kaspersky BRING ON THE FUTURE

Kaspersky Threat Management & Defense

Risikominderung im Zeitalter der digitalen Transformation

Die digitale Veränderung ist der Schlüssel zu Unternehmenswachstum und institutioneller Effektivität weltweit. Aber die Sicherung der Infrastruktur der digitalen Organisation stellt eine große Herausforderung dar. Hochentwickelte Bedrohungen und gezielte Angriffe auf einzigartige Netzwerkelemente, die versteckt und untätig sind, bis sie ausgelöst werden, kommen zu den Risikofaktoren der digitalen Transformation hinzu und gefährden das Wachstum von Unternehmen und Entwicklungsinitiativen. Zwar entwickeln sich die Techniken, die von Cyberkriminellen eingesetzt werden, ständig weiter und konzentrieren sich zunehmend auf spezifische Zielumgebungen, doch zu viele Organisationen verlassen sich immer noch auf konventionelle Sicherheitstechnologien, um sich vor aktuellen und zukünftigen Bedrohungen zu schützen.

Digitale Transformation – eine neue Rolle für die Cybersicherheit

Cybersicherheit ist neben Compliance und Datennutzung zu einer der wichtigsten strategischen Prioritäten des digitalen Geschäfts geworden. Unternehmen suchen nach Sicherheitsansätzen, die eine klare Fokussierung auf die geschäftlichen Anforderungen ermöglichen.

Neue Herausforderungen für Unternehmen:

- Bei der Reaktion auf Vorfälle fallen umfangreiche manuelle Aufgaben an
- Unterbesetzte IT-Sicherheitsteams und ein Mangel an Fachwissen
- Zu viele Sicherheitsvorfälle, die in einem begrenzten Zeitraum eine Verarbeitung, Analyse, Triage und Reaktion erfordern
- Mangel an Vertrauen und Probleme bei der Einhaltung von Vorschriften zur gemeinsamen Datennutzung, wenn die digitale Infrastruktur erweitert wird
- Mangelnde Sichtbarkeit und Probleme bei der Beweiserhebung für die Analyse nach einem Vorfall

Geschäftsvorteile

- Reduzierung finanzieller und betrieblicher Schäden aufgrund von Cyberkriminalität
- Reduzierung der Komplexität durch eine einfache, für Unternehmen konzipierte Verwaltungsschnittstelle
- Geringere Verwaltungskosten durch Automatisierung und vereinfachte Prozesse zur Einhaltung von Sicherheitsvorschriften
- ROI-Steigerung durch nahtlose Workflow-Automatisierung ohne Unterbrechung der Geschäftsabläufe
- Abgeschwächte Folgen technisch hochentwickelter Bedrohungen dank schneller Erkennung

Eine einheitliche Lösung zur Beschleunigung der Innovation in der digitalen Transformation

Kaspersky Threat Management and Defense umfasst eine einzigartige Kombination aus führenden Sicherheitstechnologien, Support- und Cybersicherheitsdiensten, die sich in hohem Maße an die Besonderheiten der Organisation anpassen und einen strategischen Ansatz verfolgen, der einheitliche Prozesse zum Schutz vor fortschrittlichen Bedrohungen und einzigartigen gezielten Angriffen bietet.

Produkte

- Kaspersky Anti Targeted Attack Platform
- Kaspersky Endpoint Detection and Response
- Kaspersky Endpoint Security for Business
- Kaspersky Hybrid Cloud Security
- Kaspersky Security for Mail Server
- Kaspersky Security for Internet Gateway
- Kaspersky Private Security Network

Services

- Kaspersky Cybersecurity Training
- Kaspersky Threat Intelligence Portal
- Kaspersky Managed Detection and Response
- Kaspersky Incident Response

Support

- Kaspersky Maintenance Service Agreement
- Kaspersky Security Account Manager
- Kaspersky Professional Services

Erwiesenermaßen die wirksamste Lösung der Branche

Gartner Peer Insights **Customers' Choice für Endpoint Detection & Response, 2020**

MITRE ATT&CK bestätigt die Qualität der Erkennung

Breach Response Test von SE Labs: **AAA Awards**

ICSA Labs, Advanced Threat Defense Test (Q3 2019): **100% Erkennungsraten, mit null falsch positiven Ergebnissen**

Spitzenreiter im Radicati APT Protection Market Quadrant 2020

Perfekte Kombination aus Technologien und Services

Darüber hinaus bietet Kaspersky auch eine Reihe von Fortbildungsprogrammen für Ihr Team sowie Threat Intelligence-Daten zur Vervollständigung Ihrer internen Untersuchungsergebnisse. Mit unserem Managed Detection and Response-Service können Sie IT-Sicherheitsressourcen einsparen, indem Sie Verarbeitungsaufgaben an uns vergeben, gegebenenfalls die gesamte Fallauswertung unseren Experten überlassen und so von unserer spezifischen Threat Hunting-Expertise profitieren. Wie auch immer der Bedarf an IT-Sicherheit in Ihrem Unternehmen aussehen mag, jetzt oder in der Zukunft – wir haben die Lösung.

Erweiterte Abwehr mit einer breiteren Perspektive

Die Kaspersky Anti Targeted Attack-Plattform mit Kaspersky EDR im Kern sichert sowohl auf Netzwerk- als auch auf Endpoint-Ebene mehrere potentielle Eintrittspunkte für Bedrohungen ab und bietet erweiterte Erkennungs- und Abwehrfunktionen. Der IT-Sicherheitsexperte ist mit einem umfassenden Toolkit ausgerüstet, um multidimensionale Bedrohungen zu erkennen, detailliert zu untersuchen, Bedrohungen vorausschauend aufzuspüren und zentralisiert auf komplexe Vorfälle zu reagieren. Sie ist vollständig in Kaspersky Endpoint Security for Business integriert, das sich einen einzigen Agenten mit Kaspersky EDR, Kaspersky Hybrid Clould Security und sowohl mit Kaspersky Security for Mail Server als auch mit Kaspersky Security for Internet Gateway teilt, um Reaktionen auf komplexe Bedrohungen auf Gateway-Ebene zu automatisieren. Dank ihres modularen Aufbaus spart diese Lösung Ihren IT-Sicherheitsteams Zeit und Aufwand, indem Verteidigungsmaßnahmen sowohl auf Netzwerk- als auch auf Endpoint-Ebene weitestgehend automatisiert ablaufen und die Vorfälle in der gemeinsamen Webkonsole übersichtlich und im Kontext dargestellt werden.

Eine vertrauenswürdige Sicherheitslösung, die vollständigen Datenschutz bietet

Für Unternehmen mit strengen Datenschutzrichtlinien wird die Objektanalyse vor Ort ohne ausgehenden Datenfluss über die Integration mit dem Kaspersky Private Security Network durchgeführt. Dadurch werden eingehende Reputationsaktualisierungen in Echtzeit geliefert, während die vollständige Isolierung der Unternehmensdaten erhalten bleibt.

Stärkung des eigenen Security Operations Center (SOC)

Um raffinierte aktuelle Cyberbedrohungen wirksam zu bekämpfen und sich an die ständigen Herausforderungen einer sich stetig ändernden Bedrohungslandschaft anzupassen, sollten Ihre Security Operations Center (SOC) mit fortschrittlichen Technologien ausgestattet sein, unterstützt von Threat Intelligence und Experten mit dem gesamten erforderlichen Fachwissen. Im Ergebnis erhalten Sie einen vollständigen Verteidigungsring gegen hoch komplexe, APT-ähnliche Angriffe und zielgerichtete Kampagnen. Innerhalb des Moduls Kaspersky Threat Management and Defense bieten wir eine Reihe von fortschrittlichen Verteidigungstechnologien und -services, um die Effektivität Ihres SOC zu stärken.

Kaspersky Managed Detection and Response

Wenn Sie auf der Suche nach umfassenden Fachkenntnissen auf dem Gebiet der Bedrohungsabwehr sind, können Sie Ihre eigenen Ressourcen mit den Fähigkeiten und Erfahrungen unserer eigenen Bedrohungsspezialisten erweitern, die dies übernehmen werden:

- die in Ihrer Umgebung gesammelten Daten überprüfen
- schnell Ihr Sicherheitsteam informieren, wenn schädliche Aktivitäten entdeckt werden
- Ratschläge geben, wie Sie reagieren und Abhilfe schaffen können.

Cyber Threats News: https://de.securelist.com/
IT-Sicherheitsnachrichten: https://www.kaspersky.de/blog/b2b/
IT-Sicherheit für KMUs: kaspersky.de/business
IT-Sicherheit für Großunternehmen: kaspersky.de/enterprise

www.kaspersky.de

Beständigkeit, Unabhängigkeit und Transparenz – das zeichnet uns aus. Wir möchten eine sichere Welt schaffen, in der Technologien uns das Leben erleichtern. Deshalb schützen wir sie, damit Menschen auf der ganzen Welt die unzähligen technologischen Möglichkeiten nutzen können. Wir tragen mit Cybersicherheit zu einer sicheren Zukunft bei.

Erfahren Sie mehr unter kaspersky.de/transparency

Proven. Transparent. Independent.