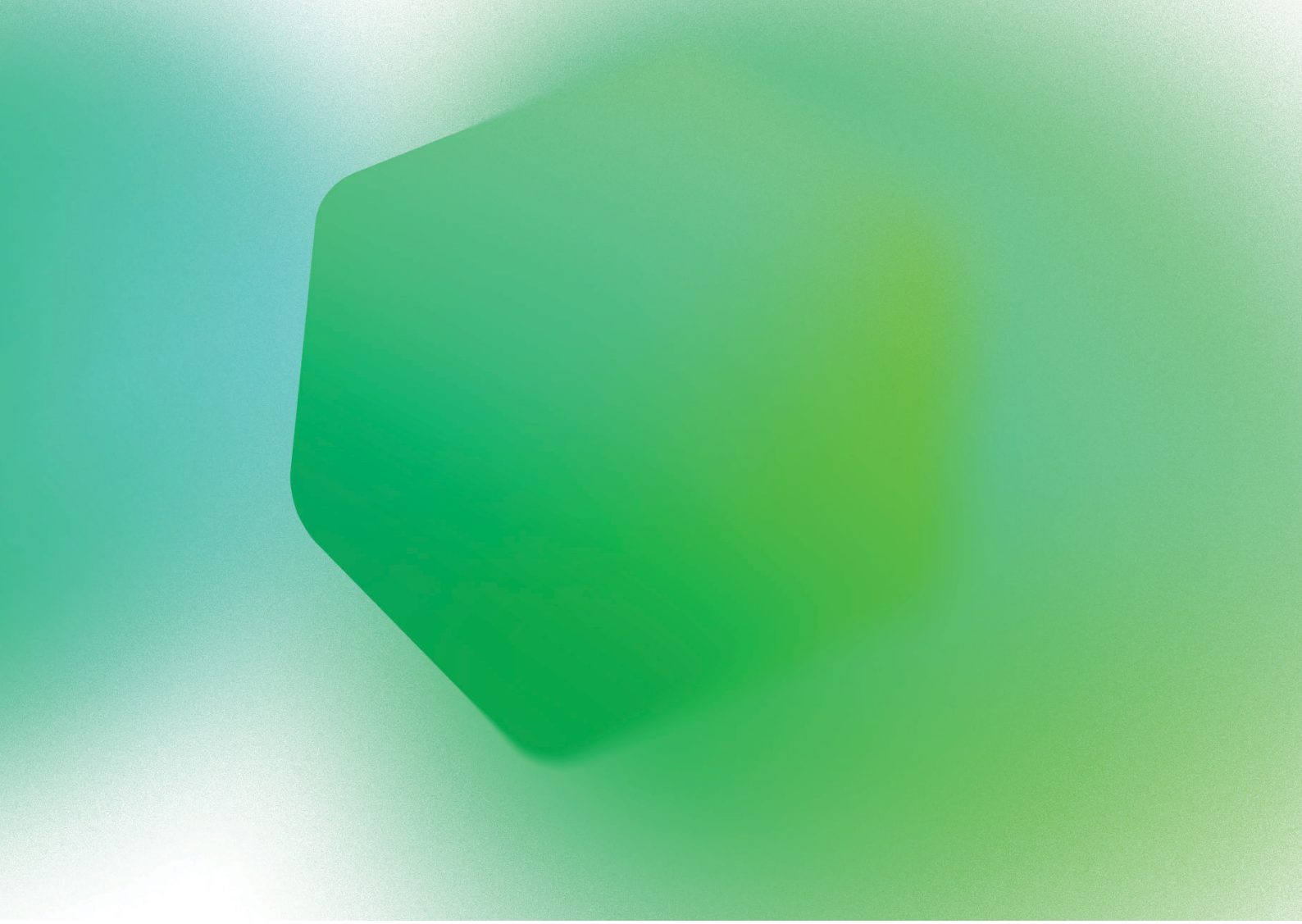


Alle notwendigen Schutzfunktionen für Ihren Umstieg auf die Cloud

Weitere Informationen finden Sie unter kaspersky.de

kaspersky

Digitaler Wandel und seine Auswirkungen auf die IT

Während Unternehmen sich dem digitalen Wandel stellen und ihre Infrastrukturen in die Cloud verlegen, gilt es eine Reihe von echten Herausforderungen zu meistern. Wie behalten ich die Kontrolle über die Unternehmenswerte – oder wird sie mir einfach aus der Hand genommen? Wie schließt man Integrationslücken und überwindet Grenzen, damit man auch wirklich alle Vorteile der Umstellung ausschöpfen kann? Und wie hält man die Auswirkungen dieser Veränderungen auf die Leistung gering, ohne die Kapitalrendite dieser nicht ganz unerheblichen Investition zu gefährden?

Der digitale Wandel hat viele Gesichter. Man braucht ganz neue IT-Funktionen für die Cloud. Vorhandene Server oder Programme werden migriert. Alte Hardware wird wegen der Verlegung in die Cloud außer Betrieb genommen. Services werden auf automatische Skalierung und Arbeitsweisen im Schnellverfahren umgestellt.

Verlegung in die Cloud: heute wichtiger denn je

Tatsächlich stehen wir noch ganz am Anfang dessen, was die Cloud-Einführung tatsächlich für uns bedeutet.

Während des Corona-Ausbruchs im Jahr 2020 und dem daraus resultierenden massenhaften Umstieg auf Fernarbeit, konnten Public Cloud-Anbieter die steigende Nachfrage noch scheinbar mühelos bedienen, indem sie Nodes im Akkord bereitstellten. Das Arbeiten von Zuhause hat auch gezeigt (als ob wir das nicht längst gewusst hätten), wie abhängig alle Bereiche des wirtschaftlichen Lebens von ununterbrochenen Online-Zugängen und -Kommunikationskanälen sind und wie erfolgreich (oder nicht erfolgreich) wir unsere Infrastrukturen ohne physischen Zugang zur Hardware-Schicht verwalten können. Unternehmen, die den Umstieg auf die Cloud bereits vollzogen hatten, konnten bereits erheblich davon profitieren in diesen Krisenzeiten, in denen Cloud-Anbieter geradezu als „Helden" besungen wurden.[1]

Eine weitere Technologie, die im Zuge der Pandemie ebenfalls sofort Aufwind bekam, ist die virtuelle Desktop-Infrastruktur (VDI). Viele Unternehmen sahen sich außer Stande, genügend Laptops und Computer zu beschaffen, die erforderlich waren, um alle Mitarbeiter mit der notwendigen Ausrüstung für Fernarbeit auszustatten. Stattdessen mussten sie ihre Angestellten bitten, mit eigenen Geräten zu arbeiten. Bei den Firmen, die bereits eine zentrale VDI-Infrastruktur eingeführt hatten, konnten Mitarbeiter immerhin auf einer Vielzahl von Geräten in einer sicheren und kontrollierten Umgebung arbeiten. VDI bietet darüber hinaus eine Vielzahl von Datensicherungsoptionen, so dass man sofort an einem beliebigen anderen Gerät weiterarbeiten kann, sollte das eigene einmal ausfallen.

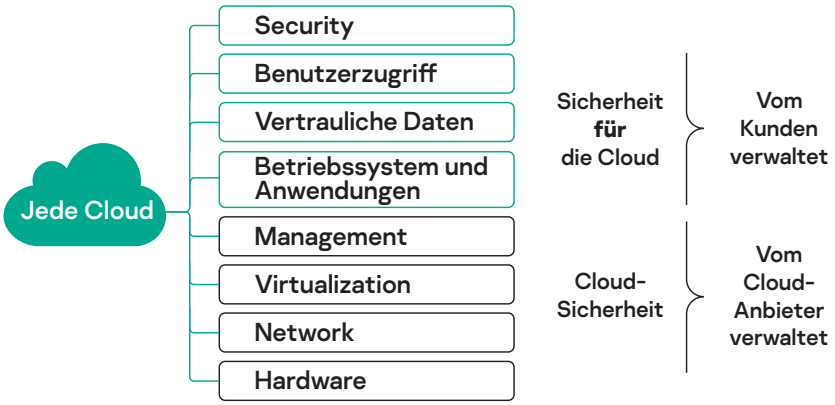
Nachdem das Arbeiten in der Cloud in Bezug auf Geschäftskontinuität und Resilienz in schwierigen Zeiten klare Vorteile gebracht hat, ist es fast unvermeidlich, dass die große Mehrheit der Unternehmen früher oder später auf diese Technologie umsteigen wird. Und der Prozess der weiteren Entwicklung mit und in der Cloud wird sehr wahrscheinlich zu einem Zwischenstadium führen, in dem wir mit einer komplexen, heterogenen und hybriden Infrastruktur arbeiten, die physische, virtuelle und Cloud-Plattformen in sich vereint – und die gleichzeitig verwaltet, abgestimmt und supported werden muss.

Wenn sich Ihre Infrastruktur plötzlich nicht mehr in Ihrem Netzwerk befindet

Es gab eine Zeit, in der wir als unsere eigenen Netzwerkentwickler und -eigentümer mithilfe eines Erkennungstools ein vollständiges Inventar unserer Workstations, Server, Services und Programme erstellen konnten. Und das war relativ einfach, weil wir die Kontrolle über unser Netzwerk hatten. Wir konnten ein Kabel nachverfolgen. Wir konnten uns in Hypervisor-Einstellungen vertiefen, um den Umfang unseres Software-definierten Netzwerks zu ermitteln.

In der Welt von IaaS ist uns diese Möglichkeit abhanden gekommen – und das ist auch gut so. Jetzt können wir uns entspannt zurücklehnen – der Hardware-Layer liegt nicht mehr in unserem Verantwortungsbereich. Dafür ist jetzt der IaaS-Anbieter zuständig.

Sicherheitsmodell mit gemeinsamer Verantwortung



1 https://www.crn.com/news/cloud/in-coronavirus-crisis-public-cloud-is-an-unsung-hero-

Aber zusammen mit der Verantwortung sind auch Kontrolle und Transparenz verloren gegangen. Natürlich kann man auch immer noch herkömmlich arbeiten, indem man beispielsweise unterschiedliche Teile der Infrastrukturen per VPN verbindet und IT-Assets in der Cloud praktisch genauso behandelt wie virtualisierte Workloads. Im Grunde genommen will man das aber ja gar nicht, weil man mit dieser traditionellen Arbeitsweise auch auf die Vorteile des neuen Ansatzes verzichtet.

Neue Tools für neue Realitäten

Und hier zeigt sich ein Dilemma. Alte Werkzeuge funktionieren in hybriden Infrastrukturen nicht gut. Gleichzeitig konzentrieren sich die neuen Tools nur auf Migrationsaspekte, wobei die Workload-Sicherheit allzu oft als Thema behandelt wird, das erst nach der Migration angegangen werden muss. Die einzig verbleibende Option besteht für die meisten von uns dann darin, unterschiedliche Sicherheitstools für die unterschiedlichen Teile der Infrastruktur zu verwenden. Mit dem Ergebnis, dass Zuständigkeiten verwässern, die Transparenz Lücken bekommt, Kontrollen nicht greifen und letztendlich Sicherheitslücken entstehen, auf die sich Cyberkriminelle liebend gern stürzen.

Damit die digitale Evolution möglich wird, müssen die von Ihnen verwendeten Werkzeuge verändert und an die neuen Realitäten angepasst werden. Sie müssen über zahlreiche Plattformen nutzbringend funktionieren, wo immer diese auch sein mögen – vor Ort, physisch oder virtualisiert oder eben „in der Cloud" – ein Begriff, der für uns schon so alltäglich geworden ist, der aber für die meisten Menschen immer noch „auf dem Computer eines anderen" bedeutet.

Durchgängige Transparenz über alle Workloads hinweg

Bei Kaspersky denken wir über Sicherheitslücken fast genauso viel nach wie über die Bedrohungen, die sich diese zunutze machen. Zweifelsohne stellt die Unfähigkeit, Richtlinien durchzusetzen, die Kontrolle zu behalten und über die gesamte Infrastruktur hinweg eine einheitliche Konfiguration zu gewährleisten, eine größere Gefahr dar als eine Schwachstelle in Ihrem Betriebssystem oder Ihrer Unternehmensanwendung. Schwachstellen in der Software können vom Software- oder Sicherheitsanbieter behoben werden. Aber wer erkennt Abweichungen in den Einstellungen auf mehreren Sicherheitsverwaltungskonsolen, die dem interessierten Angreifer einen bequemen Einstiegspunkt bieten?

Wir glauben, dass eine einzelne zentrale Verwaltungskonsole die beste Lösung für dieses Problem ist. Wenn Sie die Sicherheit für alle physischen, virtualisierten, mobilen und Cloud-Komponenten in Ihrer Umgebung nahtlos überprüfen können, ist die Gefahr eines von Menschen gemachten Fehlers, der zu einer Sicherheitslücke führt, um ein Vielfaches geringer.

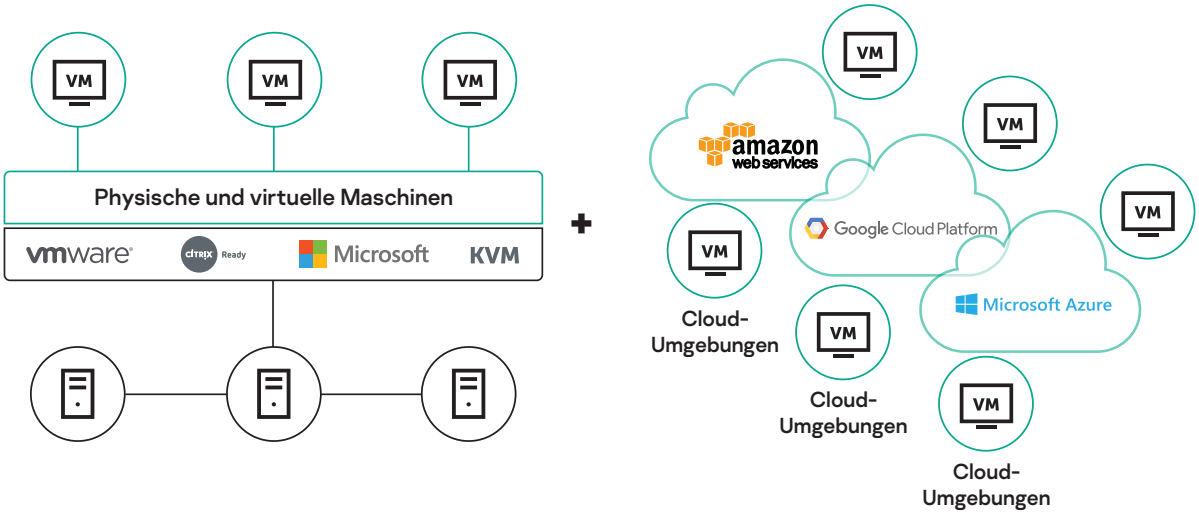
Lückenloser Schutz für komplexe hybride Unternehmen

Kaspersky Hybrid Cloud Security schützt hybride IT-Infrastrukturen mithilfe durchgängiger Transparenz und zentralen Kontrollfunktionen für alle Cloud-Umgebungen, virtualisierten Infrastrukturen und physischen Maschinen – und zwar in jeder Phase Ihres Umstellungsprozesses und darüber hinaus. Vorgaben werden jederzeit eingehalten und die Systemleistung wird nicht beeinträchtigt. Eine einzige Verwaltungskonsole mit einheitlichen Richtlinien reduziert Aufwand und Komplexität in der Verwaltung und hilft so diese alles entscheidenden Sicherheitslücken zu schließen.

Public Clouds – transparent und benutzerfreundlich

Kaspersky Hybrid Cloud Security vereinfacht die Orchestrierung der Public Cloud-Bereitstellung mit Features wie:

- Eine zentrale Verwaltungskonsole, die in einer beliebigen Zahl von untergeordneten Infrastrukturen bereitgestellt und innerhalb einer Verwaltungsserver-Hierarchie organisiert wird, um selbst sehr komplexe Bereitstellungen lückenlos bedienen zu können
- Native API-Integration in AWS-, Microsoft Azure- und Google Cloud-Plattformen
- Schutz für Windows- und Linux-Workloads
- Sehr einfache Bestandsaufnahme innerhalb der Cloud-Infrastruktur sowie automatisierte Sicherheit von Sicherheitsagents unabhängig von deren Standort
- Flexibles Tarifmodell:
  - Verbrauchsabhängige Abrechnung, wobei die Bereitstellung der Schutzfunktionen und die Rechnungslegung direkt über den Marketplace des Cloud-Anbieters erfolgen
  - Jahresverträge mit SaaS-Angebot auf ausgewählten Plattformen
  - BYOL (Bring you own License): Die Lösung kann über eine bei einem Kaspersky-Partner erworbene Lizenz aktiviert werden.



Automatische Erkennung und Einführung

Integration mit Cloud-APIs sorgt für Automation und administrative Flexibilität. Die Verwaltungskonsole muss alle Instanzen sehen können, die unter den angegebenen Konten laufen. Anhand dieser Informationen stellt sie Sicherheitsagents bereit und wendet Sicherheitsrichtlinien an. Bei neuen Instanzen wird über eine IAM-Rolle oder einen Skript-Bereitstellungsmechanismus sichergestellt, dass die Instanz ab dem Erstellungszeitpunkt sofort umfassend geschützt ist.

Automatische Skalierung von Gruppen

Dank der elastischen Konfigurierbarkeit von Kaspersky Hybrid Cloud Security kann die Lösung automatisch auf steigende Lasten reagieren, wenn neue Instanzen erstellt und von der Cloud betrieben werden. Mit Richtlinien für APIs und automatisches Skalieren wird sichergestellt, dass jede neue Instanz in jeder automatisch skalierten Gruppe umfassend geschützt wird und die von der Organisation aufgestellten Richtlinien erfüllt.

Container-Sicherheit

Einer der wesentlichen Anwendungsfälle für Public Clouds ist die Aktivierung von DevOps. Aber die Einführung und breit angelegte (und häufig unzureichend kontrollierte) Verwendung von Container-Technologien wie Docker stellt eine ständige Herausforderung für Sicherheitsmanager dar. Kaspersky Hybrid Cloud Security schützt Docker- und Windows-Container, damit Angreifer schädliche Container-Komponenten nicht als Einfallstor in die internen Bereiche einer Organisation nutzen können. Umfassender Schutz für den Speicher des Containerisierungshosts, Aufgaben für Container- und Datenimage-Scans sowie Skript-fähige Schnittstellen ermöglichen einen „Security-as-Code"-Ansatz, der auch eine Integration von Sicherheitsaufgaben in CI/CD-Pipelines vorsieht.

Virtualisierung: Ausgleich zwischen Sicherheit und Effizienz im Rechenzentrum

Auch wenn Public Clouds die IT grundlegend verändern werden, bedeutet das noch lange nicht das Ende von lokalen Virtualisierungen und Private Clouds. Erfolgreiches Risikomanagement im Unternehmen bedeutet, dass jede virtuelle Maschine (VM) und jeder Virtualisierungsspeicher geschützt wird. Während aber die Ziele für die Sicherheit von Public und Private Clouds dieselben sind (Cyberrisiken mindern und in den Griff bekommen), unterscheidet sich der Weg dorthin ganz erheblich.

Bei der Virtualisierung geht es in erster Linie darum, mehr aus lokalen Hardware-Ressourcen herauszuholen als mit rein physischen Maschinen möglich wäre. Daher muss die Leistungssteigerung, die man durch seine Investitionen in Virtualisierung erreicht hat, durch eine angemessene, speziell für den Schutz von virtuellen Umgebungen konzipierte Sicherheitslösung bewahrt werden. Für einen effektiven Virtualisierungsschutz müssen Sicherheitstasks zentralisiert, verfügbare Informationen wiederverwendet, ein Lastenausgleich zwischen den VMs hergestellt und Redundanzen ausgeräumt werden. Im Sinne eines bestmöglichen Schutzes müssen aber gleichzeitig auch alle Möglichkeiten der Virtualisierungsplattformen ausgeschöpft werden, ohne die Systemleistung zu beeinträchtigen.

Schutz für virtualisierte Server und VDI

Kaspersky Hybrid Security wurde speziell für den Einsatz in virtualisierten Umgebungen entwickelt und kommt ohne überflüssige Abläufe und Daten aus. Im Vergleich zu einer herkömmlichen Endpoint-Sicherheitslösung spart Kaspersky Hybrid Security für die Virtualisierung bis zu 30 % der Hardware-Ressourcen ein. Nach einer Analyse der Umgebung kann die Lösung oft sofort und ohne einen einzigen zusätzlichen Zyklus zu einer abschließenden Beurteilung kommen. Umfassende und flexible Funktionen zur Systemhärtung reduzieren die Angriffsfläche deutlich, verhindern das Ausführen von beliebigem Code auf Servern und blockieren Exploits – und all das ohne eine spürbare Erhöhung des Ressourcenverbrauchs.

Bei virtuellen Desktops wurde die Anmeldezeit im Vergleich zu traditionellen Endpoint-Sicherheitslösungen drastisch verkürzt, so dass bei der Skalierung und Ausweitung der Grenzen des Virtualisierungshosts keine Verzögerungen und Engpässe entstehen. In der Kaspersky Hybrid Cloud Security kommen dieselben umfangreichen Sicherheitsfunktionen zum Einsatz wie in unseren Lösungen für physische Endpoints. Damit wird eine sichere und reaktionsfähige Benutzerumgebung geschaffen, in der sich die Benutzer auf ihre Arbeit konzentrieren können, ohne Gefahr zu laufen, Opfer von dateiloser Malware, Lösegeldforderungen, Exploits und Ähnlichem zu werden. Um den spezifischen Anforderungen der Kunden gerecht zu werden, ist Kaspersky Hybrid Cloud Security in mehreren Bereitstellungsoptionen erhältlich – in Bezug auf die Komplexität der Bereitstellung, Plattformintegration und -Support, optimierte Ressourcennutzung, Funktionsumfang und letztlich in Bezug auf das Maß an Sicherheit.

Agentenlose Sicherheit

VMware bietet eine API, die neben „agentenloser" Sicherheit auf Dateiebene für die eigene vSphere-Virtualisierungsplattform auch die native Integration von Kaspersky Hybrid Cloud Security in das VMware-Ökosystem ermöglicht. Dazu gehören auch vShield Endpoint und NSX Guest Introspection sowie die gleichzeitige nahtlose und unmittelbare Einbeziehung aller virtualisierten Ressourcen. Dafür genügt eine einzige Security Virtual Machine (SVM) – eine spezielle, mit Anti-Malware-Scan-Engine und Signaturdatenbanken ausgestattete VM – pro Host, was die Ressourcen einzelner VMs schont und die Ressourcenauslastung erheblich reduziert.

Light Agent-Sicherheit

Eine weitere plattformunabhängige Anwendung, die für Kaspersky Hybrid Cloud Security übernommen wurde, ist der so genannte „Light-Agent", der für den Betrieb innerhalb des Betriebssystems jeder zu schützenden VM optimiert ist. Da sich Scan-Engine und Datenbanken auch bei diesem Ansatz zentral auf der SVM befinden, beansprucht die Light-Agent-Technologie die Systemressourcen deutlich weniger als traditionelle Lösungen mit Full Agents. Die Lösung liegt bei der Ressourcenauslastung zwischen dem agentenlosen und dem Full-Agent-Ansatz und ist darüber hinaus nicht an VMware-Technologien gebunden. Auch auf anderen beliebten Plattformen wie Microsoft Hyper-V, Citrix Hypervisor und KVM kann sie eingesetzt werden, um die Sicherheit spürbar zu erhöhen.

Mithilfe dieser Ansätze lässt sich eine sichere Virtualisierung realisieren, die eine Lösung für folgende Problembereiche bietet:

- Exzessive Ressourcennutzung. Durch das Zentralisieren der meisten Sicherheitstasks sowie den Einsatz einer einzelnen Datenbankinstanz und das Zwischenspeichern von Beurteilungen werden replizierende Signaturdatenbanken und aktive Anti-Malware-Engines auf jeder einzelnen zu schützenden VM vermieden.
- „Storms": Mit intelligentem Warteschlangen-Management, Systemausgleich und dem Zwischenspeichern von Beurteilungen auf der SVM können lässt sich der Ansturm bewältigen, der durch zeitgleiche Datenbank-Updates und/oder Anti-Malware-Scans auf jeder einzelnen VM verursacht wird. Außerdem kann das Risiko von „Schwachstellen-Fenstern" als Folge von Scan-Verzögerungen gebannt werden.
- „Instant-on"-Lücken: Datenbanken und Module können auf inaktiven VMs nicht aktualisiert werden. Daher ist eine VM vom Startzeitpunkt bis zum Abschluss des Aktualisierungsprozesses Angriffen schutzlos ausgeliefert. Dieses Problem kann durch eine ständig aktivierte, ständig aktualisierte SVM gelöst werden.

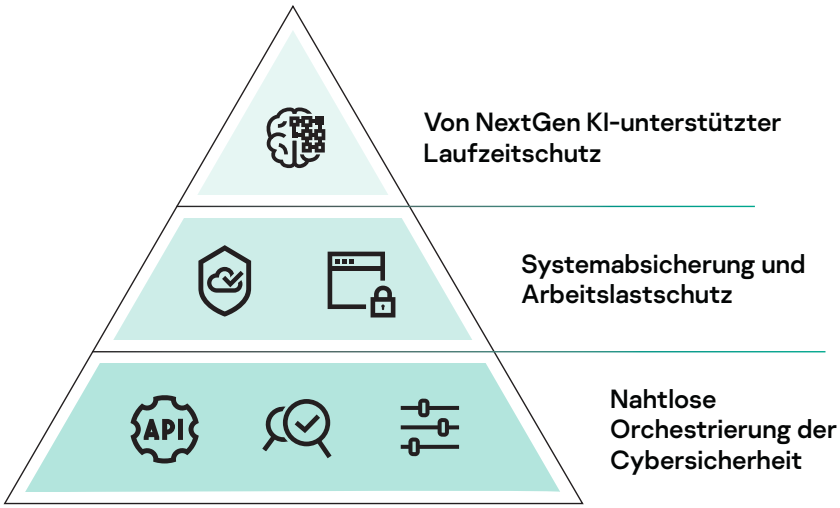
Physische Maschinen und mobile Geräte

Physische Server, aber auch physische Workstations und mobile Geräte brauchen Sicherheit. Und diese Rolle übernimmt eine weitere Kaspersky-Lösung: Kaspersky Endpoint Security for Business. Mehrere Schutz- und Kontrollebenen in Kombination mit Tools zur Automatisierung von Sicherheitsprozessen sorgen dafür, dass der Sicherheitsstatus jeder Workstation, jedes Laptops, Tablets oder Handys als Teil Ihrer breiter angelegten hybriden Infrastruktur vollständig transparent und unter Kontrolle ist und alle unter dem vielfach ausgezeichneten, erstklassigen Schutz von Kaspersky stehen.

Hervorragender Schutz

Ob auf einem Handy, einem physischen Server, einer virtuellen Maschine oder in der Cloud – für Ihre Sicherheitslösung gilt immer dieselbe Regel: Sie muss der Aufgabe gewachsen sein.

Hervorragender Schutz ist bei allen Kaspersky-Produkten und -Services stets gewährleistet. Unsere Technologien, die auf einzigartigen Informationsquellen zu Echtzeit-Bedrohungen und maschinellem Lernen basieren, werden ständig weiterentwickelt, um Ihre Endpoints vor den neuesten Exploits zu schützen und Ihre Daten und freigegebenen Ordner vor hochentwickelten Bedrohungen und Lösegeldforderungen zu schützen.



Hybrid Cloud Security nutzt immer auf denselben umfangreichen Funktionssatz, ganz gleich, ob es um den Schutz physischer oder virtueller Endpoints und Server oder um den Schutz von Arbeitslasten in Public Clouds geht. Dazu zählen:

- **Unsere vielfach ausgezeichnete Anti-Malware-Engine** stellt automatischen Echtzeitschutz auf Dateiebene für jeden Computer, jede VM und Workload bereit, sowohl beim Zugriff als auch auf Abruf.
- **Cloud-basierte Aufklärung** identifiziert im Handumdrehen neue Bedrohungen und stellt automatische Updates bereit.
- **Verhaltenserkennung** bei der Überwachung von Programmen und Prozessen schützt vor hoch entwickelten Bedrohungen und sogar vor körperloser Malware. Alle bereits vorgenommenen schädlichen Aktivitäten werden bei Bedarf per Rollback zurückgeführt.
- **Exploit-Schutz** sorgt für die Kontrolle von Systemablaufprozessen und Programmverhalten und unterstützt auf diese Weise die Abwehr hoch entwickelter Bedrohungen, einschließlich Ransomware.
- **Anti-Ransomware** schützt Cloud-Umgebungen, virtuelle und physische Endpoints sowie die zugehörigen freigegebenen Netzwerke vor Angriffen und stellt per Rollback gegebenenfalls betroffene Dateien im Zustand vor der Verschlüsselung wieder her.
- **HIPS/HIDS** dient der Aufdeckung netzwerkbasierter Eingriffe in physische und Cloud-Ressourcen.
- **Programmkontrolle** ermöglicht es Ihnen, alle Hybrid Cloud-Umgebungen für eine optimale Systemabsicherung im Modus „Default Deny" zu verankern und zu bestimmen, welche Programme wo ausgeführt werden und auf was sie zugreifen dürfen.
- **Web Control** schützt vor webbasierten Cyberbedrohungen, einschließlich solcher, die durch Unwissenheit oder Fehler von Mitarbeitern verursacht werden. Außerdem steigert die Lösung die Produktivität, indem sie die Zeit reduziert, die für die Kommunikation in sozialen Medien und irrelevantes Surfen vergeudet wird.
- **Netzwerksegmentierung** sorgt für Transparenz und automatisierten Schutz von Netzwerken mit Hybrid Cloud-Infrastruktur.
- **E-Mail-Sicherheit** einschließlich Anti-Spam schützt den E-Mail-Verkehr in Cloud-Umgebungen.
- **Websicherheit** einschließlich Anti-Phishing schützt vor Bedrohungen durch potentiell gefährliche Webseiten und Skripte.

Compliance

Compliance ist für jede Organisation eine wichtige Anforderung. Kaspersky-Produkte stellen Compliance durch mehrere Kontrollen und Funktionen sicher:

- **Verwaltungsserver-Hierarchie**: Bietet ausreichend Flexibilität, um die Komplexität der Infrastruktur in den Griff zu bekommen.
- **Verschiedene Bereitstellungsoptionen**: lokal oder in der Cloud.
- Umfassende und vielseitig konfigurierbare **Berichtfunktion und Protokollprüfung**, um Audits zu vereinfachen.
- **Rollenbasierte Zugriffssteuerung (RBAC)** stellt die Abgrenzung der Kontrollrechte zwischen den unterschiedlichen Administratorgruppen entsprechend der Organisationsstruktur und den IT-Richtlinien sicher.
- **Agenten-Passwortschutz und Selbstverteidigung,** um Manipulationen an den Sicherheitssystemen zu verhindern.
- **Sichere Kommunikation** zwischen allen Komponenten der Lösung.
- **Schwachstellenbewertung und automatisiertes Patch Management** hindern hoch entwickelte Malware und Zero-Day-Bedrohungen daran, ungepatchte Schwachstellen auszunutzen.
- **Eine benutzertransparente FIPS 140-2-zertifizierte Verschlüsselung** bietet vollständigen Schutz für vertrauliche Daten auf tragbaren Geräten und an Betriebsstandorten. Integrierte Technologien gewährleisten, dass Verschlüsselung zentral durchgesetzt werden kann.
- **Systemhärtung**: Systemsperrung mit „Default Deny" und die Abwehr von Substitutionsangriffen durch File Integrity Monitoring (FIM).
- **Gerätekontrolle** für eine fein abgestufte Kontrolle angeschlossener Speicher, Kameras, Mikrofone und sonstiger Hardware.
- **Konfigurierbarer Malware-Schutz und persönliche Firewalls** für ein Mehr an Sicherheit für Server und Workstations.

Darüber hinaus sorgen weitere Funktionen und Mechanismen, für vollständige Transparenz, ein hohes Maß an fein abgestuften Kontrollmöglichkeiten sowie kontinuierliche Verbesserung und Anpassung an die Risikolandschaft.

Digitalen Wandel sicher gestalten

Der digitale Wandel bringt eine ganze Palette von neuen Möglichkeiten – für Sie, aber auch für die Cyberkriminellen, die es auf Sie abgesehen haben. Mit den integrierten, zuverlässigen Sicherheitslösungen für hybride Umgebungen von Kaspersky schöpfen Sie alle Gelegenheiten zum Ausbau Ihrer Geschäftstätigkeit voll aus, während Sie Cyberkriminellen keine Gelegenheit zum Angriff lassen.

Kaspersky Hybrid Cloud Security: www.kaspersky.com/hybrid
Sicherheit für AWS: www.kaspersky.com/aws
Sicherheit für Microsoft Azure: www.kaspersky.com/azure
Sicherheit für Google Cloud: www.kaspersky.com/gcp

www.kaspersky.de

kaspersky BRING ON THE FUTURE