kaspersky 25 years

Kaspersky Optimum Security

Bleiben Sie versteckten Bedrohungen einen Schritt voraus – mit ressourcenschonendem EDR[1]/MDR[2].

Kaspersky Optimum Security

30 % der erfolgreichen Cyberangriffe erfolgten über seriöse Systemtools

Kaspersky Incident Response Analyst Report, 2020

Herausforderung

Ransomware, Malware und Spyware im Finanzbereich sind immer besser darin, sich der Erkennung zu entziehen. Außerdem können sie leicht und für kleines Geld über das Darknet erworben werden. Dies löst aktuell regelrechte Angriffswellen gegen Unternehmen aus.

Fortgeschrittene Angriffe auf dem Vormarsch

Moderne versteckte Bedrohungen sind so konzipiert, dass sie den herkömmlichen Endpoint-Schutz effektiv umgehen. Dies bringt erhebliche neue Risiken für alle Unternehmen mit sich. Eine nicht erkannte Bedrohung, die sich in Ihrer Infrastruktur festsetzt, kann erhebliche Verluste bedeuten, die das Geschäftsergebnis Ihres Unternehmens beeinträchtigen:

- Unterbrechung von geschäftskritischen Prozessen und Datenverluste
- erhebliche Rufschädigung und Verlust von Kunden,
- Bußgelder, Vertragsstrafen und entgangene Gewinne.

Notwendigkeit eines verstärkten Endpoint-Schutzes

Diese neuesten Angriffe **umgehen die Erkennung**, indem sie sich in seriösen Systemtools und anderen leicht verfügbaren Methoden und Technologien verstecken. So verschaffen sie sich **schnell und unbemerkt Zugang zu Ihrer Infrastruktur, nisten sich dort ein und entfalten ihre schädliche Wirkung**.

Hinzu kommt Remote Work, die Endpoints – schon immer der attraktivste Zugang zu Ihrer Infrastruktur – noch mehr zur Zielscheibe macht.

Bei ohnehin schon knapp bemessenen Ressourcen

Damit Sie den nötigen Vorsprung behalten, muss Ihr Unternehmen wirksame Verteidigungsmechanismen entwickeln.

Aber Projekte wie diese können richtig ins Geld gehen:

- Software- und Hardware-Kosten summieren sich,
- vereinzelte und fragmentierte Tools und Prozesse untergraben die Sicherheit,
- Zeit wird mit Routineaufgaben verschwendet.

45 % der Angriffe wurden anhand von verdächtigen Dateien oder Endpoint-Aktivitäten erkannt – indem deren Erkennung zu einer Priorität gemacht wurde

Siehe oben

Lösung

Kaspersky Optimum Security ist eine effektive Lösung zur Erkennung und Abwehr von Bedrohungen, die eine Sicherheitsüberwachung rund um die Uhr, automatisiertes Aufspüren von Bedrohungen und deren Abwehr ebenso umfasst wie Beratung und Unterstützung durch Kaspersky-Experten.

Optimaler Schutz

Automatisierte Prävention ist die Grundlage eines jeden Endpoint-Schutzes, gegen die gefährlicheren versteckten Bedrohungen schützt sie allerdings nur, wenn sie durch fortschrittliche Tools flankiert wird.

Kaspersky Optimum Security bietet fortschrittliche Erkennungs- und schnelle Reaktionsfunktionen auf der Basis **lernfähiger Systeme**, die allesamt aus der Cloud heraus agieren. Ihr Team kann jetzt auch solche Bedrohungen schnell und präzise abwehren, die Sie bisher mit sehr viel manuellem Aufwand bekämpfen mussten.

Optimale Investition

Keine zusätzlichen Mitarbeiter, keine Zusatzqualifikationen, keine komplizierte Installation: Mit Kaspersky Optimum Security werden wesentliche Abwehrvorgänge vereinfacht und automatisiert – und zwar ganz nach Ihren Bedürfnissen.

Mit Optionen für lokale und Cloud-Bereitstellungen sowie einem skalierbaren Toolset für umfassende Sicherheit passt sich die Lösung an Ihre Anforderungen an. So halten Sie die Komplexität des IT-Systems gering, die Nutzerproduktivität hoch und Implementierungskosten transparent.

Perfektes Gleichgewicht

Sorgen Sie für ein perfektes Gleichgewicht zwischen Vereinfachung und Effektivität, menschlicher Intelligenz und Automation, Effizienz und Funktion – ohne Ihren Schutz aufs Spiel zu setzen!

Mit Kaspersky Optimum Security können Sie das Risiko, Geld, Kunden und Ihren guten Ruf zu verlieren, auf ein Minimum reduzieren und gleichzeitig Ihre Abwehrmaßnahmen gegen neue, unbekannte und versteckte Bedrohungen stärken. Damit sind Sie gegen die sich schnell entwickelnde Bedrohungslandschaft gewappnet.

Vorteile

- **Sichern Sie sich einen Vorsprung und schützen Sie Ihr Unternehmen vor Schäden und Geschäftsunterbrechungen** durch die neuesten hochgefährlichen versteckten Bedrohungen.
- **Entwickeln Sie mithilfe des benutzerfreundlichen** EDR-Toolsets (Endpoint Detection and Response) eigene Verteidigungsmechanismen.
- **Heben Sie Ihre Erkennung im Handumdrehen auf die nächste Stufe –** mit einer leistungsstarken und benutzerfreundlichen MDR-Lösung (Managed Detection and Response).
- Senken Sie Ihr Infektionsrisiko deutlich, indem Sie Ihre **Mitarbeiter schulen und deren Sicherheitsbewusstsein stärken.**
- Schonen Sie Ihre Ressourcen durch **Automatisierung und Managed Protection.**
- Sparen Sie Zeit und Aufwand, indem Sie die verschiedenen Funktionen der Lösung **in einer einzigen zentralen Cloud- oder lokalen Konsole verwalten.**

55 % der Angriffe wurden erst nach Wochen oder noch später erkannt

Siehe oben

Hauptfunktionen

Kaspersky Optimum Security bietet eine Vielzahl an grundlegenden Funktionen zum Schutz vor versteckten Bedrohungen. Diese beruhen im Wesentlichen auf Erkennung, Analyse und Abwehr.

Hochentwickelte Erkennung

- **Lernfähige Algorithmen zur Verhaltensanalyse**, um verdächtiges Verhalten schnell und präzise zu erkennen
- **Automatisiertes Threat Hunting** auf Basis selbst entwickelter Angriffsindikatoren (IoAs), um verborgene komplexe Bedrohungen aufzuspüren, alles unterstützt von Kaspersky-Experten
- Adaptive Anomaly Control, um **die Konfiguration von Tools zur Verkleinerung der Angriffsfläche automatisch an die Profile der Benutzer anzupassen**
- Cloud-Erkennung, einschließlich einer integrierten **Cloud-Sandbox**.

Unkomplizierte Analyse

- Alle Informationen zu einem Vorfall werden automatisch **auf einer Vorfallskarte zusammengefasst**.
- **Dank Visualisierung und eines einfachen** Untersuchungsprozesses können Sie den Vorfall schnell und effizient in einer zentralen Umgebung analysieren und dann über das weitere Vorgehen entscheiden.
- Gleichzeitig werden alle Erkennungen von Kaspersky nach Angriffsindikatoren **priorisiert und untersucht, um auf Sie zugeschnittene Empfehlungen aussprechen zu können**.

Automatisierte Reaktion

- **Einzelne Vorfälle können Sie** einfach per Mausklick selbst eindämmen.
- Handlungsempfehlungen, die auf der Erfahrung der Kaspersky-Experten beruhen, gewährleisten, dass Sie auch sehr komplexe und gefährliche Bedrohungen angehen können.
- **Über Endpoints hinweg automatisierte Funktionen** helfen bei der Suche und Abwehr von analysierten oder importierten Bedrohungen im gesamten Netzwerk.

Inhalte

Nutzen Sie Kaspersky Optimum Security so, wie es Ihnen am besten passt: als Managed-Lösung mit Rund-um-die-Uhr-Schutz, als benutzerfreundliches EDR-Toolset oder als eine Mischung aus beidem. Profitieren Sie von der Erfahrung und dem Know-how der Kaspersky-Experten bei der Entwicklung Ihrer firmeninternen Erkennungs- und Abwehrfunktionen. In Kaspersky Optimum Security wurden mehrere Produkte in eine Einzellösung zusammengeführt:

Bei 31 % der erfolgreichen Cyberangriffe waren schädliche E-Mails beteiligt. Das bedeutet: Viele Angriffe hätten die Mitarbeiter selbst verhindern können.

Siehe oben

Aber das ist noch nicht alles...

Verbessern Sie Ihren bestehenden Schutz mithilfe einer Vielzahl von Tools, die auf verschiedene Aspekte Ihrer Sicherheitslösung abzielen, wie Erkennung, Untersuchung und Sicherheitsbewusstsein.

Klären Sie Ihre Mitarbeiter auf

Verkleinern Sie Ihre Angriffsfläche und senken Sie die Anzahl an Cybervorfällen. Ein Schlüsselfaktor dazu besteht in der Schärfung des Bewusstseins der Mitarbeiter gegenüber Cyberbedrohungen, die sie durch Nachlässigkeit oder Unwissenheit in ihre Infrastruktur einschleppen könnten. **Kaspersky Security Awareness** vermittelt das Wissen und die Kompetenzen, die jeder Mitarbeiter braucht, um die Infrastruktur zu schützen und seinen Beitrag zu einer sicheren Umgebung zu leisten.

Immer auf dem neuesten Stand

Cybersicherheitsexperten erhalten regelmäßig neueste Informationen zu Dateien, Hashes, IPs und URLs, die mit Bedrohungen in Zusammenhang stehen. Dadurch können sie Bedrohungen umfassender und schneller analysieren und einschätzen. Diese Zusatzinformationen stehen Ihnen jederzeit ohne zusätzliche Kosten auf dem benutzerfreundlichen **Kaspersky Threat Intelligence Portal zur Verfügung**.

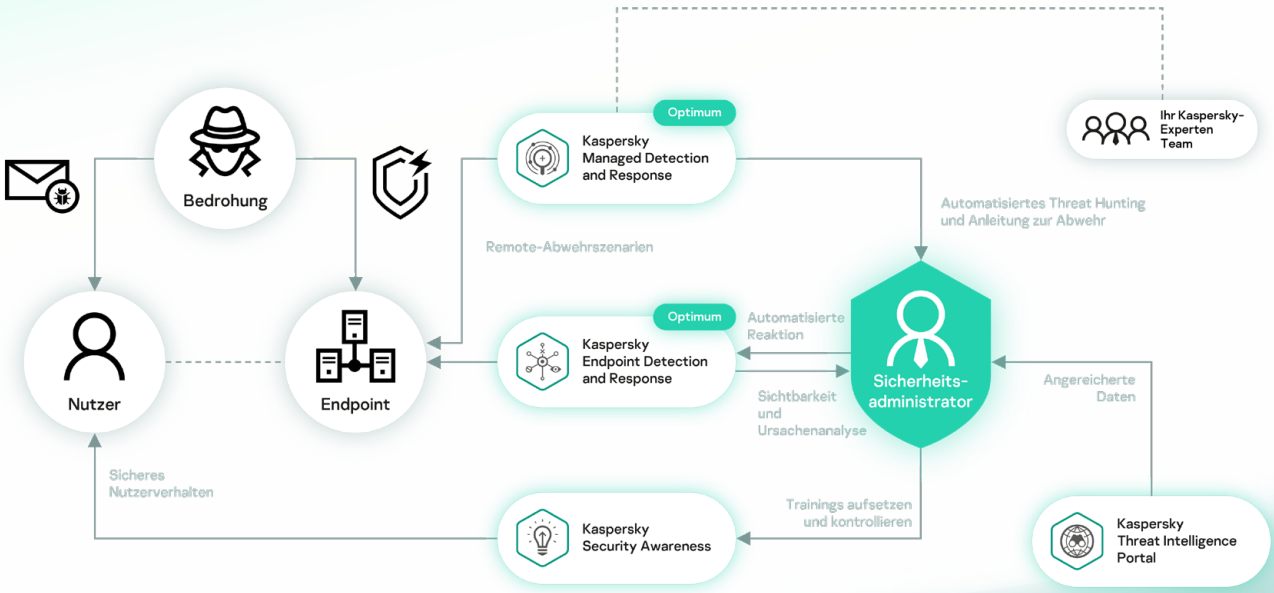
Wir unterstützen Sie

Damit ein effizienter Schutz Ihrer IT-Infrastruktur sichergestellt ist, müssen Sie Ihre Produkte anhand von Best Practices und Ihren individuellen Sicherheitsanforderungen implementieren und konfigurieren.

Maximieren Sie den ROI Ihrer Security-Lösung und stellen Sie sicher, dass diese zu 100 % funktioniert. Unsere Experten von **Kaspersky Professional Services** helfen Ihnen dabei, Ihre Sicherheitslösung zu überprüfen, zu implementieren, zu warten und zu optimieren.

Wie alles zusammenhängt

Prävention, Erkennung, Analyse, Reaktion und Mitarbeiterschulung sind in Kaspersky Optimum Security vereint. Jede Komponente hat ihren eigenen Wert und kann separat verwendet werden. Die Kombination sorgt dafür, dass sämtliche Anforderungen an den Schutz Ihrer Endpoints vor versteckten Bedrohungen in einer einzigen integrierten Lösung erfüllt werden.



44 % der Unternehmen sehen die Kosten für die Sicherung der immer komplexer werdenden Umgebungen als eines der Hauptprobleme an.

IT Security Economics 2021, Kaspersky

Benutzerfreundlich

Sie werden feststellen, dass Kaspersky Optimum Security dank der zentralen Konsole sehr benutzerfreundlich zu verwalten ist, damit Sie Ihre begrenzte Zeit und Ressourcen optimal nutzen können.

Kompletter Umfang

- Teil des Sicherheits-Ökosystems von Kaspersky, ausgehend vom Basisschutz bis hin zu optimierten erweiterten Funktionen
- Die vielfältigen Funktionen von Kaspersky Optimum Security können über eine zentrale Verwaltungskonsole bedient werden
- Mehrere Schutzebenen wirken gegen herkömmliche und versteckte Bedrohungen sowie gegen Risiken durch menschliches Versagen.

Leichtere Verwaltung

- Unsere Cloud-Verwaltungskonsole ermöglicht eine schnelle und effiziente Steuerung von jedem beliebigen Ort der Welt.
- Identische Benutzererfahrung, ob lokal oder SaaS-basiert
- Die Bereitstellung erfolgt schnell und problemlos, unabhängig davon, ob bereits Kaspersky-Lösungen genutzt werden.
- Ihr Team kann sämtliche Tools einfach und intuitiv steuern und bedienen, ohne langwierige Einarbeitung oder Umschulung.

Sparen Sie Zeit und Ressourcen

- Mit Managed Protection bauen Sie Ihre Erkennungs- und Abwehrfunktionen aus. Sie müssen nicht umfangreich in Sicherheit investieren, selbst wenn Sie über kein eigenes Personal oder Fachwissen im Bereich Cybersicherheit verfügen.
- Wesentliche Prozesse laufen automatisiert ab, was die Vorfallsreaktion schnell, präzise und effizient macht.
- Erhöhtes Sicherheitsbewusstsein unter den Mitarbeitern bedeutet, dass weniger Bedrohungen Ihre Sicherheitseinrichtungen überwinden – und damit weniger Vorfälle, die Sie bearbeiten müssen!

In der Praxis

Wie das alles in der Praxis zusammenkommt.

Penetration

Der Nutzer erhält eine Phishing-Mail oder greift auf eine schädliche Webressource zu, wobei der Host infiziert wird.

- Sicherheitsbewusstsein unter den Mitarbeitern
- Reduzierung der Angriffsfläche
- Automatische Gefahrenabwehr

Installation

In der ersten Phase der Infektion werden erforderliche Komponenten installiert, mit den C&C[1]-Servern kommuniziert und die Umgebung erkundet

- Erweiterte Erkennungsmechanismen, einschließlich ML-basierte Verhaltensanalyse und Cloud-Sandbox
- Automatisiertes Threat Hunting mit IoAs[2]
- Ursachenanalyse und IoC[3]-Scans
- Geführte und Remote-Abwehrszenarien

Rooting

Eine Reihe von Tools wird genutzt, um eine nachhaltige Wirkung zu erzielen und eventuell eine weitere horizontale Ausbreitung zu verhindern.

[1] Command and Control
[2] Angriffsindikatoren
[3] Gefährdungsindikatoren

Der stufenweise Ansatz von Kaspersky

Ausgehend von Kaspersky Security Foundations bauen wir gemeinsam mit Ihnen eine Schutzlösung auf, die sich nahtlos auf die grundlegende Vorfallsreaktion mit Kaspersky Optimum Security skalieren lässt. Als nächstes Level steht Ihnen Kaspersky Expert Security mit leistungsstarken Tools zum Schutz vor hoch komplexen Bedrohungen zur Verfügung. Sie entscheiden, welche Stufe für Sie die richtige ist:

Kaspersky Security Foundations

Blockiert die überwiegende Mehrheit der Bedrohungen automatisch

» Mehr Informationen

Kaspersky Optimum Security

Bauen Sie Ihre Verteidigung gegen komplexe Bedrohungen auf

» Mehr Informationen

Kaspersky Expert Security

Gewappnet gegen komplexe, APT-ähnliche Angriffe.

» Mehr Informationen

Wer wir sind

Wir sind ein globales, privat geführtes Cybersicherheitsunternehmen mit Hunderttausenden von Kunden und Partnern auf der ganzen Welt, das sich der Transparenz und Unabhängigkeit verpflichtet hat. Seit 25 Jahren entwickeln wir Tools und Services mit dem Ziel, Ihre Sicherheit zu gewährleisten. Unsere Technologien sind **häufig getestet und vielfach ausgezeichnet**.

IDC

Kundenbewertungen laut IDC MarketScape Worldwide Modern Endpoint Security for Enterprises 2021

Einer der besten Anbieter

AV-Test

Fortschrittlicher Endpoint-Schutz: Test des Ransomware-Schutzes

100-prozentiger Schutz

Radicati-Gruppe

Advanced Persistent Threat (APT) Market Quadrant

Top-Anbieter

Sehen Sie genauer hin

Erfahren Sie mehr über die Funktionsweise von Kaspersky EDR Optimum und finden Sie heraus, wie Sie Ihr Sicherheitsteam und Ihre Ressourcen im Kampf gegen Cyberbedrohungen entlasten:
www.kaspersky.de/enterprise-security/edr-security-software-solution

[1] Kaspersky Endpoint Detection and Response
[2] Managed Detection and Response

Cyber Threat News: de.securelist.com
IT Security News: kaspersky.de/blog/b2b
IT-Sicherheit für SMB: kaspersky.de/business
IT-Sicherheit für Großunternehmen: kaspersky.de/enterprise

kaspersky.de

© 2022 AO Kaspersky Lab.
Eingetragene Markenzeichen und Dienstleistungsmarken sind das Eigentum ihrer jeweiligen Rechtsinhaber.