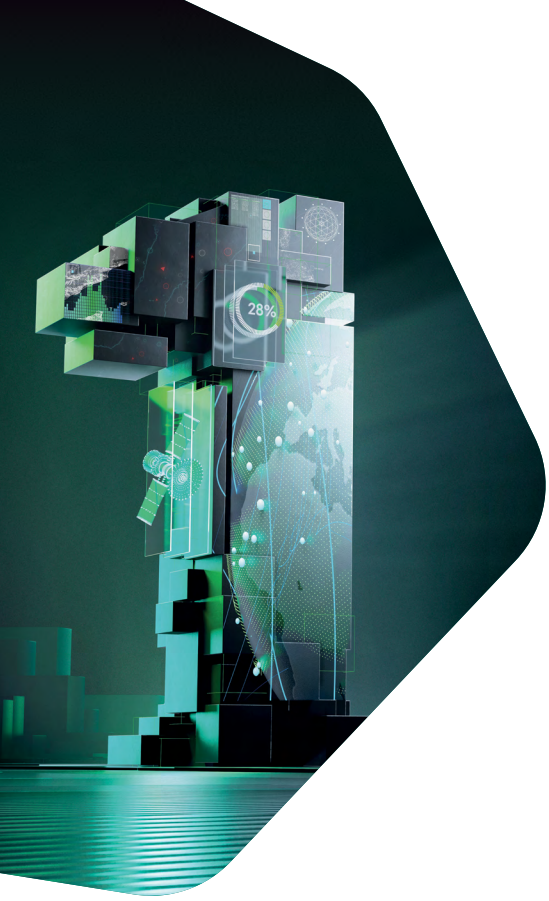

1 Partner für mehrschichtigen Cyberschutz

Cyberattacken werden immer raffinierter. Cyberkriminelle nutzen zunehmend neue und komplexe Angriffstechniken wie ausgeklügelte Malware, Erpressersoftware (Ransomware) oder dateilose Angriffe. Unbekannte oder versteckte Bedrohungen können extrem kostspielig und geschäftsschädigend sein. Deshalb brauchen Unternehmen einen zuverlässigen mehrschichtigen Cyberschutz. Kaspersky hat 25 Jahre Erfahrung im Bereich Cybersecurity und analysiert täglich über 400.000 neue Malware-Dateien. Unsere Lösungen schützen weltweit 220.000 Unternehmenskunden und 400 Millionen Nutzer. Auf der Basis dieser Erfahrung haben wir Sicherheitstools für Unternehmen unterschiedlichster Größen und Branchen entwickelt, die Sie zu einem maßgeschneiderten Rundum-Schutz-Paket zusammenstellen können.

Kaspersky Managed Detection and Response

Managed Detection & Response (MDR)

Oder: Sie müssen sich um nichts mehr kümmern…
Cyberschutz 24x7: Gegen Cyberbedrohungen gibt es keine hundertprozentige Sicherheit. Jedes Unternehmen muss mit einem Angriff rechnen. Deshalb ist es wichtig, potentielle Attacken so früh wie möglich zu erkennen und schon im Vorfeld proaktiv Abwehrmaßnahmen zu ergreifen. Mit Kaspersky Managed Detection and Response lagern Sie Ihren Cyberschutz an unsere erfahrenen Experten aus. Die Threat Hunter von Kaspersky überwachen Telemetriedaten Ihrer IT-Systeme und decken Verdächtiges sofort auf. Für diesen Service rund um die Uhr sitzen die Spezialisten in verschiedenen Security Operations Centern (SOC) auf der ganzen Welt.

Häufig dringen Cyberkriminelle in ein Netzwerk ein und breiten sich per lateral Movement aus, während sie ein geeignetes Angriffsziel ausspionieren. So können sich Schadakteure zum Beispiel dauerhaft im Active Directory festsetzen. MDR gibt Ihnen die Sicherheit, dass Incidents und gezielte Angriffe oder Advanced Persistent Threats (APT) schon im Vorbereitungsstadium identifiziert und abgeblockt werden – noch bevor Schaden entsteht.

Kaspersky Endpoint Detection and Response

Endpoint Detection & Response (EDR) Optimum

Der Flugschreiber für Ihre Endpoints
EDR ist eine technische Lösung, die tiefe Einblicke in das Geschehen auf Ihren Endpoints liefert. Ihre IT oder ein externer Dienstleister gewinnt daraus aufschlussreiche Erkenntnisse über drohende Cyberattacken und kann bei Bedarf sofort aktiv werden.

Mit Kaspersky Endpoint Detection and Response (EDR) Optimum erhalten Sie erweiterte Erkennung, einfache Untersuchung und automatische Reaktion in einem benutzerfreundlichen Paket, das Ihr Unternehmen vor den neuesten, komplexen Bedrohungen schützt.

- **Vor dem Angriff:**
  Stellen Sie sich vor, dass ein verwandtes Unternehmen Opfer eines Cyberangriffs wurde: Mit EDR können Sie proaktiv nach spezifischen Warnzeichen suchen. Gefährdungsindikatoren, Indicators of Compromise (IoC), sind bei verschiedenen Quellen erhältlich. In Kaspersky Endpoint Detection and Response (EDR) Optimum lassen sich IoCs einspielen und das Server- und Clientnetzwerk darauf scannen. Tritt ein erhöhtes Risiko zutage, können Cybersecurity-Experten unverzüglich Gegenmaßnahmen ergreifen.

- **Nach dem Angriff ist vor dem Angriff:**
  Im Falle eines Cyberangriffs speichern traditionelle Virenscanner oder Endpoint Protection (EPP) Lösungen nur wenig oberflächliche Informationen zum Incident. Dagegen zeichnet EDR detailliert auf, was auf Ihren Endpoints passiert – ähnlich wie ein Flugschreiber. Sie erhalten wichtige Daten für die Ursachenanalyse (Root Cause Analysis). So können Sie ähnliche Vorfälle in Zukunft gezielt verhindern. Sollte eine forensische Analyse nötig sein, verfügen Sie über die erforderlichen Daten.

Kaspersky Endpoint Security for Business

Endpoint Security for Business

Endpoint-Schutz der nächsten Generation
Kaspersky Endpoint Security for Business schützt zuverlässig vor Ransomware und Angriffen mit dateiloser Malware. Kann ein Word-Makro bei Ihnen immer noch Schaden anrichten? Die Adaptive Anomaly Control in unserer State-of-the-art Endpoint Protection hält Angriffe auf, bevor sie beginnen. Kaspersky-Experten erstellen mithilfe von Verhaltensanalyse-Algorithmen Kontrollregeln und verhindern so z.B. PowerShell Aufrufe aus MS Office. Eine einheitliche Konsole, wahlweise on-prem oder in der Cloud, ermöglicht Gerätekontrolle ebenso wie Webkontrolle. Ob bekannt oder unbekannt – mit der Exploit-Prävention verhindern Sie das Ausnutzen von Schwachstellen und mit dem integrierten Patch Management schließen Sie Sicherheitslücken! Und sollten doch einmal Dateien beschädigt werden, können Sie diese mit der Remediation Engine zurückholen. Weitere Pluspunkte unserer ausgereiften Lösung sind: Machine Learning und Zugriff auf das Kaspersky-eigene Security Network (KSN), eine cloudbasierte Echtzeit-Reputationsdatenbank.

Kaspersky Security Awareness

Security Awareness

Machen Sie Ihre Mitarbeiter zur ersten Verteidigungslinie
80 Prozent aller Cybervorfälle lassen sich auf menschliche Fehler zurückführen. Kaspersky hat ein effektives Gesamtkonzept zum Aufbau von Cybersicherheits-Know-how im Unternehmen entwickelt. Die Bandbreite reicht von allgemeinen Trainings, die Ihr Team sensibilisieren und motivieren, über Fachschulungen für Help-Desk-Mitarbeiter bis zu hochspezialisierten Expertenkursen (zum Beispiel zu YARA-Regeln). Führen Sie doch mal einen eigenen Pentest durch! Die Kaspersky Automated Security Awareness Platform (KASAP) stellt dazu einen integrierten Phishing Simulator bereit.

Kaspersky Threat Intelligence

Threat Intelligence (TI)

Schutz durch Wissen – bleiben Sie den Angreifern einen Schritt voraus
Kaspersky bietet ein breites Portfolio an Threat Intelligence Services wie Data Feeds, Cloud Sandbox oder Threat Lookup. Sie erhalten damit Zugriff auf die umfassende Gefährdungsdatenbank und das Expertenwissen von Kaspersky im IT- und OT-Umfeld. SOC-Teams oder IT-Security Spezialisten, die sich mit forensischen Untersuchungen beschäftigen, profitieren von wertvollen Einblicken in die aktuelle Bedrohungslandschaft. Oder Sie werten mit den Daten Ihre digitalen Abwehrsysteme wie Firewall, IPS (Intrusion Prevention System) / IDS (Intrusion Detection System) oder SIEM (Security Information and Event Management) auf.

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

kaspersky.de

kaspersky BRING ON THE FUTURE