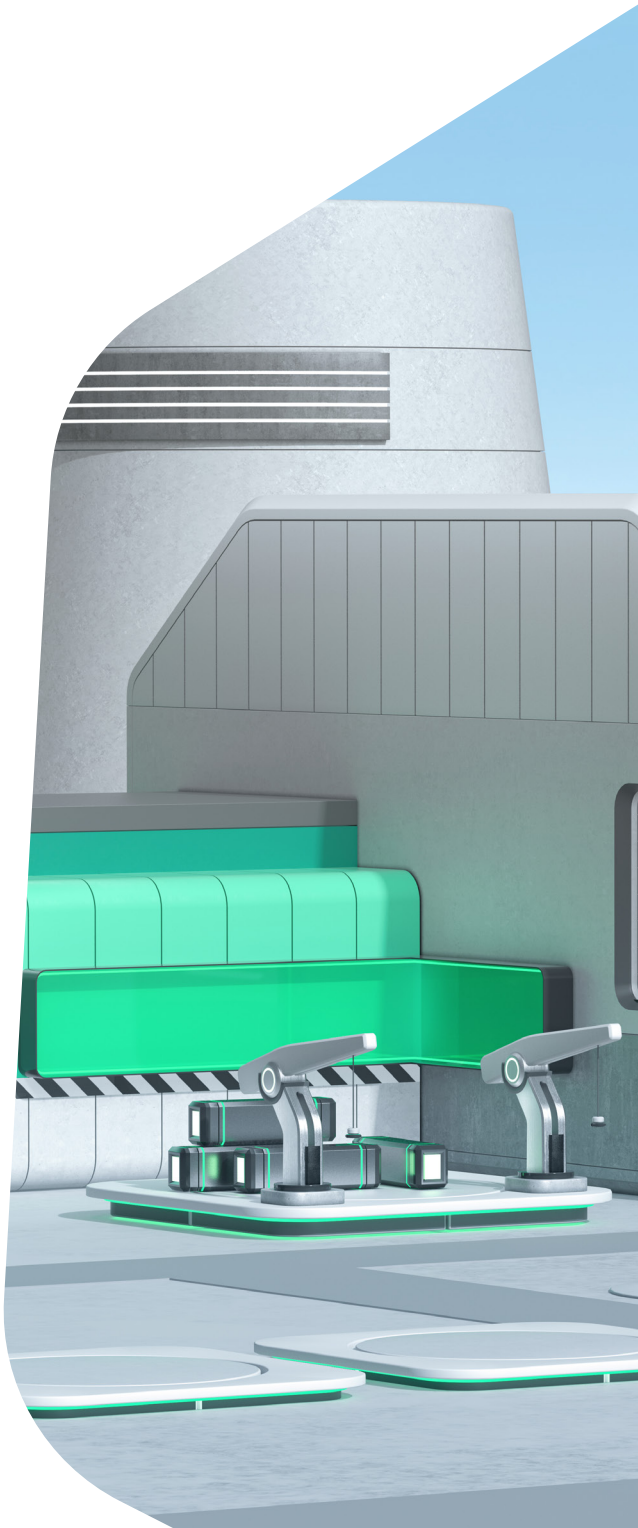
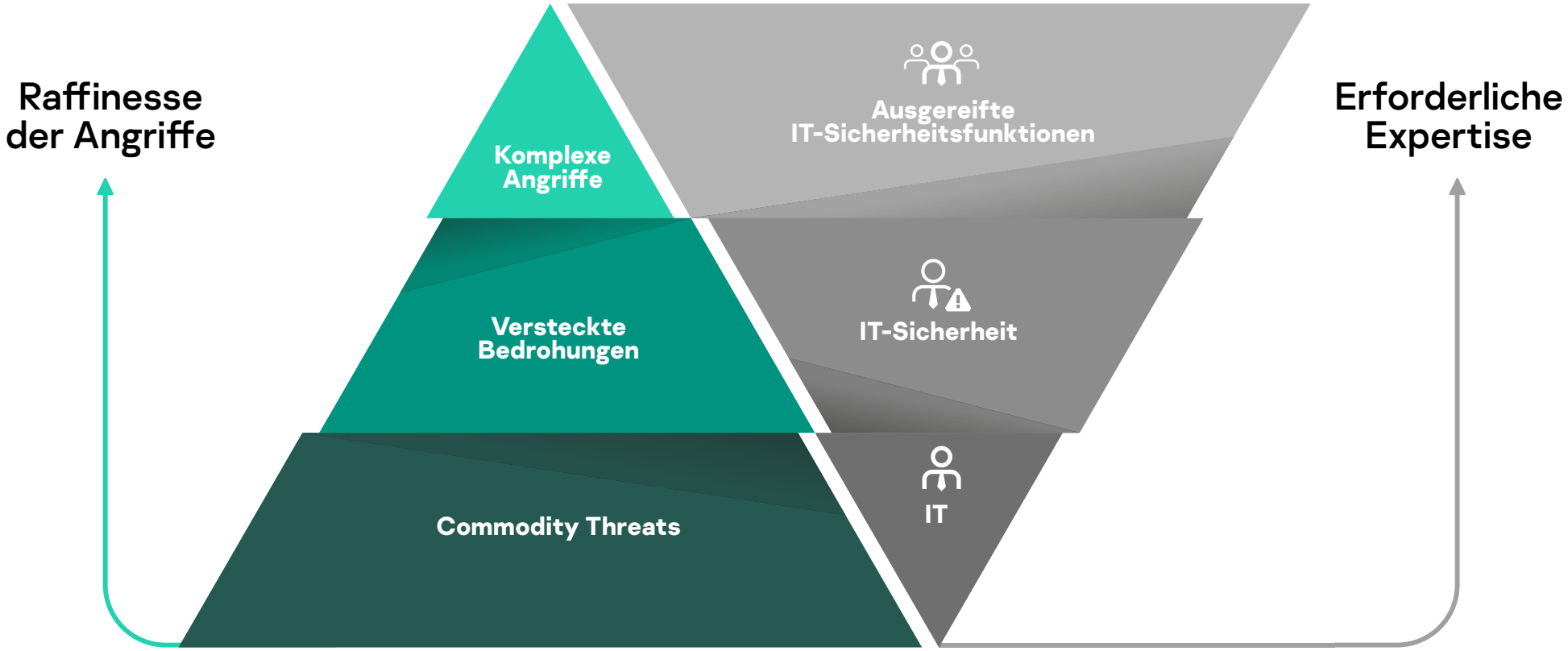
# Kaspersky Security for Enterprise

# 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 für Sicherheitslösungen
- "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)
- Sonstiges

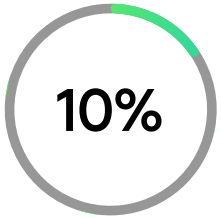
## Eigenschaften

- Kurzfristige Sicherheitsplanung
- Abhängigkeiten von Technologien und Funktionen
- 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.**

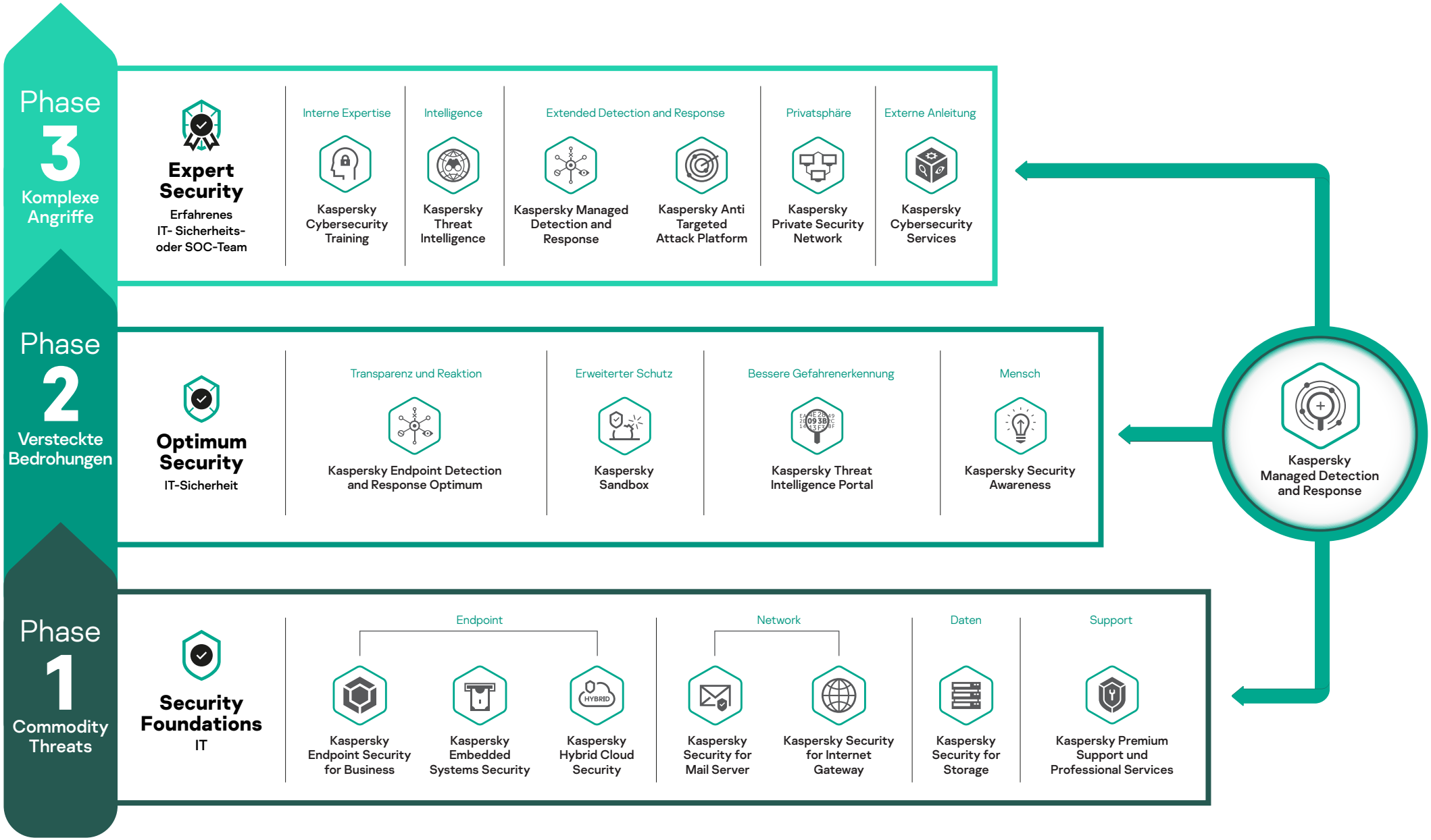



der Unternehmen ermitteln Angriffe fast sofort


sind die zusätzlichen Kosten einer Datenschutzverletzung, wenn diese nach sieben Tagen entdeckt wird

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 Verteidigungsmaßnahmen

**2** Erforderliche Kenntnisse

**5** Anpassung und Skalierbarkeit

**2** Investitionsumfang

## Vorteile für Ihr Unternehmen

- Senkung der 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 Flexibilität zur Auslagerung des IT-Sicherheitsmanagements

## Praktische Anwendungen

- Reduzierte Angriffsrisiken mit der am häufigsten ausgezeichneten Technologie für Endpoint-Schutz
- Patch Management für Ihre IT-Umgebung mit Management aus der Cloud oder einer lokalen 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 unterschiedliche Betriebssysteme

# 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 dauerhaft für ein optimiertes Risikomanagement in unterschiedlichen Umgebungen.

**Für die folgenden Zielsetzungen geeignet:**

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


## Vorteile für Ihr Unternehmen

- 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

**2** Erforderliche Kenntnisse

**5** Anpassung und Skalierbarkeit

**2** Investitionsumfang

## Vorteile für Ihr Unternehmen

- Unterbrechungsfreie Geschäftsprozesse in Bereichen, in denen die finanziellen, rechtlichen und rufbezogenen Auswirkungen eines Angriffs verheerend sein könnten
- Upgrades sind nicht mehr zwingend erforderlich, da ältere und zurzeit nicht ersetzbare, szenariospezifische 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
- 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

## Vorteile für Ihr Unternehmen

- 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 Rechtsproblemen 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 webbasierte Bedrohungen auf Ihre Endpoints auswirken
- Verringern des Risikos von Virenbefall und Kontrolle der Internetnutzung
- Reduzieren der Workloads von IT-/IT-Sicherheitsteams durch automatisches Blockieren webbasierte Bedrohungen bereits am Einstiegspunkt


## Vorteile für Ihr Unternehmen

- 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 Datenspeicher-Sicherheit sowie der durch Lösungen von Kaspersky geschützten Endpoints und Server

**3** Erforderliche Kenntnisse

**4** Anpassung und Skalierbarkeit

**3** Investitionsumfang

## Vorteile für Ihr Unternehmen

- 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

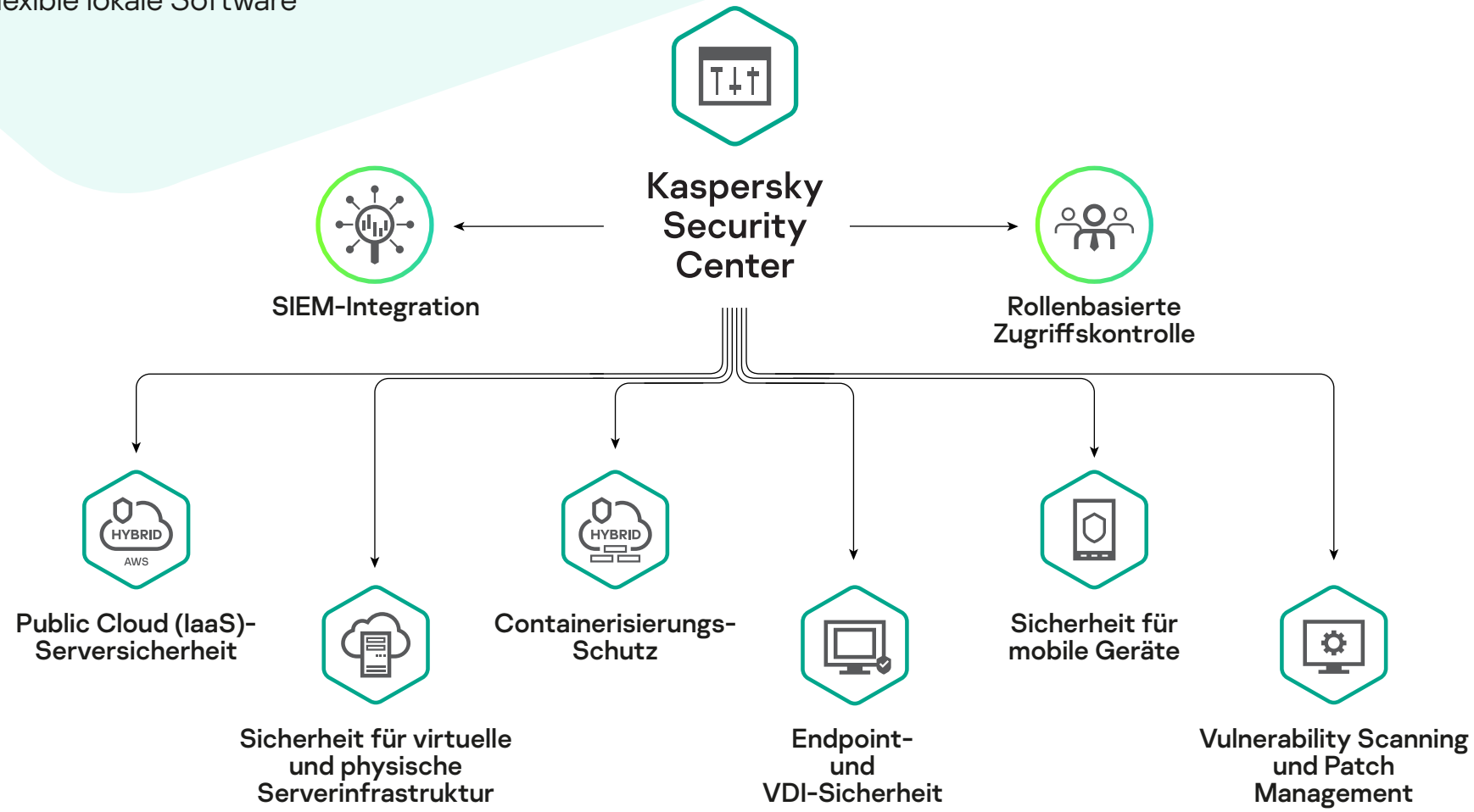
## Praktische Anwendungen

- 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 einzigen 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
- Flexible lokale 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. 24/7 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

## Vorteile für Ihr Unternehmen

- 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.

**Für die folgenden Zielsetzungen geeignet:**

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

## Vorteile für Ihr Unternehmen

- 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 richtet sich an Organisationen mit Basiswissen im Bereich der Cybersicherheit, um eine Reihe von versteckten Bedrohungen anzugehen. 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-Scans (Gefährdungsindikatoren) und automatischer oder Einzelklick-Maßnahmen.

**Für die folgenden Zielsetzungen geeignet:**

- Mehr Transparenz in Bezug auf Bedrohungen über sämtliche Endpoints hinweg
- 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

## Vorteile für Ihr Unternehmen

- 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 mit bekannten Taktiken, Techniken und Vorgehensweisen 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

## Vorteile für Ihr Unternehmen

- 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 ihren aktuellen Schutzstatus

**2** Erforderliche Kenntnisse

**5** Anpassung und Skalierbarkeit

**4** Investitionsumfang

# Kaspersky Sandbox

Kaspersky Sandbox schützt automatisch vor neuen und unbekannten Bedrohungen, die den Endpoint-Schutz umgehen. Sie 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 Abwehr versteckter Bedrohungen
- Automatisierte fortschrittliche Erkennung
- Optimierung von Mitarbeiter-Workloads und erforderlicher Expertise

1 **Erforderliche Kenntnisse**

3 **Anpassung und Skalierbarkeit**

2 **Investitionsumfang**

## Vorteile für Ihr Unternehmen

- Reduziertes IT-Sicherheitsrisiko und Gewährleistung der 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

- Ermöglicht tiefgehende dynamische Analyse und Erkennung von unbekannten und schwer zu erfassenden Bedrohungen
- Bietet automatisierte Reaktionen 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 Cybersicherheitsexperten 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


## Vorteile für Ihr Unternehmen

- 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 unterhaltsames Modul zur Festigung der neu erworbenen 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

**2** Erforderliche Kenntnisse

**4** Anpassung und Skalierbarkeit

**3** Investitionsumfang

## Vorteile für Ihr Unternehmen

- Reduzierung der Anzahl durch Menschen verursachter Sicherheitsvorfälle im Hinblick auf bessere Geschäftskontinuität und Beschränken der Auswirkungen eines Vorfalls
- 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

# 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

## Vorteile für Ihr Unternehmen

- 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

Die Kaspersky Anti Targeted Attack Platform kombiniert fortschrittliche Bedrohungserkennung auf Netzwerkebene und EDR-Funktionen und fungiert so als eine Extended Detection and Response-Lösung. So wird durch unsere Threat Intelligence und das MITRE ATT&CK-Framework umfassender Schutz vor APTs gewährleistet. 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
- Verkürzung der MTTD (mittlere Zeit bis zur Erkennung)/MTTR (mittlere Zeit bis zur Reaktion)
- Stärkung Ihres Security Operations Centers
- Verbesserte Sicherheitsstellung unter Schutz der Privatsphäre

**5** Erforderliche Kenntnisse

**3** Anpassung und Skalierbarkeit

**5** Investitionsumfang

## Vorteile für Ihr Unternehmen

- 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 von Kaspersky. Alle Funktionen von Kaspersky Managed Detection and Response Optimum in Verbindung mit Managed Threat Hunting mit bekannten Taktiken, Techniken und Vorgehensweisen (TTPs), direktem telefonischen Zugang zu den SOC-Analysten von Kaspersky, bis zu 3 Monate Aufbewahrung von Rohdaten, privilegiertem Zugriff auf Kaspersky Threat Intelligence sowie einer API zur Integration mit Ticketing-Systemen von Drittanbietern, was den Zeitaufwand für die Workflow-Verwaltung erheblich reduziert.

**Für die folgenden Zielsetzungen geeignet:**

- Mehr Zeit für Ihr erfahrenes internes IT-Sicherheitsteam, um kritischen Vorfällen Priorität einzuräumen
- Effizienzsteigerungen beim Sicherheitsteam durch Stärkung interner Best Practices mithilfe der Expertise von Kaspersky

**2** Erforderliche Kenntnisse

**5** Anpassung und Skalierbarkeit

**5** Investitionsumfang

## Vorteile für Ihr Unternehmen

- Alle Vorteile eines Security Operations Centers, 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 eine ganze Riege von 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 Petabytes an Daten zu Bedrohungen, seriösen 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

## Vorteile für Ihr Unternehmen

- 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
- Stärkung der Vorgänge im Security Operations Center
- Aufbau interner Fähigkeiten für Threat Research

## Vorteile für Ihr Unternehmen

- 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

**4** Erforderliche Kenntnisse

**3** Anpassung und Skalierbarkeit

**4** Investitionsumfang

# 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, um 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

## Vorteile für Ihr Unternehmen

- 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

**3** Erforderliche Kenntnisse

**5** Anpassung und Skalierbarkeit

**4** Investitionsumfang

# Kaspersky Private Security Network

Das Kaspersky Private Security Network ermöglicht Unternehmen, fast alle Vorteile unserer weltweiten, cloudbasierten 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

## Vorteile für Ihr Unternehmen

- 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

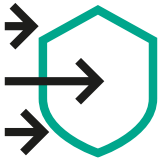
**5** Anpassung und Skalierbarkeit

**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.

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 können Sie ein Cybersicherheitssystem aufbauen, das sich kontinuierlich an die neuen Herausforderungen des Unternehmens anpasst und optimal darauf reagieren kann.

# Warum Kaspersky?

## Häufig getestet. Vielfach ausgezeichnet

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












## MITRE ATT&CK bestätigt die Qualität der Erkennung

MITRE | ATT&CK®




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

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

Kaspersky erhielt die Auszeichnung „Gartner Peer Insights Customers' 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