kaspersky

Kaspersky Security for Enterprise

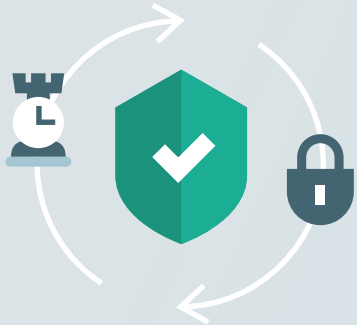
Infos zum Kaspersky Enterprise-Portfolio

Der Aufbau einer Sicherheitsgrundlage für Ihr Unternehmen durch 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 Enterprise Portfolio von Kaspersky ist auf die Sicherheitsanforderungen heutiger Unternehmen abgestimmt und bietet Organisationen mit unterschiedlichem technischem Reifegrad einen schrittweisen Ansatz. Dieser Ansatz umfasst unterschiedliche Schutzebenen vor allen Arten von Cyberbedrohungen. Selbst äußerst komplexe Angriffe werden erkannt, die Reaktion auf Vorfälle erfolgt schnell und angemessen, und zukünftige Bedrohungen können verhindert werden.

Die Rolle der Endpoint-Sicherheit für die langfristige Planung

Herkömmlicher Prozess bei der Entwicklung von Sicherheitslösungen



Entscheidungsfindung:

- Markttrends
- Siloansatz bei Sicherheitslösung
- Feuerwehrstrategie
- Compliance-orientiert

Einsatz herkömmlicher Produkte:

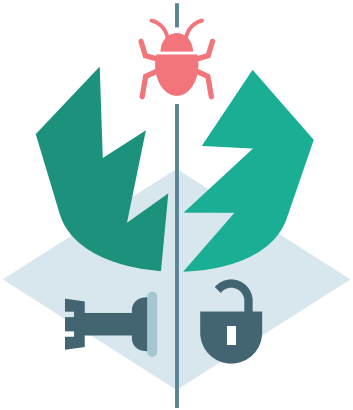
- EPP
- Firewalls/NGFW
- Web Application Firewall
- Data Loss Prevention
- SIEM

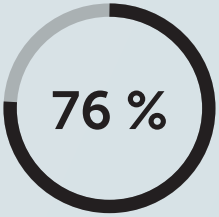
Eigenschaften

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

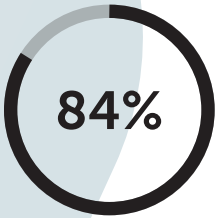
Gründe für das Fehlschlagen herkömmlicher Ansätze

- Immer komplexere Bedrohungen und Bedrohungslandschaft
- Komplexität von Cybersicherheits-Technologien
- Unternehmensanforderungen für eine langfristige Cybersicherheitsstrategie





aller Warnungen werden durch Endpoints generiert



aller Endpoint-Datenschutzverletzungen beziehen sich auf mehr als einen Endpoint

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.

3 Schritte für eine erweiterte Cybersicherheitsplanung in Unternehmen

2

Hoch entwickelte Bedrohungen und zielgerichtete Angriffe

Fortschrittlicher Schutz

Schwerpunkt auf erweiterter Erkennung und schneller Reaktion auf komplexe, nicht durch Präventivschutz erkannte Bedrohungen

Endpoints

Kaspersky Endpoint Detection and Response

Services

Kaspersky Targeted Attack Discovery Service

1

Breiter gefächerte Bedrohungslandschaft

Sicherheitsgrundlage

Systemhärtung und automatisches Blockieren der maximal möglichen Anzahl von Bedrohungen

Endpoints

Kaspersky Endpoint Security for Business

Kaspersky Embedded Systems Security

Netzwerk

Kaspersky Secure for Mail Server

Kaspersky Security for Internet Gateway

3

Zielgerichtete Kampagnen und andere Cyberwaffen

Integrierter Cybersicherheitsansatz

Vorbereitung auf Angriffe auf APT-Ebene Umfassende Expertise, erweiterte Fähigkeiten zur Bedrohungsanalyse und fortlaufendes Threat Hunting

Kaspersky Threat Management & Defense

Netzwerk

Kaspersky Anti Targeted Attack

Intelligence

Kaspersky Threat Intelligence

Kunden

Kaspersky Cybersecurity Training

Privatsphäre

Kaspersky Private Security Network

Cloud

Kaspersky Hybrid Cloud Security

Support

Premium-Support und professionelle Services von Kaspersky

Daten

Kaspersky Security for Storage

Kunden

Kaspersky Security Awareness

4 geschäftliche Vorteile bei diesem Ansatz

Die Grundlage zur Entwicklung einer langfristigen Cybersicherheitsstrategie unter Berücksichtigung der jeweiligen geschäftlichen Anforderungen und der Trends in der Bedrohungslandschaft

Optimierte Investitionen in Sicherheitstechnologie und reduzierte Betriebskosten

Reduzierung finanzieller und betrieblicher Schäden aufgrund von Cyberkriminalität

ROI-Steigerung durch nahtlose Workflow-Automatisierung ohne Unterbrechung der Geschäftsabläufe

1 Sicherheitsgrundlage

Automatische Präventionstechnologien und erhöhtes Sicherheitsbewusstsein

Blockieren der maximal möglichen Anzahl von Bedrohungen

Ideal für kleinere Unternehmen ohne spezielles Sicherheitsteam oder mit nur sehr begrenzter Cybersicherheitsexpertise

- Automatische Multi-Vektor-Prävention einer großen Menge möglicher Vorfälle aufgrund von Commodity Threats
- Ein überaus wichtiger Schritt für mittelgroße bis große Unternehmen zum Aufbau einer integrierten Schutzstrategie vor komplexen Bedrohungen

Endpoints

- **Kaspersky Endpoint Security for Business**
- **Kaspersky Embedded Systems Security**

Cloud

- **Kaspersky Hybrid Cloud Security**

Netzwerk

- **Kaspersky Secure Mail Gateway**
- **Kaspersky Security for Internet Gateway**

Kunden

- **Kaspersky Security Awareness**

Daten

- **Kaspersky Security for Storage**

Support

- **Kaspersky Premium Support**
- **Kaspersky Professional Services**

Kaspersky Endpoint Security for Business

Endpoints sind die Quelle für die meisten Cyberangriffe. Eingeschränkte Schutz- und Automatisierungsfunktionen führen zu einer Überlastung der Experten durch Sicherheitsvorfälle. Jeder Endpoint kann potentiell zur Ursache für Störungen des Geschäftsbetriebs werden. Mit Kaspersky Endpoint Security for Business lassen sich Bedrohungen verhindern und Endpoints härten, indem adaptive Sicherheit mit erweiterten Kontrolltools kombiniert werden. Bedrohungen werden abgeblockt, noch bevor sie sich negativ auf die Unternehmensdaten oder die Benutzerproduktivität auswirken. Auch, wenn sich der jeweilige Endpoint nicht innerhalb des Unternehmensnetzwerks befindet.

Ideal für

Unternehmen mit wachsenden und immer unterschiedlicheren Anforderungen an die IT

Unternehmen, die Möglichkeiten und Häufigkeit von Benutzerfehlern reduzieren wollen, die zu Sicherheitsverletzungen führen

Geschäftsvorteile

Schutz vor Geschäftsausfällen und menschlichen Fehlern

Unterstützung des digitalen Wandels und Schutz der mobilen Belegschaft

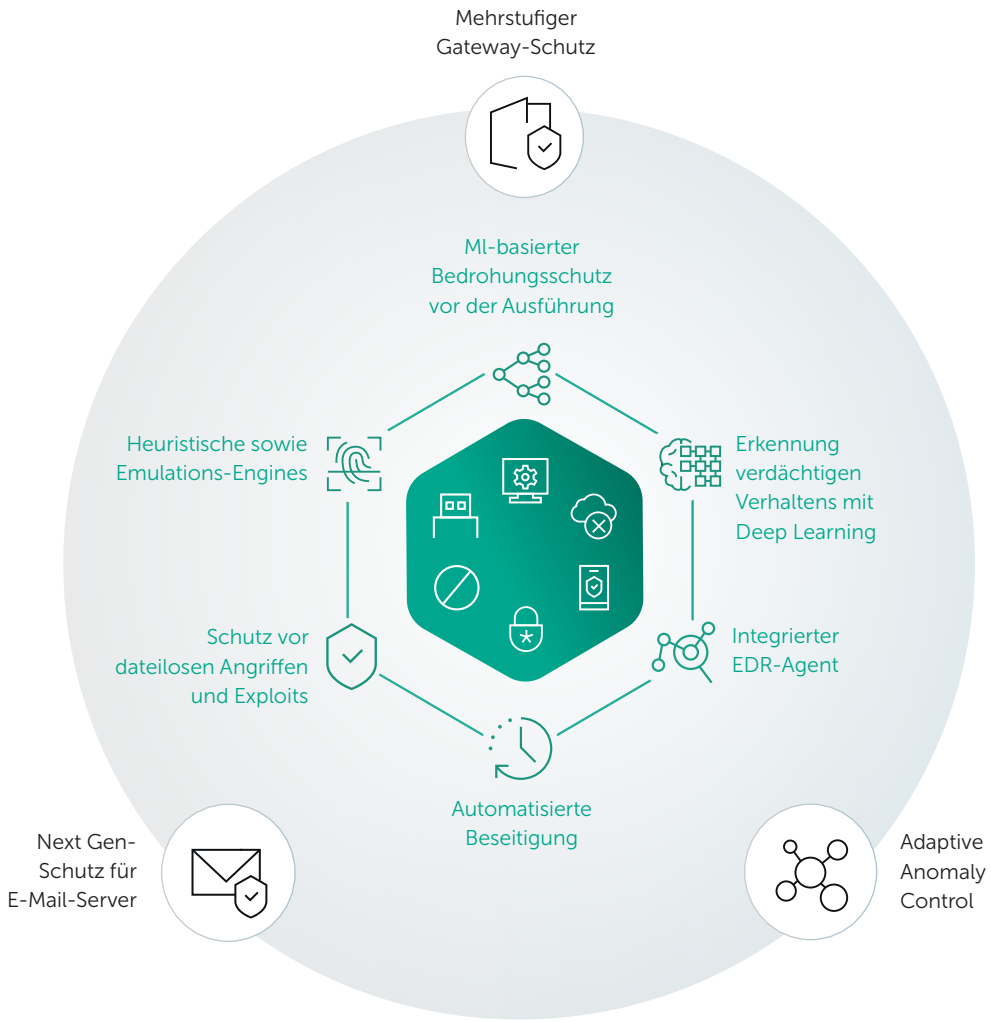
Bessere Vorbereitung auf Audits: Ermitteln und Beheben von Schwachstellen, Konfigurationsänderungen und nicht verschlüsselten Geräten

Maximierter ROI durch eine reduzierte Angriffsfläche und weniger zu verwaltende Vorfälle

Kontrolle über jeden Endpoint über eine einzige Konsole und einen zentralen Agent

Anwendungsfälle

- Reduzieren des Risikos für Angriffe durch adaptive Härtung, Endpoint-Schutz, E-Mail- und File Server sowie Internet-Gateways
- Sicherstellen von Endpoint-Compliance mit gesetzlichen Anforderungen
- Automatisierung von Erkennung, Reaktion und Softwarebereitstellung, damit Sicherheitsexperten sich auf andere Aufgaben konzentrieren können
- Optimierte Integration und Einführung anderer Sicherheitstechnologien


Mehrstufiger Gateway-Schutz
Ml-basierter Bedrohungsschutz vor der Ausführung
Heuristische sowie Emulations-Engines
Erkennung verdächtigen Verhaltens mit Deep Learning
Schutz vor dateilosen Angriffen und Exploits
Integrierter EDR-Agent
Automatisierte Beseitigung
Next Gen-Schutz für E-Mail-Server
Adaptive Anomaly Control

Kaspersky Hybrid Cloud Security

Hybrid Cloud Security ist eine Lösung, mit der sich der digitale Wandel vereinfachen und die Virtualisierung oder die Verschiebung von Workloads in die Cloud sicher durchführen lässt. Dank der patentierten Light Agent-Technologie kann die Sicherheitsfunktion zentralisiert und auf intelligente Weise optimiert werden, was die Ressourcenauslastung des Hypervisors stark reduziert. Die native Integration mit einer Vielzahl von Virtualisierungs-, Container- und Public-Cloud-Plattformen bietet fortlaufende Transparenz und Kontrolle innerhalb der gesamten Infrastruktur. Eine umfassende Reihe von Sicherheitstechnologien, die über dieselbe Konsole verwaltet werden, sorgt dauerhaft für ein optimiertes Risikomanagement in unterschiedlichen Umgebungen.

Ideal für

Unternehmen, die ihre Server- und Desktop-Workloads virtualisieren

Unternehmen, die ihre Infrastrukturen in die Public Cloud verschieben oder darin verwalten

Unternehmen, die Public Clouds und Containers für die Entwicklungsarbeit einsetzen

Geschäftsvorteile

Fortlaufende Transparenz und Kontrolle über alle Rechenzentren und Cloud-Bereitstellungen hinweg

Reduzierung von Angriffsfläche und Verweilzeit, daher erschwerte laterale Bewegung

Freisetzung von bis zu 30 % der Hypervisor-Ressourcen und Reduzierung der Anmeldezeit von Minuten auf Sekunden

Unterstützung von Compliance

Sicherstellen einer effizienten Zusammenarbeit zwischen IT-, Informationssicherheits- und Entwicklungsteams, daher weniger Risiken und Sicherheitslücken

Anwendungsfälle

- Ressourcenschonender Schutz für virtualisierte Serverinfrastrukturen
- Sicherheit für VMWare und Citrix VDI
- Sorgt durch Einhaltung zentraler Sicherheitsanforderungen für Compliance
- Schutz für Cloud-Workloads für AWS- und Azure-Instanzen mit automatischer Bereitstellung und konstanter Transparenz durch native API-Integration
- Sichere Entwicklungsarbeiten durch Containerschutz und Verwaltungs-API

Kaspersky Security for Mail Server

Kaspersky Security for Mail Server bietet Schutz vor E-Mail-basierten Bedrohungen, weil diese nicht den Endpoint erreichen können, an dem die meisten Social Engineering- und Malware-Angriffe stattfinden. Alle Arten von Malware, einschließlich Ransomware und Miner, sowie Phishing-Versuche werden blockiert, wobei besonderer Wert auf das Verhindern von Business Email Compromise gelegt wird. Die Lösung blockiert unerwünschte Massen-E-Mails und nicht gewünschte Datenübertragungen.

Ideal für

Unternehmen mit einer gut entwickelten IT-Umgebung, die Bedenken hinsichtlich Datenschutz und Datensicherheit haben

Unternehmen, die sich stark auf E-Mail-Kommunikation stützen und eine präzise Verwaltung benötigen

Unternehmen, die ihre APT-Erkennungsdaten mit E-Mail-Kontext bereichern und APT-E-Mail-Komponenten blockieren möchten

Geschäftsvorteile

Erhöhte Produktivität durch Blockieren unerwünschter Massen-E-Mails, einschließlich Spam, und Bereitstellung von E-Mail-Kategorien für eine bequemere Kommunikationsverwaltung

Trägt durch Blockieren von E-Mail-basierten Bedrohungen zur Vermeidung von Geschäftsunterbrechungen bei

Bessere Datensicherheit, da die Übertragung unerwünschter Datentypen verhindert wird

Weniger Verwaltungsaufwand für Services durch Reduzierung von Vorfällen auf Benutzerebene

Erhöhte Leistungsfähigkeit der vorhandenen E-Mail-Gateway-Sicherheit durch zusätzliche umfassende Erkennungsfunktionen – ohne Fehlalarme

Anwendungsfälle

- Funktioniert mit einer Vielzahl externer Mail Transfer Agents oder als eine virtuelle All-in-One-Appliance
- Bietet API-integrierte E-Mail-Sicherheit für Microsoft Exchange-Server, sowohl am Gateway, als auch auf Ebene des Posteingangs
- Blockiert die Übertragung unerwünschter Dateitypen
- Integration mit Kaspersky Anti Targeted Attack zum Blockieren von APT-E-Mail-Komponenten

Kaspersky Security for Internet Gateway

Kaspersky Security for Internet Gateway bietet Schutz vor web-basierten Bedrohungen auf Ebene des Unternehmens-Verteidigungsnetzwerks und hindert sie daran, das Hauptziel aller Angriffe zu erreichen: den Endpoint. Die Lösung trägt dazu bei, dass Angriffe aufgrund von Social Engineering verhindert werden und blockiert alle Arten von Malware, darunter Ransomware und Miner, sowie Phishing-Versuche. In Verbindung mit Ihrem vorhandenen Unternehmens-Proxyserver erzielen Sie mit dieser Lösung eine erhöhte Leistung. Alternativ können Sie sie als einsatzbereite, virtuelle All-in-One-Appliance bereitstellen.

Ideal für

Unternehmen mit einer gut entwickelten IT-Umgebung, die Bedenken hinsichtlich Datenschutz und Datensicherheit haben

MSPs und xSPs (einschließlich Telekommunikationsanbietern)

Geschäftsvorteile

Verhindern von Störungen des Geschäftsbetriebs durch Blockieren web-basierter Bedrohungen, bevor sie jemand durch Klicken „hereinlässt"

Erhöhte Leistungsfähigkeit der vorhandenen Web-Gateway-Sicherheit durch zusätzliche umfassende Erkennungsfunktionen – ohne Fehlalarme

Weniger Verwaltungsaufwand für Services durch Reduzierung der Anzahl von Vorfällen auf Benutzerebene

Risikominderung durch Überwachung der Internetnutzung und der Übertragung bestimmter Dateitypen

Mandantenfähigkeit als Vorteil für MSPs

Anwendungsfälle

- Blockieren schädlicher und Phishing-Webressourcen und heruntergeladener Malware
- Verhindern der Nutzung nicht erwünschter Webressourcen
- Möglichkeit der Verwaltung unterschiedlicher Workspaces mit jeweils eigenen Regeln
- Herausfiltern unerwünschter Dateitypen in beide Richtungen und auf Grundlage mehrerer Kriterien
- Integration mit Kaspersky Anti Targeted Attack als Websensor und Blockieren zielgerichteter Angriffskomponenten je nach den erweiterten Erkennungsergebnissen

Kaspersky Security for Storage

Einfach zugänglicher, vernetzter Speicher kann leicht zur Quelle für Infektionen über die gesamte Infrastruktur hinweg werden – und auch ein Ziel von Bedrohungen wie Ransomware. Kaspersky Security for Storage schützt Ihre Unternehmensdaten und verhindert eine Infizierung des Netzwerks durch breit gefächerte Schutztechnologien, die durch globale Threat Intelligence unterstützt werden. Die Lösung umfasst spezifische Funktionen wie Remote Anti-Cryptor, was bei der Integration mit Speichersystem-APIs aktiviert wird.

Ideal für

Unternehmen mit einer gut entwickelten IT-Umgebung, die Bedenken hinsichtlich Datenschutz und Datensicherheit haben

Unternehmen wie Banken, E-Commerce und Versicherungen, die mit einer großen Menge vertraulicher/privater Daten arbeiten

Geschäftsvorteile

Schutz von Daten bei der Verbindung von Speichern ohne Zugriff auf die Speichersoftware

Weniger Verwaltungsaufwand und mehr Sicherheit dank einer Verwaltungskonsole mit einer einzigen Ansicht

Aufrechterhalten der Geschäftskontinuität, indem gespeicherte Daten sicher vor remote ausgeführter Ransomware und Crypto-Wipern gespeichert wird

Unterstützung von Compliance durch Bereitstellung von Sicherheitsfunktionen für eine Vielzahl von Modellen, die dann als regulierte Speichervorrichtungen verwendet werden können

Anwendungsfälle

- Schutz für Netzwerkspeicher und die darauf ausgeführten Server
- Bei Aufnahme einer Datei in den sicheren Speicher oder bei Änderung einer vorhandenen Datei wird auf Angriffsversuche überprüft; auch On-Demand-Scans sind möglich
- Bei einer Remote-Dateiverschlüsselung wird die Quelle im Netzwerk erkannt und blockiert, um weiteren Schaden zu verhindern*

* Nur mit der für bestimmte Speicher verfügbaren API-Integration

Kaspersky Embedded Systems Security

Mit leistungsstarker Threat Intelligence, Malware-Erkennung in Echtzeit, umfassender Anwendungs- und Gerätesteuerung und flexibler Verwaltung bietet Kaspersky Embedded Systems Security einen umfassenden Schutz speziell für Embedded Systems.

Ideal für

Finanzdienstleistungen

Einzelhandel und Transport

Geldautomaten- und POS-Service Provider

Geschäftsvorteile

Minderung des Risikos von Bedrohungen, die auf bestimmte Finanzinfrastrukturen abzielen

Einhaltung von Compliance-Anforderungen in Vorschriften wie z. B. PCI/DSS und SWIFT

Optimierung der Verwaltungskosten dank einer einzigen Verwaltungskonsole

Anwendungsfälle

- Schutz geografisch verteilter und nur selten aktualisierter Embedded Systems, die ganz bestimmte und einzigartige Sicherheitsprobleme verursachen
- Schutz für nicht unterstütztes Windows XP, das nach wie vor auf Low-End-Hardware sehr verbreitet ist
- Effizientes Design bietet leistungsstarke Sicherheit ohne Risiko einer Systemüberlastung

Kaspersky Premium Support (MSA) Service

Beim Eintreten eines Sicherheitsvorfalls ist die Zeit bis zur Erkennung und Beseitigung ein kritischer Faktor. Das schnelle Erkennen und Lösen eines Problems kann erhebliche Kosteneinsparungen für das Unternehmen bedeuten. Unsere Maintenance Service Agreement (MSA)-Pläne sind genau im Hinblick auf dieses Ziel konzipiert. Rund um die Uhr Zugang zu unseren Experten, angemessene Priorisierung von Problemen mit garantierten Reaktionszeiten und privaten Patches – alles, was nötig ist, um Ihr Problem so bald wie möglich zu beheben.

Ideal für alle Unternehmen, die Kaspersky-Produkte einsetzen

Geschäftsvorteile

Geschäftskontinuität dank speziell zugewiesener, abrufbarer Experten, die das Problem übernehmen und möglichst schnell eine Lösung herbeiführen

Geringere Kosten bei Sicherheitsvorfällen durch Zugang zu einer priorisierten Support-Hotline, garantierte Reaktionszeiten und private Patches

Spezieller Technical Account Manager als ihr Vertreter bei Kaspersky mit der Berechtigung, alle erforderlichen Spezialisten zur Lösung des Problems einzusetzen

Anwendungsfälle

- Direkte Weiterleitung Ihres Problems an Experten im Kaspersky-Headquarter, die darauf spezialisiert sind, schnellstmöglich die richtige Lösung zu finden
- Umfassende Sicherheit durch Schutzmaßnahmen, die genau auf Ihr System zugeschnitten sind, darunter priorisierte Hotfixes und personalisierte Patches
- Weniger Zeitaufwand für Wartung und Fehlerbehebung für Ihre internen Ressourcen

Kaspersky Professional Services

Service

Cybersicherheit bedeutet eine erhebliche Investition. Setzen Sie sich deshalb mit Experten zusammen, die genau wissen, wie Sie Ihre Sicherheit optimieren können, um die individuellen Anforderungen Ihres Unternehmens zu erfüllen. Unsere Sicherheitsexperten arbeiten gemäß unserer Best Practices und helfen in der gesamten IT-Infrastruktur Ihres Unternehmens beim Deployment, der Konfiguration und der Aktualisierung von Kaspersky-Produkten.

Kaspersky Professional Services umfassen:

- Implementierung und Upgrade
- Konfiguration
- Produktschulung
-

Ideal für alle Unternehmen, die Kaspersky-Produkte einsetzen

Geschäftsvorteile

Maximierter ROI für Ihre Sicherheitslösungen, weil sie immer voll einsatzfähig sind

Kostensenkungen bei den internen IT-Mitarbeitern

Reduzierte Ausfallzeiten durch regelmäßige Audits der Produktkonfigurationen, sodass immer die aktuellsten Abwehrmechanismen verfügbar sind

Kürzere Produkteinführungszeiten, sodass die Vorteile aus dem implementierten Produkt schneller genutzt werden können

Anwendungsfälle

- Geringere Implementierungsrisiken, die sich möglicherweise negativ auf den Schutz auswirken, die Produktivität beeinträchtigen und sogar zu Ausfallzeiten führen
- Minimierte Auswirkungen bei der Implementierung Ihrer neuen Sicherheitslösung auf das Tagesgeschäft und Senkung der Gesamtkosten für die Implementierung
- Vorbereitung Ihrer Mitarbeiter auf eine fortlaufende Produktwartung durch unsere Produkttrainingsprogramme. So werden Fehler verhindert sowie die Produktkompatibilität und Funktionsprinzipien erläutert

Kaspersky Security Awareness

Unsere computergestützten Trainingsprogramme sorgen für neue Gewohnheiten und Verhaltensmuster bei Mitarbeitern und sensibilisieren diese für Cybergefahren. Das Kaspersky Security Awareness Schulungsportfolio umfasst Folgendes: Automated Security Awareness Platform (ASAP) – Awareness-Schulung für alle Mitarbeiter, bei der konkrete Kenntnisse zur alltäglichen Cybersicherheit vermittelt werden. Cybersecurity for IT Online (CITO) – Schulung für allgemeine IT-Spezialisten, bei der es um praktische Fähigkeiten zum Erkennen eines möglichen Angriffsszenarios und zur Erfassung von Vorfallsdaten geht. Kaspersky Interactive Protection Simulation (KIPS) – Cybersicherheits-Planspiel für Entscheider.

Ideal für

Unternehmen mit wachsenden und immer unterschiedlicheren Anforderungen an die IT

Unternehmen, die das Risiko von Benutzerfehlern reduzieren wollen, die zu Sicherheitsverletzungen führen

Geschäftsvorteile

Schutz für Unternehmen von innen

Nachhaltig hohes Cybersicherheitsbewusstsein in der gesamten Unternehmenskultur

Bis zu 80 % weniger menschliche Fehler

Anwendungsfälle

- Förderung von cyber-sicherem Verhalten durch typische Szenarien und Situationen, Simulationen von Cyberangriffen, verschiedene Aufgaben und Erklärungen
- Potentielle Bedrohungen sollen schneller erkannt und die Fähigkeiten vermittelt werden, mit ihnen umzugehen
- Vermittelt praktische Fähigkeiten, die für das Erkennen eines möglichen Angriffs bei einem vermeintlich gutartigen PC-Vorfall und für das Sammeln von Vorfallsdaten zur Übergabe an die IT-Sicherheitsabteilung unerlässlich sind
- Fördert bei der Geschäftsführung und bei Entscheidungsträgern ein besseres Verständnis für die Sicherheit

2 Fortschrittlicher Schutz

Fortschrittliche Erkennungstechnologien und zentrale Reaktion

Maximale Automatisierung im Erkennungsstadium und Reaktion auf komplexe Bedrohungen anhand von Präventionstechnologie

- Im Wachstum, zunehmend komplexe IT-Umgebungen mit einer erhöhten Angriffsfläche
- Kleines Sicherheitsteam mit begrenzter Erfahrung
- Verfügt über grundlegende Fähigkeiten zur Vorfallsreaktion

Ideal für mittelgroße Unternehmen:

Endpoint

Kaspersky Endpoint Detection and Response

Kunden

Kaspersky Cybersecurity Training

Services

Kaspersky Targeted Attack Discovery

Netzwerk

Kaspersky Anti-Targeted Attack

Privatsphäre

Kaspersky Private Security Network

Intelligence

Kaspersky Threat Intelligence

Kaspersky Endpoint Detection and Response

Zur schnellen und erfolgreichen Verteidigung gegen hoch entwickelte Bedrohungen müssen Präventionstechnologien durch fortschrittliche Funktionen für Endpoint Detection and Response ergänzt werden. Kaspersky EDR ist eine Speziallösung zur Abwehr hoch entwickelter Bedrohungen für Ihre Endpoints und nutzt denselben zentralen Agent wie unsere führende Schutzlösung Kaspersky Endpoint Security. Kaspersky EDR bietet eine umfassende Übersicht über alle Endpoints im Unternehmensnetzwerk und ermöglicht die Automatisierung von Routineaufgaben, damit komplexe Bedrohungen schnell erkannt, priorisiert, untersucht und neutralisiert werden können.

Ideal für

Großunternehmen

Unternehmen, die bereits Kaspersky Endpoint Security einsetzen

SOCs und Incident Response Teams

Geschäftsvorteile

Mindern der Risiken durch hoch entwickelte Bedrohungen und zielgerichtete Angriffe

Optimierung der Verwaltungskosten durch Aufgabenautomatisierung und eine einzelne, vereinfachte und für Unternehmen konzipierte Oberfläche

Schnellere und effizientere Vorfallsbearbeitung ohne zusätzliche Kosten

Erhöhte Produktivität, sodass Ihre IT- und Sicherheitsteams Zeit für andere Aufgaben haben

Unterstützung von Compliance durch interne Sicherheitsrichtlinien und gesetzliche Anforderungen

Anwendungsfälle

- Für den gesamten Endpoint Protection-Zyklus, von der automatischen Blockierung von Bedrohungen bis hin zu komplexen Vorfallsreaktionen bei hoch entwickelten Bedrohungen, über einen einzelnen Agent
- Schneller Zugriff auf Endpoint-Daten, selbst wenn infizierte Workstations nicht verfügbar oder die Daten verschlüsselt sind
- Zur Ergänzung der Vorfallsuntersuchung anhand von Threat Hunting, IoA-Analysen und MITRE ATT&CK-Zuordnung
- Schnelle Reaktion bei verteilten Infrastrukturen anhand umfassender automatisierter Aktionen

Kaspersky Anti Targeted Attack

Die Anzahl und Raffinesse zielgerichteter Angriffe nimmt ständig zu. Um diesen neu aufkommenden Bedrohungen entgegenzutreten, müssen Sie Ihre Sicherheitssysteme fortlaufend anpassen. Kaspersky Anti Targeted Attack bietet fortschrittliche Bedrohungserkennung auf Netzwerkebene mit voll automatischer Datenerfassung, Analyse und Korrelation und ermöglicht so einen detaillierten Einblick in den Umfang der Bedrohung. So lässt sich Ihre Unternehmensinfrastruktur ohne zusätzliche Ressourcen effektiv vor komplexen Bedrohungen und zielgerichteten Angriffen schützen.

Ideal für

Großunternehmen

SOC-Teams

MSSPs

Alle Unternehmen, die für Compliance sorgen müssen

Geschäftsvorteile

Mindern der Risiken, die durch hoch entwickelte Bedrohungen und zielgerichtete Angriffe entstehen

Reduzierung von finanziellen und betrieblichen Schäden durch Einführung eines einzigen, zuverlässigen Systems zum Schutz vor komplexen Angriffen

Optimierung der Verwaltungskosten durch Aufgabenautomatisierung und eine einzelne, vereinfachte und für Unternehmen konzipierte Oberfläche

Aufgabenoptimierung durch nahtlose Workflow-Automatisierung ohne Unterbrechung der Geschäftsabläufe

Sicherstellen von Compliance mit gesetzlichen Anforderungen

Anwendungsfälle

- Schnelles Erkennen der Aktionen von Cyberkriminellen, die Präventionstechnologien umgehen wollen, durch zentrale Überwachung und Kontrolle potentieller Eintrittspunkte in die Infrastruktur
- Die Erkennung von Bedrohungssignalen und Korrelation von Multi-Vektor-Vorfällen innerhalb eines Angriffs zu einem Gesamtbild ermöglicht eine effektivere Untersuchung
- Zeitnahe Bereitstellung aller erforderlichen Informationen zu den erkannten Bedrohungen an das Vorfallsreaktionsteam

Kaspersky Private Security Network

Das Kaspersky Private Security Network ermöglicht es Unternehmen, fast alle Vorteile unserer weltweiten Cloud-basierten Bedrohungsinformationen zu nutzen, ohne ihre Daten außerhalb des geschützten Perimeters preiszugeben. Damit bildet es die vollständig private, lokale und persönliche Version des Kaspersky Security Network für ein einzelnes Unternehmen.

Ideal für

Unternehmen mit strengen Vorschriften zur Beschränkung des Datenzugriffs

Wichtige Infrastrukturen mit physisch isolierten Netzwerken

Telekommunikations-, Managed Security- und andere Serviceanbieter

Geschäftsvorteile

Herausragende Threat Detection für Ihr Unternehmen

Schnellere Reaktionszeiten durch Echtzeitzugriff auf Bedrohungs- und Reputationsstatistiken

Erhöhte betriebliche Effizienz durch Minimierung von Fehlalarmen

Unterstützt die vollständige Einhaltung von gesetzlichen Vorschriften zur Sicherheit isolierter Netzwerke und Umgebungen

Anwendungsfälle

- Alle Vorteile der Cloud-basierten Sicherheit, ohne dass vertrauliche Informationen außerhalb Ihrer überwachten Infrastruktur preisgegeben werden
- Möglichkeit der Entwicklung eines angepassten Schutzes durch Einbringen Ihrer eigenen Ergebnisse
- Geeignet für isolierte wichtige Netzwerke

Kaspersky Targeted Attack Discovery

Service

Kaspersky Targeted Attack Discovery ist ein umfassender Assessment-Service für Gefährdungen, der erkennt, ob Sie einem Angriff ausgesetzt sind, was passiert und wer der Bedrohungsakteur ist. Unsere Experten erkennen, identifizieren und analysieren laufende sowie vergangene Vorfälle und stellen eine Liste der dadurch betroffenen Systeme zusammen. Wir unterstützen Sie dabei, schädliche Aktivitäten aufzudecken, die möglichen Vorfallsquellen zu erkennen und möglichst effektive Beseitigungsmaßnahmen zu planen.

Ideal für

Unternehmen ohne oder mit nur unerfahrenen Sicherheitsteams

Regierungsbehörden

Kritische Infrastrukturen

1 Erforderliche Kenntnisse

5 Anpassung und Skalierbarkeit

3 Kosten

Geschäftsvorteile

Verhindern und Minimieren von Schäden aus infizierten Systemen und somit erhebliche Kostensenkungen

Sorgt für ein anhaltend gutes Vertrauensverhältnis zu Ihren Kunden, Partnern und Investoren

Vermeiden von Strafen und Bußgeldern durch den Gesetzgeber

Stärkung der Abwehrmaßnahmen gegen zukünftige Vorfälle durch Empfehlungen zu Abhilfemaßnahmen

Anwendungsfälle

- Ermöglicht Einblicke in die digitale Umgebung Ihres Unternehmens und die damit verbundenen Risiken
- Bessere Risikoeinschätzung durch intensive Überprüfung der IT-Infrastruktur und der Daten (z. B. Protokolldateien) und Analyse der ausgehenden Netzwerkverbindungen
- Erkennen von Anzeichen für laufende oder vergangene Angriffe innerhalb Ihrer Netzwerke
- Untersuchung, wie sich ein Angriff auf Ihre Systeme auswirkt, und wie Sie sich wehren können

Kaspersky Threat Intelligence

Die Bekämpfung heutiger Cyberangriffe erfordert eine umfassende Sicht auf die von den Bedrohungsakteuren eingesetzten Taktiken und Tools. Diese Informationen zu generieren und die effektivsten Gegenmaßnahmen zu identifizieren, erfordert ständige Wachsamkeit und ein hohes Maß an Fachwissen. Mit Petabytes an aussagekräftigen Bedrohungsdaten, fortschrittlichen Machine Learning-Technologien und einem Pool weltweit agierender Experten unterstützt Sie Kaspersky mit der neuesten Threat Intelligence aus der ganzen Welt. So halten Sie Ihre Cyber-Immunität auch gegen bisher unbekannte Cyberangriffe aufrecht.

Ideal für

Großunternehmen

Regierungsbehörden

SOCs und Incident Response Teams

MSSPs

Geschäftsvorteile

Sofortige Bedrohungserkennung, um Unterbrechungen des Geschäftsbetriebs zu vermeiden

Minimierung potentieller finanzieller Verluste aus Sicherheitsvorfällen

Gewährleistung kosteneffektiver Investitionen in bestimmte Technologien und die richtigen Mitarbeiter anhand zeitnaher Informationen zu Bedrohungen für Ihr Unternehmen

Verhindert, dass Mitbewerber aufgrund des Verlusts von geistigem Eigentum einen Wettbewerbsvorteil erlangen können

Unterstützung beim Aufbau einer **vorausschauenden und anpassbaren Abwehr**

Anwendungsfälle

- Stärkung der Netzwerksicherheitslösungen durch fortlaufend aktualisierte **Threat Data Feeds**
- Effektive Priorisierung großer Mengen von Sicherheitswarnungen und anhand von **Threat Data Feeds** und **CyberTrace** sofortige Identifizierung der Warnungen, die an die Incident Response Teams eskaliert werden sollten
- Situationsbewusstsein in Echtzeit und effektivere Nutzung von Threat Intelligence Feeds mit **CyberTrace**
- Einblicke in die digitale Umgebung Ihres Unternehmens und Mindern der damit verbundenen Risiken dank **angepasstem Threat Intelligence Reporting**

Kaspersky Cybersecurity Training: Incident Response

Service

Sicherheitsschulungen sind angesichts der zunehmenden und sich ständig ändernden Bedrohungslage für Unternehmen unerlässlich. IT-Sicherheitsbeauftragte müssen in erweiterten Sicherheitstechniken ausgebildet werden, die eine wichtige Komponente des effektiven Bedrohungsmanagements und der Strategien zur Risikominimierung im Unternehmen bilden. Kaspersky Cybersecurity Training gibt Ihrem internen Sicherheitsteam das erforderliche Wissen an die Hand, um die sich ständig ändernde Bedrohungslandschaft zu bewältigen.

Ideal für

Großunternehmen

Regierungsbehörden

SOCs und Incident Response Teams

MSSPs

3 Erforderliche Kenntnisse

3 Anpassung und Skalierbarkeit

2 Kosten

Geschäftsvorteile

Schnelles und effektives Mindern der potentiellen Schäden aus Sicherheitsvorfällen und somit erhebliche Kostenreduzierungen

Vermeiden von Strafen und Bußgeldern durch den Gesetzgeber

Sorgt für ein anhaltend gutes Vertrauensverhältnis zu Ihren Kunden, Partnern und Investoren

Stärkung der Abwehrmaßnahmen gegen zukünftige Vorfälle durch Erfahrung

Anwendungsfälle

- Abgrenzung von APTs von anderen Bedrohungen
- Einblicke in unterschiedliche Angriffstechniken und die Anatomie zielgerichteter Angriffe
- Anwenden bestimmter Überwachungs- und Erkennungsmethoden
- Aufstellen effektiver Erkennungsregeln
- Rekonstruktion der Vorfallschronologie und -logik und Verfolgen des Workflows zur Vorfallsreaktion

3 Integrierter Cybersicherheitsansatz

Threat Management and Defense

Vorbereitung auf Angriffe auf APT-Ebene

Ideal für Unternehmen mit großer Erfahrung, die mit Threat Intelligence und Threat Hunting vertraut sind

- Komplexe und verteilte Umgebungen
- Internes Sicherheitsteam oder SOC
- Höhere Kosten von Vorfällen und Datenschutzverletzungen
- Nachweis von Compliance erforderlich

Services

- **Kaspersky Managed Protection**
- **Kaspersky Incident Response**

Kunden

- **Kaspersky Cybersecurity Training**

Intelligence

- **Kaspersky Threat Intelligence**

Kaspersky Threat Management and Defense

Kaspersky Threat Management and Defense ist eine spezielle Lösung, mit der ein umfassendes Framework zur schnellen Bedrohungserkennung, Vorfallsuntersuchung, Vorfallsreaktion und Vorfallsbeseitigung bereitgestellt wird. Dies umfasst globale Threat Intelligence, fortschrittliche Bedrohungserkennungs- und Reaktionstechnologien. Außerdem eine Reihe von Cybersicherheitsschulungen, fortlaufendes Threat Hunting und Reaktion auf Bedrohungen, die zum Ziel haben, die vorhandenen Sicherheitsschutzmaßnahmen zu umgehen. Die Lösung kann in Ihre aktuelle Betriebsstrategie integriert werden, um komplexe Bedrohungen abzuwehren, vorhandene Schutztechnologien zu ergänzen und Sie bei Bedarf durch umfassende Expertise zu unterstützen.

Ideal für

Großunternehmen

Regierungsbehörden

SOCs und Incident Response Teams

MSSPs

Geschäftsvorteile

Minimierung der finanziellen und betrieblichen Schäden von Cyberkriminalität und Aufrechterhalten eines stabilen Geschäftsbetriebs

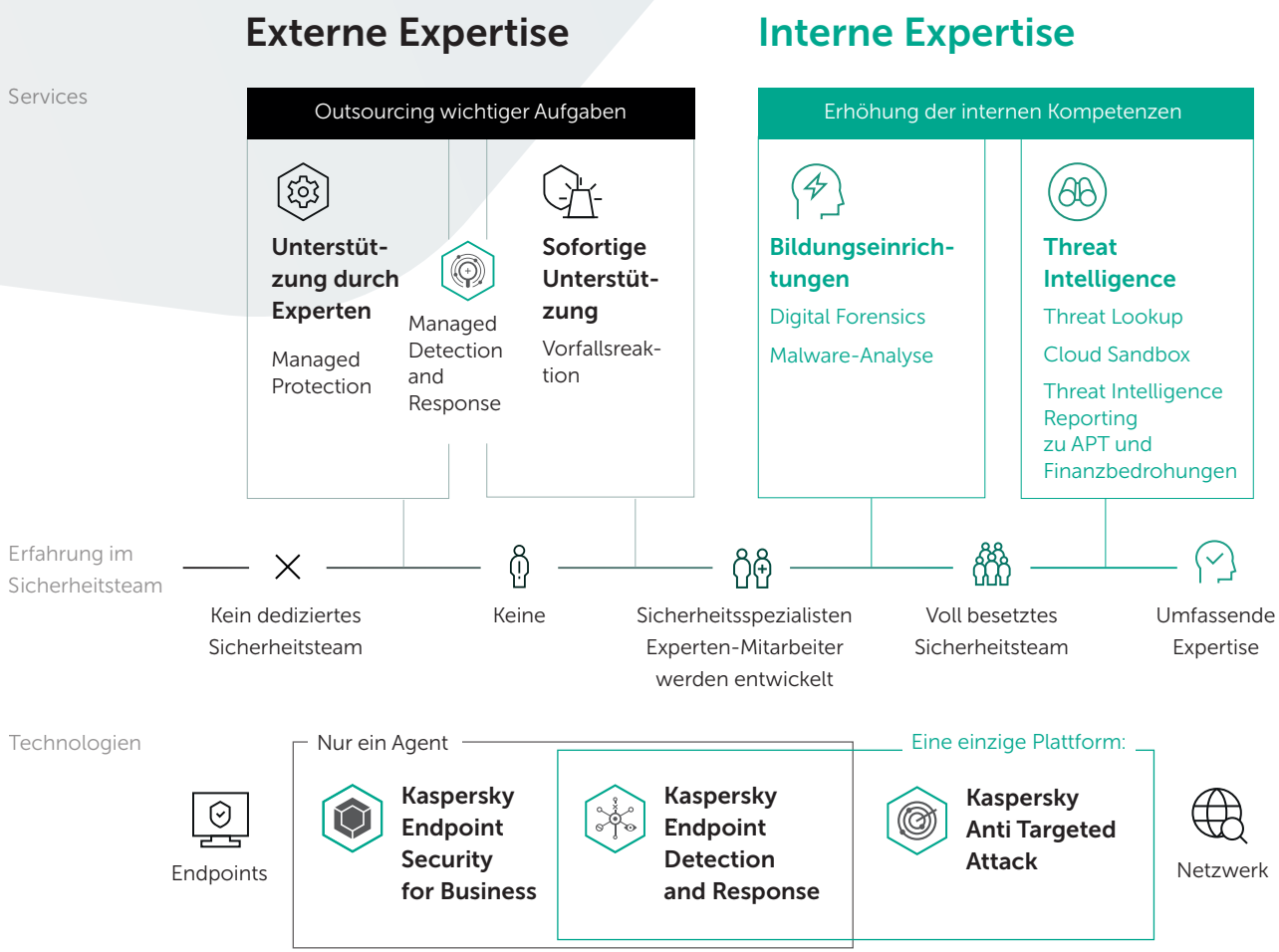
ROI-Steigerung durch nahtlose Automatisierung ohne Unterbrechung der Geschäftsabläufe

Geringere Mitarbeiterfluktuation und erhöhte betriebliche Effizienz durch Entwicklung interner Expertise

Bereitstellung umfassender und kosteneffektiver Informationssicherheitsstrategien anhand von angepassten Bedrohungsmodellen

Anwendungsfälle

- Automatisierung zeitaufwändiger Beweiserfassung und manueller Routineaufgaben anhand einer umfassenden Technologieplattform
- Funktionen zum Erkennen, Priorisieren, Untersuchen und Reagieren auf Bedrohungen durch proaktive Threat Intelligence
- Strategie zum Bedrohungsmanagement in Unternehmen durch Bereitstellung erweiterter Fähigkeiten
- Erkennen unbekannter und hoch entwickelter Bedrohungen, mit denen Präventionstechnologien umgangen werden sollen, durch Threat Hunting
- Zugriff auf Expertise von Drittanbietern für effektive Untersuchung und Reaktion auf komplexe Vorfälle


Externe Expertise
Interne Expertise
Services
Outsourcing wichtiger Aufgaben
Erhöhung der internen Kompetenzen
Unterstützung durch Experten
Managed Protection
Managed Detection and Response
Sofortige Unterstützung
Vorfallsreaktion
Bildungseinrichtungen
Digital Forensics
Malware-Analyse
Threat Intelligence
Threat Lookup
Cloud Sandbox
Threat Intelligence Reporting zu APT und Finanzbedrohungen
Erfahrung im Sicherheitsteam
Kein dediziertes Sicherheitsteam
Keine
Sicherheitsspezialisten
Experten-Mitarbeiter werden entwickelt
Voll besetztes Sicherheitsteam
Umfassende Expertise
Technologien
Nur ein Agent
Eine einzige Plattform:
Endpoints
Kaspersky Endpoint Security for Business
Kaspersky Endpoint Detection and Response
Kaspersky Anti Targeted Attack
Netzwerk

Aspekte, die es für eine langfristige Cybersicherheitsstrategie zu berücksichtigen gilt

Siloansatz bei der Cybersicherheit bedeutet geschäftliche Risiken

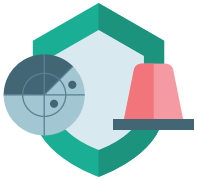
Aufgrund der steigenden Kosten bei Netzwerk- und Datenschutzverletzungen sind Unternehmen, die einen Wandel vornehmen wollen, starkem finanziellem Druck ausgesetzt. Deshalb ist das Thema Cybersicherheit heute so wichtig. Um in dieser Umgebung erfolgreich zu sein, muss die Cybersicherheit fester Bestandteil 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 und im Endergebnis müssen neue Prozesse und Maßnahmen zur Vorfallsbehandlung aufgestellt werden, damit ähnliche Angriffe in Zukunft verhindert werden können. Die vorhandenen Abwehrmaßnahmen müssen also fortlaufend verbessert werden.

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 und die jeweiligen Abwehrmaßnahmen 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 funktionieren. Auf diese Weise kann ein Cybersicherheitssystem geschaffen werden, das sich kontinuierlich an die neuen Herausforderungen für das Unternehmen anpasst und auf diese reagiert.

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.com/de/top3

Vielfach empfohlen

Kaspersky wurde erneut als „Gartner Peer Insights Customer's Choice for Endpoint Protection Platforms" mit einer hohen Kundenzufriedenheit von 4,6 von 5 ausgezeichnet (Stand: 28. Mai 2019).*

Äußerst transparent

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

*Gartner Peer Insights Customers' Choice umfasst die subjektiven Meinungen individueller Endnutzerrezensionen, -bewertungen und -daten, die mithilfe dokumentierter Methoden untersucht werden. Sie stellen weder die Ansichten noch eine Empfehlung von Gartner oder seinen Tochterunternehmen dar. Artikel auf der Website

Kontakt

Informationen zu Partnern in Ihrer Nähe finden Sie hier: https://www.kaspersky.de/partners
Kaspersky for Business: www.kaspersky.de/business
Enterprise Cybersecurity: www.kaspersky.de/enterprise
IT Security News: https://www.kaspersky.de/blog/b2b/
Unser einzigartiger Ansatz: www.kaspersky.de/true-cybersecurity

#bringonthefuture

www.kaspersky.de

kaspersky

Bring on the Future

www.kaspersky.de