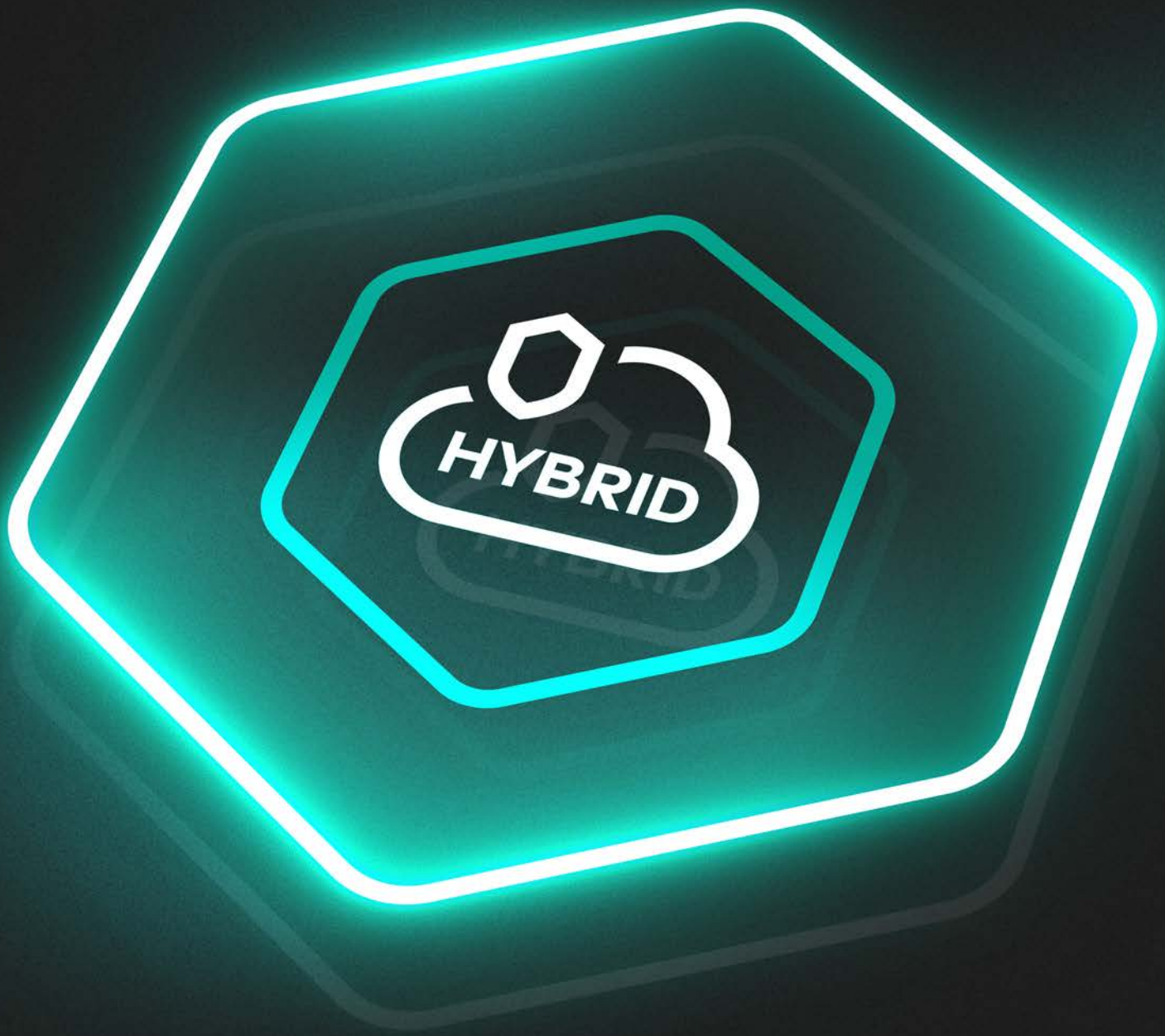


Kaspersky Hybrid Cloud Security

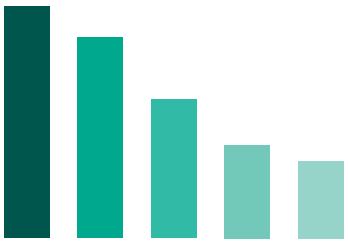
kaspersky BRING ON THE FUTURE

Im Zuge des digitalen Wandels steigen immer mehr Unternehmen immer schneller auf die Cloud um. Einerseits bieten Initiativen zur Förderung des digitalen Wandels Unternehmen zwar viele Vorteile, wie zum Beispiel Effizienzsteigerungen. Andererseits gibt es aber auch eine Kehrseite: Die Infrastrukturen werden komplexer, was zu erheblichen Problemen in Bezug auf Sicherheitsrisiken, Governance, Personalressourcen, Leistungsoptimierung sowie zu neuen Vorschriften und Kosten führt. Mit Kaspersky Hybrid Cloud Security können Sie all diesen Herausforderungen effektiv begegnen.

Leistungsstarker und Cloud-nativer Schutz für Ihre Hybrid-Umgebungen

Mit Kaspersky Hybrid Cloud Security können Sie den Umstieg auf die Cloud und die Geschäftstätigkeit im Ganzen sicherer und effizienter gestalten. Dieses eine Produkt sichert Ihre gesamte hybride Infrastruktur, senkt Risiken, reduziert den Verbrauch von Virtualisierungsressourcen und unterstützt die Einhaltung gesetzlicher Vorschriften. Kaspersky Hybrid Cloud Security sorgt für mehr Transparenz und eine vereinfachte Verwaltung und spart Ihnen und Ihrem Team wertvolle Zeit und finanzielle Ressourcen. Um die Sicherheit brauchen Sie sich keinen Kopf mehr zu machen, sondern können sich voll und ganz auf die anderen Aspekte der digitalen Transformation konzentrieren.

Die größten Cloud-Herausforderungen



- Sicherheit **81 %**
- Cloud-Verwaltungskosten **79 %**
- Governance und Compliance **75 %**
- Verwaltung der Multi-Cloud **72 %**
- Cloud-Migration **71 %**

Laut State of the Cloud Report von Flexera 2021

Umfassender Schutz bezüglich der besonderen Sicherheitsrisiken hybrider Umgebungen

- Der mehrstufige Schutz vor Bedrohungen bekämpft proaktiv eine breite Palette von Cyberangriffen, darunter Malware, Phishing und vieles mehr.
- Lernfähige Systeme, gestützt durch menschliche Expertise, liefern hohe Erkennungsraten bei minimalen Fehlalarmen.
- Bedrohungsdaten in Echtzeit helfen bei der Abwehr neu aufkommender Angriffsformen.

Cloud-nativer Ansatz für bestmögliche Sicherheit in hybriden Infrastrukturen

- Unsere leistungsstarke Engine schützt die gesamte hybride Infrastruktur, unabhängig von der Arbeitslast – physisch, virtualisiert, in der Private, Public oder Hybrid Cloud.
- Der zugrundeliegende plattformunabhängige Ansatz ist nativ in Public Clouds integrierbar, wodurch diese vollständig DevOps-fähig werden.
- Light Agents, die für jedes Betriebssystem optimiert sind, reduzieren den Verbrauch von Virtualisierungsressourcen um bis zu 30 % und schaffen damit Freiraum für andere Einsatzbereiche.

Kosteneffizienz und einfache Verwaltung für einen erfolgreichen Umstieg auf die Cloud

- Dank eines flexiblen Lizenzmodells zahlen Sie nur für die Funktionen, die Sie auch wirklich benötigen, damit Sie den größten Nutzen aus Ihrer Investition ziehen.
- Eine einheitliche Cloud-Konsole vereinfacht das Sicherheitsmanagement Ihrer gesamten Infrastruktur und spart wertvolle Mitarbeiterressourcen in der IT.
- Die unkomplizierte Bestandsaufnahme der Cloud-Infrastruktur und die automatisierte Sicherheit, unabhängig vom Standort der Agents, sorgen gleichermaßen für maximale Transparenz.

Compliance-fähige Sicherheit für stark regulierte Branchen

- Dieses flexible und vielseitige Produkt wurde entwickelt, um Sie dauerhaft bei der vollständigen Einhaltung gesetzlicher Vorschriften zu unterstützen, und zwar durch Technologien, die von der Systemhärtung und dem Selbstschutz bis hin zu Vulnerability Assessment und Automated Patch Management reichen.
- Die breite Palette an Funktionen ermöglicht weitreichende Anpassungen an Compliance-Anforderungen und die aktuelle Risikolandschaft, so dass Ihre Sicherheit stets auf dem neuesten Stand der Gesetzgebung bleibt.

Funktionen

Mehrschichtiger Schutz vor Bedrohungen

Globale Threat Intelligence	Sammelt Echtzeitdaten über den Zustand der Bedrohungslandschaft und deren Veränderungen.
Lernfähige Systeme	Macht die enorme Menge an global verfügbaren Bedrohungsdaten durch lernfähige Algorithmen und menschliche Expertise greifbar.
Schutz vor Bedrohungen im Web und für E-Mails	Schutzfunktion vor Web- und E-Mail-Bedrohungen sichert virtuelle und Remote-Desktops.
Protokollprüfung (Log Inspection)	Protokollprüfung untersucht Protokolldateien im Hinblick auf optimale Betriebshygiene.
Verhaltensanalyse	Schützt durch die Überwachung von Programmen und Prozessen vor hochentwickelten Bedrohungen, wie körperloser oder skriptbasierter Malware.
Remediation Engine	Die Remediation Engine sorgt ggf. für das Rollback aller schädlichen Aktivitäten innerhalb von Cloud-Umgebungen.
Exploit Prevention	Bietet wirksamen Schutz bei vollständiger Kompatibilität mit geschützten Anwendungen und minimalen Auswirkungen auf die Systemleistung.
Funktionalität zum Schutz vor Ransomware	Schützt unternehmenskritische Daten vor jeglicher Form von Erpressungsversuchen. Dazu gehört auch das Unterbinden von Remote-Verschlüsselungen und die Entschlüsselung betroffener Dateien in den ursprünglichen Zustand.
Schutz vor Bedrohungen im Netzwerk	Network Threat Protection dient der Aufdeckung netzwerkbasierter Eingriffe in Cloud-Ressourcen.
Container-Schutz	Verhindert, dass Infektionen über manipulierte Container in die hybride IT-Infrastruktur eingeschleust werden.

Systemhärtung für mehr Stabilität

Programmkontrolle	Ermöglicht die Verankerung aller Hybrid Cloud-Umgebungen im Modus „Default Deny" für eine optimale Systemabsicherung. Auf diese Weise können Sie die Palette der ausgeführten Programme auf rechtmäßige und vertrauenswürdige Programme beschränken.
Gerätekontrolle	Gerätekontrolle legt fest, welche virtuellen Geräte auf einzelne Cloud-Umgebungen zugreifen dürfen.
Webkontrolle	Regelt die Verwendung von Webressourcen durch virtuelle und Remote-Desktops, um Risiken zu minimieren und die Produktivität zu fördern.
Host-basierte Angriffsüberwachung (HIPS)	Weist gestarteten Programmen Vertrauenskategorien zu und schränkt auf diese Weise den Zugriff auf kritische Ressourcen sowie die Möglichkeiten dieser Programme ein.
File Integrity Monitoring	Überwachung der Dateiintegrität trägt dazu bei, die Integrität von kritischen Systemkomponenten und anderen wichtigen Dateien zu gewährleisten.
Vulnerability Assessment und Patch Management	Zentralisiert und automatisiert wesentliche Sicherheits-, Systemkonfigurations- und Verwaltungsaufgaben, wie z. B. Vulnerability Assessment, Bereitstellung von Patches und Updates, Bestandsverwaltung und Rollouts von Programmen.

Übergreifende Transparenz

Zentrales Sicherheitsmanagement	Diese Schutzfunktion für Endpoints und Server über die gesamte Infrastruktur hinweg können Sie über eine einzige zentrale Konsole verwalten – im Büro, in Ihrem Rechenzentrum und in der Cloud.
Cloud-API	Die nahtlose Integration mit öffentlichen Umgebungen ermöglicht das Erkennen der Infrastruktur, die automatisierte Bereitstellung von Agenten und die richtlinienbasierte Verwaltung sowie eine einfachere Bestands- und Sicherheitsbereitstellung.
Flexible Verwaltungsoptionen	Bieten Flexibilität durch Mehrmandantenfähigkeit, genehmigungsorientiertes Account Management und rollenbasierte Zugriffssteuerung, während die Vorteile der einheitlichen Orchestrierung über einen einzelnen Server erhalten bleiben.
SIEM-Integration	Dank der Möglichkeit zur Integration des Produkts mit dem „Security Information and Management System" können verschiedene Aspekte der Cybersicherheit im Unternehmen an einem Ort zusammengeführt werden – über das gesamte hybride IT-Netzwerk hinweg.

Warum Kaspersky Hybrid Cloud Security?

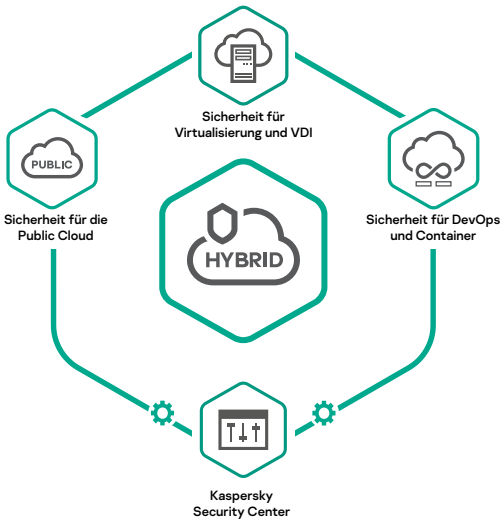
30 %

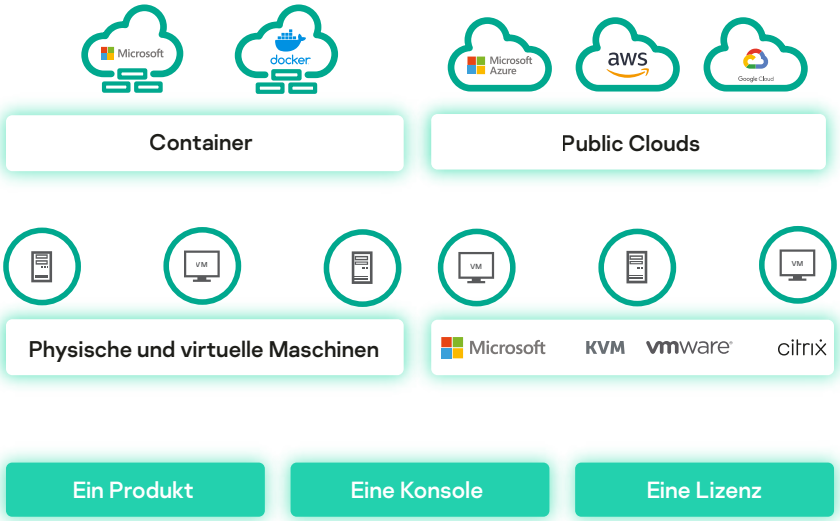
Einsparungspotenzial bei den Virtualisierungshardware-Ressourcen im Vergleich zu traditionellen Endpoint-Sicherheitslösungen

TOP 3

anhaltend hervorragende Bewertungsergebnisse. Auch im vergangenen Jahr haben Kaspersky-Produkte in zahlreichen unabhängigen Tests mit 57 ersten Plätzen sowie 63 Top-3-Platzierungen wieder hervorragend abgeschnitten (weitere Informationen finden Sie unter kaspersky.de/top3).

Ein Produkt für alle Sicherheitsanforderungen in der Cloud





Ein Produkt | **Eine Konsole** | **Eine Lizenz**

Kundenmeinungen

„Diese Lösung hilft, virtuelle und Cloud-Umgebungen zu schützen, ohne die Systemleistung zu beeinträchtigen oder die Benutzererfahrung zu stören."

„Sämtliche Sicherheitslösungen lassen sich in einer einzigen Lizenz zusammenführen."

„Die Notwendigkeit zur Installation zusätzlicher Antiviren-Software und anderer Agents entfällt."

„Zentral verwaltete Cloud-Lösung für den Schutz von Daten. Alles an einem Ort."

„Der Schutz gilt sofort für alle VMs, weil man keine neuen Updates herunterladen muss."

„Optimale Lösung, die ganz ohne lange Administratorschulungen auskommt."

Auszüge aus Bewertungen bei Amazon und Gartner

Demo anfordern

www.kaspersky.de