kaspersky

# Kaspersky B2B-Portfolio

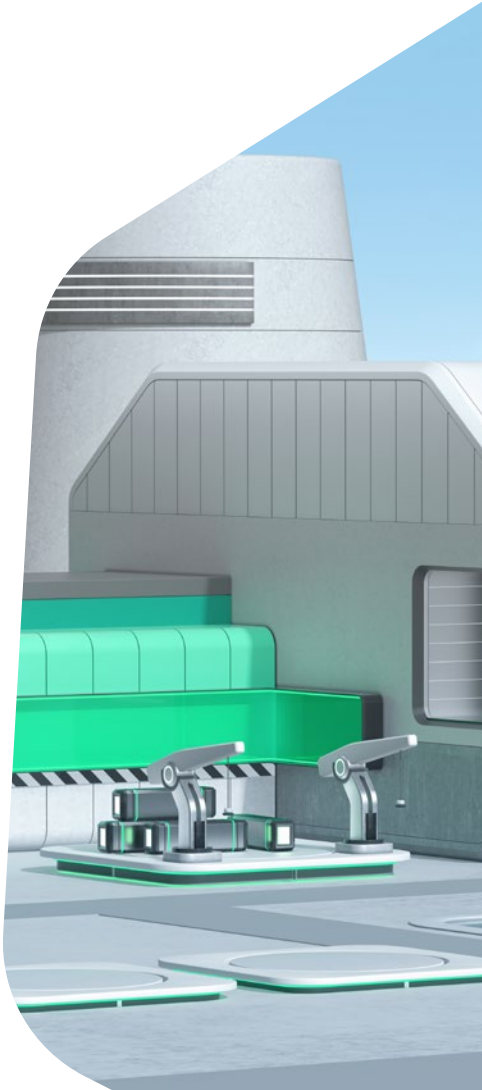
# Inhalt

# Infos zum Kaspersky 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.

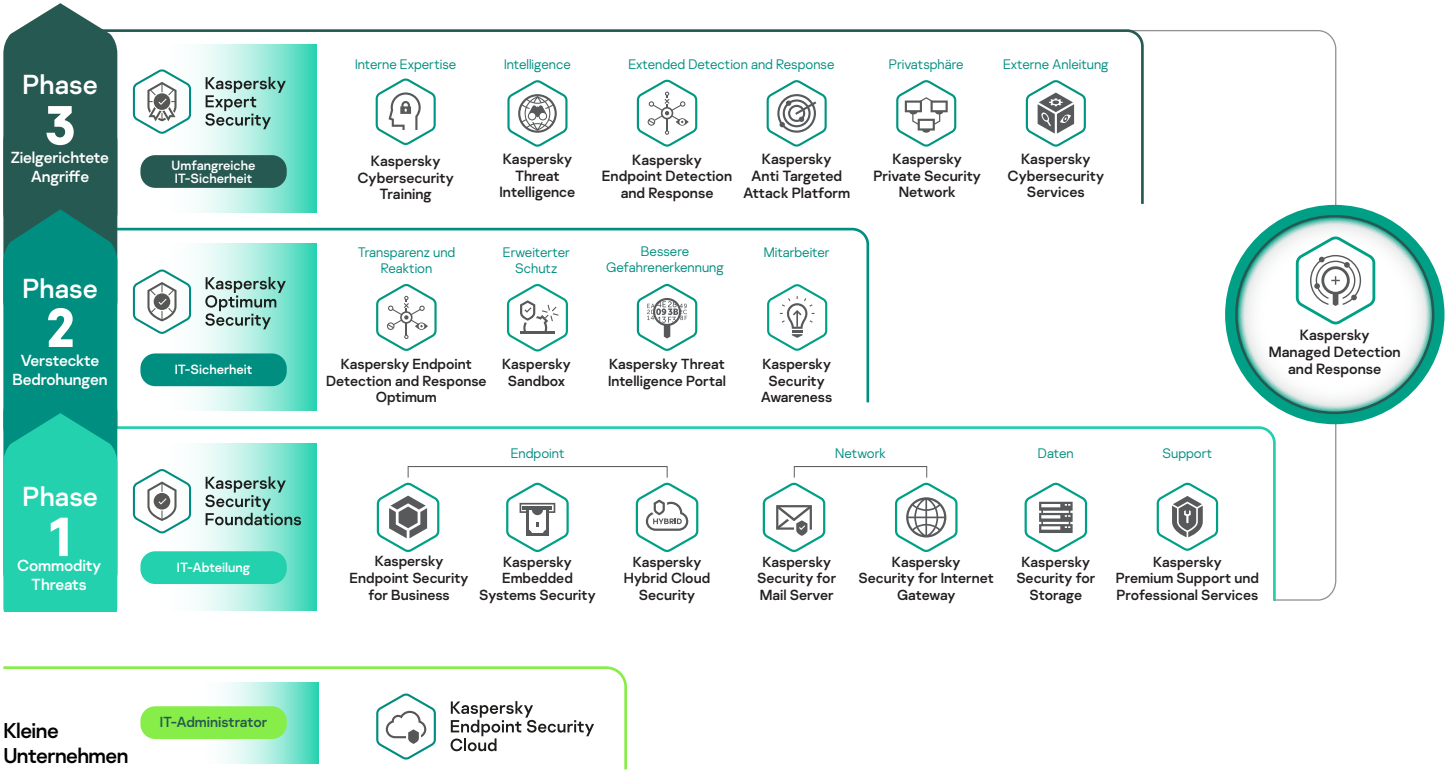
Das B2B-Portfolio von Kaspersky ist auf die Sicherheitsanforderungen von Unternehmen abgestimmt und bietet Organisationen unterschiedlicher Größe und mit unterschiedlichem technischen Reifegrad bei der IT-Sicherheit einen einzigartigen stufenweisen Cybersicherheitsansatz. Dieser Ansatz vereint verschiedene Schutzebenen gegen alle Arten von Cyberbedrohungen und unterstützt Unternehmen bei der automatischen Verhinderung von 90 % der Bedrohungen. Unternehmen können darüber hinaus jederzeit neue und hochentwickelte Funktionen zur Bekämpfung weitaus raffinierterer Bedrohungen hinzufügen wenn sie diese benötigen.

Kaspersky ist Ihr Partner auf dem Gebiet der Cybersicherheit, der das große Ganze im Blick hat, damit Sie unbesorgt sein und sich auf Innovation konzentrieren können.



## Expertise zur Abwehr unterschiedlicher Bedrohungsarten

# Kasperskys Cybersicherheitskonzept – Schritt für Schritt



Die Notwendigkeit langfristiger Sicherheitsplanung

# Herkömmliche kurzfristige Sicherheitsplanung

**Entscheidungsfindung:**

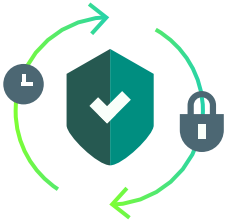
- Markttrends
- Silo-Sicherheitslösung
- Feuerwehrstrategie
- Compliance-orientiert

**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 das Versagen herkömmlicher Ansätze:

- Immer komplexere Bedrohungen und Bedrohungslage
- 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

# Kaspersky Security for Enterprises

Zum Inhaltsverzeichnis

Phase
3
Zielgerichtete Angriffe

# Kaspersky Expert Security

Zum Inhaltsverzeichnis

# Kaspersky Expert Security

## Worum geht es?

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.

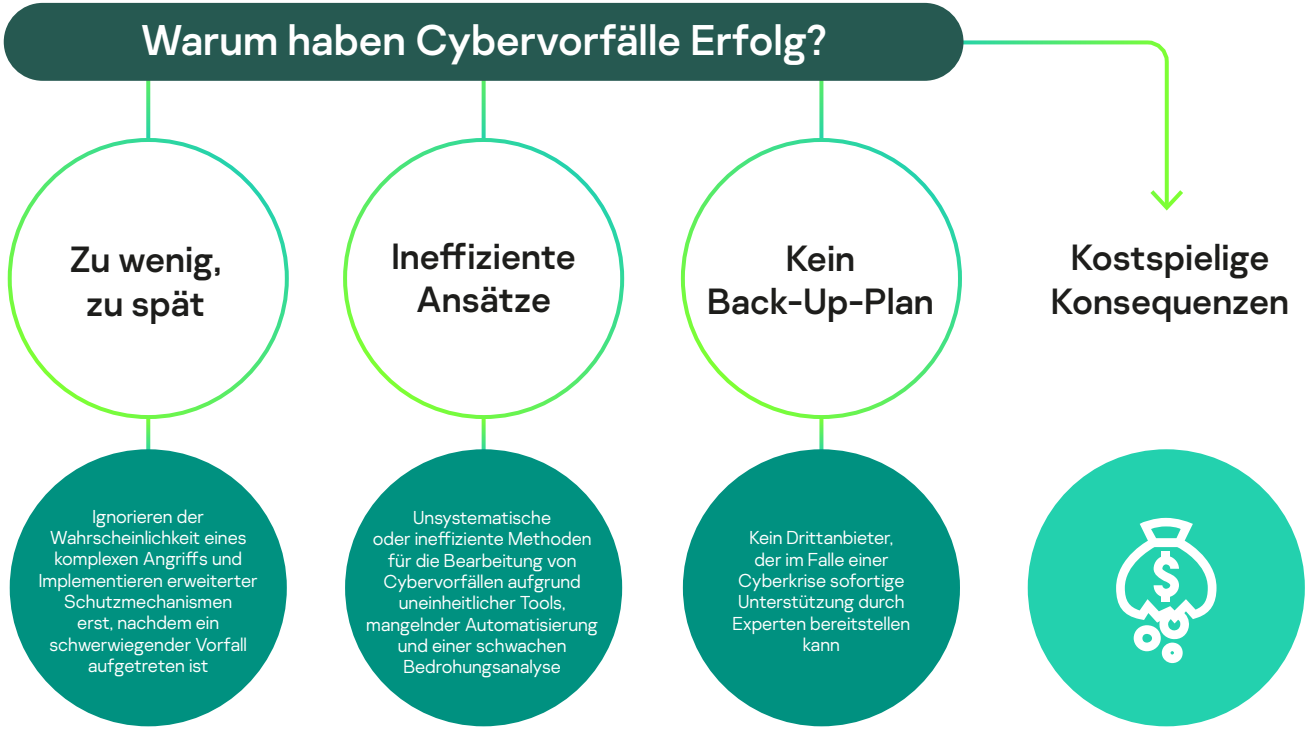
## Ideal für:

- 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

## Welche Aktion(en) führt es aus?

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

## Herausforderungen



## 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

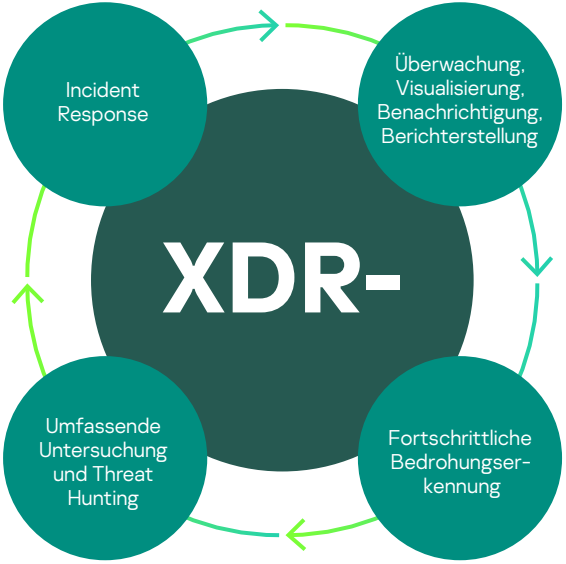
**Wissen wird** mit Bedrohungsanalysen angereichert und Experten im Umgang mit komplexen Vorfällen **geschult.**

### 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 komplexer Angriffe.

Eine zentrale Plattform reduziert Warnstufen durch Bereitstellung von Threat Intelligence-basiertem Kontext und verhindert "Alarmermüdung" ("alert fatigue").

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

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

**Wichtige Produkte**

Kaspersky Anti Targeted Attack

Kaspersky Endpoint Detection and Response

Informiert

## 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

Informiert

## 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.

Führt zu Zeit- und Kostenersparnis weil in Zeiten der Ressourcenknappheit keine neuen Mitarbeiter eingestellt werden müssen.

Führt zu erhöhter Bindung und Motivation bei internen Mitarbeitern weil sie sich beruflich weiterbilden können.

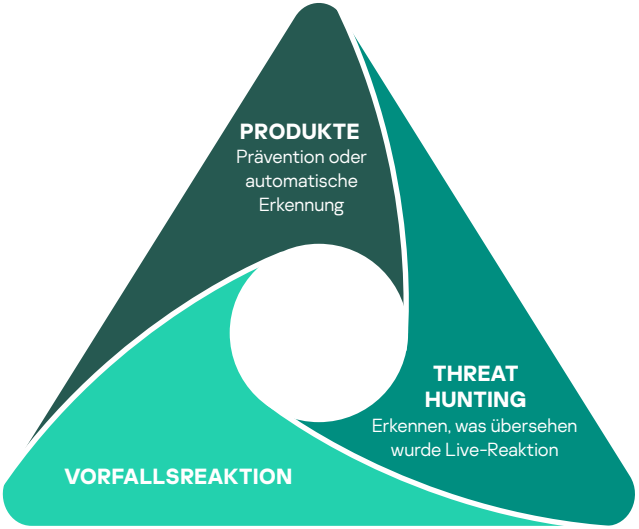
Umfassende Schulungen lassen sich an Ihre Anforderungen anpassen und können vor Ort, remote oder auf Abruf bereitgestellt werden.

**Wichtige Produkte**

Kaspersky Cybersecurity Training

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.

Umfassende Erkennungsfunktionen, gestützt durch die seit mehr als 20 Jahren gleichbleibend qualitativ hervorragende Forschung zu zielgerichteten Angriffen, filtern irreführende False Positives und kostspielige False Negatives heraus.

Sofortiger Support von äußerst erfahrenen Ermittlern auf dem Gebiet von Cyberbedrohungen ermöglicht Ihnen die schnelle und effektive Behebung der komplexesten Vorfälle.

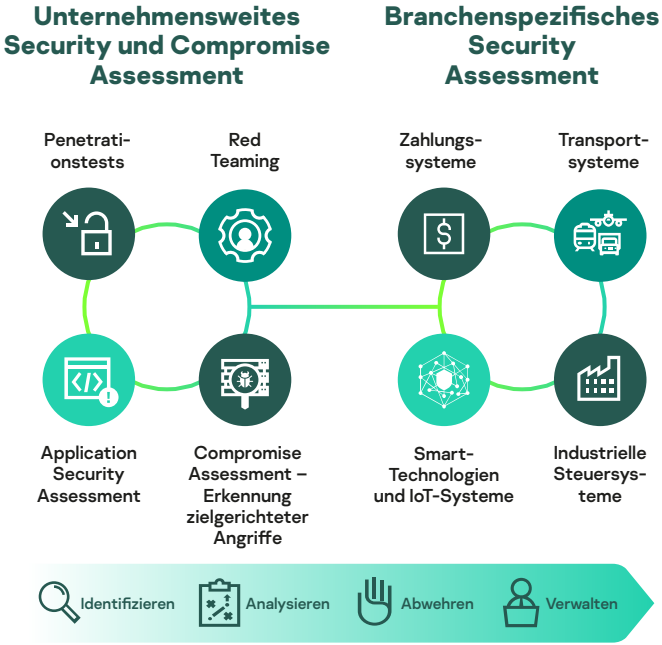
**Wichtige Services**

Kaspersky Managed Detection and Response

Kaspersky Incident Response

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
- Kaspersky Targeted Attack Discovery

## Genau hinschauen lohnt sich.

**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 Schulungen zur Cybersicherheit

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

### Kaspersky Extended Detection and Response


### Kaspersky Security und Compromise Assessment

- Targeted Attack Discovery
- Penetrationstests
- Red Teaming
- Application Security Assessment
- Branchenspezifisches Security Assessment (ICS, Zahlungssysteme, Transport, IoT)

### 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 unvergleichlichen Abwehrmechanismen durch eine einzige Konsole

### Hochwertige Threat Intelligence informiert über jeden Schritt im Zyklus des Vorfallsmanagements.

Ausgezeichnet als Leader in The Forrester Wave™: External Threat Intelligence Services 1. Quartal, 2021, "Kaspersky enables significantly increased security operational efficiencies, minimizing attack 'dwell time'." (Kaspersky ermöglicht eine erheblich höhere betriebliche Effizienz bei der Sicherheit, wodurch die "Verweildauer" eines Angriffs verkürzt wird.)

### 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.

Phase
2
Versteckte Bedrohungen

# Kaspersky Optimum Security

Zum Inhaltsverzeichnis

# Kaspersky Optimum Security

## Worum geht es?

- Kaspersky Optimum Security schützt Unternehmen vor neuen, unbekannten und versteckten Bedrohungen.
- Effektive Bedrohungserkennung und Response-Lösung und damit Ressourcen schonen
- Sicherheitsüberwachung rund um die Uhr, automatisiertes Threat Hunting und geführte und verwaltete Responses, unterstützt von Kaspersky-Experten

## Ideal für:

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

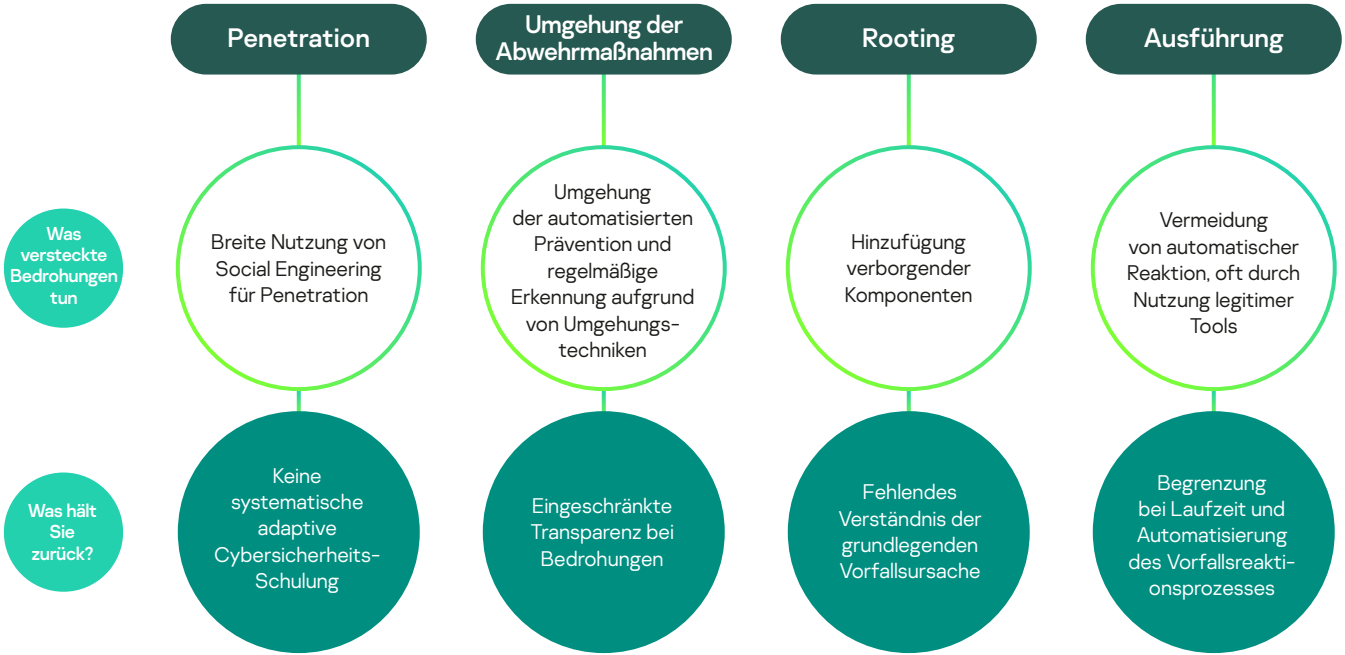
## Welche Aktion(en) führt es aus?

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

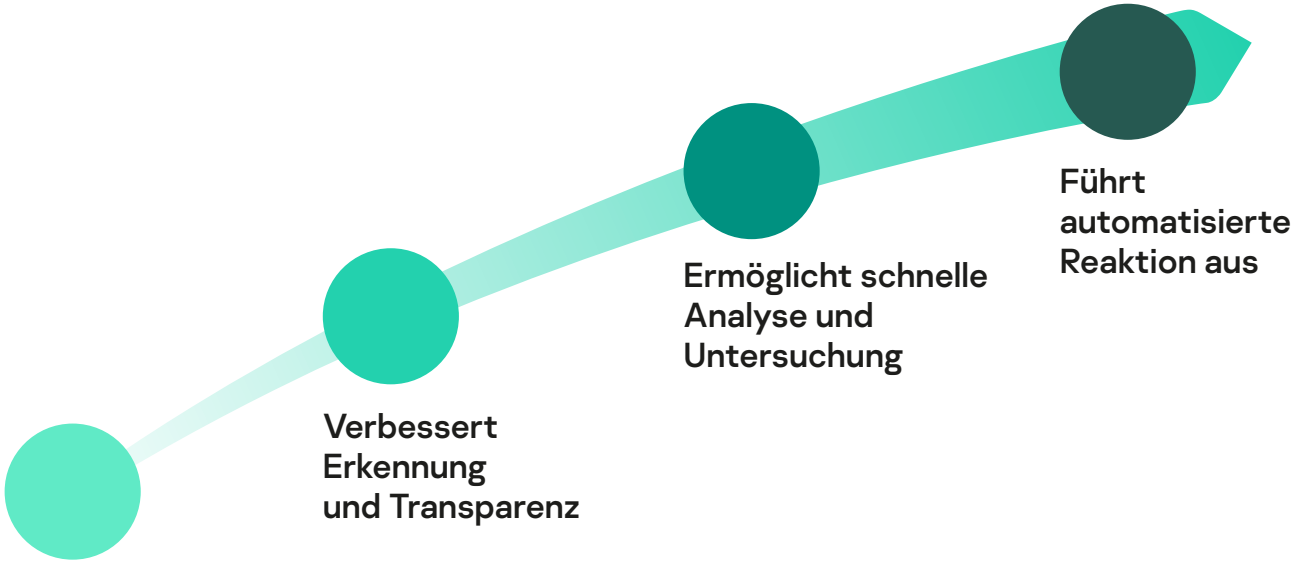
## Herausforderungen

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

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



## Umgang von Kaspersky Optimum Security mit diesen 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.

### Sprechen Sie spezialisierte Teams an.

Festigen Sie die Rolle von IT-Generalisten als erste Verteidigungslinie. Schulen Sie Ihr PR-Team, minimieren Sie möglichen Imageschaden und verringern Sie direkte finanzielle Verluste.

### Rüsten Sie alle Mitarbeiter aus.

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

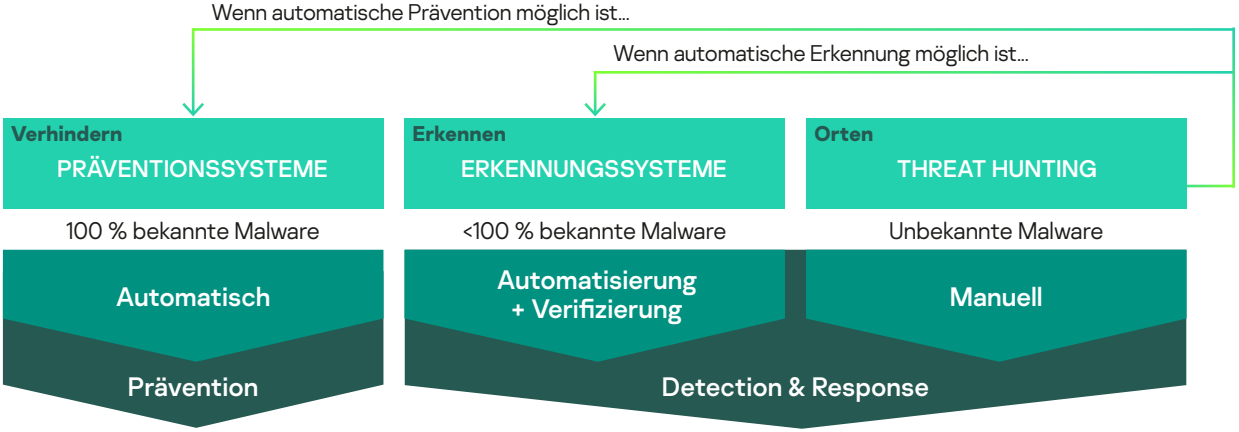
### Stellen Sie sicher, dass Kenntnisse auch angewendet werden.

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

**Wichtige Produkte:** Kaspersky Security Awareness

# 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:**

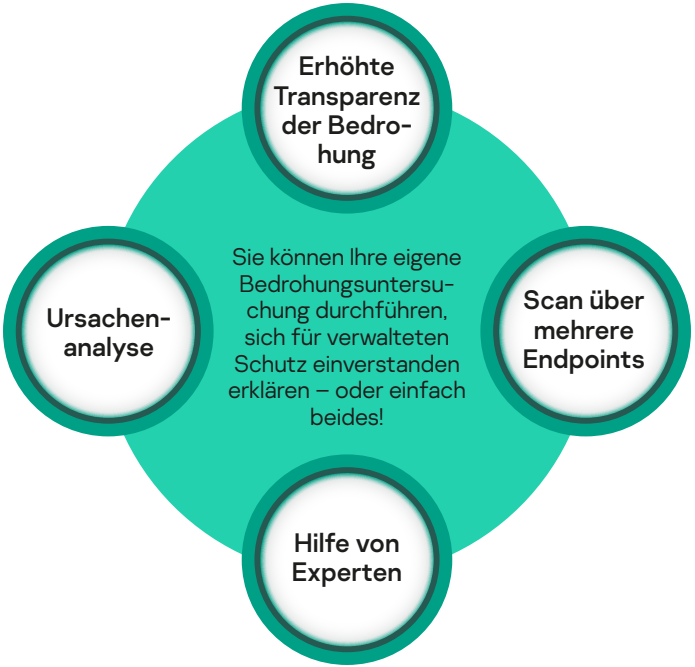
Kaspersky Endpoint Detection and Response (EDR)

Kaspersky Managed Detection and Response (MDR)

Kaspersky Sandbox

## 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

Kaspersky-Experten verwenden führende TI[2]- und KI-fähige Tools, um Ihre Bedrohungsdaten zu analysieren.

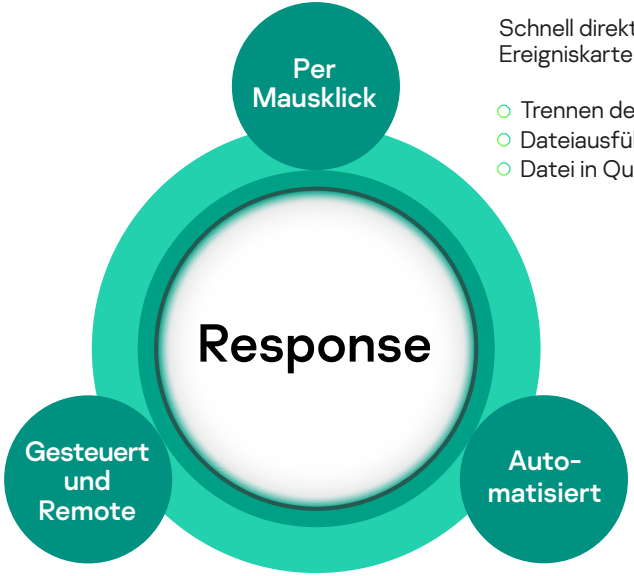
[1]Gefährdungsindikator
[2]Threat Intelligence

**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:

- Trennen des Hosts
- Dateiausführung verhindern
- Datei in Quarantäne setzen

Sie erhalten detailliete Berichte und Empfehlungen zu Reaktionen – oder Sie erlauben Kaspersky-Experten, spezifische Remote-Reaktionen durchzuführen.

Sie können die Infrastruktur für IoCs[1] von erkannten Bedrohungen scannen, wobei sofort eine automatisierte Reaktion angewendet wird – alles über ein einfaches Kontrollkästchen.

[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 erkundet.

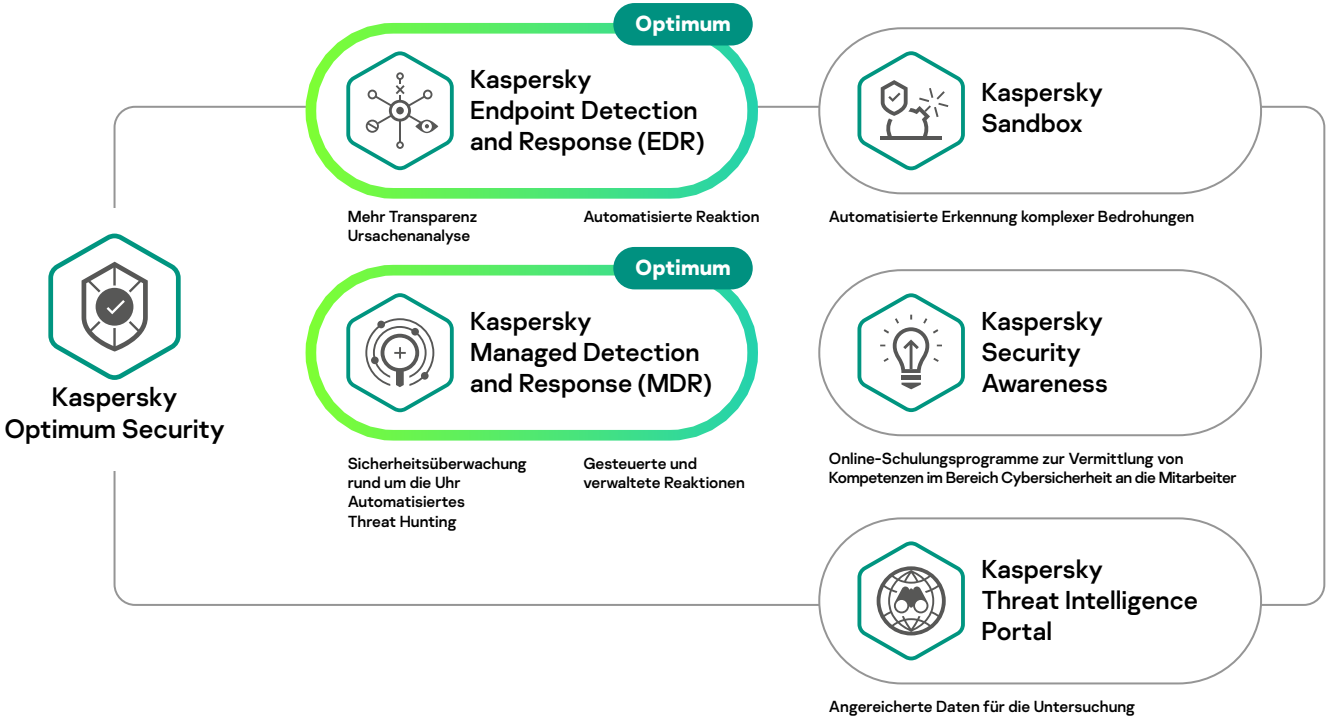
### Rooting

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]Angriffsindikatoren
[3]Gefährdungsindikator

## Genau hinschauen lohnt sich.



## Wichtige Alleinstellungsmerkmale

### Unterstützt Hybrid-Umgebungen

- Workstations
- Server
- Virtuelle Maschinen
- Public clouds

### Einfachheit und Effizienz

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-
Bedrohungen

# Kaspersky Security Foundations

Zum Inhaltsverzeichnis

# Kaspersky Security Foundations

## Ideal für:

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

## Worum geht es?

Die Cloud-basierte Phase der Bedrohungsverhinderung ermöglicht jedem Unternehmen, Commodity Cyberbedrohungen auf jedem Gerät, in VDI- und Hybrid Server-Infrastrukturen automatisch zu stoppen. Liefert eine durchschnittliche Investitionsrendite von 441 % wie in der TEI-Kundenbefragung von Forrester nachgewiesen.

## Welche Aktion(en) führt es aus?

- 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

## 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 zu funktionieren und zwar sicher.

All dies unter einen Hut zu bringen ist ein ständiger Kampf.

### Wer hält Sie zurück?

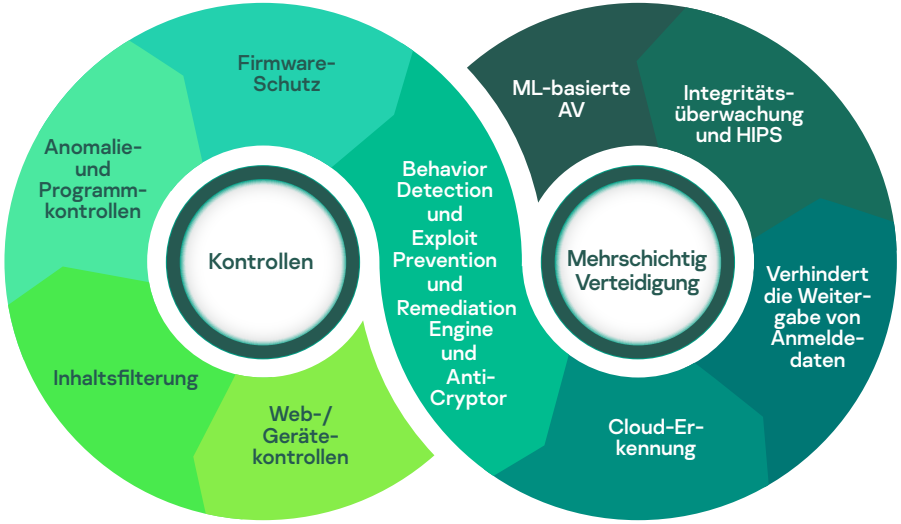
- Unfähigkeit, den Schutz von Unternehmens- und Kundendaten vor Exposition und Verlust zu gewährleisten
- Mangelnde Sicherheitskultur bei den Endnutzern
- Strikte Budget- und Ressourcenbeschränkungen
- Verlust von IT-Transparenz und Kontrolle
- Alte Systeme und lückenhafter Schutz, wodurch wichtige Teile der Infrastruktur gefährdet sind

## Die Antwort von Kaspersky Security Foundations auf diese Herausforderungen

| | |
|---|---|
| Unfähigkeit, Unternehmens- und Kundendaten zu schützen | **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 Abwehr auf jeder Ebene ohne Ausfallzeiten und Datenverluste bietet, umfassend geschützt.

**Wichtige Produkte:**

- Kaspersky Endpoint Security for Business
- Kaspersky Hybrid Cloud Security
- Kaspersky Security for Mail Server
- Kaspersky Security for Internet Gateway
- Kaspersky Embedded System Security

## 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

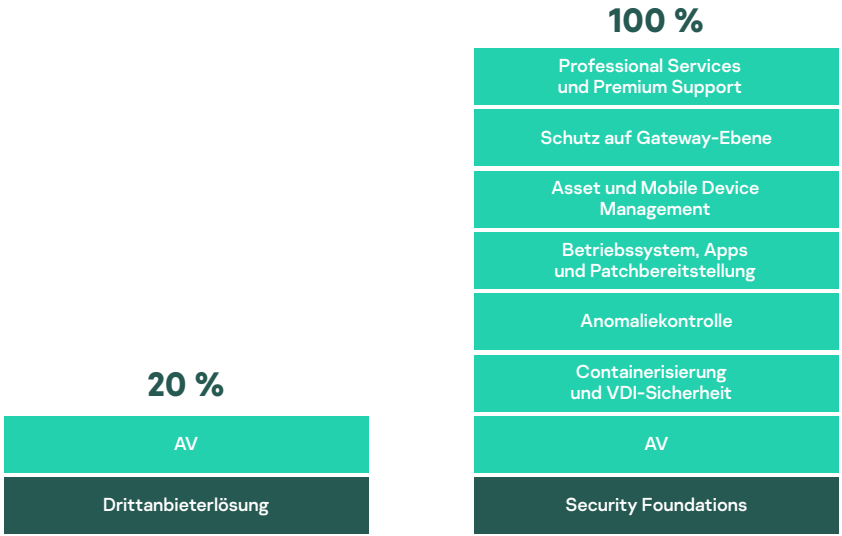
Kaspersky Security Foundations (Basisschutz) blockiert schädliche Angriffe, bevor sie zum Endbenutzer gelangen, damit Mitarbeiter ihr Unternehmen nicht mehr versehentlich einem Angriff aussetzen. Erleben Sie selbst, wie leicht Sie bindend über Richtlinien festlegen können, welche vertrauenswürdigen Anwendungen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

**Wichtige Produkte:**

- Kaspersky Endpoint Security for Business
- Kaspersky Hybrid Cloud Security
- Kaspersky Security for Mail Server
- Kaspersky Security for Internet Gateway

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

Wir zwingen Ihnen keine unnötigen Technologien auf, aber alle vollautomatisierten Technologien, die Sie benötigen, sind ohne zusätzliche Kosten enthalten:




### Wichtiges Alleinstellungsmerkmal

Kaspersky Security Foundations trifft die Vorauswahl der vielfach ausgezeichneten Technologien, die sich für Unternehmen wie Ihres eignen. Damit Sie keinen Beitrag für etwas zahlen müssen, was Sie gar nicht benötigen, oder Mühe damit haben, die zu umfangreiche Funktionalität anzuwenden und zu warten.

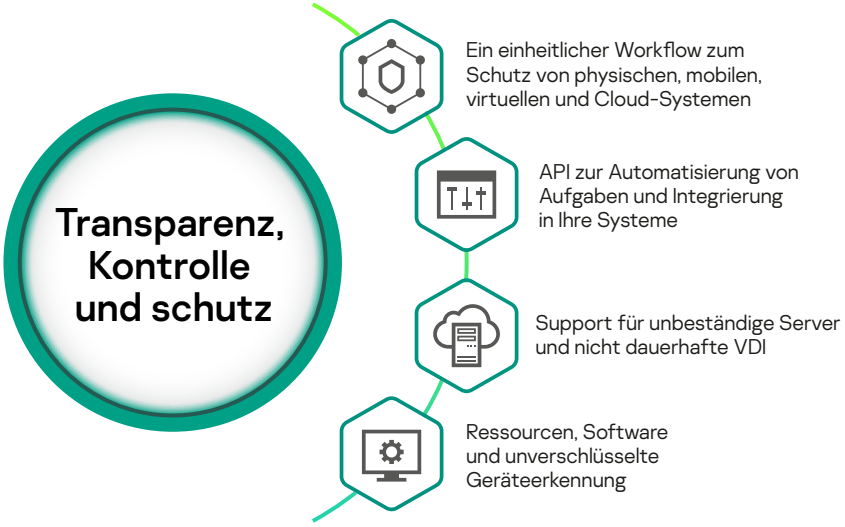
Sie erhalten herausragende Sicherheit, die zu Ihren aktuellen Anforderungen und Ihrem Budget passt, mit dem Wissen im Hinterkopf, dass Ihnen Kaspersky Security Foundations bei Bedarf die erforderlichen Agents für künftige EDR-, MDR- und XDR-Bereitstellung über Ihre gesamte Infrastruktur hinweg bereitstellt.

**Wichtige Produkte:**

- Kaspersky Endpoint Security for Business
- Kaspersky Hybrid Cloud Security
- Kaspersky Security for Mail Server
- Kaspersky Security for Internet Gateway

## Transparenz, Kontrolle und Schutz Ihrer gesamten IT-Infrastruktur

Kaspersky Security Foundations bietet eine einzige Konsole, die Ihnen vollständige Transparenz über Ihre gesamten IT-Bestände hinweg gibt. Sie umfasst eine breite Palette an Betriebssystemen und Hybrid-Infrastrukturen, indem sie Folgendes bietet:




### Wichtiges Alleinstellungsmerkmal

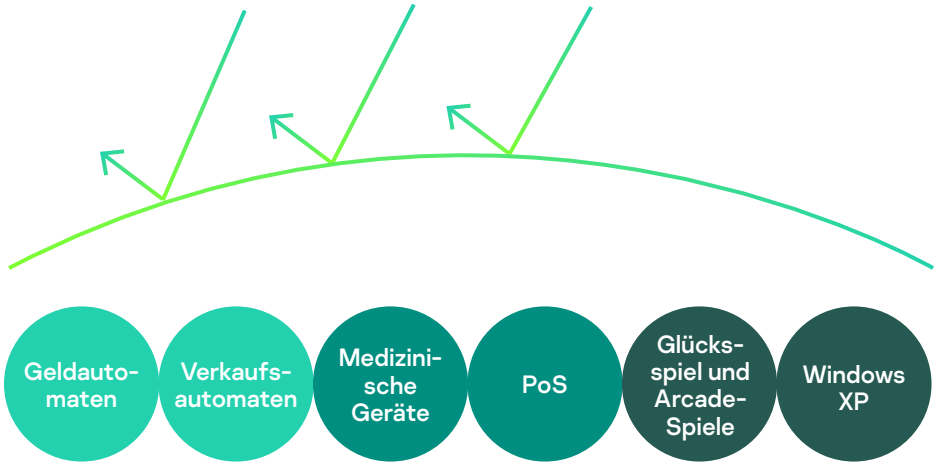
Die Module von Kaspersky Security Foundations sind perfekt aufeinander abgestimmt und sorgen für Sicherheit, Transparenz, Kontrolle und Schutz aller Aspekte Ihrer IT-Infrastruktur – von Mobilgeräten und VDI über virtuelle Server bis hin zu Public Cloud-Infrastrukturen.

**Wichtige Produkte:**

- Kaspersky Endpoint Security for Business
- Kaspersky Hybrid Cloud Security
- Kaspersky Security for Mail Server
- Kaspersky Security for Internet Gateway
- Kaspersky Embedded System Security

## 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 noch nicht bereit für ein Upgrade sind.




**Wichtige Produkte:**

- Kaspersky Embedded System Security
- Kaspersky Security for Internet Gateway
- Kaspersky Security for Mail Server

## 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 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 einzige 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 automatisch Cyberbedrohungen auf jedem Gerät, in VDIs, Gateways und Hybrid Server-Infrastrukturen.

### Hoher ROI

Die Benutzerfreundlichkeit wird durch unsere guten Bewertungen von Kunden jeglicher Größe in Rezensionen im Rahmen von Gartner Peer Insights sowie in Analystenstudien der Branche bestätigt. Kaspersky Security Foundations generiert hervorragende Investitionsrenditen (ROI) – nachgewiesen in TEI-Kundenbefragungen von Forrester.

## Genau hinschauen lohnt sich.

### Kaspersky Security Foundations

- Kaspersky Endpoint Security for Business
- Kaspersky Hybrid Cloud Security
- Kaspersky Embedded System 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 an vorderster Front vor Bedrohungen aus dem Internet
- Unterstützung bei der Bereitstellung, Konfiguration und Wartung

# Kaspersky Security für kleine und mittelständische Unternehmen

Zum Inhaltsverzeichnis

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

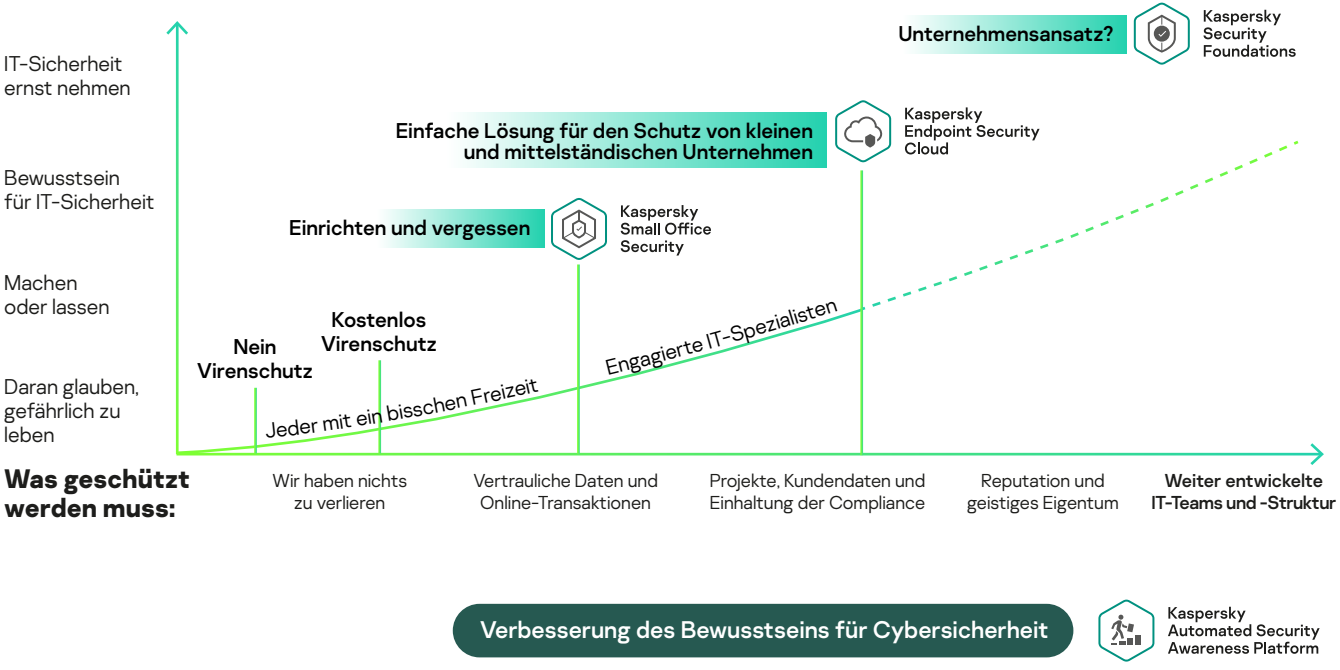
### Cyberbedrohungen

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, diese zu handhaben.

### Ressourcenüberlastung

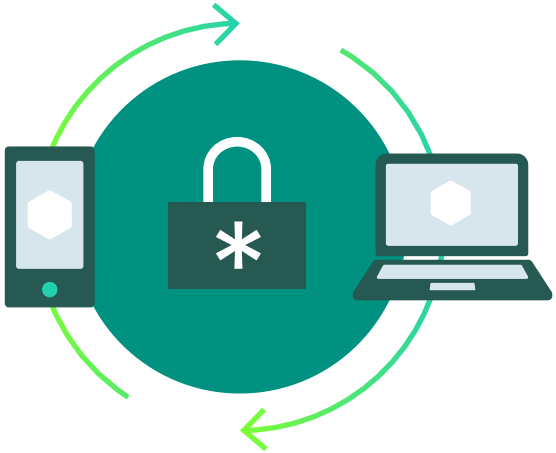
Die richtigen Sicherheitslösungen machen der IT-Abteilung das Leben leichter, nicht schwerer. Wenn Sie ein kleines oder mittelständisches Unternehmen führen, sind Ihre Mitarbeiter vermutlich oft überlastet. Deshalb müssen Sie effizient arbeiten und sich für eine Sicherheitslösung entscheiden, die sofortigen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

# Der schlanke IT-Sicherheitsansatz von Kaspersky



# Kaspersky Small Office Security

**Ideal**, wenn es keinen IT-Spezialisten in Ihrem Unternehmen gibt und der- oder diejenige, der oder die am versiertesten auf dem IT-Gebiet ist, Dinge in Ordnung bringen muss.



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, einfach einrichten und vergessen
- Wirksam – Schutz vertraulicher Daten und Ihres Geschäftsbetriebs vor Datenschutzverletzungen, Strafen und entgangenen Gewinnen

# 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

Bei Kaspersky ASAP handelt es sich um ein effektives und benutzerfreundliches Online-Tool, das Mitarbeitern Wissen im Bereich Cybersicherheit vermittelt und diese motiviert, sich entsprechend zu verhalten. Die Lösung basiert auf der mehr als 20-jährigen Erfahrung von Kaspersky im Bereich der IT-Sicherheit. Dank benutzerfreundlicher Bedienung und Automatisierungsfunktionen bietet sie in jeder Phase Unterstützung: von der Zieleinrichtung bis hin zur Ergebnisauswertung.

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

- Stärkung des Sicherheitsbewusstseins der Mitarbeiter und Vermittlung von sofort umsetzbarem Wissen
- Effektive Schulungen, die sehr wenig Zeit beanspruchen und keine speziellen Ressourcen oder Kenntnisse auf dem Gebiet Cybersicherheit erfordern

## 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

## Aspekte, die es für eine langfristige Cybersicherheitsstrategie zu berücksichtigen gilt

### Siloansatz 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 Erstplatzierungen erreicht als andere Sicherheitsanbieter. Und das Jahr für Jahr.
www.kaspersky.de/top3


## MITRE ATT&CK bestätigt die Qualität der Erkennung

MITRE | ATT&CK®




Kaspersky wurde erneut als „Gartner Peer Insights Customers' Choice for Endpoint Protection Platforms" ausgezeichnet.

Kaspersky ist „Customers' Choice" bei den „Gartner Peer Insights „Voice of the Customer": EDR Solutions"

Kaspersky erhielt die Auszeichnung „Gartner Peer Insights Customer's Choice of 2020 for Secure Web Gateways"

**Proven.**
**Transparent.**
**Independent.**

## Äußerst transparent

Mit fünf aktiven Transparency Centern und dank statistischer Verarbeitung in der Schweiz können wir optimale Datenhoheit garantieren.

kaspersky