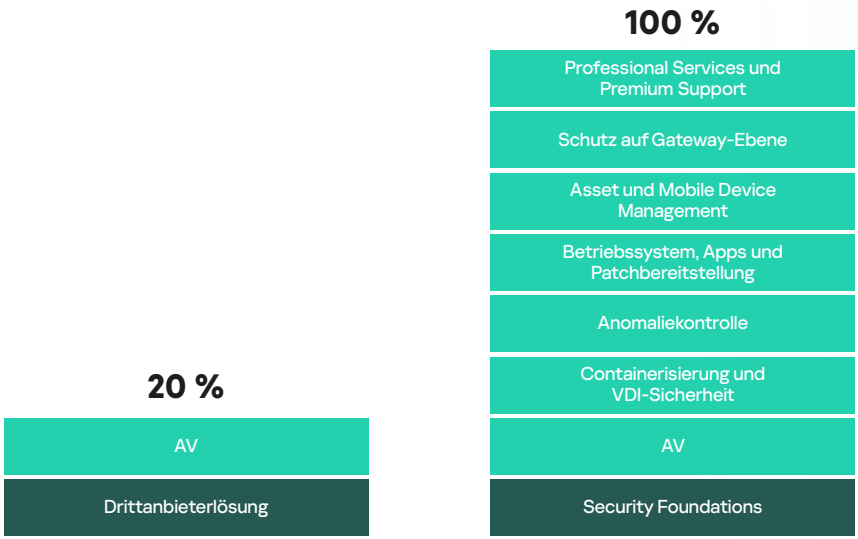
Kaspersky Security Foundations (Basisschutz) blockiert schädliche Angriffe, bevor sie zum Endbenutzer gelangen, damit Mitarbeiter ihr Unternehmen nicht mehr versehentlich einem Angriff aussetzen. Erleben Sie selbst, wie leicht Sie bindend über Richtlinien festlegen können, welche vertrauenswürdigen Anwendungen Ihre Nutzer ausführen und welche Geräte sie an das System anschließen dürfen.

Wichtige Produkte:

- **Kaspersky Endpoint Security for Business** — Weitere Informationen
- **Kaspersky Hybrid Cloud Security** — Weitere Informationen
- **Kaspersky Security for Mail Server** — Weitere Informationen
- **Kaspersky Security for Internet Gateway** — Weitere Informationen

Optimierte Bandbreite an Technologien, die das Beste aus Ihrem Budget und Ressourcen herausholen

Diese vollautomatisierten Technologien sind ohne zusätzliche Kosten enthalten:



Wichtiges Alleinstellungsmerkmal

Kaspersky Security Foundations umfasst vielfach ausgezeichnete Technologien, die Ihr Unternehmen wirksam vor Cyberbedrohungen schützen.

Sie profitieren von umfassender Sicherheit, die genau auf Ihre Anforderungen und Ihr Budget zugeschnitten ist. Bei Bedarf können die erforderlichen Agents für EDR, MDR und XDR über Ihre gesamte Infrastruktur hinweg bereitstellt werden.

Wichtige Produkte:

Kaspersky Endpoint Security for Business
Weitere Informationen

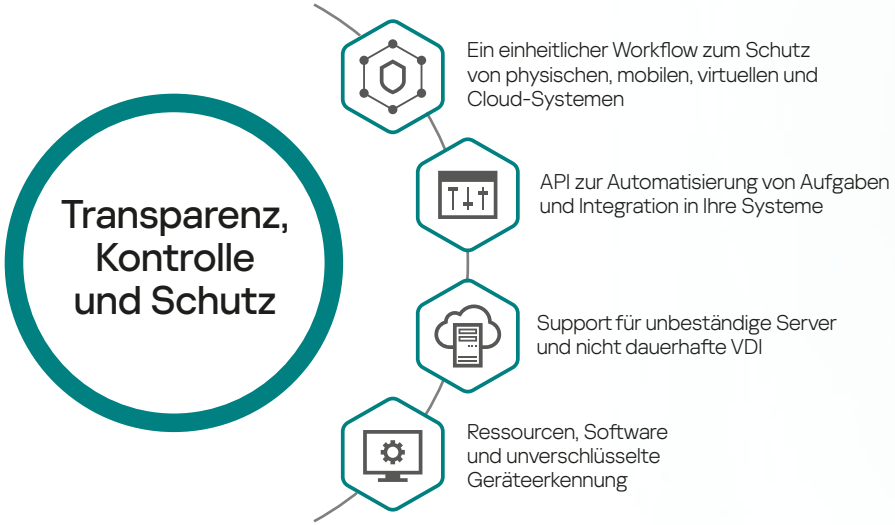
Kaspersky Hybrid Cloud Security
Weitere Informationen

Kaspersky Security for Mail Server
Weitere Informationen

Kaspersky Security for Internet Gateway
Weitere Informationen

Transparenz, Kontrolle und Schutz Ihrer gesamten IT-Infrastruktur

Kaspersky Security Foundations bietet eine einzige Konsole, die vollständige Transparenz über Ihre gesamten IT-Bestände hinweg gewährleistet. Die Stufe deckt eine breite Palette an Betriebssystemen und Hybrid-Instrastrukturen ab:



Wichtiges Alleinstellungsmerkmal

Kaspersky Security Foundations bietet maßgeschneiderte Sicherheit, Transparenz, Kontrolle und Schutz aller Aspekte Ihrer IT-Infrastruktur – von Mobilgeräten und VDI über virtuelle Server bis hin zu Public Cloud-Infrastrukturen.

Wichtige Produkte:

Kaspersky Endpoint Security for Business
Weitere Informationen

Kaspersky Hybrid Cloud Security
Weitere Informationen

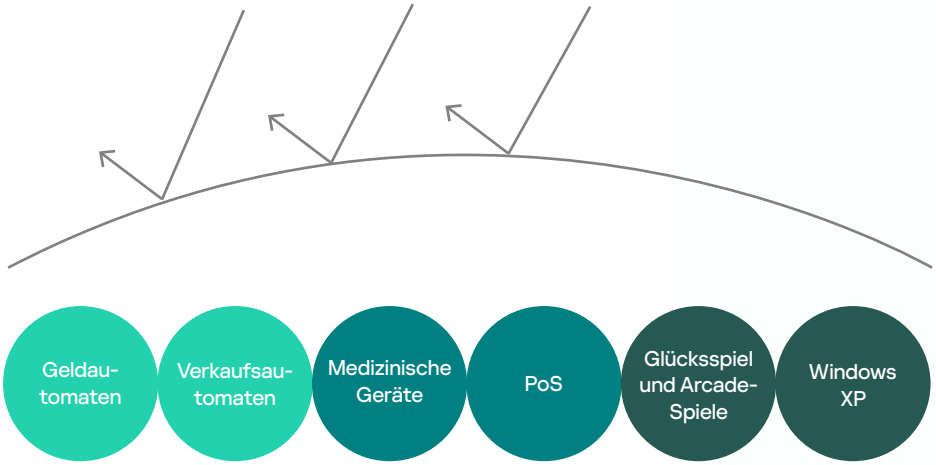
Kaspersky Security for Mail Server
Weitere Informationen

Kaspersky Security for Internet Gateway
Weitere Informationen

Kaspersky Embedded Systems Security
Weitere Informationen

Schutz für ältere Betriebssysteme und eigens entwickelte Sonderlösungen

Spezialisierte Computer mit einfacher Hardware und älterer Software benötigen ebenso spezialisierten Schutz. Das gilt auch für ältere Endpoints.



Die Vorteile

Kaspersky Security Foundations bietet abgestufte Kontrollen und vielfach ausgezeichneten Schutz für ältere Betriebssysteme und Speziallösungen mit sehr begrenzten CPU- und Speicherressourcen. Zudem lassen sich alle Sicherheitsmodule, auch die für Ihre anderen Endpoints, über eine einzige Konsole verwalten.

Wichtige Produkte:

- **Kaspersky Embedded Systems Security** — Weitere Informationen
- **Kaspersky Security for Internet Gateway** — Weitere Informationen
- **Kaspersky Security for Mail Server** — Weitere Informationen

Wichtige Alleinstellungsmerkmale

Hervorragende Leistung auf allen Geräten

Kaspersky Security Foundations bietet abgestufte Kontrollen und vielfach ausgezeichneten Schutz für ältere Betriebssysteme und Speziallösungen mit sehr begrenzten CPU- und Speicherressourcen. Zudem lassen sich alle Sicherheitsmodule, auch die für Ihre anderen Endpoints, über eine einzige Konsole verwalten.

Zentrale Verwaltung der gesamten IT-Bestände

Unsere Konsole und unser einheitlicher Sicherheits-Workflow wurden speziell dafür entwickelt, vollständige IT-Transparenz und maximale Flexibilität zu bieten, wodurch sich Richtlinien schnell und effizient durchsetzen lassen und Risiken minimiert werden.

Maximale Automatisierung für jegliche Infrastruktur

Unsere Produkte wurden für Unternehmen mit begrenzten IT-Ressourcen entwickelt. Sie verhindern automatisiert Cyberbedrohungen auf jedem Gerät, in VDIs, Gateways und Hybrid Server-Infrastrukturen.

Hoher ROI

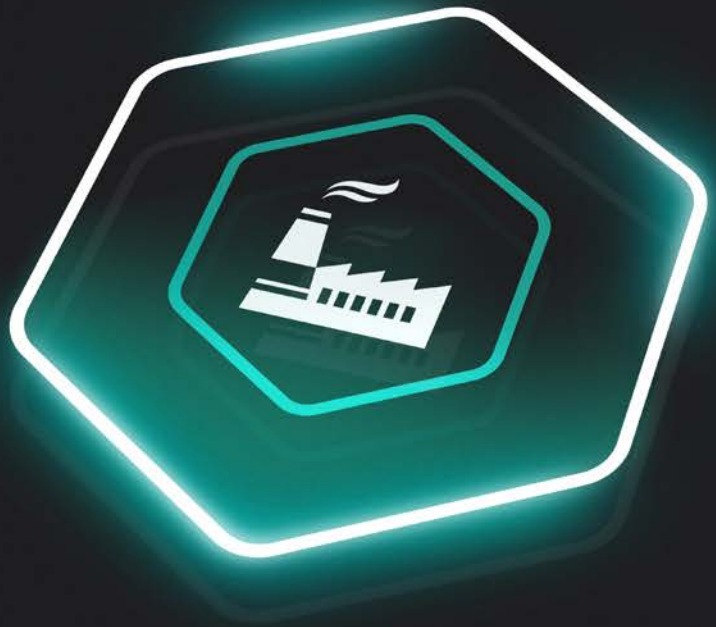
Die Benutzerfreundlichkeit wird durch hohe Bewertungen von Kunden jeglicher Größe im Rahmen von Gartner Peer Insights sowie in Branchenanalysen bestätigt. Kaspersky Security Foundations generiert einen hervorragenden ROI – nachgewiesen in TEI-Kundenbefragungen von Forrester.

Übersicht

Kaspersky Security Foundations

- **Kaspersky Endpoint Security for Business**
- **Kaspersky Hybrid Cloud Security**
- **Kaspersky Embedded Systems Security**
- **Kaspersky Security for Storage**
- **Kaspersky Security for Mail Server**
- **Kaspersky Security for Internet Gateway**
- **Kaspersky Professional Services**
- **Kaspersky Premium Support**

- Schutz für Unternehmensbenutzer und Mobilgeräte
- Serverschutz in hybriden Umgebungen
- Schutz für virtuelle Desktops (VDI)
- Schutz für spezielle Endpoints und ältere PCs
- Schutz vor dem häufigsten Angriffsvektor: E-Mail
- Schutz vor Bedrohungen aus dem Internet
- Unterstützung bei der Bereitstellung, Konfiguration und Wartung



Kaspersky Industrial Cybersecurity

Zurück zum Inhaltsverzeichnis

So schützen wir Industrieunternehmen

Transparenz

Interne Experten werden richtig ausgestattet, damit sie komplexe Cybersicherheitsvorfälle abwehren und die Arbeitslast optimieren können.

Risikomanagement

Wir unterstützen Sie dabei, Richtlinien durchzusetzen, Kontrollen zuzuweisen und Bedrohungen zu stoppen, ohne Prozesse zu beeinträchtigen.

Zentralisierung

Wir helfen dabei, schnell auf Vorfälle zu reagieren, erfolgreiche Implementierungen einfach zu replizieren und die komplexe verteilte Infrastruktur zu verwalten.

Lösung für industrielle Großkonzerne

Plattform mit nativ integrierten Technologien, Schulungen und Expertenservices

Kaspersky Single Management Platform

Plattform

Kaspersky Industrial Cybersecurity

for Nodes

Endpoint-Schutz, Erkennung und Reaktion

for Networks

Analyse des Netzwerkverkehrs, Erkennung und Reaktion

Services

Schulung und Sensibilisierung

Kaspersky Security Awareness

Kaspersky Cybersecurity Training

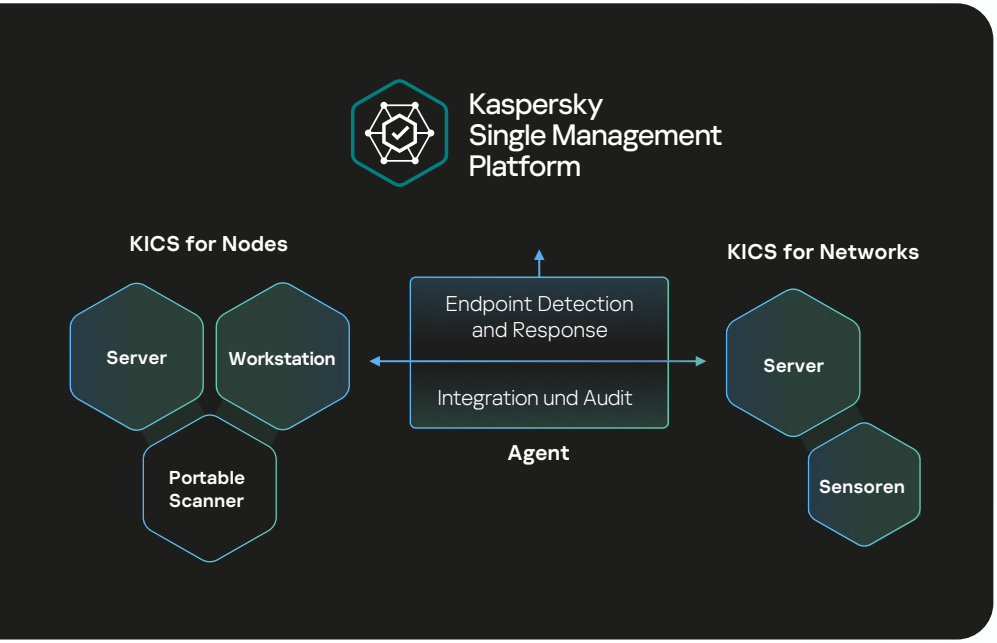
Expert Services und Intelligence

Kaspersky Threat Intelligence

Kaspersky Security Assessment

Kaspersky Incident Response

Plattform-Architektur und wesentliche Funktionen



Kaspersky Industrial Cybersecurity

Analyse des Netzwerkverkehrs sowie der Endpoints

Analyse des Netzwerkverkehrs sowie Endpoint-Sensoren zur Erkennung von Eindringlingen auf der niedrigsten Stufe (ICS-Protokolle, DPI und IDS-Signaturen)

Risiko- und Assetverwaltung

Analyse des Netzwerkverkehrs sowie Endpoint-Sensoren zur Erkennung von Eindringlingen auf der niedrigsten Stufe (ICS-Protokolle, DPI und IDS-Signaturen)

Endpoint-Erkennung, Reaktion und Audit

Malware-Schutz, Software- und Geräte-Whitelisting und vieles andere mehr. Zudem ermöglicht ICS EDR die Ursachenanalyse von Vorfällen in OT-Umgebungen

Kaspersky Industrial CyberSecurity: Ganzheitliche Sicherheit für industrielle Systeme

Schulungen und Sensibilisierung

- Professionelle Schulung im Bereich Vorfalls-reaktion und Untersuchung in OT
- Basisschulungen für OT-Spezialisten

Assessments und andere Sicherheitsservices

- Penetrationstests
- Cybersecurity Assessments
- APT-Berichte
- Managed Detection and Responsen Service
- ICS-CERT-Beratung

Threat Intelligence

- Untersuchung auf Schwachstellen und Malware-Datenbank

Incident Response

- IR und Forensics Service (remote und vor Ort)
- Handbuch-Vorbereitung und Simulation

Wichtige Alleinstellungsmerkmale

Zertifiziert

Industrielle Anbieter haben bestätigt, dass mehr als 150 ihrer Automatisierungssysteme mit der Kaspersky Industrial Cybersecurity-Plattform kompatibel sind.

Kompatibel

Nachweislich kompatibel mit unterschiedlichen nationalen Anforderungen an die Sicherheit kritischer Infrastrukturen sowie Best Practices und internationale Normen.

Effizient

Wir schützen Industrieunternehmen zuverlässig.
Ob Einzelstandort oder global agierendes Unternehmen: Unsere Lösung steht für Leistung, Effizienz und hervorragende Skalierbarkeit.

Zukunftssicher

Offene Plattform, ineinander greifendes Produktportfolio, hervorragende Integrationsmöglichkeiten sowie mehr als 25 Jahre Erfahrung machen Kaspersky zu einem zuverlässigen Partner, auf den bereits jetzt mehr als 600 Industriekonzerne weltweit vertrauen.

Kaspersky Security für kleine und mittelständische Unternehmen

Zurück zum Inhaltsverzeichnis

Herausforderungen bei der IT-Sicherheit, vor denen kleine und mittelständische Unternehmen stehen

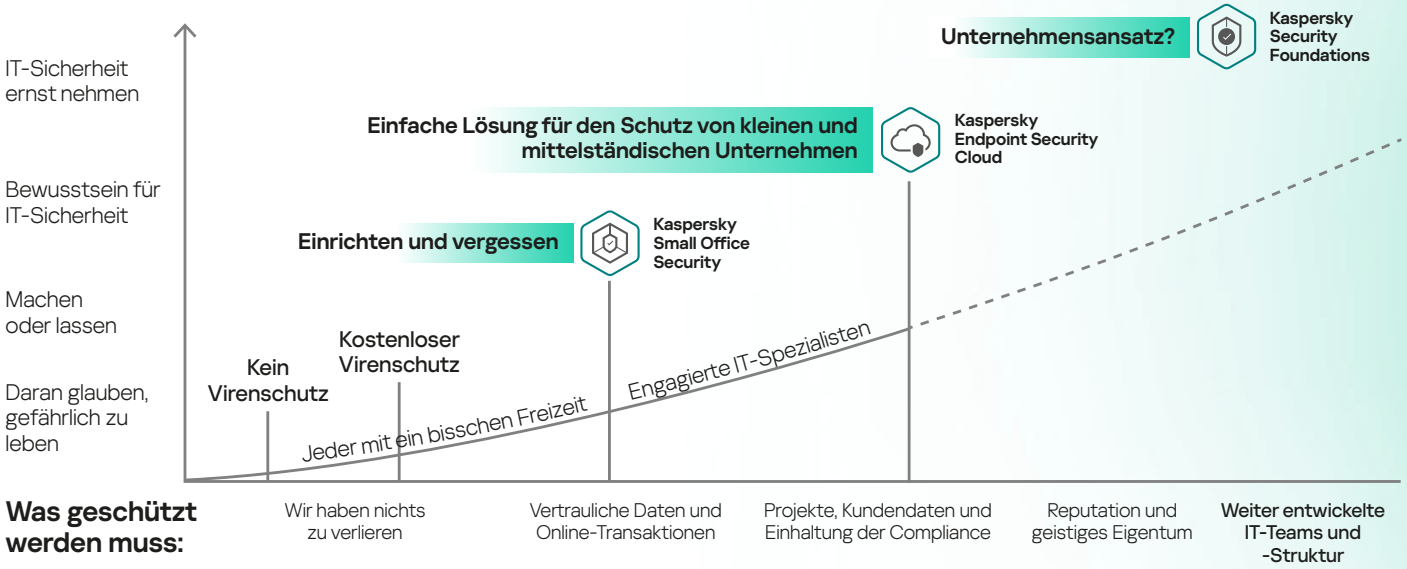
Cyberbedrohungen

Nicht jede Lösung ist in jedem Unternehmen gleichermaßen einsetzbar. Kleinere Unternehmen stehen vielen der gleichen Bedrohungen wie große Unternehmen gegenüber, verfügen aber nicht über die gleichen Ressourcen.

Ressourcenüberlastung

Die richtigen Sicherheitslösungen machen der IT-Abteilung das Leben leichter, nicht schwerer. Wenn Sie ein kleines oder mittelständisches Unternehmen führen, sind Ihre Mitarbeiter vermutlich oft überlastet. Deshalb müssen Sie effizient arbeiten und sich für eine Sicherheitslösung entscheiden, die sofortigen Schutz bietet und nur minimale Anforderungen an Budget, Zeit und Aufwand stellt.

Der schlanke IT-Sicherheitsansatz von Kaspersky



Verbesserung des Bewusstseins für Cybersicherheit

Kaspersky Automated Security Awareness Platform

Kaspersky Small Office Security

Ideal, wenn es keinen IT-Spezialisten in Ihrem Unternehmen gibt

Kaspersky Small Office Security verbindet die Einfachheit von Sicherheitsprodukten für Privatanwender mit speziellen Funktionen – so ist Ihr Unternehmen stets rundum geschützt. Die Lösung ist einfach zu installieren, noch einfacher zu bedienen und bietet vielfach getesteten und ausgezeichneten Schutz für Computer, File-Server, Laptops und Mobilgeräte. KSOS schützt zuverlässig vor Online-Angriffen, Finanzbetrug, Ransomware und Datenverlust.

Wichtige Alleinstellungsmerkmale

- Schnell –Installation in weniger als 10 Minuten
- Benutzerfreundlich – Sofortiger Schutz nach der Einrichtung
- Wirksam – Schutz vertraulicher Daten und Ihres Geschäftsbetriebs vor Datenschutzverletzungen, Strafen und entgangenen Gewinnen

Weitere Informationen

Kaspersky Endpoint Security Cloud

Mit Kaspersky Endpoint Security Cloud erhalten Sie eine einzige Lösung für alle Anforderungen an die IT-Sicherheit in Ihrer Organisation. Sie können ungestört weiterarbeiten, während Kaspersky Ransomware, dateilose Malware, Zero-Day-Angriffe und andere Bedrohungen abwehrt. Dank unseres Cloud-basierten Ansatzes können Nutzer auf jedem beliebigen Gerät immer und überall sicher online arbeiten.

Ideal für Unternehmen, die einen IT-Administrator haben, der für alle IT-Aufgaben verantwortlich ist, und die Ressourcen einsparen möchten.

- Müheloser Schutz für Unternehmen ohne Abstriche bei IT-Ressourcen, Zeit oder Budget
- Automatisierung von Routine-Abläufen reduziert IT-Kosten und setzt Ressourcen für andere Aufgaben frei
- Unterstützt sichere Cloud-Migration mit Erkennung von Schatten-IT und Schutz für Microsoft Office 365

Umfassende Agilität

- Sofort einsatzbereit
- Keine Investition in Hardware
- Freigesetzte Ressourcen
- Verbrauchsbasierte Abrechnung
- Für Outsourcing geeignet

Kaspersky Automated Security Awareness Platform

Kaspersky ASAP ist ein benutzerfreundliches Online-Tool, das Mitarbeitern fundiertes Wissen im Bereich Cybersicherheit vermittelt. Die Lösung basiert auf mehr als 25 Jahren Erfahrung im Bereich Cybersecurity. Dank benutzerfreundlicher Bedienung und Automatisierungsfunktionen bietet sie in jeder Phase Unterstützung: von der Zieleinrichtung bis hin zur Ergebnisauswertung.

Ideal, wenn Sie sich sicherheitsbewusste Mitarbeiter und effizienteren Schutz vor Online-Bedrohungen wünschen.

- Stärkung des Sicherheitsbewusstseins der Mitarbeiter und Vermittlung von sofort umsetzbarem Wissen
- Effektive Schulungen, für deren Durchführung und Verwaltung keine speziellen Ressourcen oder Vorkenntnisse erforderlich sind

Wichtige Alleinstellungsmerkmale

- Reduziert die Zahl der von Menschen verursachten Vorfälle, sodass Geschäftskontinuität gewährleistet und die Auswirkungen eines Vorfalls minimiert werden.
- Verbesserte Cybersicherheitskultur für Ihr Unternehmen
- Geringer Zeitaufwand für die Einführung und Umsetzung von Schulungsprogrammen

Weitere Informationen

Aspekte, die es für eine langfristige Cybersicherheitsstrategie zu berücksichtigen gilt

Silo-Ansatz bei der Cybersicherheit bedeutet geschäftliche Risiken

Aufgrund der steigenden Kosten bei Netzwerk- und Datenschutzverletzungen sind Unternehmen einem starkem finanziellem Druck ausgesetzt. Deshalb ist das Thema Cybersicherheit heute so wichtig wie noch nie. Um in dieser Umgebung erfolgreich zu sein, muss die Cybersicherheit fester Bestandteil jeder Unternehmensstrategie sein und zudem eine wichtige Rolle bei Risikomanagement und langfristiger Planung spielen.

Cybersicherheit ist nicht nur das Ziel, sondern auch der Weg

Der Sicherheitsplan eines Unternehmens muss regelmäßig überprüft und angepasst werden, da ständig neues Wissen und neue Tools verfügbar sind. Jeder Sicherheitsvorfall muss eingehend analysiert werden. Daraus resultierend müssen neue Prozesse und Maßnahmen zur Vorfallsbehandlung aufgestellt werden, damit ähnliche Angriffe in Zukunft verhindert werden können. Die vorhandenen Abwehrmaßnahmen müssen also kontinuierlich verbessert werden.

Aspekte, die es für eine langfristige Cybersicherheitsstrategie zu berücksichtigen gilt

Sicherheitsbewusstsein, Kommunikation und Kooperation sind in einer Welt, in der sich Cyberbedrohungen rasant weiterentwickeln, der Schlüssel zum Erfolg.

Mehr als 80 % aller Cybersicherheitsvorfälle entstehen durch menschliche Fehler. Mitarbeiterschulungen auf allen Ebenen sind unerlässlich, um das Sicherheitsbewusstsein im ganzen Unternehmen zu erhöhen und alle Mitarbeiter zu motivieren, auch dann auf Cyberbedrohungen zu achten, wenn sie glauben, dass dies nicht zu ihren Aufgaben gehört.

Mitarbeiter, die sich der Wichtigkeit einer vorausschauenden Erkennung und Reaktion bewusst sind, sind die erste Verteidigungslinie im Kampf gegen Cyberbedrohungen.

Traditionelle Präventionssysteme sollten in Verbindung mit Erkennungstechnologien, Bedrohungsanalysen, Reaktionsfunktionen und vorausschauenden Sicherheitstechniken implementiert werden. So können Sie ein Cybersicherheitssystem aufbauen, das sich kontinuierlich an die neuen Herausforderungen anpasst und optimal auf diese reagieren kann.

Warum Kaspersky?

Häufig getestet. Vielfach ausgezeichnet

Kaspersky hat in unabhängigen Tests mehr erste Plätze erreicht als andere Sicherheitsanbieter. Und das Jahr für Jahr. www.kaspersky.de/top3

MITRE ATT&CK bestätigt die Qualität der Erkennung

MITRE | ATT&CK®

IDC ANALYZE THE FUTURE

Kaspersky wurde im Rahmen von IDC MarketScape als „Major Player“ ausgezeichnet: Worldwide Modern Endpoint Security for Enterprise and Small and Mid-size Businesses 2021, Vendor Assessments.

THE RADICATI GROUP, INC.

Die Radicati Group hat Kaspersky als „Top Player“ im Rahmen des „Endpoint Security – Market Quadrant 2021“ ausgezeichnet. Kaspersky wurde im Advanced Persistent Threat Protection – Market Quadrant 2022 von Radicati zum dritten Mal in Folge als „Top Player“ ausgezeichnet.

Proven.
Transparent.
Independent.

Transparenz auf höchstem Niveau

Mit neun aktiven Transparenzzentren und dank statistischer Verarbeitung in der Schweiz können wir optimale Datenhoheit garantieren.

kaspersky

www.kaspersky.de