

kaspersky

Kaspersky Security für kleine und mittelständische Unternehmen



Herausforderungen für SMB

Cyberbedrohungen

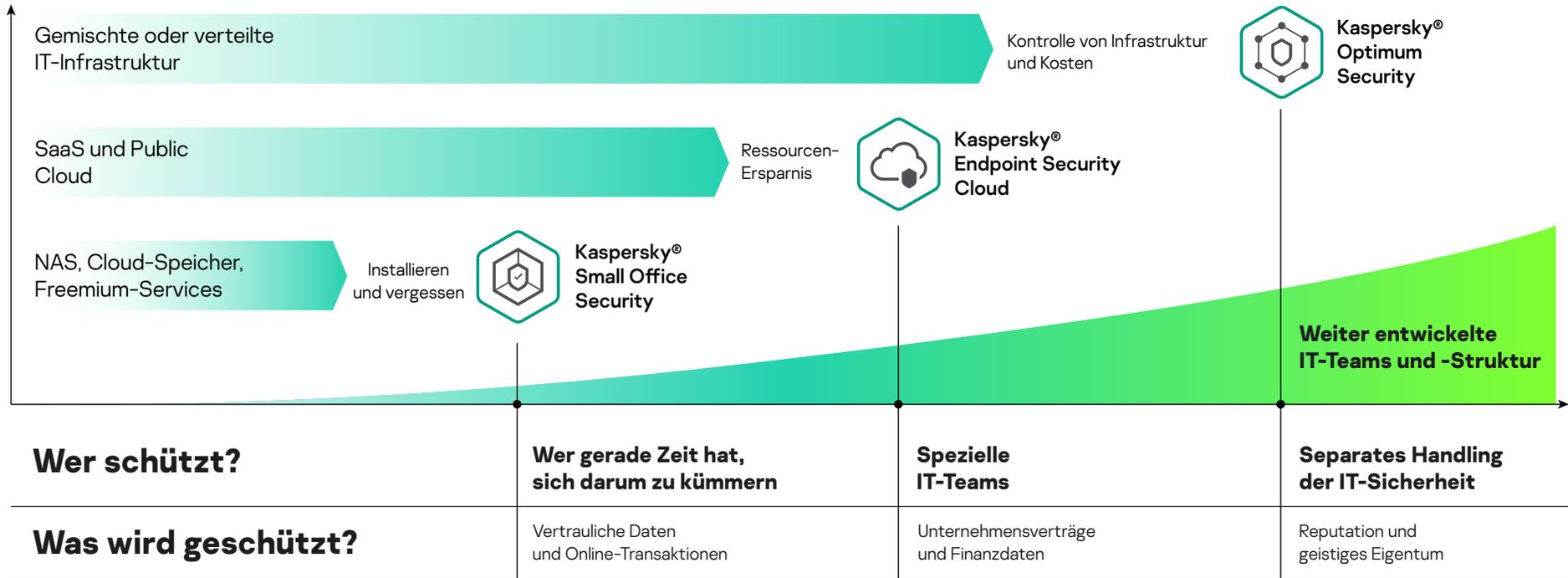
Nicht jede Lösung ist in jedem Unternehmen gleichermaßen einsetzbar. Kleinere Unternehmen kämpfen gegen die gleichen Cyberbedrohungen wie große Konzerne. Allerdings mangelt es ihnen oft an Ressourcen zur Bekämpfung.

Ressourcenüberlastung

Die richtigen Sicherheitslösungen machen überlasteten IT-Abteilungen 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.



Produkte von Kaspersky, die auf sich wandelnde IT-Teamstrukturen ausgerichtet sind



On-Demand-Schutz

Schutz der O365-Kollaboration



Kaspersky® Security for Microsoft Office 365

Security Awareness Trainings



Kaspersky® Automated Security Awareness Platform



Ihr Team von Kaspersky Small Office Security

Kaspersky Small Office Security wurde speziell für kleine Unternehmen ohne eigene IT-Spezialisten entwickelt. Die Lösung ist einfach zu installieren, noch einfacher zu bedienen und bietet vielfach getesteten und ausgezeichneten Schutz für Computer, File-Server, Laptops und Mobilgeräte und schützt zuverlässig vor Online-Angriffen, Finanzbetrug, Ransomware und Datenverlust.

Für die folgenden Zielsetzungen geeignet:

- Sofort einsatzbereiter Schutz, der Sicherheit gewährleistet, während Sie sich um Ihr Kerngeschäft kümmern

Vorteile für Ihr Unternehmen

- Installation in weniger als 10 Minuten
- Sofortiger Schutz und einfache Verwendung – einfach einrichten und vergessen
- Schutz vertraulicher Daten und Ihres Geschäftsbetriebs vor Datenschutzverletzungen, Strafen und entgangenen Gewinnen.

Praktische Anwendungen

- Mehrere Schutzebenen in einem benutzerfreundlichen Paket
- Maximale Sicherheit für Ihr Unternehmen bei minimalem Aufwand

0 Erforderliche Kenntnisse

1 Anpassung und Skalierbarkeit

1 Investitionsumfang



Kaspersky Endpoint Security Cloud

Kaspersky Endpoint Security Cloud bietet eine Komplettlösung für alle Sicherheitsanforderungen Ihrer Unternehmens-IT. 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.

Für die folgenden Zielsetzungen geeignet:

- Effektive Lösung, die Ihr Unternehmen immer und überall schützt

Vorteile für Ihr Unternehmen

- Sofort einsatzbereit
- Keine Investitionen in Hardware
- Schont Ressourcen
- Verbrauchsbasierte Abrechnung
- Perfekt für Outsourcing

Praktische Anwendungen

- 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
- Sichere Cloud-Migration mit Erkennung von Schatten-IT und Schutz für Microsoft Office 365

1 Erforderliche Kenntnisse

2 Anpassung und Skalierbarkeit

1 Investitionsumfang



Kaspersky Endpoint Security for Business

Der Ruf Ihres Unternehmens muss geschützt werden, deshalb geht unsere Lösung über den reinen Schutz und die Kontrolle jedes einzelnen Endpoints hinaus. Kaspersky Endpoint Security for Business erkennt Bedrohungen, auch dateilose, im Anfangsstadium, während der Schutz von Hochleistungsservern durch Server Hardening und zusätzliche Kontrollen verbessert wird um den Verlust wichtiger Daten zu verhindern. Wird im Hinblick auf flexibles Sicherheitsmanagement über die Cloud oder lokal bereitgestellt.

Für die folgenden Zielsetzungen geeignet:

- Verhindert, dass Mitarbeiter Ihr Unternehmen und sich selbst einem Angriff aussetzen
- So viele Endpoint-Vorfälle wie möglich werden automatisch verarbeitet
- Schutz unterschiedlicher Umgebungen mit flexiblen und bewährten Verteidigungsmaßnahmen

Vorteile für Ihr Unternehmen

- Senkt die Betriebskosten durch automatischen Schutz vor verschiedenen Bedrohungen mit einem einzigen Produkt
- Durchgängiger Schutz für jedes Gerät an jedem Ort sorgt für Geschäftskontinuität
- Unterstützt die Einhaltung von Compliance-Anforderungen bei gleichzeitiger vollständiger Flexibilität zur Auslagerung des IT-Sicherheitsmanagements

Praktische Anwendungen

- Senkt Angriffsrisiken mit der am häufigsten ausgezeichneten Technologie für den Endpoint-Schutz
- 100-prozentiger Schutz für Ihren IT-Bestand mit Cloud-bzw. lokaler Verwaltung, aktuelles Patching und einfache Migration der Schutzlösungen von Drittanbietern
- Erweiterungsmöglichkeiten mit EDR, SIEM und anderen Technologien ohne zeitaufwändiges Re-Imaging von Endpoints
- Integrierte Verschlüsselungsverwaltung, Löschen per Fernzugriff und Gerätekontrolle für unterschiedliche Betriebssysteme, damit Ihre Daten geschützt bleiben und Compliance-Vorgaben erfüllt werden

3 Erforderliche Kenntnisse

5 Anpassung und Skalierbarkeit

2 Investitionsumfang

Schritte zur Erhöhung der Sicherheit in Organisationen vor 2020



Erstens

EPP¹ implementieren

Ergebnis: Schutz gegen eine Vielzahl von Bedrohungen sowie Verringerung der Angriffsfläche und automatisierte Mechanismen zur Eindämmung



Zweitens

Implement Sandbox

Ergebnis: Erkennung von Bedrohungen, die auf die Umgehung von EPP ausgelegt sind, indem diese automatisch über einen längeren Zeitraum in der Sandbox analysiert werden



Drittens

EDR² implementieren

Ergebnis: Verbesserte Transparenz dank Ursachenanalyse und Abwehr von hochentwickelten Bedrohungen in der gesamten Infrastruktur

Aufgrund der COVID-19-Pandemie sahen sich im Jahr 2020 Organisationen weltweit gezwungen, ihre IT-Infrastruktur quasi über Nacht auszuweiten, um Fernarbeit zu ermöglichen.

Jetzt ist es an der Zeit, alle drei Schritte in einem einzigen zusammenzufassen, um Geschäftskontinuität zu gewährleisten.

1 – Endpoint Protection-Plattform

2 – Kaspersky Endpoint Detection and Response



Kaspersky Optimum Security

Dank unserer fest integrierten Cybersicherheitslösung mit Endpoint Detection and Response im Kern können Sie sich ganz einfach neuen Anforderungen anpassen. Endpoint Security, Sandbox und EDR bilden eine eng integrierte Lösung mit zahlreichen Technologien, die nahtlos zusammenarbeiten und so das Risiko verringern, einem erfolgreichen hoch entwickelten oder zielgerichteten Angriff zu erliegen. Darüber hinaus lassen sich damit Sicherheitsaufgaben an jedem Endpoint automatisieren.

Für die folgenden Zielsetzungen geeignet:

- Dringend benötigte Absicherung von Fern- und Büro-Arbeitsplätzen
- Reduzieren der Anzahl von Endpoint-Vorfällen, die manuell verarbeitet werden müssen
- Mehr Transparenz in Bezug auf Bedrohungen über sämtliche Endpoints hinweg

Vorteile für Ihr Unternehmen

- Maximale Ausschöpfung von flexiblen Arbeitsmodellen, ohne Abstriche bei der Sicherheit
- Reduziertes IT-Sicherheitsrisiko und Gewährleistung der Geschäftskontinuität
- Reduziert das Risiko von finanziellen Verlusten und Rufschädigung im Zusammenhang mit einem Cyberangriff auf ein Minimum
- Senkung der Betriebskosten durch automatisierte Abwehr

Praktische Anwendungen

- Reduzierte Angriffsrisiken mit der am häufigsten ausgezeichneten Technologie für den Endpoint-Schutz
- Ermöglicht tief gehende dynamische Analyse und Erkennung von unbekanntem und schwer zu erfassenden Bedrohungen
- Automatische Reaktion bei erkannten Bedrohungen oder während der Untersuchung mit nur wenigen Klicks
- Patch Management für Ihre IT-Umgebung mit Management aus der Cloud oder einer lokalen Konsole
- Intuitives Einbinden neuer Technologien wie EDR und anderer Funktionen ohne Re-imaging der Endpoints

3 Erforderliche Kenntnisse

4 Anpassung und Skalierbarkeit

2 Investitionsumfang



Kaspersky Security for Microsoft Office 365

Kaspersky Security for Microsoft Office 365 ist die erste Wahl, wenn es um den Schutz Ihres Cloud-orientierten Unternehmens vor bekannten und unbekanntem Bedrohungen geht. Die Ausbreitung von Angriffen durch Phishing, Ransomware, schädlichen Anhängen, Spam und Business Email Compromise (BEC) wird umgehend gestoppt, wobei keine speziellen IT-Kenntnisse für die Installation und Anwendung erforderlich sind.

Für die folgenden Zielsetzungen geeignet:

- Für alle, die auf der Suche nach einer integrierten Schutzlösung von einem vertrauenswürdigen Sicherheitsanbieter sind

Vorteile für Ihr Unternehmen

- Umfassender Schutz für Microsoft Office 365
- Nahtlose Integration in Microsoft Office 365 mit nur wenigen Klicks
- Keine Auswirkungen auf die Produktivität – keine E-Mail-Verzögerungen, keine Latenz
- Unterstützung für DSGVO und Daten-Compliance

Praktische Anwendungen

Eine Lösung zum Schutz von:

- Exchange Online
- OneDrive
- SharePoint Online
- Teams





Kaspersky Automated Security Awareness Platform (ASAP)

Kaspersky ASAP ist ein effektives und benutzerfreundliches Online-Tool, das Mitarbeitern Wissen im Bereich Cybersicherheit vermittelt und den richtigen Umgang mit Cyberbedrohungen fördert. 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.

Für die folgenden Zielsetzungen geeignet:

- Stärkung des Sicherheitsbewusstseins der Mitarbeiter und Vermittlung von sofort umsetzbarem Wissen
- Effektive Schulungen, die nicht viel Zeit in Anspruch nehmen, keine spezielle Ressourcen oder Vorkenntnisse erfordern

Vorteile für Ihr Unternehmen

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

Praktische Anwendungen

- Vermittlung von Wissen und Kompetenzen, damit sich Mitarbeiter sicher verhalten
- Vermittlung der richtigen Grundhaltung gegenüber Cybersicherheitsthemen
- Sorgt dafür, dass einmal erworbene Sicherheitskompetenzen dauerhaft verinnerlicht werden

1 Erforderliche Kenntnisse

4 Anpassung und Skalierbarkeit

3 Investitionsumfang



Managed Service Provider-Programm von Kaspersky

Unser Sicherheitsportfolio für MSPs umfasst flexible, leistungsstarke Tools, um die Kundeninfrastruktur zu sichern, zu überwachen und zu managen – von einer einzigen, einfach zu verwaltenden Konsole aus. Bieten Sie Ihren Kunden Next Gen-Cybersicherheitslösungen für physische und virtualisierte Infrastrukturen, lokal oder in der Cloud.

Für die folgenden Zielsetzungen geeignet:

- Perfekte Startbedingungen für Ihr Service-Angebot mit intuitiven Lösungen und automatisiertem Betrieb
- Dutzende neue Sicherheitsservices für Ihr Portfolio, die Sie per Upselling anbieten können, damit Sie stets eine Antwort auf die sich ändernden Anforderungen Ihrer Kunden haben.

Vorteile für Ihr Unternehmen

- Und all das erreichen Sie auf einfache, effektive Weise und ganz ohne zusätzliche Ressourcen oder Hardware-Investitionen.
- Integrieren Sie die Sicherheitslösungen in Ihre bevorzugten RMM- und PSA-Plattformen: ConnectWise® Automate™, ConnectWise® Manage™, Autotask®, Tigerpaw® One SolarWinds® N-central®

Praktische Anwendungen

- Weiten Sie Ihre Geschäftstätigkeit aus, indem Sie vielfältige Sicherheitsservices anbieten und per Upselling vertreiben.
- Steigern Sie Ihren Umsatz und gewinnen Sie neue Kunden mit branchenführender IT-Sicherheit
- Heben Sie sich von der Konkurrenz ab, indem Sie maßgeschneiderte Services und individuelle Threat Intelligence anbieten.

1 Erforderliche Kenntnisse

5 Anpassung und Skalierbarkeit

1 Investitionsumfang

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®



Das GARTNER PEER INSIGHTS CUSTOMERS' CHOICE-Logo ist ein Markenzeichen bzw. eine Handelsmarke von Gartner, Inc. und/oder seinen Tochterunternehmen und wird hier mit Genehmigung seines Eigentümers verwendet. Alle Rechte vorbehalten. Gartner Peer Insights Customers' Choice bezieht subjektive Meinungen von individuellen Endnutzerrezensionen, -bewertungen und -daten ein, die mithilfe dokumentierter Methoden untersucht werden. Sie stellen weder die Ansichten noch eine Empfehlung von Gartner oder seinen Tochterunternehmen dar.

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“



Äußerst transparent

Mit unserem ersten aktiven Transparency Center und dank statistischer Verarbeitung in der Schweiz können wir optimale Datenhoheit garantieren.



SYSTEM LOCKED
PLEASE TRY AGAIN

192 65
121 78
CLAMP
CLAMP
85
74

192 65
121 78
CLAMP
CLAMP
85
74

192 65
121 78
CLAMP
CLAMP
85
74

kaspersky

2021 KASPERSKY LABS GMBH.