



Zugersee

combined.swiss

SECUREdatacenter

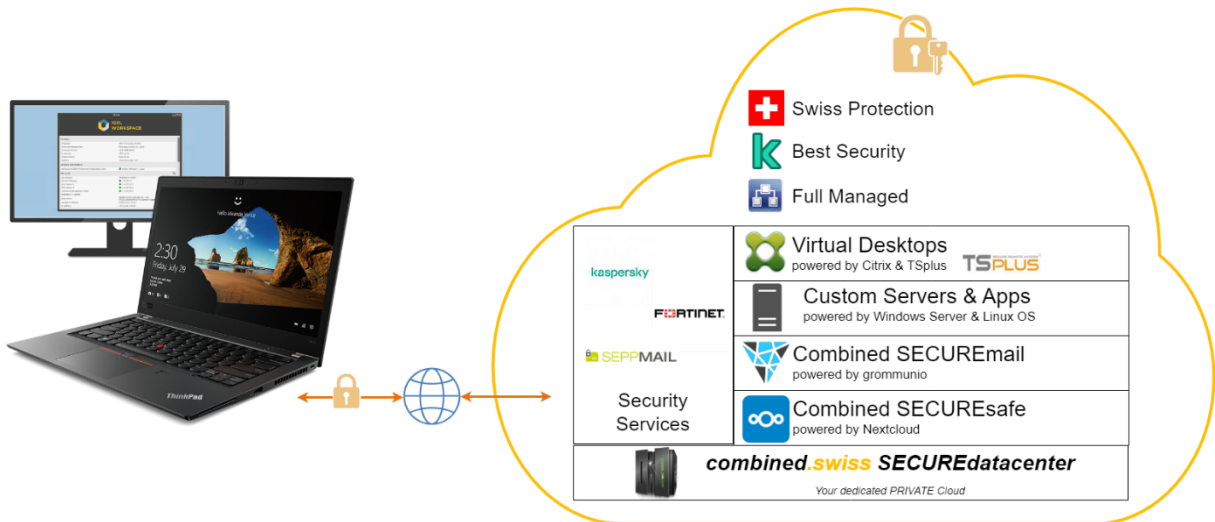
LEISTUNGSBESCHREIBUNG

Combined Networks GmbH

Löberenstrasse 10

CH-6300 Zug - Schweiz

Ihre Reise in die digitale Zukunft beginnt hier. Mit unseren Data Center Services aus der Schweiz haben Sie einen zuverlässigen Partner an Ihrer Seite, der Ihnen nicht nur Sicherheit, sondern auch die Freiheit bietet, neue Wege zu gehen. Lassen Sie uns gemeinsam das Abenteuer Ihrer Unternehmensentwicklung gestalten – sicher, stabil und voller Möglichkeiten.



Diese Leistungsbeschreibung unterliegt laufenden Anpassungen aufgrund technologischer Entwicklungen oder Änderungen durch Drittanbieter. Der Funktionsumfang und die Verfügbarkeit einzelner Leistungen können sich durch Updates oder Änderungen seitens der Softwarelieferanten ändern. Massgeblich ist die jeweils aktuelle Version, die auf unserer Webseite veröffentlicht wird, sowie die offiziellen Angaben der jeweiligen Softwarelieferanten.

Die Vertragsbedingungen sind im Dokument «Service Level Agreement» (SLA) sowie auf unserer Webseite festgehalten.

Die Vorteile von **combined.swiss SECUREdatacenter** für kleine und mittlere Unternehmen:

Infrastruktur und Verfügbarkeit

Bereitstellung einer dedizierten privaten Cloud-Umgebung: Unsere Lösung stellt eine dedizierte virtuelle Infrastruktur für die Nutzung von virtuellen Maschinen (VMs) bereit. Diese private Umgebung bietet maximale Isolation und Sicherheit, da alle Ressourcen ausschliesslich für den jeweiligen Kunden verwendet werden.

Flexibilität und Skalierbarkeit: Die Umgebung kann bedarfsgerecht angepasst werden, und zusätzliche Ressourcen für einzelne VMs können durch uns skaliert werden. Eine Erhöhung der Ressourcen führt zu einer entsprechenden Anpassung der monatlichen Gebühr. Dadurch wird sichergestellt, dass die Leistung der Anwendungen optimiert und der Ressourcenbedarf dynamisch gesteuert werden kann.

Keine zusätzlichen Lizenzkosten: Alle notwendigen Lizenzen für das Betriebssystem (Windows oder Linux), den Endpunktschutz und das Backup-System sind im Leistungsumfang enthalten. Dies reduziert die Komplexität und sorgt dafür, dass keine versteckten Kosten entstehen.

Anwendungslizenzen: Lizenzen für Drittanbieter-Anwendungen, Software oder spezifische Dienste, die vom Kunden genutzt werden, sind nicht in den Leistungen enthalten und müssen separat vom Kunden erworben und lizenziert werden.

Verantwortung des Kunden: Der Kunde ist dafür verantwortlich, alle notwendigen Anwendungslizenzen zu erwerben und sicherzustellen, dass diese korrekt in der Umgebung installiert und verwendet werden.

Hohe Verfügbarkeit: Wir garantieren eine Verfügbarkeit für Ihre virtuellen Maschinen und Cloud-Infrastruktur gemäss unserem SLA (Service Level Agreement).

Vertragsbasiert: Die detaillierte Verfügbarkeitsgarantie, einschliesslich der maximalen erlaubten Ausfallzeiten und der Reaktionszeiten im Falle von Störungen, ist in einem formalisierten SLA dokumentiert, das als Grundlage für die Zusammenarbeit dient.

Sicherheitsmanagement

Maximaler Datenschutz: Minimierte Telemetrie-Daten nach technischen Möglichkeiten für besseren Schutz der Privatsphäre.

Verwalteter Endpunktschutz mit Managed Detection and Response (MDR): Kontinuierliche, rund um die Uhr automatisierte Bedrohungserkennung und -abwehr.

Security Operations Center (SOC) 24x7: Permanente Überwachung durch ein Expertenteam, um Cyberangriffe zu erkennen und zu stoppen. Powered by Kaspersky NEXT Complete Security

Redundante Firewall-Architektur: Um eine hohe Verfügbarkeit sicherzustellen, setzen wir auf eine redundante Architektur. Sollte eine Firewall ausfallen, übernimmt die andere nahtlos, ohne die Sicherheitslage zu gefährden.

Schutz des ein- und ausgehenden Internetverkehrs: Der ausgehende Verkehr wird durch einen Web Proxy geschützt, während der eingehende Verkehr durch eine Web Application Firewall (WAF) überwacht und vor Angriffen auf Webanwendungen abgesichert wird.

Online Backups: Wir sichern Ihre virtuellen Maschinen und Daten täglich, um eine schnelle und effiziente Systemwiederherstellung im Falle eines Ausfalls oder einer Störung zu gewährleisten. Das tägliche Backup ist standardmässig im Service enthalten. Zusätzliche Optionen, wie z. B. Continuous Backup, können im SLA definiert werden und sind kostenpflichtig.

Offline-Backups: Zusätzlich zur täglichen Sicherung erfolgt eine regelmässige Offline-Auslagerung der Backups in ein separates, sicheres Repository. Diese Massnahme schützt vor Datenverlust durch Cyberangriffe oder Katastrophen und stellt sicher, dass die Daten in einem externen, sicheren Standort aufbewahrt werden.

Umfassende Verschlüsselung: Sämtliche Datenübertragungen zwischen virtuellen Maschinen und anderen Systemen sind durch sichere Protokolle wie TLS geschützt, während auch alle Backups verschlüsselt werden, um unbefugten Zugriff selbst bei physischen Sicherheitslücken zu verhindern.

Sicherer Zugriff: Um den Zugriff auf Ihre virtuelle Umgebung zu schützen, setzen wir Multi-Faktor-Authentifizierung (MFA) ein. Dies erfordert, dass sich Benutzer nicht nur mit einem Passwort, sondern auch mit einem zweiten Sicherheitsfaktor (z. B. einem Code, der auf dem Smartphone generiert wird) authentifizieren.

IT-Automatisierung und Wartung

Automatisierte Updates: Wir führen regelmässige Updates und Hotfix-Installationen durch, um sicherzustellen, dass Ihre virtuelle Umgebung stets aktuell und sicher bleibt. Die Auswahl und Durchführung der Updates erfolgt durch uns und umfasst Betriebssysteme, Sicherheitsupdates sowie von uns verwaltete Anwendungssoftware. Ein Anspruch auf einen bestimmten Updatezyklus besteht nicht. Individuelle Updatezyklen sind optional und kostenpflichtig.

Minimierung der Ausfallzeiten: Alle Updates werden so durchgeführt, dass die Auswirkungen auf Verfügbarkeit und Leistung der VMs minimal sind. Kunden ohne 24x7-Betrieb haben standardmässig ein festes Wartungsfenster von 23:00 Uhr bis 01:00 Uhr (täglich). Geplante Wartungsarbeiten werden rechtzeitig angekündigt.

Echtzeitüberwachung: Wir überwachen Ihre Umgebung rund um die Uhr auf Anomalien und Leistungsprobleme. Unsere Systeme erkennen automatisch potenzielle Probleme, bevor sie sich auf die Nutzererfahrung auswirken.

Schnelle Reaktionszeiten: Unser Team reagiert schnell auf Alarme und Vorfälle, um sofortige Massnahmen zu ergreifen und Ausfallzeiten zu minimieren. Der Support ist jederzeit erreichbar, um etwaige Störungen schnell zu beheben.

Microsoft Windows Server Datacenter oder Linux OS: Sie haben die Wahl zwischen verschiedenen Betriebssystemen, die auf Ihren virtuellen Maschinen laufen können. Wir bieten sowohl Microsoft Windows Server Datacenter als auch Linux-basierte Systeme an, je nach den Anforderungen Ihrer Anwendungen.

Kompatibilität: Beide Systeme sind vollständig kompatibel mit gängigen Cloud-Anwendungen und bieten die Flexibilität, verschiedene Softwarelösungen zu integrieren.

Support und Benutzerfreundlichkeit

Flexible Zugriffsoptionen: Nutzer können von jedem Ort und mit jedem Gerät (Laptop, Smartphone, etc.) auf die private Cloud-Umgebung zugreifen. Dies wird durch sichere VPN-Verbindungen und Single Sign-On (SSO)-Technologien ermöglicht, die eine nahtlose Benutzererfahrung bei gleichzeitig hoher Sicherheit bieten.

Zugriffssteuerung: Die Verwaltung von Benutzerrechten und -zugängen erfolgt zentral. Nur autorisierte Nutzer haben Zugriff auf kritische Ressourcen.

Combined Service Desk Silber: Support während unserer Bürozeiten gemäss Webseite. Support-Leistungen werden separat verrechnet. Detaillierte Informationen zu den Service-Levels und Leistungen finden Sie in der Leistungsbeschreibung für den Servicedesk.

Drittanbieter-AGB gelten zusätzlich: Für bestimmte Komponenten und Softwarelösungen gelten die AGB von Drittanbietern.

Combined SECUREsafe

Ein sicherer Ort für all Ihre Daten. Ein absolut sicheres System, um all Ihre Daten auf allen gewünschten Geräten zu synchronisieren. Alle Daten verbleiben auf Ihrem eigenen virtuellen Server. Combined SECUREsafe kombiniert mit Combined SECUREworkplace ist die sicherste Lösung der Schweiz um Ihr digitales Gold zu schützen.

Powered by Nextcloud, die am häufigsten eingesetzte selbst-gehostete Plattform für Dateifreigabe und Zusammenarbeit im Web.

Das Angebot umfasst alle Leistungen von **combined.swiss SECUREdatacenter** sowie zusätzlich:

Geräteunabhängige und sichere Synchronisation: Greifen Sie von jedem Gerät aus sicher auf Ihre Dateien zu.

Offline-Dateizugriff: Mit Desktop-Clients auch ohne Internetverbindung auf Ihre Daten zugreifen.

Mobile Apps: Zugriff und Synchronisation von Dateien über Smartphones und Tablets.

Lokale Synchronisation: Synchronisieren Sie nur spezifische Dateien oder Ordner auf Ihren Geräten.

Individuelle Zugriffsberechtigungen: Verwalten Sie detaillierte Rechte für Benutzer und Gruppen.

Versionierung und Wiederherstellung: Einfaches Zurücksetzen von Dateien auf frühere Versionen bei Bedarf.

Combined SECUREmail

Combined SECUREmail fasst alle Anforderungen moderner, digitaler Kommunikation und Kollaboration effizient zusammen. Dies beinhaltet die Geräte- und Betriebssystem unabhängige Verwaltung sensibler Daten wie E-Mail, Kontakte, Kalender, Chat, Video Konferenz und vieles mehr.

Mit Open-Source Technologie auf Linux-Basis ist Combined SECUREmail skalierbar und erfüllt höchste Sicherheitsanforderungen.

Powered by grommunio, die fortschrittlichste alternative OpenSource-Lösung im Bereich Kommunikation und Zusammenarbeit.

Das Angebot umfasst alle Leistungen von **combined.swiss SECUREdatacenter** sowie zusätzlich:

E-Mail, Kontakte, Kalender und Aufgaben: Eine umfassende Lösung für Ihre Kommunikation und Zusammenarbeit.

Chat und Videokonferenz: Diese Funktionen sind optional verfügbar und können gegen Aufpreis implementiert werden.

Geräteunabhängige Synchronisation: Nahtloser Zugriff und Synchronisation auf allen Geräten (Outlook, iOS, Android, Thunderbird und mehr).

Redundantes Mailgateway: Betrieb einer zentralen Mailgateway-Lösung mit erweitertem Schutz.

SwissSign E-Mail-Silver-Zertifikat: Inklusive für eine vertrauenswürdige und sichere Kommunikation.

SEPPmail-Verschlüsselung: Inklusive E-Mail-Verschlüsselung und -Signierung für sichere E-Mail-Kommunikation.