Redefining Hosting –
Reinventing Security

kyberio
Secure Public Cloud (SPC)

Leistungsbeschreibung
Stand: 22.08.2025

kyberio.

kyberio.com

kyberio.

Leistungsbeschreibung
kyberio Secure Public Cloud (SPC)

Diese Leistungsbeschreibung dient als Grundlage für die Bereitstellung und Nutzung einer Public-Cloud-Infrastruktur, die auf der Open-Source-Plattform OpenStack basiert. Sie richtet sich an Unternehmen und Organisationen, die eine skalierbare, flexible und standardisierte Cloud-Umgebung benötigen, um moderne IT-Workloads effizient und sicher betreiben zu können. Die in diesem Dokument beschriebenen Leistungsmerkmale definieren den technischen und betrieblichen Rahmen der angebotenen Cloud-Dienste und gelten verbindlich für alle Nutzer der Plattform.

Mit der Bereitstellung dieser OpenStack-basierten Public Cloud verfolgt der Anbieter das Ziel, eine hochverfügbare und performante Infrastruktur bereitzustellen, die gleichzeitig maximale Transparenz, Kontrolle und Interoperabilität gewährleistet. Die Plattform orientiert sich an etablierten Industriestandards und unterstützt den Aufbau und Betrieb virtueller Ressourcen auf Basis von Infrastructure-as-a-Service (IaaS).

Die OpenStack-Technologie wurde dabei bewusst gewählt, da sie eine offene, herstellerunabhängige Alternative zu proprietären Public-Cloud-Angeboten bietet und eine hohe Flexibilität bei der Integration bestehender Systeme ermöglicht. Gleichzeitig schafft sie die technologische Basis für automatisierte, skalierbare und mandantenfähige Cloud-Umgebungen, die sowohl für Entwicklungs- und Testzwecke als auch für produktive Workloads geeignet sind. Individuelle Erweiterungen, spezifische Konfigurationen und zusätzliche Services werden im Rahmen separater Vereinbarungen geregelt.

Allgemeine Beschreibung

Die auf OpenStack basierende Secure Public-Cloud (SPC) stellt eine moderne, hochverfügbare und flexibel skalierbare Infrastruktur bereit, die sich gezielt an Unternehmen richtet, die höchsten Wert auf Sicherheit, Souveränität und Transparenz legen. Das Sicherheitsdesign der Plattform umfasst isolierte Mandantentrennung, umfassende Zugriffskontrollen sowie durchgängige Verschlüsselungskonzepte. Die Cloud-Plattform selbst ist nach ISO 27001 auf Basis des IT-Grundschutzes vom BSI zertifiziert und erfüllt alle Anforderungen an Datenschutz und Informationssicherheit. In Kombination mit dem ausschließlichen Betrieb in deutschen Rechenzentren ist der Dienst vollständig DSGVO-konform und bietet Unternehmen eine vertrauenswürdige und rechtssichere Cloud-Lösung.

Die Nutzung der Plattform erfolgt nach dem Pay-per-Use-Modell, wobei Ressourcen in drei klar definierten Leistungsklassen angeboten werden. So können Kunden entsprechend ihrer Anforderungen zwischen verschiedenen Preis-Leistungs-Verhältnissen wählen und jederzeit flexibel skalieren – sei es in Bezug auf Rechenleistung, Speicher oder Netzwerkressourcen.

Durch die native Unterstützung hybrider Architekturen lässt sich die Public Cloud nahtlos mit bestehenden, lokal betriebenen Infrastrukturen (Private Clouds oder On-Premise-Systemen) kombinieren. Damit ist auch ein stufenweiser Umzug oder eine Erweiterung der eigenen IT-Landschaft problemlos realisierbar.

Die Plattform versteht sich als deutsche, IT-souveräne Cloud-Lösung, die alle Datenhaltung und Verarbeitung ausschließlich in Deutschland sicherstellt. Sie bietet eine vertrauenswürdige Alternative zu nicht-europäischen Anbietern und entspricht den strengen Vorgaben der DSGVO sowie weiterer branchenspezifischer Regularien.

Als technologische Grundlage wurde mit OpenStack eine weltweit etablierte Open-Source-Cloud-Plattform gewählt, die sich durch hohe Flexibilität, offene Standards und ein aktives Entwickler-Ökosystem auszeichnet. OpenStack ermöglicht die vollständige Kontrolle über virtuelle Ressourcen, eine umfassende API-Nutzung sowie eine einfache Integration in bestehende DevOps- und Automatisierungsprozesse. Darüber hinaus garantiert die Offenheit der Plattform langfristige Investitionssicherheit, da keine Abhängigkeiten zu proprietären Technologien bestehen.

Wesentliche Leistungsmerkmale

Sicherheitsorientiertes Design

Die Public Cloud wurde konsequent nach dem Prinzip „Security by Design“ entwickelt und bietet eine mandantenfähige Architektur mit strikter Netzwerksegmentierung, Verschlüsselung auf Daten- und Transportebene sowie umfassendem Zugriffsmanagement. Sicherheitsfunktionen wie rollenbasierte Zugriffskontrolle (RBAC) und individuelle Security-Gruppen erhöhen zusätzlich den Schutz sensibler Daten und Systeme.

Flexible Skalierung & Pay-per-Use-Modell

Ressourcen wie CPU, RAM und Storage können jederzeit bedarfsgerecht angepasst werden. Die Abrechnung erfolgt verbrauchsabhängig, sodass Kunden nur für tatsächlich genutzte Leistungen zahlen.

Hybride Cloud-Fähigkeit

Die Plattform erlaubt eine nahtlose Integration in bestehende IT-Umgebungen, wodurch hybride Cloud-Setups möglich werden – beispielsweise durch direkte VPN- oder private Netzwerkverbindungen zu lokalen Rechenzentren oder anderen Cloud-Plattformen. Das erleichtert die schrittweise Migration oder die Erweiterung bestehender Workloads.

OpenStack-Technologie mit offener API

OpenStack als etabliertes Open-Source-Cloud-Framework ermöglicht maximale Gestaltungsfreiheit und volle Kontrolle über die eigene Cloud-Infrastruktur. Dank offener Standards und standardisierter APIs lässt sich die Plattform nahtlos in bestehende DevOps-Umgebungen integrieren und umfassend automatisieren. Ohne Herstellerbindung (kein Vendor Lock-in) bietet OpenStack eine zukunftssichere Basis für individuelle Anforderungen und nachhaltiges Wachstum.

Variable Storage-Klassen

Die Cloud-Plattform stellt verschiedene Storage-Performance-Klassen bereit, um individuelle Anforderungen optimal abzudecken. Kunden können zwischen Standard-Storage für allgemeine Workloads, Performance-Storage für datenintensive Anwendungen und lokal angebundenem NVMe-Storage für besonders latenzsensible und IOPS-intensive Szenarien wählen. So lässt sich die Speicherleistung gezielt an den tatsächlichen Bedarf anpassen – flexibel, skalierbar und effizient.

Flexible CPU-Zuweisung

Die Cloud-Plattform bietet virtuelle CPUs (vCPUs) sowohl als dedizierte Ressourcen für maximale Performance als auch im Overcommit-Modell mit einer Überbuchung von bis zu 2:1 an. So können Kunden je nach Anforderung zwischen garantierter Rechenleistung und kosteneffizienter Ressourcenteilung wählen, ohne auf Skalierbarkeit und Flexibilität verzichten zu müssen.

Technische Details

Hardware

Die Cloud-Plattform wird auf hochwertiger HPE-Hardware betrieben, die speziell für den professionellen Einsatz in Rechenzentren konzipiert ist. Die verbauten Prozessoren bieten eine

Mindesttaktfrequenz von 2,60 GHz, wodurch eine solide und leistungsfähige Grundlage für die Ausführung verschiedenster Workloads gewährleistet ist. Diese Hardwarebasis sorgt für zuverlässige Performance und hohe Effizienz– ideal für den stabilen Betrieb sowohl standardisierter als auch anspruchsvoller Cloud-Anwendungen.

Hardware

Unsere Storage-Systeme bieten hohe Verfügbarkeit und Performance – sei es als Datenträger-Volumes für Cloud-Server, S3-kompatibler Object Storage, lokaler High-Performance-Speicher oder verteilte Dateisysteme. Je nach Einsatzzweck stehen verschiedene Speicherarten zur Verfügung, die sich hinsichtlich der möglichen IOPS (Input/Output Operations Per Second), der maximalen Bandbreite und des Speicherplatzes unterscheiden, um optimale Lösungen für unterschiedliche Anforderungen zu gewährleisten.

Datenträger-Leistungsklassen (Maximalwerte)

Storage-Klasse	IOPS	Bandbreite	BURST
Standard	1.000	100 MB / Sekunde	2.000 / 200 MB/s
Performance	10.000	250 MB / Sekunde	20.000 / 400 MB/s
Performance-Plus	20.000	400 MB / Sekunde	30.000 / 500 MB/s
NVME	bis zu 100.000		

Volumes (Block Storage)

Die Volumes dienen als Datenträger der Cloud Server (bis zu 26 je Server), und werden von unserem hochverfügbaren und 3 fach-redundanten Storage-System bereitgestellt.

Mit Volume-Snapshots können Sie den Zustand eines Volumes vor wichtigen Arbeiten sichern und bei Bedarf ein System wiederherstellen.

S3 Object Storage

Unser S3-kompatibler Object Storage basierend auf OpenStack Swift bietet skalierbaren Speicherplatz und wird nach tatsächlicher Nutzung (Speicherplatz + verbrauchte Bandbreite) abgerechnet. Der Zugriff kann durch ACLs abgesichert und Dateien wahlweise über ein CDN (Content-Distribution-Network) ausgeliefert werden.

Netzwerk

Alle Systeme innerhalb der SPC sind über einen leistungsstarken internen 100G-Uplink angebunden. Diese hoch performante interne Netzwerkstruktur gewährleistet einen schnellen und zuverlässigen Datenaustausch zwischen den einzelnen Komponenten der Plattform – sowohl innerhalb einzelner Projekte als auch über Verfügbarkeitszonen hinweg. Damit wird eine optimale Grundlage für skalierbare und latenzarme Cloud-Anwendungen geschaffen.

Die Plattform unterstützt nativ sowohl IPv4- als auch IPv6-Netzwerke und ermöglicht so zukunftssichere Konnektivität und Interoperabilität.

Durch die integrierte Netzwerküberwachung werden Verfügbarkeit und eventuelle Anomalien kontinuierlich überprüft. Auffälligkeiten im Datenverkehr – etwa durch missbräuchliche Nutzung oder technische Störungen – werden automatisch erkannt und können zeitnah adressiert werden.

Für den Schutz vor externen Bedrohungen steht optional ein DDoS-Schutz zur Verfügung, der bei Bedarf aktiviert werden kann und unerwünschten Datenverkehr effizient filtert.
Darüber hinaus bietet die Plattform die Möglichkeit, sogenannte Floating IPs zu nutzen – öffentliche IP-Adressen, die flexibel auf virtuelle Maschinen oder Dienste innerhalb der Cloud geroutet werden können, um eine hohe Erreichbarkeit und Ausfallsicherheit zu ermöglichen.
Sollten Sie über eigene IP-Subnetze (z.B. als RIPE-Mitglied) verfügen, können Sie diese innerhalb unserer Cloud-Plattform als öffentliche IP-Adressen nutzen (Bring your own IP-Space). Die Netze können hierbei wahlweise statisch oder dynamisch (durch Sie mittels BGP gesteuert) geroutet werden.

Security (onboard)

Innerhalb der OpenStack-Plattform bieten Security Groups eine zentrale und flexible Möglichkeit zur Steuerung des Netzwerkzugriffs auf virtuelle Maschinen. Sie fungieren als virtuelle Firewalls, mit denen eingehender und ausgehender Datenverkehr auf Port- und Protokollebene definiert und kontrolliert werden kann. Regeln lassen sich individuell pro Instanz oder projektweit konfigurieren, was eine feingranulare Absicherung von Cloud-Ressourcen ermöglicht – ohne den Einsatz zusätzlicher externer Firewalls. So lassen sich beispielsweise nur bestimmte Quell-IP-Adressen, Netzbereiche oder Dienste wie SSH oder HTTPS gezielt zulassen oder blockieren. Die Konfiguration erfolgt dabei direkt über das Cloud-Interface oder automatisiert über die API, was eine einfache Integration in bestehende Sicherheitskonzepte und DevSecOps-Prozesse erlaubt.

Mittels der inkludierten NAT-Funktionalität lassen sich virtuelle Maschinen innerhalb abgeschotteter, privater Netzwerke sicher betreiben, während gleichzeitig gezielter Zugriff auf externe Ressourcen ermöglicht wird.

Ebenfalls bereits standardmäßig verfügbar ist das VLAN-Routing auf Tenant-Ebene, das es Nutzern ermöglicht, komplexe und segmentierte Netzwerktopologien innerhalb ihrer virtuellen Umgebung abzubilden. Mehrere virtuelle Netzwerke lassen sich über softwarebasierte Router miteinander verbinden, wodurch eine logische Trennung von Workloads, Sicherheitszonen oder Mandanten geschaffen wird. Diese Funktionalität erlaubt eine feingranulare Steuerung des Datenverkehrs sowie die Umsetzung individueller Sicherheitsrichtlinien – ganz ohne Eingriffe in die physische Netzwerkstruktur.

Features

Zentrale Domain und Multi-Projekt-Fähigkeit

Jeder Kunde erhält auf der Plattform eine eigene zentrale Domain, die als übergeordnete Verwaltungsinstanz dient. Innerhalb dieser Domain können beliebig viele Projekte (auch als virtuelle Data Center oder Tenants bezeichnet) eingerichtet werden, die unabhängig voneinander betrieben, verwaltet und abgerechnet werden können. Dies ermöglicht eine klare organisatorische Trennung unterschiedlicher Geschäftsbereiche, Kundenumgebungen oder Entwicklungsstufen – bei gleichzeitiger zentraler Kontrolle und Übersicht.

Plausibilitäts- und Affinity-Regeln

Die Plattform unterstützt die Definition von Plausibilitäts- und Affinity-Regeln, mit denen Kunden steuern können, wie und wo ihre Ressourcen innerhalb der Cloud-Infrastruktur platziert werden. Affinity-Regeln ermöglichen es beispielsweise, bestimmte virtuelle Maschinen auf demselben oder verschiedenen physischen Hosts zu betreiben, um Ausfallsicherheit oder Performance-Optimierungen zu gewährleisten.

Plausibilitätsregeln sorgen dafür, dass nur kompatible oder gewünschte Ressourcen-kombinationen zusammenarbeiten, wodurch die Stabilität und Effizienz der Umgebung erhöht werden.

Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit

Zur Absicherung des Zugangs zur zentralen Domain und den darin betriebenen Projekten kann auf Wunsch eine Multi-Faktor-Authentifizierung (MFA) aktiviert werden. Diese zusätzliche

Sicherheitsmaßnahme sorgt dafür, dass neben den regulären Zugangsdaten ein weiterer Authentifizierungsfaktor abgefragt wird, wodurch unbefugter Zugriff effektiv verhindert wird. Die MFA kann flexibel an die Anforderungen des Kunden angepasst und nahtlos in den Login-Prozess integriert werden.

Social Login über Google und GitHub

Als zusätzliche Komfort- und Sicherheitsfunktion bietet die Plattform die Möglichkeit, sich mittels Social Login über Google- oder GitHub-Accounts anzumelden. Diese Integration ermöglicht eine einfache, schnelle und sichere Authentifizierung, ohne separate Zugangsdaten verwalten zu müssen. Kunden profitieren dadurch von einer flexiblen und benutzerfreundlichen Zugangsmethode, die gleichzeitig den Schutz der Plattform durch bewährte Authentifizierungsmechanismen großer Anbieter erhöht.

Aktueller Betriebsstatus und zukünftige Erweiterungen

Derzeit wird die Cloud-Plattform temporär innerhalb einer einzelnen Verfügbarkeitszone betrieben, um einen stabilen und sicheren Betrieb zu gewährleisten. Perspektivisch ist jedoch geplant, das Angebot durch die Integration weiterer Verfügbarkeitszonen deutlich zu erweitern. Dadurch wird die Plattform zukünftig noch widerstandsfähiger, ausfallsicherer und flexibler, um den steigenden Anforderungen unserer Kunden optimal gerecht zu werden. Wir sind zuversichtlich, dass diese Erweiterungen die Leistungsfähigkeit und Verfügbarkeit der Cloud nachhaltig steigern werden.

Optionale Services

Diese können im Dokument „Leistungsbeschreibung Managed Service.pdf“ entnommen werden.

API-Kompatibilität

Die Plattform bietet umfassende API-Kompatibilität, die es Kunden ermöglicht, sämtliche Funktionen und Ressourcen programmatisch zu steuern und zu automatisieren. Dies unterstützt moderne DevOps- und Cloud-Native-Ansätze, bei denen Infrastruktur als Code verwaltet wird. Durch standardisierte Schnittstellen lassen sich Deployments, Skalierungen und Konfigurationsänderungen nahtlos in bestehende Workflows und CI/CD-Pipelines integrieren, was die Effizienz und Agilität bei der Nutzung der Cloud erheblich steigert.

Mitwirkungspflicht des Kunden

Der Kunde trägt die volle Verantwortung für die korrekte Funktionalität, Konfiguration und den Betrieb der innerhalb der Plattform betriebenen internen Instanzen. Jegliche Fehler oder Fehlkonfigurationen, die aus der Nutzung dieser Instanzen resultieren, liegen im Verantwortungsbereich des Kunden.

Bei Bedarf können Dienstleistungen durch kyberio in Anspruch genommen werden, die der Unterstützung dienen.

Abrechnung

Das Vergütungsmodell basiert auf einer stundengenauen Erfassung und Abrechnung der tatsächlich genutzten Ressourcen. Kunden zahlen somit ausschließlich für die Leistungen und Kapazitäten, die sie tatsächlich in Anspruch nehmen, ohne feste Vorauszahlungen oder Pauschalen. Dieses flexible Modell ermöglicht eine transparente und bedarfsgerechte Kostenkontrolle.

Vertragslaufzeit / Rabatte

Es besteht keine Mindestvertragslaufzeit für die Nutzung der Cloud-Dienste. Für Kunden, die sich jedoch verbindlich zur Nutzung vordefinierter Ressourcen über eine Laufzeit von 12, 24 oder 36 Monaten verpflichten, bieten wir attraktive Rabattierungen an. Dieses Modell ermöglicht es, Kosten zu optimieren und langfristige Planungssicherheit zu schaffen, während zugleich maximale Flexibilität für andere Kunden gewährleistet bleibt.

Service Level Agreement (SLA)

Diese können im beigefügten Dokument „kyb_SLA_Cloud.pdf“ entnommen werden.

Vertragsende

Das Vertragsverhältnis endet mit der Löschung des Kundenaccounts. Besteht zum Zeitpunkt der Löschung noch ein vertragliches Commitment auf bestimmte Ressourcen, so werden diese gemäß der vereinbarten Bindungsfrist weiterhin berechnet, auch wenn die Ressourcen nicht mehr aktiv genutzt werden.

kyberio.

Sie haben Fragen?

Wir stehen gerne zur Verfügung:
kyberio GmbH
Cloud Solution Consulting
E-Mail: sales@kyberio.com
Tel.: 0511 72160 - 140

kyberio GmbH
Am Mittelfelde 29
30519 Hannover

+49 511 71260-0
info@kyberio.com
kyberio.com

Geschäftsführer:
Florian Dierks
Simon Künzel

Amtsgericht Hannover
HRB 202097
USt.-ID: DE204915504

Commerzbank AG
IBAN DE42 2508 0020 0111 0858 00
BIC DRES DE FF 250