



**Kaspersky®  
Endpoint Security  
for Business**

# Schützen Sie, was Ihnen am wichtigsten ist

Budgets für IT-Sicherheit spiegeln häufig nicht die steigenden Geschäftsanforderungen und die sich verschärfende Bedrohungslage wider. Um den Herausforderungen von heute und morgen zu begegnen, müssen Ressourcen optimiert werden. Aber wie finden Sie die richtige Sicherheitslösung? Eine, die jedes Element Ihrer IT-Infrastruktur vor den fortschrittlichsten Cyberbedrohungen schützt und in der schnelllebigen IT-Landschaft Geschäftsunterbrechungen verhindert, ohne Ihr Budget zu überlasten?

Fragen Sie einfach unsere Kunden. Kaspersky Endpoint Security for Business bietet umfassende adaptive Sicherheit, die sich nach Ihren Geschäftsanforderungen skalieren lässt und die Geschäftskontinuität und Assets mit zahlreichen fortschrittlichen Technologien schützt. Das Ergebnis spricht für sich selbst.

Erstklassige Bedrohungsinformationen sind Teil unserer DNS und beeinflussen unser gesamtes Tun. Als unabhängiges Unternehmen sind wir agiler, denken anders und reagieren schneller, um Cyberbedrohungen zu neutralisieren – unabhängig von ihrem Ursprung oder Zweck. So bieten unsere Produkte und Lösungen nicht nur Cybersicherheit, sondern True Cybersecurity.

## True Cybersecurity, die die Konkurrenz hinter sich lässt

Die Technologien von Kaspersky Endpoint Security for Business schaffen das perfekte Gleichgewicht zwischen Leistung und effizientem Schutz. Und genau durch dieses Gleichgewicht erreichen unsere Produkte mit die höchsten Erkennungsraten der Branche, wie unabhängige Tests immer wieder bestätigen. Kaspersky Lab zählt in [Gartner's Critical Capabilities for Endpoint Protection Platforms 2018](#) zu den drei führenden Anbietern in jedem Anwendungsfall.



Common Criteria



Ready  
for GDPR



### Optimale Effizienz

Der adaptive Schutz, der von führenden Experten entwickelt wurde, schont Ressourcen und minimiert den Verwaltungsaufwand. Schutz- und Machine-Learning-basierte Technologien erkennen und blockieren Endpoint-Bedrohungen unabhängig von Ursprung oder Ziel. Und wenn Sie angegriffen werden, können schädliche Aktionen rückgängig gemacht werden, damit Ihre Benutzer weiterarbeiten können.



### Individuell auf Ihre Umgebung zugeschnitten

Schützen Sie vielfältige Umgebungen und skalieren Sie die Lösung einfach nach Ihren Anforderungen – selbst in heterogenen IT-Infrastrukturen. Darüber hinaus können Sie selbst entscheiden, ob Sie die vordefinierten Einstellungen ändern und wann Sie neue Funktionen implementieren.



### Kundenzufriedenheit

Mit nur einem Produkt schützen Sie Ihre Daten unabhängig von ihrem Standort vor Bedrohungen – mit transparentem Preis- und Lizenzmodell. Unsere Kunden teilen uns immer wieder mit, dass sie mit den Ergebnissen unserer Lösung außerordentlich zufrieden sind. Diese Zufriedenheit wurde in den letzten sechs Jahren auch immer wieder von unabhängigen Tests bestätigt ([Top 3](#)).

1 **Schützt Server, Gateways und Endpoints.**

2 **Optimiert die Sicherheitsverwaltung über eine einheitliche Konsole.**

3 **Reduziert Komplexität und Betriebskosten.**

4 **Unterstützt die Delegation von Verantwortungsbereichen in Ihrem Team.**

5 **Steigert die Produktivität durch Cloud-basierte Nutzungskontrollen.**

6 **Schützt Schwachstellen dauerhaft, um die Zahl potenzieller Angriffsvektoren zu vermindern.**

7 **Spart Zeit durch die Automatisierung von Betriebssystem- und Software-Deployment.**

# Mehr als Endpoint-Schutz – heute und in Zukunft

Dank umfangreicher Quellen für Echtzeit-Bedrohungsinformationen und maschinelles Lernen entwickeln sich unsere Technologien ständig weiter, damit Sie Ihr Unternehmen vor den neuesten und komplexesten Cyberbedrohungen schützen können.

## Blockiert Ransomware, dateilose Angriffe und Kontoübernahmen

Schützen Sie Ihre Endpoints vor den neuesten Exploits, und schützen Sie Ihre Daten und freigegebenen Ordner vor hoch entwickelten Bedrohungen und Ransomware.

**Die Verhaltenserkennung** implementiert einen **Memory-Schutz**-Mechanismus, der systemkritische Prozesse überwacht und verhindert, dass Anmeldedaten von Benutzern und Administratoren gestohlen werden.

## Reduziert die Angriffsfläche für programm-basierte Angriffe

Mit den integrierten Kontrollen können Sie Ihre Angriffsfläche für unbekannt Bedrohungen erheblich reduzieren, indem Sie bestimmen, welche Programme und Aktionen auf Ihren Endpoints ausgeführt werden dürfen. **Adaptive Anomaly Control** – eine Komponente, die Sicherheitsstufen automatisch auf die höchste Ebene anhebt, die für die Rolle des jeweiligen Benutzers sinnvoll ist – wird von der Programmkontrolle sowie topaktuellen Whitelisting-Datenbanken ergänzt.

## Erkennt mehr Angriffe und Eindringversuche – selbst die ausgefallensten

Angreifer nutzen Rootkits und Bootkits, um ihre Aktivitäten vor den Sicherheitslösungen zu verbergen. Die Anti-Rootkit-Technologie ist Teil des mehrstufigen Schutzes von Kaspersky Lab und hilft bei der Erkennung selbst der verborgensten Infektionen sowie bei ihrer Neutralisierung. Integrierte Sensoren und die Integration in **Kaspersky Endpoint Detection & Response** ermöglichen die Erfassung und Analyse großer Onshore-Datenmengen ohne Auswirkungen auf die Produktivität der Benutzer.

## Regelt den Zugriff auf vertrauliche Daten und Aufnahmegeräte

Unsere Lösung schränkt Programmberechtigungen entsprechend den zugeordneten Vertrauensstufen ein und begrenzt so den Zugriff auf Ressourcen wie etwa verschlüsselte Daten. Das **Host Intrusion Prevention System** (HIPS) arbeitet parallel mit einer lokalen und einer Cloud-basierten Reputationsdatenbank (**Kaspersky Security Network** oder kurz KSN). Es kontrolliert Programme und schränkt den Zugriff auf kritische Systemressourcen sowie Audio- und Video-Aufnahmegeräte ein.

## Stoppt Webbedrohungen, bevor sie Ihre Endpoints erreichen

Unsere Sicherheitstechnologien filtern Gateway-Datenverkehr und blockieren automatisch eingehende Gefahren, bevor diese Ihre Endpoints und Server erreichen. So werden das Risiko von Schwachstellen-Exploits sowie der Aufwand für IT-Sicherheitsmitarbeiter deutlich reduziert.

## Ressourcenschonend und effektiv auch ohne regelmäßige Updates

Unsere Wissensdatenbank umfasst 50 TB an Daten und über vier Milliarden Hashes – doch diese riesigen Datenmengen wirken sich nicht im Geringsten auf Ihre Ressourcen oder die Performance aus. Einheitlicher Cloud-Modus für Schutzkomponenten liefert optimale Sicherheit bei minimalen Auswirkungen auf PC-Ressourcen und Bandbreitenauslastung.

Unser mathematisches Modell analysiert über 100 000 Testfunktionen und verwendet 10 Millionen Verhaltensprotokolle, um die Modelle zu „trainieren“ – und das in einem kompakten, clientseitigen 2-MB-Paket.

## Rationalisierung von IT-Aufgaben

Die Remote-Bereitstellung von Drittanbietersoftware ist nur der Anfang. **Das automatisierte Vulnerability Assessment und Patch Management**, das auf Echtzeitinformationen zu ausgenutzten Schwachstellen basiert, hält potenziell anfällige Software auf dem neuesten Stand, damit sich Ihre IT-Administratoren auf wichtigere Aufgaben konzentrieren können.

## Verhindert Datenschutzverletzungen

Nutzen Sie die integrierte **Microsoft BitLocker-Verwaltung**, um die Windows-interne Verschlüsselung zu aktivieren, oder **verschlüsseln** Sie Ihre Daten nach FIPS 140-2 und Common Criteria: EAL2+. Die zentral verwaltete **Gerätekontrolle** schützt vor den Folgen von Datenverlust auf nicht genehmigten oder unverschlüsselten tragbaren Geräten sowie vor dem Hochladen infizierter Daten von einem Gerät.

## Unterstützung für Remote- und Mobile-Szenarien

Der integrierte Schutz vor **Bedrohungen, die gezielt auf mobile Daten ausgerichtet sind**, stoppt Versuche, Geräteschwachstellen als Sprungbrett für die Infiltration der Infrastruktur zu nutzen. Sie können Ihre **vorhandene EMM-Lösung** nutzen, um den Schutz für Mobilgeräte zu implementieren und zu konfigurieren, und Ihre Sicherheit an aktuellen Geschäftsprozessen ausrichten.

## Gesteigerte Effizienz dank zentraler Verwaltung für alle Plattformen

Die Webkonsole bietet Ihnen vollständige Transparenz und Kontrolle über alle Workstations, Server und Mobilgeräte – egal, wo sich diese befinden und welche Aktivitäten sie ausführen. Kaspersky Endpoint Security for Business ist nahezu unbegrenzt skalierbar und bietet Zugriff auf Lizenzierung, Remote-Fehlerbehebung und Netzwerkkontrollen. Die zentrale Verwaltung wird ergänzt durch Active Directory-Integration, **rollenbasierte Zugriffskontrolle** und integrierte Dashboards.

## Mehr Produktivität, weniger Bedrohungen

Der **Cloud-basierte Spam-Schutz** von Kaspersky Lab erkennt sogar raffinierteste Spam-Nachrichten in beliebigen Sprachen – mit minimalem Verlust wertvoller Kommunikation durch Fehlalarme. Je geringer der Zeitaufwand und die Risiken für bzw. durch Spam, desto mehr **System- und Mitarbeiterressourcen lassen sich einsparen**.

## Weniger Aufwand für Updates und viele weitere Vorteile

Nutzen Sie nahtlose Upgrades für neue Produktversionen, einschließlich verschlüsselter Geräte. Selbst während der Migration zwischen Windows-Versionen bleibt der Schutz jederzeit aktiv. Mit einheitlichen Sicherheitsrichtlinien und vordefinierten Einstellungen bietet Ihnen Kaspersky Endpoint Security for Business die Freiheit, selbst zu entscheiden, ob und wann Sie Einstellungen übernehmen und wann Sie mit allen aktuellen Einstellungen und Richtlinien zu neuen Versionen migrieren.

Unsere IaaS-Lösung bietet verbesserte Fehlertoleranz und garantiert weniger als vier Stunden Ausfallzeit pro Jahr. Gleichzeitig erhalten Sie dank einer Verwaltungskonsole, die Bereitstellungen in den Cloud-Umgebungen von Amazon und Microsoft Azure unterstützt, umfassende Flexibilität hinsichtlich Sicherheitseinstellungen und Updatezyklen. Verwenden Sie die Webkonsole zusammen mit oder anstelle der MMC-basierten Konsole.

Die Tools und Technologien von **Kaspersky Endpoint Security for Business** sind optimal auf drei verschiedene Stufen verteilt und erfüllen so die steigenden Sicherheits- und IT-Anforderungen an jedem Punkt Ihrer Unternehmensentwicklung.



Unternehmen mit reiferen IT-Umgebungen, die neue und ältere Systeme verbinden, müssen ihre Sicherheit an die Anforderungen und Beschränkungen der einzelnen Systeme anpassen. Unsere umfassende Sicherheitslösung für Endpoints, Gateways und Server ermöglicht Ihnen genau das und bietet Ihnen zuverlässige Sicherheit, die Sie an Ihre IT-Umgebung anpassen können.



Entscheiden Sie sich für die Stufe „Advanced“, wenn Sie die Sicherheit Ihres Unternehmens noch weiter steigern möchten. Diese Stufe sichert nicht nur Ihre Endpoints und Server, sondern liefert auch zusätzliche Sicherheitsebenen zum Schutz vertraulicher Daten, zur Beseitigung von Schwachstellen und zur Vereinfachung von Verwaltungsaufgaben.



Im Zuge der Digitalisierung Ihrer Betriebsabläufe müssen Sie sämtliche Linux-Server, Mac-Laptops und Android-Mobilgeräte schützen. Wir liefern agile Sicherheit, mit der Sie jeden Endpoint in Ihrem Unternehmen schützen können: über eine einzige Lösung mit einer zentralen flexiblen Verwaltungskonsole.

**Mehr Sicherheit – genau dort, wo Sie sie brauchen**

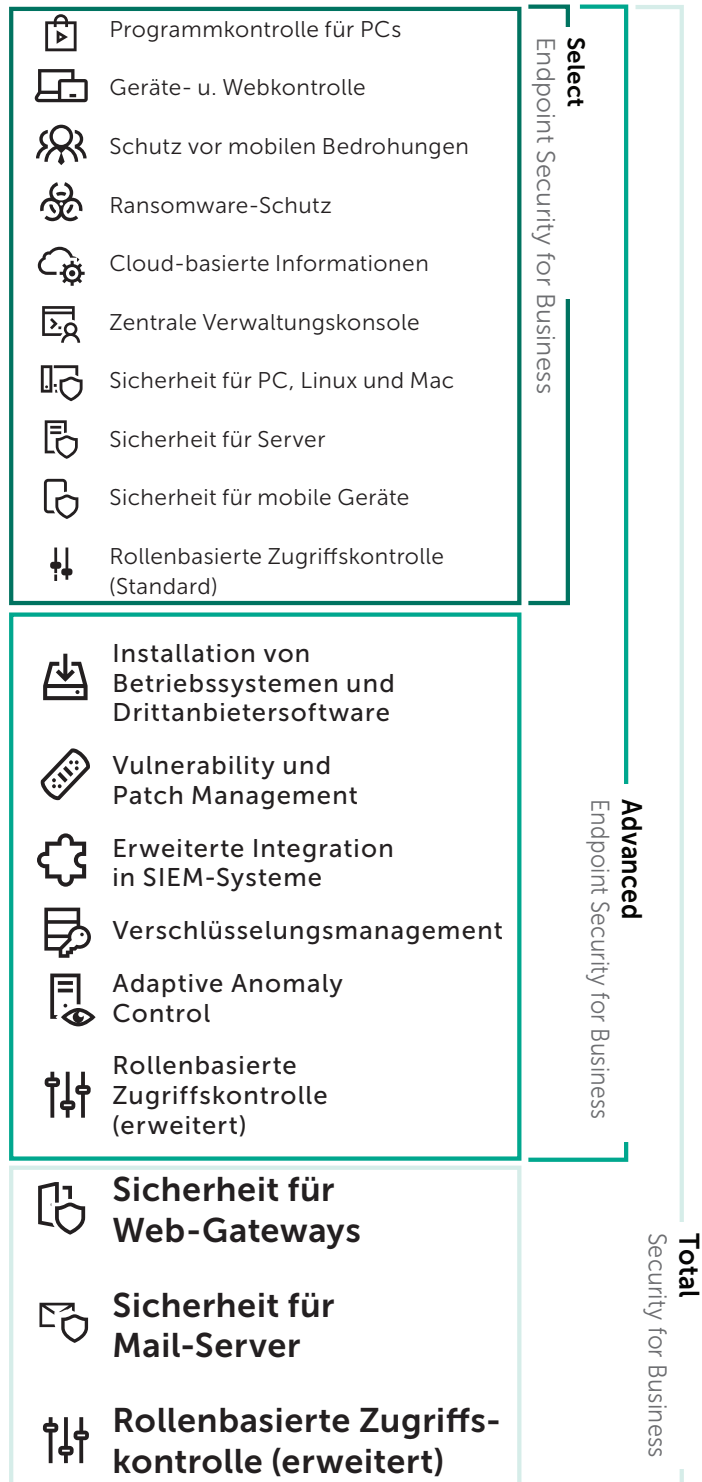
Für Kunden von Kaspersky Endpoint Security for Business Select sind die folgenden Komponenten bereits in unsere Stufen „Advanced“ und „Select“ als separate Add-ons enthalten:

- Kaspersky Vulnerability und Patch Management: Automatisiert und zentralisiert die Erkennung von Software-Schwachstellen sowie das zugehörige Patch Management und schützt vor Bedrohungen wie Ransomware.
- Kaspersky-Verschlüsselung: Nutzen Sie die Full-Disk- oder File-Level-Verschlüsselung und greifen Sie per einmaliger Anmeldung direkt auf verschlüsselte Dateien zu.

Sie können die Add-ons nach dem Kauf einfach über die einheitliche Verwaltungskonsole aktivieren.

# Welche Stufe ist die richtige für Sie?

Wir unterstützen Sie bei Verwaltung und Schutz Ihres Unternehmens. Unabhängig von Ihren individuellen und immer neuen IT-Anforderungen bietet Ihnen **Kaspersky Endpoint Security for Business** die ideale Lösung.



## Support und Services

Wir sind in mehr als 200 Ländern mit 35 Niederlassungen weltweit tätig und bieten engagierten Support rund um die Uhr, der sich in unseren Maintenance Service Agreement-Paketen (MSA) widerspiegelt. Unsere professionellen Serviceteams stehen bereit, um sicherzustellen, dass Sie den maximalen Nutzen aus Ihrer Lösung ziehen. Sie bieten Unterstützung bei der Implementierung wie auch bei kritischen Vorfällen.

## True Cybersecurity. Fragen Sie einfach unsere Kunden



Auch 2018 wurde Kaspersky Lab im Rahmen der **Gartner Peer Insights Customers' Choice for Endpoint Protection** ausgezeichnet. Als die Kategorie „Endpoint-Schutz“ 2017 eingeführt wurde, gewann Kaspersky Lab den **Platinum Award**, die höchste Auszeichnung in dieser Kategorie. Wir freuen uns über dieses Maß an Anerkennung von den Menschen, deren Urteil uns am wichtigsten ist – unseren Kunden –, und sind stolz auf die Bewertung von **4,7 von 5** für Endpoint-Protection-Plattformen.

### Unvergleichliche Transparenz und Compliance

Unternehmen sind auf Neutralität und Datenhoheit angewiesen – unsere Produkte scannen Daten zwar, sie sammeln sie jedoch nicht. Die statistischen Daten werden zur Gewährleistung der geopolitischen Neutralität in der Schweiz verarbeitet. Die Eröffnung des ersten Transparenzzentrums unserer Branche bringt uns dem Ziel, vollständig transparent zu sein, ein Stück näher. Unsere Hoffnung ist, dass andere Anbieter unserem Beispiel folgen werden.

## Bei Entscheidungsträgern beliebt

Vergessen Sie den Marketing-Hype: Hören Sie lieber auf die vielen Empfehlungen von Kunden, die Kaspersky Endpoint Security for Business bereits nutzen und die Vorteile der Lösung genießen:

- Dauerhaft herausragender Schutz: Dank einfacher Upgrades sind Ihre Systeme immer aktuell und bereit, auch die neuesten Cyberbedrohungen abzuwehren
- Benutzerfreundliche und zentralisierte Verwaltung: ein Server, eine Webkonsole, ein einzelner Agent
- Enge Integration der Komponenten: intern entwickelt, mit der Erfahrung aus Jahrzehnten voller unabhängiger Tests und Bestnoten
- Alles mit nur einem Produkt: transparentes Preis- und Lizenzmodell

#### Qualitätsprüfer

Branche Fertigung

Rolle Infrastruktur und Betrieb

Unternehmensgröße Unter 50 Mio. USD

Letzter Stand 25. Oktober 2018

<https://kas.pr/epp-ref2>

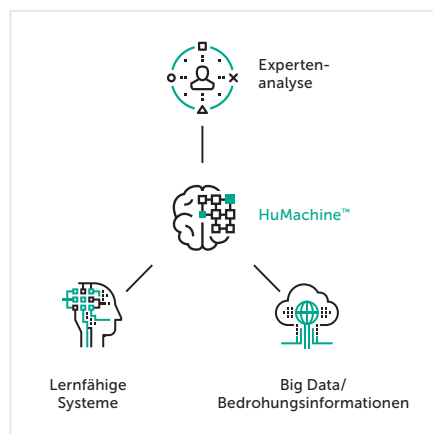
„Umfassender Schutz mit schneller Implementierung.“

## Sehen Sie selbst

Erleben Sie True Cybersecurity selbst! Auf dieser [Seite](#) können Sie die vollständige Version von Kaspersky Endpoint Security for Business testen.

## Blick auf das Ganze – IT-Sicherheitslösungen für Unternehmen von Kaspersky Lab

Der Schutz von Endpoints ist entscheidend, befindet sich jedoch noch in den Kinderschuhen. Ganz gleich, ob Sie auf den Branchenführer vertrauen oder bei Ihrer Sicherheitsstrategie mit nur einem Anbieter arbeiten – Kaspersky Lab bietet Produkte für Hybrid-Cloud-Infrastrukturen sowie für ältere Windows XP-Systeme an, die sich gegenseitig ergänzen oder unabhängig voneinander funktionieren. So müssen Sie weder auf Leistung noch auf Flexibilität verzichten. Weitere Informationen finden Sie auf unserer [Webseite](#).



Kaspersky Lab

Finden Sie einen Partner in Ihrer Nähe: [www.kaspersky.de/partners](http://www.kaspersky.de/partners)

Kaspersky for Business: [www.kaspersky.de/business-security](http://www.kaspersky.de/business-security)

Enterprise Cybersecurity: [www.kaspersky.de/enterprise](http://www.kaspersky.de/enterprise)

IT-Sicherheitsnachrichten: [www.kaspersky.de/blog/b2b/](http://www.kaspersky.de/blog/b2b/)

#truecybersecurity  
#HuMachine

[www.kaspersky.de](http://www.kaspersky.de)

© 2019 Kaspersky Labs GmbH. Alle Rechte vorbehalten. Eingetragene Markenzeichen und Handelsmarken sind das Eigentum ihrer jeweiligen Rechtsinhaber.