kaspersky

Cybersecurity-Portfolio für Unternehmen

Kaspersky Security für kleine und mittelständische Unternehmen

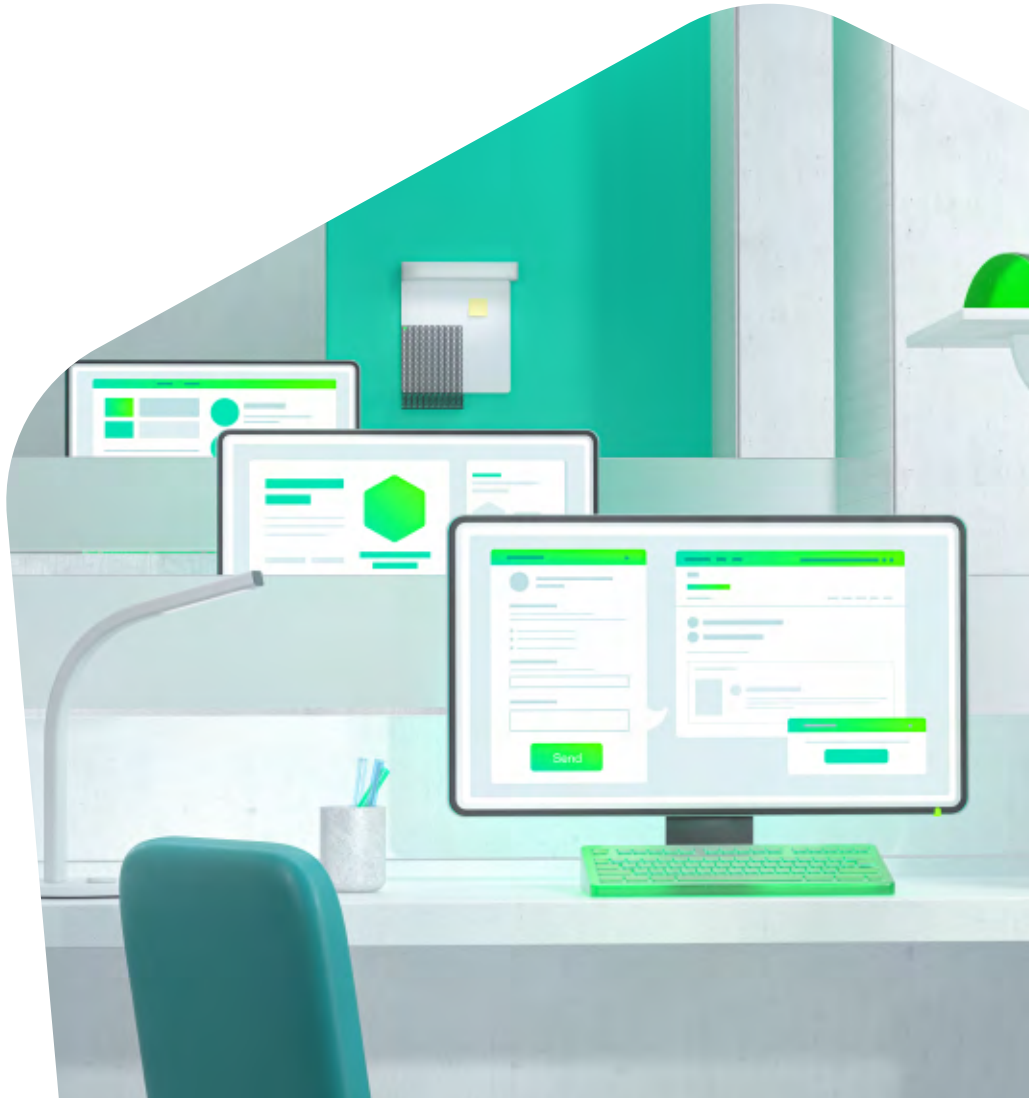
Herausforderungen für SMB

Cyberbedrohungen

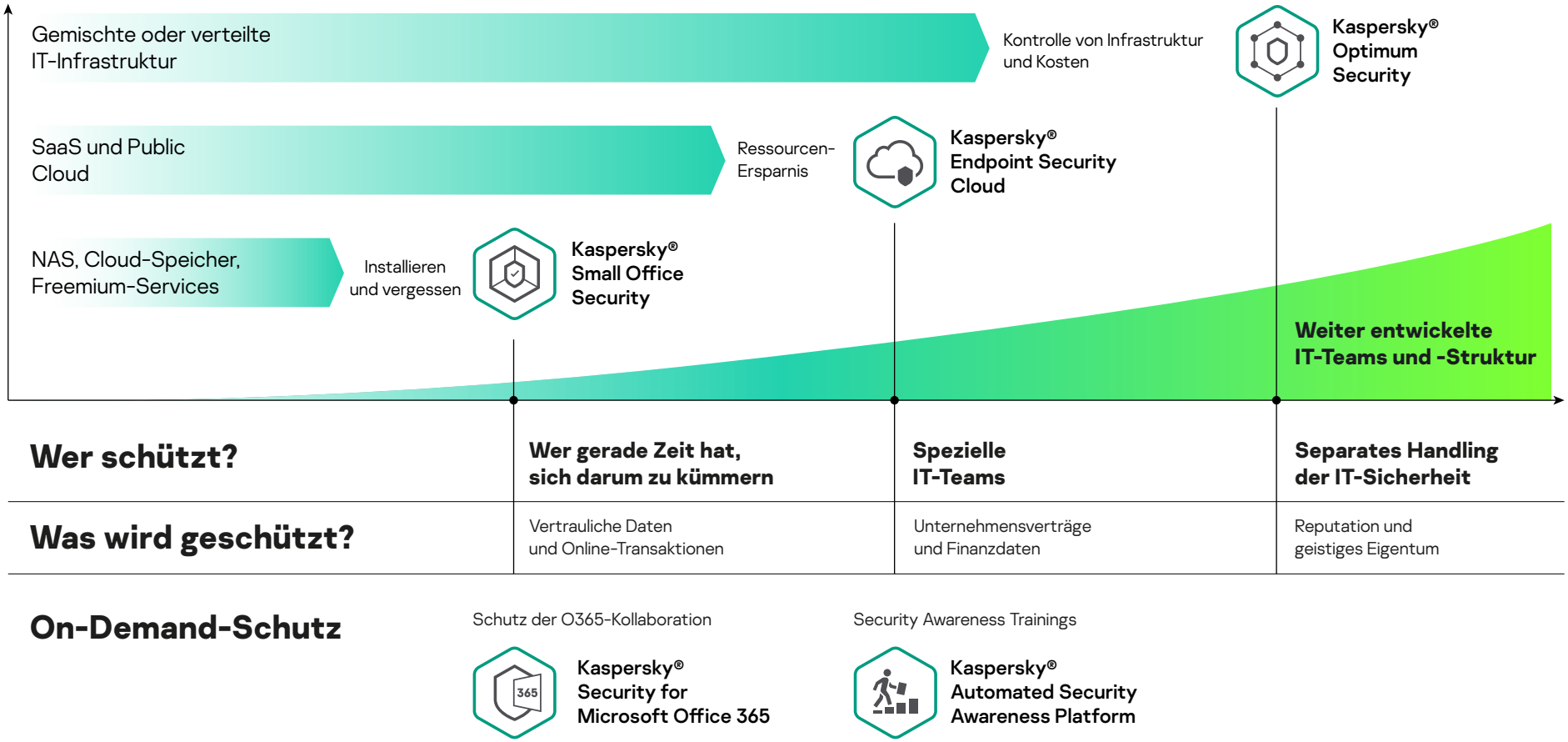
Nicht jede Lösung ist in jedem Unternehmen gleichermaßen einsetzbar. Kleinere Unternehmen kämpfen gegen die gleichen Cyberbedrohungen wie große Konzerne. Allerdings mangelt es ihnen oft an Ressourcen zur Bekämpfung.

Ressourcenüberlastung

Die richtigen Sicherheitslösungen machen überlasteten IT-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.



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



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

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

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

Schritte zur Erhöhung der Sicherheit in Organisationen vor 2020

Erstens

EPP[1] 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

EDR[2] 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 Cybersicherseitslösung 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

3 Erforderliche Kenntnisse

4 Anpassung und Skalierbarkeit

2 Investitionsumfang

Vorteile für Ihr Unternehme

- 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 unbekannten 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

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 unbekannten 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

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®

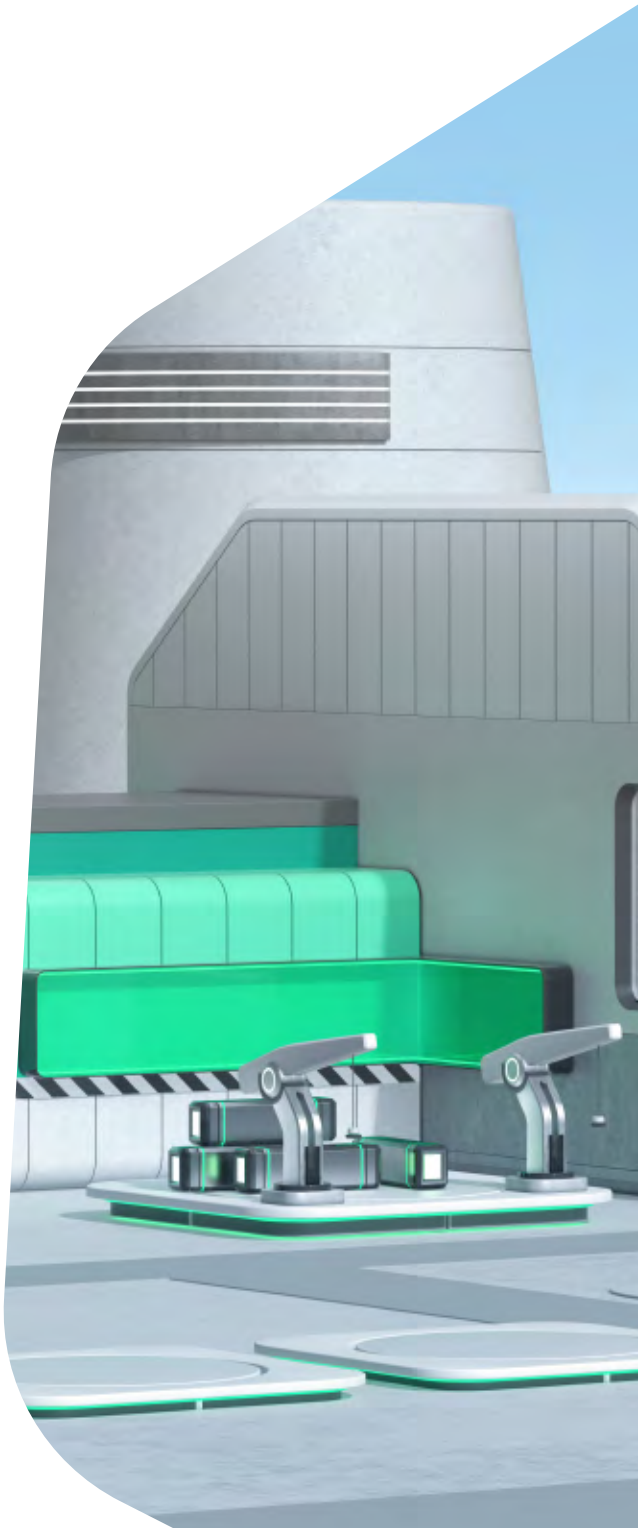
Praktische Anwendungen

- 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.

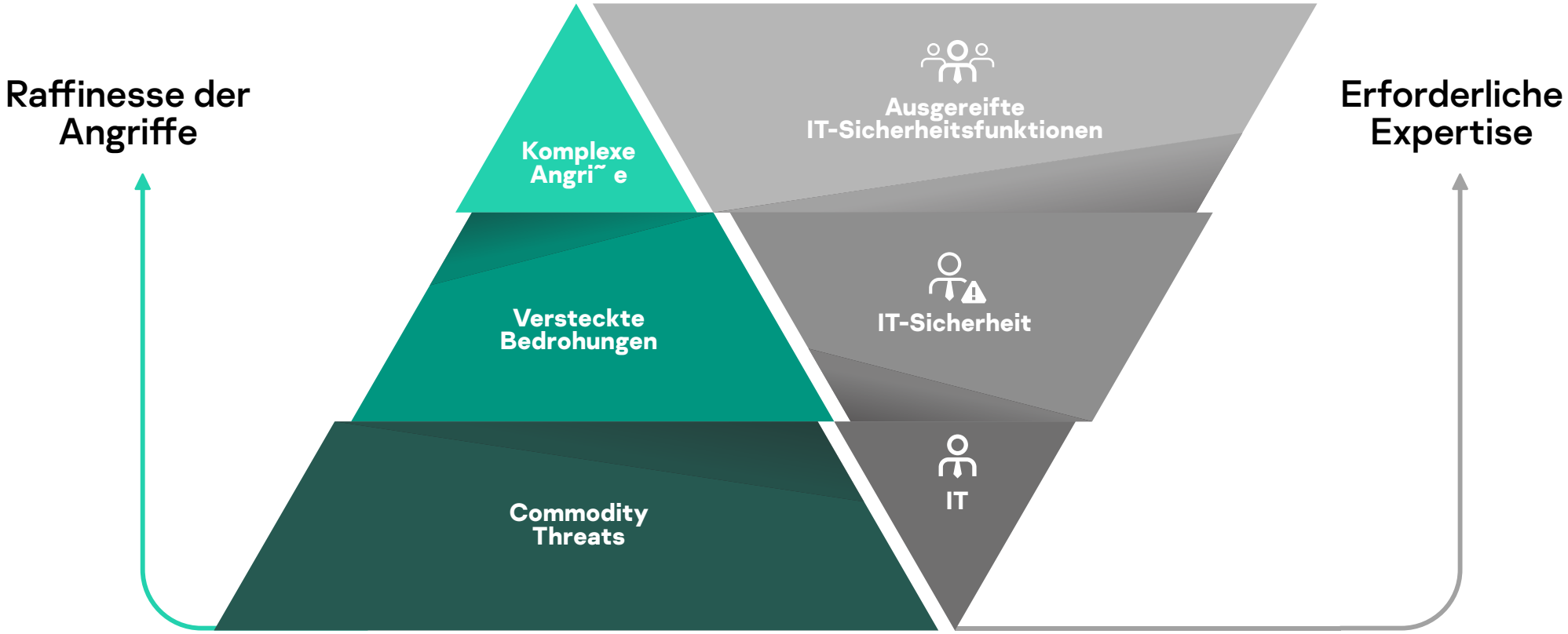
Kaspersky Security for Enterprise

Infos zum Kaspersky Enterprise-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 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 Sicherheitsfunktionen für alle Arten von Cyberbedrohungen. Selbst äußerst komplexe Angriffe werden erkannt, die Reaktion auf Vorfälle erfolgt schnell und angemessen, und zukünftige Bedrohungen können verhindert werden.



Expertise zur Abwehr unterschiedlicher Bedrohungsarten



Kurzfristige und langfristige Sicherheitsplanung

Herkömmlicher Prozess bei der Entwicklung von Sicherheitslösungen

Entscheidungsfindung:

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

Einsatz herkömmlicher Produkte:

- Endpoint Protection Platforms (EPP)
- Firewalls / Next Generation Firewalls (NGFW)
- Web Application Firewalls (WAF)
- Data Loss Prevention (DLP)
- Sicherheitsinformationen und Vorfallsmanagement-Systeme (SIEM)
- Weitere Produkte

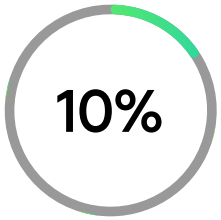
Eigenschaften

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

Gründe für das Versagen traditioneller Ansätze:

- Immer komplexere Bedrohungen und Bedrohungslage
- Komplexität von Cybersicherheits-Technologien
- Erfolgreicher digitaler Wandel im Unternehmen erfordert eine langfristige Cybersicherheitsstrategie

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.

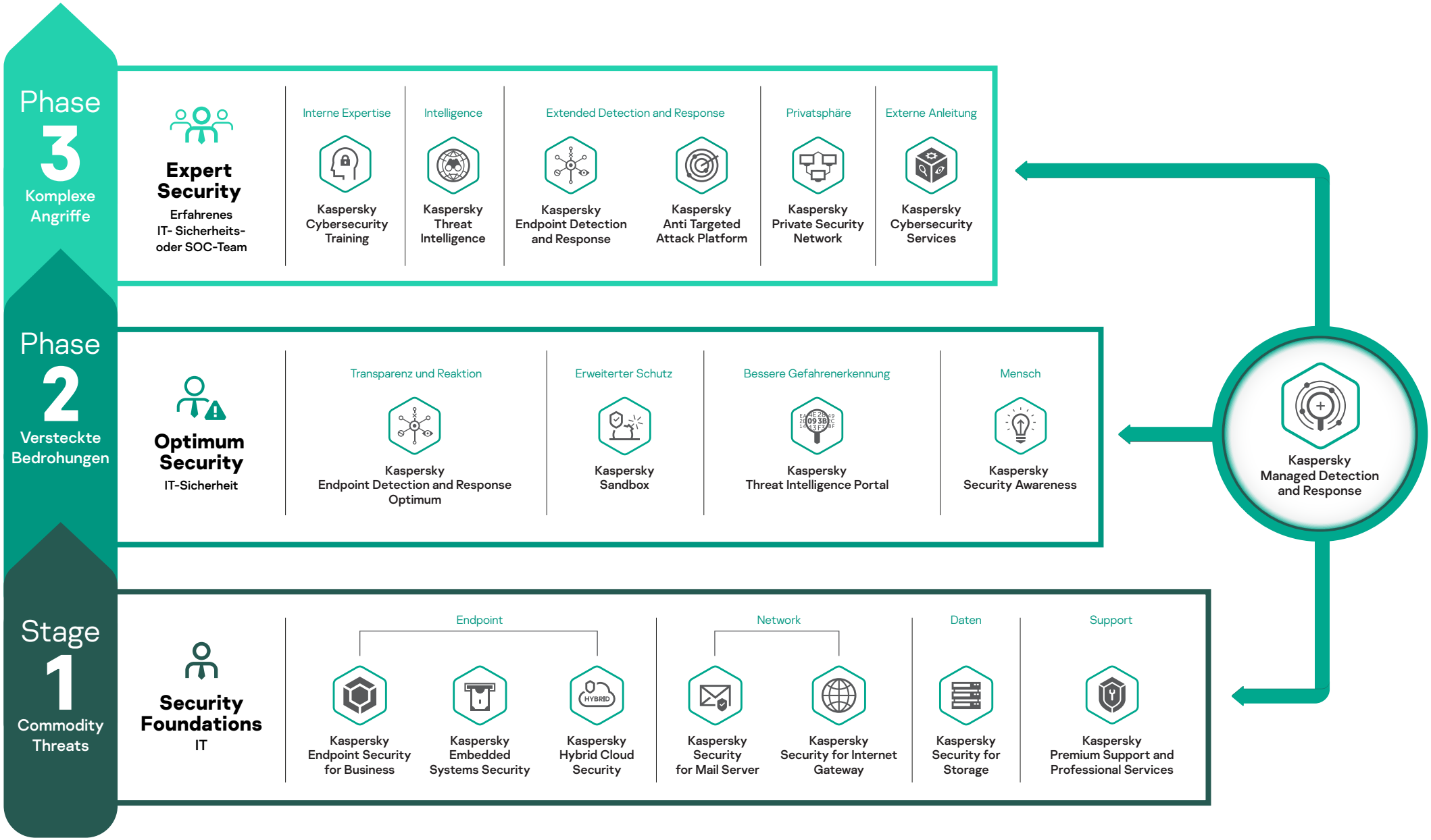


der Unternehmen ermitteln Angriffe fast sofort

Die zusätzlichen Kosten einer Datenschutzverletzung bei Entdeckung nach sieben Tagen

Quelle: Bericht „Wirtschaftlichkeit der IT-Sicherheit 2020“ von Kaspersky

Kasperskys Cybersicherheitskonzept – Schritt für Schritt



Phase 1
Security Foundations

Blockieren der maximal möglichen Anzahl von Bedrohungen

- Eine grundlegende Phase für Unternehmen aller Größen und Infrastruktur-Komplexität zum Aufbau einer integrierten Strategie zum Schutz vor komplexen Bedrohungen
- In der Regel ausreichend für kleinere Unternehmen mit reinen IT-Teams ohne IT-Sicherheitsexperten

Kaspersky Endpoint Security for Business

Der Ruf Ihres Unternehmens darf auf keinen Fall leiden. Deshalb leisten wir mehr als „nur“ Ihre Endpoints zu schützen und zu kontrollieren. Kaspersky Endpoint Security for Business schützt Ihr Unternehmen vor allen Arten von Bedrohungen, von BIOS- bis hin zu dateilosen Bedrohungen. Dank optimiertem Server-Schutz werden die Abwehrmaßnahmen bei Hochleistungsservern durch bestimmte Kontrollen gestärkt, die den Verlust von personenbezogenen Daten und Finanzinformationen verhindern. Wird im Hinblick auf flexibles Sicherheitsmanagement über die Cloud oder On-Premise bereitgestellt.

Für die folgenden Zielsetzungen geeignet:

- Verhindern, dass Mitarbeiter Ihr Unternehmen und sich selbst einem Angriff aussetzen
- Reduzieren der Anzahl von Endpoint-Vorfällen, die manuell verarbeitet werden müssen
- Schutz unterschiedlicher Umgebungen mit flexiblen und bewährten Verteidigungsmaßnahme

Ihre Vorteile

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

Praktische Anwendunge

- Reduzierte Angriffsrisiken mit der am häufigsten ausgezeichneten Technologie für den Endpoint-Schutz
- Patch Management für Ihre IT-Umgebung mit Management aus der Cloud oder einer On-Premise-Konsole
- Einfache und schnelle Migration von Drittanbieterlösungen
- Intuitives Einbinden neuer Technologien wie EDR und anderer Funktionen ohne Neuinstallation auf den Endpoints
- Schutz Ihrer Daten unter Erfüllung von Compliance-Vorgaben durch integrierte Verschlüsselungsverwaltung, einschließlich Löschen per Fernzugriff und Gerätekontrolle für verschiedene BS

Kaspersky Hybrid Cloud Security

Kaspersky Hybrid Cloud Security vereinfacht und schützt den digitalen Wandel in Ihrem Unternehmen durch Virtualisierung oder Verlagern von Workloads in die Cloud. Die patentierte Light-Agent-Technologie verringert die Auslastung von Hypervisor-Ressourcen erheblich.
Die native Integration mit einer Vielzahl von Virtualisierungs-, Container- und Public-Cloud-Plattformen bietet Transparenz und Kontrolle innerhalb der gesamten Infrastruktur. Eine umfassende Reihe von Sicherheitstechnologien, die über dieselbe Konsole verwaltet werden, sorgt für ein optimiertes Risikomanagement in unterschiedlichen

Für die folgenden Zielsetzungen geeignet:

- Virtualisierung von Server- und Desktop-Workloads
- Verschieben oder Managen von Infrastrukturen in Public Clouds (IaaS)
- Integration von Sicherheitsfunktionen in Entwicklungsteam-Pipelines
- Sichere Nutzung der Containerisierung

2 Erforderliche Kenntnisse

5 Anpassung und Skalierbarkeit

2 Investitionsumfang

Ihre Vorteile

- Minimierte finanzielle Verluste und Rufschädigung durch reduzierte Angriffsfläche und Verweildauer des Angreifers
- Optimierte IT-Kosten durch Freisetzen von bis zu 30 % der Hypervisor-Ressourcen
- Unterstützung von Compliance durch Einhaltung zentraler Sicherheitsanforderungen
- Sicherstellen einer effizienten Zusammenarbeit zwischen IT-, Informationssicherheits- und Entwicklungsteams, daher weniger Risiken und Sicherheitslücken

Praktische Anwendungen

- Transparenz und Kontrolle über alle Rechenzentren und Cloud-Bereitstellungen hinweg
- Sicherheit für VMWare und Citrix VDI
- Schutz für Cloud-Workloads für AWS-, Azure- und Google Cloud-Instanzen mit automatischer Bereitstellung und konstanter Transparenz durch native API-Integration
- Sicherheit für Entwicklungsteams durch Container-Schutz, Integrationsschnittstellen für Pipelines und Management-API

Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security ist eine spezielle, mehrstufige Lösung zum Schutz von Windows-basierten eingebetteten Geräten sowie älteren Endpoints auf nicht mehr unterstützten Betriebssystemen. Programmkontrolle wird mit optionalem Malware-Schutz kombiniert, einschließlich Exploit Prevention sowie Schutz vor Netzwerkbedrohungen, Integritätsüberwachung und weiteren, auf Ihre Prozesse und Gerätefunktionen angepassten Sicherheitsebenen.

Für die folgenden Zielsetzungen geeignet:

- Schutz für ATMs, PoS-Systeme, medizinische Geräte oder andere nicht-branchengängige eingebettete Systeme
- Optimierte Sicherheit für Systeme, auf denen veraltete Hardware und Betriebssysteme ausgeführt werden (einschließlich veralteter Endpoints)
- Integration der Sicherheit Ihrer eingebetteten Infrastruktur in das Sicherheits-Ökosystem von Kaspersky

Ihre Vorteile

- Unterbrechungsfreie Geschäftsprozesse in Bereichen, in denen die finanziellen, rechtlichen und rufbezogenen Auswirkungen eines Angriffs verheerend sein könnten
- Upgrades sind nicht mehr zwingend notwendig, da ältere und aktuell nicht ersetzbare Endpoints beliebig lange genutzt werden können
- Umfassende Compliance durch zuverlässige Schutzmechanismen, einschließlich der von den Aufsichtsbehörden empfohlenen

Praktische Anwendungen

- Konfigurieren eines möglichst effektiven Sicherheitssystems anhand unterschiedlicher Sicherheitsebenen und -szenarien im Hinblick auf Nutzung und Kapazitäten
- Langfristiger und müheloser Schutz für Bereiche, in denen häufige Wartungsvorgänge unmöglich sind
- Verhindern von Insider-Angriffen – eines der Hauptrisiken bei eingebetteten Geräten, die nicht über E-Mail oder das Internet angegriffen werden können.
- Schutz von Geräten mit schlechter Internetverbindung

Kaspersky Security for Mail Server

Kaspersky Security for Mail Server verhindert, dass E-Mail-basierte Bedrohungen wie Crimeware, Ransomware, Phishing und Spam bis zu Ihren Endpoints durchdringen, an denen die meisten Malware-Programme und Social-Engineering-Betrugsmaschen eingesetzt werden. Die Cloud-basierte KI-Implementierung sowie On-Premise-Modelle für maschinelles Lernen sorgen für hohe Erkennungsraten mit äußerst niedrigen False Positives und bieten Schutz vor ausgeklügelten E-Mail-Bedrohungen, darunter Business Email Compromise (BEC). Spam-Nachrichten werden blockiert, noch bevor sie Schaden anrichten.

Für die folgenden Zielsetzungen geeignet:

- Verstärkter Schutz vor Massen- und zielgerichteten Angriffen über E-Mail
- Abdeckung zahlreicher E-Mail-Sicherheitsszenarien auf unterschiedlichen Plattformen und Bereitstellungsschemas

3 Erforderliche Kenntnisse

4 Anpassung und Skalierbarkeit

2 Investitionsumfang

Ihre Vorteile

- Weniger Störungen durch Malware- und Social Engineering-Angriffe über E-Mail
- Erhöhte Mitarbeiterproduktivität durch Eliminieren von Ablenkungen durch Spam
- Reduzierte Workloads für IT-/IT-Sicherheitsteams und optimierte Betriebskosten
- Minimiertes Risiko von rechtlichen Problemen und Rufschädigung durch Kontrolle der E-Mail-Inhaltsübertragung

Praktische Anwendungen

- Stärkung des Infrastruktur-Schutzes auf Ebene des E-Mail-Servers durch Blockieren von Bedrohungen bevor sie Benutzer und Endpunkte erreichen
- Erhöhung der vorhandenen Gateway-Sicherheit ohne zusätzliche False Positives
- Festigung Ihrer Kaspersky Threat Detection-Funktionen durch zusätzlichen Kontext und automatisierte Reaktionsfunktionen auf Gateway-Ebene

Kaspersky Security for Internet Gateway

Kaspersky Security for Internet Gateway mit dem Kernprogramm Kaspersky Web Traffic Security bietet zuverlässigen Schutz vor webbasierten Cyberbedrohungen auf Gateway-Ebene. Darunter Malware, Ransomware, Miner, Online-Phishing und schädliche Webressourcen. Mit dieser Software können Sie auch die Nutzung des World Wide Web kontrollieren und gemäß den Unternehmensrichtlinien den Zugriff auf bestimmte Webressourcen sowie die Übertragung bestimmter Dateitypen einschränken.

Für die folgenden Zielsetzungen geeignet:

- Verhindern, dass sich web-basierte Bedrohungen auf Ihre Endpoints auswirken
- Verringern des Risikos von Virenbefall und Kontrolle der Internetnutzung
- Reduzieren der Workloads von IT-/IT-Sicherheitsteams durch automatisches Blockieren web-basierter Bedrohungen bereits am Einstiegspunkt

Ihre Vorteile

- Minimierte Störungen des Geschäftsbetriebs und weniger Sicherheitsvorfälle innerhalb des Netzwerks
- Erhöhte Effizienz bei IT-/IT-Sicherheitsteams und optimierte Betriebskosten
- Schutz des Unternehmens vor Social Engineering-Bedrohungen online
- Kontrolle des Onlinezugriffs auf bestimmte Webressourcen

Praktische Anwendungen

- Gestärkter Endpoint-Schutz auf Gateway-Ebene
- Ergänzung und Stärkung der vorhandenen Sicherheit von Web-Gateways ohne Erhöhung von False Positives
- Schutz von Geräten, die aus Geschäfts- oder Auslastungsgründen auf Endpoint-Ebene nicht umfassend geschützt werden können
- Festigung Ihrer Kaspersky Threat Detection-Funktionen durch zusätzlichen Kontext und der Möglichkeit für eine automatisierte Reaktion auf Gateway-Ebene

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.

Für die folgenden Zielsetzungen geeignet:

- Schutz vernetzter Speicher vor externen Angriffen und Virenausbreitung
- Schutz wertvoller Daten auf vernetzten Speichern vor Ransomware-Angriffen
- Management der Storage-Sicherheit sowie der von Kaspersky geschützten Endpoints und Server

Ihre Vorteile

- Geschäftskontinuität durch Verhindern von Malware-Infektionen über Datenspeicher
- Einfachere Compliance und zuverlässiger Schutz für regulierte Datenspeicher
- Weniger Bedienungsaufwand durch zentrales Management mit anderen Lösungen von Kaspersky für Endpoint- und Serverschutz

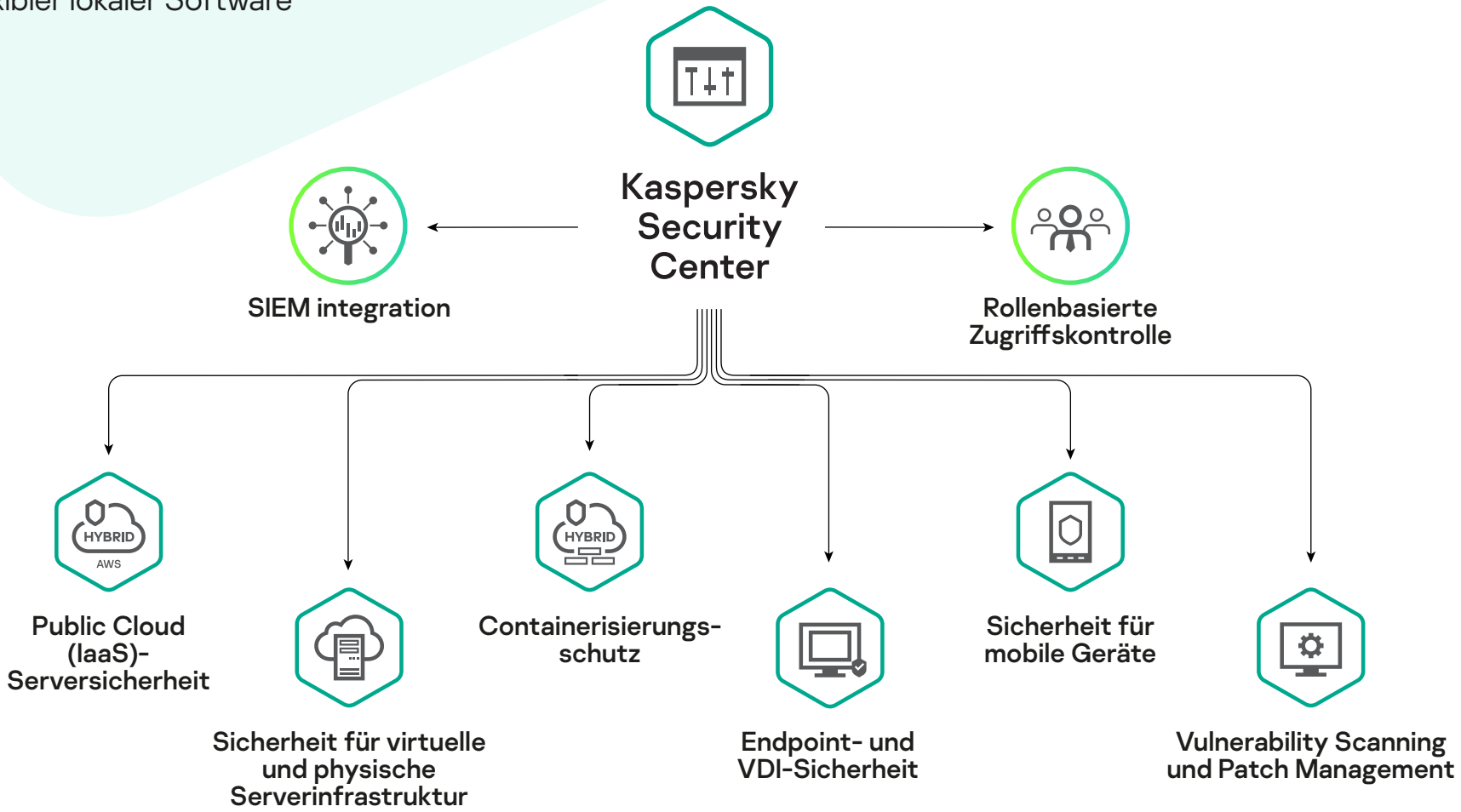
Praktische Anwendungen

- Schutz von NAS, DAS oder SAN oder einer beliebigen Kombination dieser Speicher in Ihrer Infrastruktur
- Schutz der für die Sicherheitslösung eingesetzten Datenspeicher und Server mit einem Produkt
- Verhindern von Datenverlust durch Remote-Ausführung von Cryptors

Zentrales Sicherheitsmanagement

Kaspersky Security Center für das Management unterschiedlicher Workloads und eine richtlinienbasierte Kontrolle, bereitgestellt als:

- Skalierbare SaaS
- Flexibler lokaler Software



Kaspersky Premium Support (MSA)

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 schnell wie möglich zu beheben.

Für die folgenden Zielsetzungen geeignet:

- Sie haben die Gewissheit, dass Ihre IT-Systeme geschützt sind, und das nicht nur durch zuverlässige Sicherheitstechnologien, sondern auch durch die Expertise und den Einsatz der weltweit anerkannten Spezialisten von Kaspersky

Ihre Vorteile

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

Praktische Anwendungen

- Direkte Weiterleitung Ihres Problems an Experten, die darauf spezialisiert sind, schnellstmöglich die richtige Lösung zu finden
- Durchgängiger Schutz dank proaktiver, auf Ihr System zugeschnittener Maßnahmen
- Weniger Zeitaufwand für Ihre internen Teams bei Wartung und Fehlerbehebung

Kaspersky Professional Services

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. IT-Infrastruktur

Für die folgenden Zielsetzungen geeignet:

- Beschleunigung, Optimierung und Anpassung Ihrer Kaspersky-Lösung im Hinblick auf die effektivsten Cybersicherheitspraktiken

Ihre Vorteile

- Maximierter ROI für Ihre Sicherheitslösungen, weil sie immer voll einsatzfähig sind
- Kostensenkungen bei internen IT-Mitarbeitern
- Minimierte Auswirkungen bei der Implementierung der neuen Sicherheitslösung auf das Tagesgeschäft und Senkung der Gesamtkosten für die Implementierung
- Schnellere und effektivere Bearbeitung kritischer Vorfälle

Praktische Anwendungen

- Geringere Implementierungsrisiken, die sich möglicherweise negativ auf den Schutz auswirken, die Produktivität beeinträchtigen und sogar zu Ausfallzeiten führen
- Reduzierte Ausfallzeiten durch regelmäßige Audits der Produktkonfigurationen, sodass immer die aktuellsten Abwehrmechanismen verfügbar sind
- Kürzere Produkteinführungszeiten, sodass die Vorteile der Software sofort genutzt werden können

Phase 2
Optimum Security

Fortschrittliche Erkennungstechnologien und zentrale Reaktion

Ermöglicht kleineren Cybersicherheitsteams den Umgang mit Bedrohungen, die die automatische Prävention umgehen – mit einer ressourcenoptimierten, organisch von Security Foundations aus aufgebauten Lösung.

Kaspersky Endpoint Detection and Response Optimum

Kaspersky Endpoint Detection and Response (EDR) Optimum bietet Unternehmen grundlegendes Cybersicherheits-Know-how, um eine Reihe versteckter Bedrohungen zu bewältigen. Die Lösung umfasst die Schutzfunktionen von Kaspersky Endpoint Security for Business – Advanced und wird über das Kaspersky Security Center gemanagt. Das Produkt bietet ein benutzerfreundliches Toolkit anhand einer vereinfachten Ursachenanalyse, IoC (Gefährdung-sindikatoren)-Scans und automatische oder Einzelklick-Maßnahmen.

Für die folgenden Zielsetzungen geeignet:

- Erhöhung der Bedrohungstransparenz an allen Endpoints
- Verkürzung der MTTR (mittlere Zeit bis zur Reaktion)
- Optimierung von IT-Sicherheitsressourcen und Steigerung der Effizienz

3 Erforderliche Kenntnisse

4 Anpassung und Skalierbarkeit

3 Investitionsumfang

Ihre Vorteile

- Minimiertes Risiko finanzieller Schäden sowie Rufschädigungen durch Bedrohungen, die den präventiven Schutz umgehen
- Optimierte Mitarbeiter-Workloads und Ressourcennutzung durch straffere Workflows und Automatisierungsfunktionen
- Gesteigerte Effizienz durch ein kostenbewusstes, benutzerfreundliches und einfach zu erlernendes Tool, das keine umfassende Expertise erfordert

Praktische Anwendungen

- Genaue Einblicke in Endpoint-Sicherheitsbenachrichtigungen
- Eingehendere Analyse der am Host erkannten Bedrohungen, um Umfang und Ursache zu bestimmen
- Erkenntnisse zur aktuellen Bedrohungslage des Unternehmens durch Suchen nach von Dritten importierten IoCs
- Automatische Reaktion bei erkannten Bedrohungen oder während der Untersuchung mit nur wenigen Klicks

Kaspersky Managed Detection and Response Optimum

Kaspersky Managed Detection and Response Optimum bietet Ihnen durch schnelle und skalierbare Bereitstellung eine sofort ausgereifte IT-Sicherheitsfunktion, ohne dass in zusätzliche Mitarbeiter oder Expertise investiert werden muss. Patentierte maschinelle Lernmodelle, herausragende, ständig aktualisierte Threat Intelligence und automatisiertes Threat Hunting anhand proprietärer Angriffsindikatoren (IoA) sorgen dafür, dass Ihr Unternehmen fortlaufend vor komplexen Bedrohungen geschützt ist.

Für die folgenden Zielsetzungen geeignet:

- Einrichtung und Verbesserung bei frühzeitiger effektiver Bedrohungserkennung und -reaktion durch unterbrechungsfreie Überwachung
- Reduzieren der Anfälligkeit Ihres Unternehmens für hochentwickelte Bedrohungen, ohne dass Ihr eigenes Sicherheitsteam viel Zeit auf das Erlernen neuer Fähigkeiten und Lösungen aufwenden muss

Ihre Vorteile

- Die Gewissheit, dass Sie jederzeit vor den neuesten Bedrohungen geschützt sind
- Geringere Gesamtkosten für die Sicherheit, ohne eine ganze Riege von eigenen Sicherheitsexperten einstellen und schulen zu müssen

Praktische Anwendungen

- Schützen mit System
  durch automatische Prävention, Erkennung und Reaktion bei Bedrohungen für Ihre Netzwerke
- Schnelle Reaktion auf Vorfälle mit umfassender Kontrolle aller Abwehrmaßnahmen
- Umfassender Echtzeiteinblick in alle Erkennungsaktionen, die betroffenen Ressourcen und ihr aktueller Schutzstatus

Kaspersky Sandbox

Kaspersky Sandbox schützt automatisch vor neuen und unbekannten Bedrohungen, die den Endpoint-Schutz umgehen. Die Lösung ergänzt Kaspersky Endpoint Security for Business und unterstützt Unternehmen dabei, den Schutz ihrer Endpoints und Server vor bisher unbekannter Malware, neuen Viren und Ransomware, Zero-Day-Exploits und anderen Bedrohungen erheblich zu erhöhen, ohne neue IT-Sicherheitsanalysten einstellen zu müssen.

Für die folgenden Zielsetzungen geeignet:

- Bessere Verteidigung bei versteckten Bedrohungen
- Automatisierung hochentwickelter Erkennungsmaßnahmen
- Optimierung von Mitarbeiter-Workloads und erforderlicher Expertise

1 Erforderliche Kenntnisse

3 Anpassung und Skalierbarkeit

2 Investitionsumfang

Ihre Vorteile

- Reduziertes IT-Sicherheitsrisiko und erhöhte Geschäftskontinuität
- Schutz vor bekannten und unbekannten Bedrohungen ohne Einbußen bei Endpoint-Performance oder Benutzerproduktivität
- Minimierte Arbeitskosten durch Automatisierung manueller Vorgänge
- Kostenoptimierung beim Schutz vor hochentwickelten Bedrohungen in Zweigstellen

Praktische Anwendungen

- Vereinfachung tiefgehender dynamischer Analysen und Erkennung unbekannter und versteckter Bedrohungen
- Automatische Abwehr auf allen geschützten Endpoints
- Vermeiden von Auswirkungen auf die Produktivität und erhöhte Sicherheit für stark ausgelastete Endpoints durch Auslagern der ressourcenintensiven Verhaltensanalyse an die Sandbox
- Integration mit Drittanbieter-Lösungen über eine API
- Reduzieren von Arbeitsstunden dank einfacher Installation und vollständig automatischer Funktionsweise der Sandbox, ohne dass geschulte IT- oder Cybersicherheits-Experten erforderlich sind

Kaspersky Threat Intelligence Portal

Das Kaspersky Threat Intelligence Portal bietet Ihnen unser gesamtes Wissen zu Cyberbedrohungen in einem einzigen, leistungsstarken Webservice. Sie können verdächtige Bedrohungsindikatoren wie Dateien, Datei-Hashes, IP-Adressen oder URLs überprüfen. Objekte werden im Portal mittels verschiedener Technologien zur Bedrohungserkennung analysiert, z. B. Reputationsanalysen über das Kaspersky Security Network, strukturelle maschinelle Lernmodelle und erweiterte dynamische Erkennung über die Kaspersky Cloud Sandbox. Dabei wird ermittelt, ob ein Objekt in den Bereich „Gut“, „Schlecht“ oder „Nicht kategorisiert“ fällt. Anhand von Kontextdaten können Sie Bedrohungen besser priorisieren und effektiver darauf reagieren.

Für die folgenden Zielsetzungen geeignet:

- Kostenloser Zugang zu einer vertrauenswürdigen Quelle für Bedrohungsinformationen
- Effektivere Priorisierung von Vorfällen
- Schnellere Untersuchung und Bedrohungserkennung

3 Erforderliche Kenntnisse

4 Anpassung und Skalierbarkeit

0 Investitionsumfang

Ihre Vorteile

- Vermeiden kostspieliger Programme für kommerzielle Threat Intelligence
- Effektiver Schutz Ihrer Netzwerke durch zeitnahen Zugriff auf überprüfte Daten

Praktische Anwendungen

- Validierung/Priorisierung, welche Alarme oder Vorfälle basierend auf Auswirkungen und Risikoniveaus reale Bedrohungen darstellen
- Sofortige Erkennung, welche Warnmeldungen an das Vorfallsreaktionsteam weitergeleitet werden sollten
- Herausfiltern echter Bedrohungen aus der Masse und Bestimmen, wo Ressourcen für die Vorfallsreaktion konzentriert werden sollen
- Informationen zu einer bestimmten Beobachtung oder einem bestimmen Angriff finden, ohne komplizierte Suchen in verschiedenen Datenbanken durchführen zu müssen
- Aufspüren zuvor unentdeckter Bedrohungen

Kaspersky Security Awareness

Kaspersky Security Awareness ist eine Zusammenstellung computerbasierter interaktiver Schulungsprogramme zur Verbesserung der Sicherheitskompetenzen von Mitarbeitern. Sie werden motiviert, in allen Unternehmensbereichen sichere Verfahren einzuführen. Das Programm umfasst Folgendes:

- Kaspersky Interactive Protection Simulation & CyberSafety Management Games – für Engagement und Motivation
- Interaktives Assessment Tool – um den richtigen Startpunkt zu bestimmen
- Online Learning Platform & Cybersecurity for IT Online – um praktische Fähigkeiten zu erwerben
- [dis]connected – ein Videospiel zur Festigung der neu erlernten Fähigkeiten.

Für die folgenden Zielsetzungen geeignet:

- Reduzieren der Anzahl von Vorfällen, die auf Unwissen oder Nachlässigkeit von Mitarbeitern zurückzuführen sind
- Entwickeln eines guten Bewusstseins für Cybersicherheitsmaßnahmen bei Mitarbeitern auf allen Ebenen
- Einführen einer starken Cybersicherheitskultur im Unternehmen dank vorgefertigter Lösungen

Ihre Vorteile

- Reduzierung der Anzahl durch Menschen verursachter Sicherheitsvorfälle im Hinblick auf bessere Geschäftskontinuität und Beschränken der Auswirkungen von Vorfällen
- Engagement und Lernanreiz bei Mitarbeitern bei gleichzeitiger Unterstützung von Cybersicherheitsmaßnahmen und -initiativen durch die Geschäftsleitung
- Verbesserte Cybersicherheitskultur im ganzen Unternehmen

Praktische Anwendungen

- Bereitstellung von Fähigkeiten und Expertise zur Einführung und Aufrechterhaltung sicherer Verhaltensweisen
- Fördern des richtigen Umgangs mit Cybersicherheitsproblemen
- Befähigen von Mitarbeitern, bei der täglichen Arbeit bessere Ergebnisse zu erzielen, ohne das Unternehmen Cybersicherheitsrisiken auszusetzen

2 Erforderliche Kenntnisse

4 Anpassung und Skalierbarkeit

3 Investitionsumfang

Phase 3
Expert Security

Vorbereitung auf komplexe, APT-ähnliche Angriffe

Konzentration auf erweiterte Abwehrmaßnahmen anhand von Threat Intelligence, Unterstützung durch Experten und Wissenstransfer, sodass erfahrene IT-Sicherheitsteams komplexe Bedrohungen und gezielte Angriffe bewältigen können.

Kaspersky Endpoint Detection and Response

EDR-Tool mit leistungsstarken Funktionen für IT-Sicherheitsexperten, das umfassende Transparenz, erstklassige Threat Detection und effiziente Analysen sowie schnellen Zugriff auf die erfassten Daten ermöglicht. Der Untersuchungsvorgang beruht auf retrospektiver Analyse, proprietären Angriffsindikatoren (IoAs) und MITRE ATT&CK-Mapping sowie proaktivem Threat Hunting und Zugang zu Kaspersky Threat Intelligence. Erkennen Sie die gesamte Abfolge von Gefährdungen sowie mehrstufige komplexe Angriffe auf Endpoints und reagieren Sie angemessen und schnell.

Für die folgenden Zielsetzungen geeignet:

- Stärkung des Endpoint-Schutzes
- Verbesserung der internen Incident Response-Fähigkeiten bei Reduzierung der Zeit bis zur Erkennung (MTTD) und der Zeit bis zur Reaktion (MTTR)
- Fördern von proaktiven Threat-Hunting-Vorgängen

4 Erforderliche Kenntnisse

3 Anpassung und Skalierbarkeit

4 Investitionsumfang

Ihre Vorteile

- Erleichterte Überwachung Ihrer wichtigsten Ressourcen
- Mindern von Cybersicherheitsrisiken und finanziellen/betrieblichen Schäden durch Vorfälle an Endpoints
- Reduzierte Betriebskosten für die IT-Sicherheit durch vereinfachte Endpoint-Vorfallsanalyse und -reaktion
- Sicherstellen von Compliance mit gesetzlichen Anforderungen

Praktische Anwendungen

- Effektive Erkennung (mit bewährten Fähigkeiten durch MITRE-Beurteilung) und schnelle Reaktion auf hochentwickelte Angriffe auf Endpoint-Ebene
- Nachträgliche Analysen und effektive Untersuchungen zentral zusammengestellter Daten
- Zentrales Vorfallsmanagement mit geführten Untersuchungen und Reaktionen
- Aufspüren versteckter Bedrohungen mit automatisierten und proaktiven Threat Hunting-Funktionen
- Als Teil der Kaspersky Anti Targeted Attack Platform bietet Kaspersky EDR eine erweiterte Lösung zur Bedrohungserkennung und -reaktion

Kaspersky Anti Targeted Attack Platform

Kaspersky Anti Targeted Attack Platform vereint erweiterte Bedrohungserkennung auf Netzwerkebene und EDR-Funktionen. Die Plattform fungiert als Extended Detection and Response-Lösung, die einen umfassenden APT-Schutz auf Grundlage unserer Threat Intelligence bietet und dem MITRE-ATT&CK-System zugeordnet ist. Ihre IT-Sicherheitsexperten erhalten alle erforderlichen Tools, um erweiterte, multidimensionale Bedrohungen zu erkennen, effektiv zu untersuchen, proaktiv nach Bedrohungen zu forschen und schnell eine zentrale Reaktion bereitzustellen – und all das mit einer einzigen Lösung.

Für die folgenden Zielsetzungen geeignet:

- Aufbau umfassender Abwehrmaßnahmen für äußerst ausgeklügelte Angriffe mit einem einzigen, leistungsstarken System
- Umfassende Transparenz im gesamten Unternehmen
- Reduzieren von MTTD und MTTR
- Stärkung Ihres Security Operations Center
- Verbesserte Sicherheitsstellung unter Schutz der Privatsphäre

5 Erforderliche Kenntnisse

3 Anpassung und Skalierbarkeit

5 Investitionsumfang

Ihre Vorteile

- Geminderte Cybersicherheitsrisiken und reduzierte finanzielle, betriebliche und Rufschäden aufgrund von komplexen zielgerichteten Angriffen
- Reduzierte IT-Sicherheitskosten durch Optimierung und Automatisierung des Vorfallsmanagements
- Sicherstellen von Compliance mit gesetzlichen Anforderungen

Praktische Anwendungen

- Schutz mehrerer potentieller Einstiegspunkte für Bedrohungen auf Netzwerk- und Endpoint-Ebene
- Schnelle Erkennung hochentwickelter Bedrohungen, die vorhandene präventive Technologien umgehen
- Aufspüren versteckter Bedrohungen mit automatisierten und proaktiven Threat Hunting-Funktionen
- Bereitstellen zeitnaher Informationen zu erkannten Bedrohungen an das IT-Sicherheitsteam zur eingehenderen Untersuchung
- Zentrale Reaktion auf komplexe Vorfälle mithilfe umfassender, automatischer Szenarien

Managed Detection and Response Expert

Überlassen Sie zeit- und ressourcenintensive Vorfallsanalysen und Untersuchungen den Experten bei Kaspersky. Sie erhalten alle Features und Funktionen von Kaspersky Managed Detection and Response Optimum in Verbindung mit Managed Threat Hunting, direkten telefonischen Zugang zu den SOC-Analysten von Kaspersky, bis zu 3 Monate Aufbewahrung von Rohdaten, privilegierten Zugriff auf Kaspersky Threat Intelligence sowie eine API zur Integration mit Ticketing-Systemen von Drittanbietern, was den Zeitaufwand für die Workflow-Verwaltung erheblich reduziert.

Für die folgenden Zielsetzungen geeignet:

- Freisetzen der Zeit Ihres erfahrenen internen IT-Sicherheitsteams, damit kritischen Vorfällen Priorität eingeräumt werden kann
- Effizienzsteigerungen beim Sicherheitsteam durch Stärkung interner Best Practices mithilfe der Expertise von Kaspersky

Ihre Vorteile

- Alle Vorteile eines Security Operations Center, ohne selbst eines einrichten zu müssen
- Maximierter Nutzen aus Ihren Kaspersky-Sicherheitslösungen
- Geringere Gesamtkosten für die Sicherheit und für zukünftige Investitionen in diesem Bereich durch Stärkung der Sicherheitsfunktionen ohne eigene Sicherheitsexperten einstellen und schulen zu müssen

Praktische Anwendungen

- Individuell zugeschnittene Bedrohungserkennung, Priorisierung, Untersuchung und Reaktion
- Beratung durch unsere Experten für zusätzlichen Kontext zu den in Ihren Netzwerken beobachteten Bedrohungen
- Rückwirkendes Threat Hunting mithilfe neuer Threat Intelligence
- Bessere Vorfallsuntersuchung durch Abfrage der gesamten Wissensdatenbank von Kaspersky nach Bedrohungen und ihren Beziehungen untereinander

Kaspersky Threat Intelligence

Kaspersky Threat Intelligence bietet umfassenden und relevanten Kontext im gesamten Vorfallsmanagementzyklus. Unsere spezifischen und praktischen Erkenntnisse können in unterschiedlichen Formen und Formaten bereitgestellt und reibungslos in Ihre vorhandenen Sicherheits-Workflows integriert werden. Das Portfolio umfasst Feeds mit Bedrohungsinformationen, branchen- und bedrohungsspezifische menschenlesbare Berichte und ein durchsuchbares Repository mit Petabyte an Daten zu Bedrohungen, legitimen Objekten und ihren unterschiedlichen Beziehungen.

Für die folgenden Zielsetzungen geeignet:

- Optimieren von Abwehr- und Erkennungsfunktionen
- Umstieg von einer reaktiven auf eine proaktive Sicherheitsstellung
- Erweitern des Threat-Intelligence-Programms im Unternehmen
- Bessere Entscheidungsfindung im Bereich strategische Sicherheit

4 Erforderliche Kenntnisse

5 Anpassung und Skalierbarkeit

5 Investitionsumfang

Ihre Vorteile

- Geringere Mitarbeiterfluktuation durch Vorbeugung von Burnout bei Analysten
- Effizientere Sicherheitsvorgänge, minimierte Störungen des Geschäftsbetriebs und möglichst geringe Vorfallsauswirkungen
- Optimierung des ROI durch Abstimmen Ihrer IT-Sicherheitsinvestitionen mit der spezifischen Bedrohungslage

Praktische Anwendungen

- Festigen von Sicherheitslösungen durch fortlaufend aktualisierte, maschinenlesbare Cyberbedrohungsdaten
- Verbesserte Priorisierung bei Benachrichtigungen durch Erkennen, welche Warnmeldungen an das Vorfallsreaktionsteam weitergeleitet werden sollten
- Effektivere Untersuchungen durch Mitarbeiter, da Beziehungen zwischen erkannten Bedrohungen aufgezeigt werden
- Rechtfertigen des IT-Sicherheitsbudgets durch Darlegen klarer und relevanter Risikoszenarien

Kaspersky Cybersecurity Training

Angesichts des ständig wachsenden Volumens hochentwickelter Bedrohungen ist die Weiterentwicklung von Fähigkeiten im Unternehmen ein wichtiger Faktor. IT-Sicherheitsbeauftragte müssen in erweiterten Sicherheitstechniken ausgebildet werden, die eine wichtige Komponente des effektiven Bedrohungsmanagements und der Strategien zur Risikominimierung im Unternehmen bilden. Z. B. Reverse Engineering, Erstellen von YARA-Regeln und Arbeiten mit digitalem Beweismaterial. Kaspersky Cybersecurity Training gibt Ihrem internen Sicherheitsteam das erforderliche Wissen an die Hand, um die sich ständig ändernde Bedrohungslage zu bewältigen.

Für die folgenden Zielsetzungen geeignet:

- Steigerung der internen IT-Sicherheitsexpertise
- Unterstützung für Vorgänge im Security Operations Center
- Aufbau interner Fähigkeiten für Threat Research

4 Erforderliche Kenntnisse

3 Anpassung und Skalierbarkeit

4 Investitionsumfang

Ihre Vorteile

- Ermöglicht dem SOC-Team, potentielle Schäden durch Sicherheitsvorfälle schneller und effektiver zu mindern
- Zeit- und Kosteneinsparungen für die Einstellung erfahrener Mitarbeiter, die sich dann noch in die spezifischen Umstände in Ihrem Unternehmen einfinden müssen
- Erhöhte Bindung und Motivation bei internen Mitarbeitern durch wissensbasierte berufliche Weiterentwicklung.

Praktische Anwendungen

- Bessere Vorfallsreaktion dank Malware-Analyse mit umfassenden Erkenntnissen zur jeweiligen Bedrohung und Entwicklung äußerst effektiver Reaktionspläne
- Beweiskette auf Host- oder Netzwerksystemen, um die Ursachen eines Vorfalls aufzuzeigen und zukünftig ähnliche Vorfälle sowie rechtliche Schritte zu vermeiden
- Skalierbare, schnelle und effektive Vorfallsreaktionsprozesse zur erfolgreichen Wiederherstellung nach einer Vielzahl von Bedrohungen im Unternehmensnetzwerk

Kaspersky Cybersecurity Services

Kaspersky Cybersecurity Services bieten Zugang zur umfassenden Expertise von Kaspersky bei der Reaktion auf Vorfälle im Bereich Informationssicherheit. Dabei werden vergangene und laufende Angriffsversuche aufgezeigt sowie unternehmensweite und branchenspezifische Security Assessments durchgeführt, um Sicherheitslücken zu schließen, noch bevor sie ausgenutzt werden können, und zukünftige Angriffe zu verhindern. Durch Zusammenarbeit mit den Experten bei Kaspersky können Ihre internen IT-Sicherheitsteams zunehmend komplexe Bedrohungen effizienter bekämpfen.

Für die folgenden Zielsetzungen geeignet:

- Unterstützung durch einen erfahrenen Partner bei einem Vorfall
- Beurteilen, ob Ihre vorhandenen Erkennungs- und Präventionssysteme ausreichen sind
- Dafür sorgen, dass Sie einen proaktiven Ansatz in puncto Sicherheit verfolgen

3 Erforderliche Kenntnisse

5 Anpassung und Skalierbarkeit

4 Investitionsumfang

Ihre Vorteile

- Sicherstellen, dass Schäden selbst aus komplexen Vorfällen durch fortlaufenden Zugang zu anerkannter IT-Sicherheitsexpertise minimiert werden
- Erheblich reduzierte Kosten für potentielle Ausfallzeiten und Vermeiden negativer Publicity
- Vollständige Einhaltung gesetzlicher Vorschriften, sodass Strafen vermieden werden

Praktische Anwendungen

- Schnellere Wiederherstellung von Systemen und geschäftlichen Abläufen
- Erkennen von Angriffsversuchen und Abmildern der Auswirkungen, bevor sie zum Problem werden
- Mehr Sicherheit für branchenspezifische Infrastrukturen
- Bewerten von Abwehrmaßnahmen und Identifizieren von Schwachpunkten

Kaspersky Private Security Network

Das Kaspersky Private Security Network ermöglicht 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.

Für die folgenden Zielsetzungen geeignet:

- Schutz der vertraulichen Daten in Unternehmen mit strikten Richtlinien für die Weiterleitung von Daten außerhalb der IT-Infrastruktur
- Erfüllen selbst der anspruchsvollsten Datenschutzrichtlinien
- Erleichterte Informationsweitergabe zu Threat Intelligence im Unternehmen, um erhöhten Schutz zu bieten und die Reaktionszeiten zu verkürzen

Ihre Vorteile

- Geschäftskontinuität durch effiziente Erkennung und Reaktion, unterstützt durch internen Informationsaustausch
- Erhöhte betriebliche Effizienz, da Fehlalarme möglichst vermieden werden
- Unterstützt die vollständige Einhaltung von gesetzlichen Vorschriften zur Sicherheit isolierter Netzwerke und Umgebungen

Praktische Anwendungen

- Schutz Ihrer isolierten, möglicherweise Air-Gap-Infrastruktur ohne Kompromisse bei der Effektivität der Bedrohungserkennung
- Aufbau einer landesweiten Einrichtung zum Datenaustausch
- Integration Ihrer vorhandenen Threat Detection-Lösungen von Kaspersky mit beliebigen anderen Kaspersky-B2B-Lösungen über Ihr eigenes, internes Threat Intelligence-Netzwerk

5 Erforderliche Kenntnisse

5 Anpassung und Skalierbarkeit

5 Investitionsumfang

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 definiert werden, damit ähnliche Angriffe in Zukunft verhindert werden können. Die vorhandenen Abwehrmaßnahmen müssen also kontinuierlich verbessert werden.

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

Über 80 % aller Cybersicherheitsvorfälle sind auf menschliche Fehler zurückzuführen. 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 neue Herausforderungen für das Unternehmen anpasst und auf diese reagiert.

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

kaspersky