kaspersky BRING ON THE FUTURE

Kaspersky Optimum Security

Verschaffen Sie sich ein Höchstmaß an Cybersicherheit mit Managed Protection und Cloud-basierter Endpoint Detection & Response.

Herausforderung

Sie müssen Ihr Unternehmen effektiv und ohne übermäßigen Zeit- und Ressourcenaufwand vor neuen, unbekannten und versteckten Bedrohungen schützen.

30 % der erfolgreichen Cyberangriffe erfolgten über seriöse Systemtools[1]

Hoch entwickelte Angriffe auf dem Vormarsch

Die heute üblichen versteckten Bedrohungen – die zudem auf die effektive Umgehung des Endpoint-Schutzes ausgelegt sind – bergen viel größere Risiken für Unternehmen als früher, da die Angriffe immer schwerer zu erkennen, zu analysieren und abzuwehren sind. Eine nicht erkannte Bedrohung, die sich in Ihrer Infrastruktur festsetzt, kann erhebliche Verluste bedeuten, die das Geschäftsergebnis Ihres Unternehmens beeinträchtigen:

- Unterbrechung geschäftskritischer Prozesse,
- erhebliche Rufschädigung und Verlust von Kunden,
- Bußgelder, Vertragsstrafen und entgangene Gewinne.

Notwendigkeit eines verstärkten Endpoint-Schutzes

Die heute üblichen versteckten Bedrohungen sind weitaus schlagkräftiger geworden, weil sich Kriminelle seriöser Systemtools und vorgefertigter Methoden und Technologien bedienen, um schneller und unerkannt in Ihre Infrastruktur einzudringen, sich dort festzusetzen und größtmöglichen Schaden anzurichten.

Diese Situation wird noch weiter verschärft durch die Auflösung der Perimeter und die Zunahme von Fernarbeit, durch die Endpoints – schon immer ein beliebtes Einfallstor in die Infrastruktur – noch stärker in den Fokus rücken.

Bei ohnehin schon knapp bemessenen Ressourcen

Um Ihrer Endpoint-Sicherheit den notwendigen Vorsprung zu verschaffen, müssen Sie in Ihrem Unternehmen wirksame Reaktionsfunktionen gegen Vorfälle entwickeln.

Doch die damit verbundenen Kosten können schnell aus dem Ruder laufen:

- Software- und Hardware-Kosten summieren sich,
- vereinzelte und fragmentierte Sicherheitstools und -prozesse beeinträchtigen die Sicherheit,
- viel Zeit wird mit Routineaufgaben verschwendet.

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.

45 % der Angriffe wurden anhand von verdächtigen Dateien oder Endpoint-Aktivitäten erkannt[1]

Fortschrittlicher Schutz vor Bedrohungen

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 Sie gegen die sich schnell entwickelnde Bedrohungslandschaft gewappnet sind.

Schnelle und skalierbare Komplettlösung

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, die allesamt aus der Cloud heraus agieren. Cybersicherheitsmitarbeiter können jetzt auch die Bedrohungen schnell und präzise angehen, die bisher nur mit sehr viel manuellem Aufwand abgewehrt werden konnten.

Perfekt zugeschnittene Investition

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

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

Hauptvorteile

- Sichern Sie sich einen Vorsprung und schützen Sie Ihr Unternehmen vor Schäden und Geschäftunterbrechungen durch die neueste Welle tödlicher versteckter Bedrohungen
- Entwickeln Sie mithilfe des benutzerfreundlichen EDR-Toolsets (Endpoint Detection & Response) eigene Verteidigungsmechanismen
- Senken Sie das Infektionsrisiko deutlich, indem Sie Ihre Mitarbeiter schulen und deren Sicherheitsbewusstsein stärken
- Sparen Sie wertvolle Ressourcen durch Automatisierung und Managed Protection-Funktionen
- Sparen Sie Zeit und Aufwand, indem Sie die verschiedenen Funktionen der Lösung in einer einzigen zentralen Cloud- oder lokalen Konsole verwalten

Hauptfunktionen

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

Bei 55 % der Angriffe dauerte es Wochen oder länger, bis sie entdeckt wurden[1]

Hochentwickelte Erkennung

- Lernfähige Algorithmen zur Verhaltensanalyse, um verdächtiges Verhalten schnell und präzise zu erkennen
- Automatisiertes Threat Hunting auf Basis selbst entwickelter Angriffsindikatoren, um verborgene komplexe Bedrohungen aufzuspüren, unterstützt von Kaspersky-Experten
- Adaptive Anomaly Control, um die Konfiguration von Tools zur Reduzierung der Angriffsfläche automatisch an die Profile der Benutzer anzupassen

Vereinfachte Untersuchung

- 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 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
- Auf der Erfahrung der Kaspersky-Experten beruhende Handlungsempfehlungen 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

Anwendung

Kaspersky Optimum Security umfasst eine Reihe von Tools und wichtigen Funktionen, die als Ganzes in den unterschiedlichen Phasen eines Angriffs zur effektiven Prävention, Erkennung und Abwehr von Bedrohungen eingesetzt werden können:

Penetration

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

Installation

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

Rooting

Es folgt die Festsetzung im System über eine Reihe von Tools – auch seriösen und systemeigenen – und eventuell eine weitere horizontale Ausbreitung

Sicherheitsbewusstsein unter den Mitarbeitern

Erweiterte Erkennungsmechanismen, einschließlich ML-basierte Verhaltensanalyse und Sandbox

Reduzierung der Angriffsfläche

Automatisiertes Threat Hunting mit IoAs[2]

Ursachenanalyse und IoC[3]-Scans

Automatische Gefahrenabwehr

Geführte und Remote-Abwehrszenarien

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

Weiterer Schutz

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

Bei 31 % der erfolgreichen Cyberangriffe waren schädliche E-Mails beteiligt, was bedeutet, dass viele von den Mitarbeitern selbst hätten verhindert werden können[1]

Zusätzliche Erkennungsebene

Erkennen Sie mit **Kaspersky Sandbox** neue und unbekannte Bedrohungen noch schneller und zuverlässiger: Anhand patentierter Erkennungsalgorithmen und Anti-Umgehungstechniken werden Bedrohungen in einer isolierten Umgebung automatisch analysiert. Vorkonfigurierte Abwehrmechanismen werden automatisch in Gang gesetzt, was die Erkennungsfähigkeit ganz ohne Verwaltungsaufwand (abgesehen von der Erstinstallation) erheblich steigert.

Vorsprung bei der Vorfallsuntersuchung

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

Der Mensch als Schlüssel zur Cybersicherheit

Der Schlüssel zu einer Reduzierung der Angriffsfläche und der Anzahl an Vorfällen besteht in der Schärfung des Bewusstseins unter Ihren Mitarbeitern gegenüber Cyberbedrohungen, denen sie durch Nachlässigkeit oder Unwissenheit Tür und Tor öffnen können. **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.

Funktionsweise

Es liegt ganz bei Ihnen, wie Sie Kaspersky Optimum Security nutzen möchten: als Managed-Lösung mit Rund-um-die-Uhr-Schutz, als benutzerfreundliches EDR-Toolset oder als eine Mischung aus beidem, damit Sie von der Erfahrung und dem Know-how der Kaspersky-Experten bei der Entwicklung Ihrer firmeninternen Erkennungs- und Abwehrfunktionen profitieren. In Kaspersky Optimum Security wurden mehrere Produkte in eine Einzellösung zusammengeführt:

Im Betrieb

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

56 % der Befragten geben an, dass Ihr Unternehmen aufgrund eines Mangels an Cybersicherheitsmitarbeitern gefährdet ist[2]

Kompletter Umfang

- Teil des gesamten Angebots an Sicherheitslösungen 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
- Eine Lösung mit mehreren Schutzebenen gegen herkömmliche und versteckte Bedrohungen sowie Gefahren, die von Menschen-gemachten Fehlern ausgehen

Benutzerfreundliche Verwaltung

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

Zeit- und Ressourcenersparnis

- Managed Protection ist vor allem für Organisationen geeignet, die nicht über die Mitarbeitern oder das entsprechende Fachwissen im Bereich IT-Sicherheit verfügen, um Erkennungs- und Abwehrfunktionen ohne die damit verbundenen Sicherheitsinvestitionen aufzubauen
- Wesentliche Cybersicherheitsprozesse laufen automatisiert ab, was die Vorfallsreaktion schneller, präziser und effizienter macht
- Erhöhtes Sicherheitsbewusstsein unter den Mitarbeiter bedeutet, dass weniger Bedrohungen Ihre Sicherheitseinrichtungen überwinden – und damit weniger Vorfälle, die Sie verarbeiten müssen!

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 und letzten Endes mit Kaspersky Expert Security in die Anwendung leistungsstarker Tools zum Schutz vor hoch komplexen Bedrohungen mündet.

Sie entscheiden, welche Stufe für Sie die richtige ist:

Kaspersky Security Foundations

Blockiert die überwiegenden Mehrheit der Bedrohungen automatisch

- Automatisierte Multi-Vektor-Prävention von Commodity-Bedrohungen – der überwiegenden Mehrheit aller Cyberangriffe
- Die Grundstufe für Unternehmen jeglicher Größe und Infrastruktur-Komplexität zum Aufbau einer integrierten Abwehrstrategie
- Zuverlässiger Endpoint-Schutz für Unternehmen mit kleinen IT-Teams, deren Sicherheitsexpertise noch im Aufbau begriffen ist

Kaspersky Optimum Security

Aufbau eines Schutzes vor versteckten Bedrohungen für:

- Unternehmen mit einem kleinen Sicherheitsteam mit grundlegender Erfahrung im Bereich Cybersicherheit
- Unternehmen mit einer IT-Umgebung, deren Größe und Komplexität zunimmt und damit auch die Angriffsfläche
- Unternehmen, denen es an Cybersicherheitsressourcen mangelt – bei gleichzeitigem erhöhten Sicherheitsbedarf
- Die Entwicklung wirksamer Verteidigungsmechanismen hat an Bedeutung gewonnen

Kaspersky Expert Security

Gründe für ein Unternehmen, sich für komplexe und APT-ähnliche Angriffe zu wappnen:

- Komplexe und verteilte IT-Umgebung,
- erfahrenes IT-Sicherheitsteam oder bereits vorhandenes Security Operations Center (SOC),
- abnehmende Risikobereitschaft wegen höherer zu erwartender Kosten durch Sicherheitsvorfälle und Datenschutzverletzungen,
- Sorge um Einhaltung gesetzlicher Vorschriften.

Weitere Informationen zur Funktionsweise von Kaspersky Optimum Security im Kampf gegen Cyberbedrohungen bei gleichzeitiger Entlastung von Sicherheitsteams und Ressourcen finden Sie unter: http://go.kaspersky.com/optimum_DE

1 Kaspersky Incident Response Analyst Report 2019, Kaspersky, 2020
2 (ISC)2 Studie zu Mitarbeitern in der Cybersicherheit, (ISC)2 2020

Cyber Threats News: de.securelist.com
IT Security News: www.kaspersky.de/blog/b2b

www.kaspersky.de