



*Lago di Zugo*

***combined.swiss***

***SECUREdatacenter***

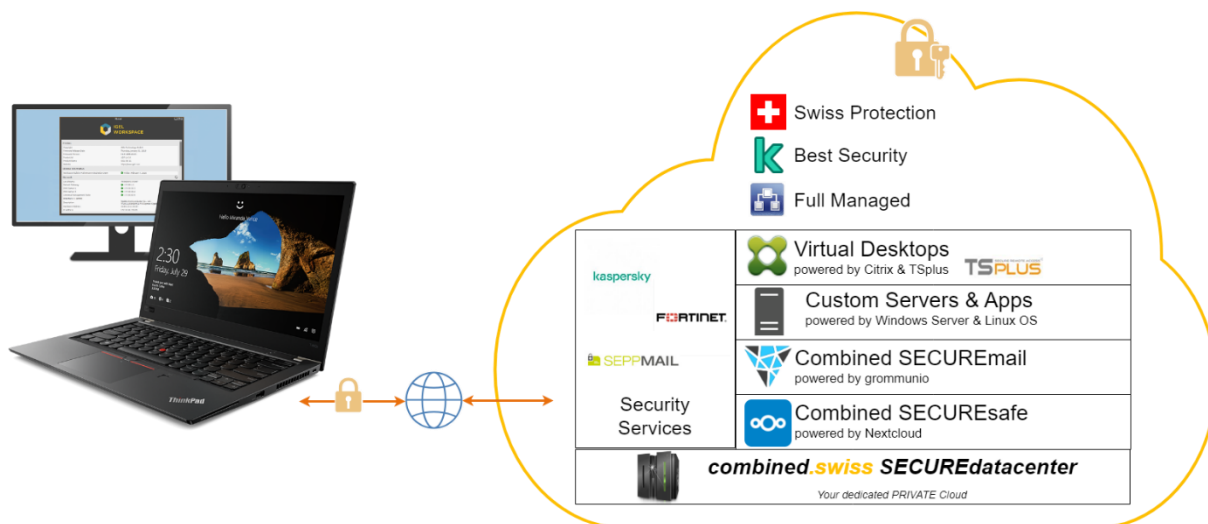
***DESCRIZIONE DEL SERVIZIO***

*Combined Networks GmbH*

*Löberenstrasse 10*

*CH-6300 Zugo - Svizzera*

Il vostro viaggio nel futuro digitale inizia qui. Con i nostri servizi di data center dalla Svizzera, avete al vostro fianco un partner affidabile che non solo vi offre sicurezza, ma anche la libertà di aprire nuovi orizzonti. Accompagniamo la vostra azienda in un viaggio di crescita - in modo sicuro, stabile e pieno di opportunità.



Questa descrizione del servizio è soggetta a modifiche continue a causa di sviluppi tecnologici o cambiamenti da parte di fornitori terzi. La gamma di funzioni e la disponibilità di singoli servizi possono variare a seguito di aggiornamenti o modifiche da parte dei fornitori di software. Fa fede la versione attuale pubblicata sul nostro sito web, nonché le indicazioni ufficiali dei rispettivi fornitori di software.

Le condizioni contrattuali sono definite nel documento «Service Level Agreement» (SLA) e pubblicate sul nostro sito web.

I vantaggi di **combined.swiss SECUREdatacenter** per le piccole e medie imprese:

## Infrastruttura e disponibilità

**Ambiente cloud privato dedicato:** la nostra soluzione prevede un'infrastruttura virtuale dedicata per l'utilizzo di macchine virtuali (VM). Questo ambiente privato garantisce il massimo livello di isolamento e sicurezza, in quanto tutte le risorse sono utilizzate esclusivamente dal rispettivo cliente.

**Flessibilità e scalabilità:** l'ambiente può essere adattato in base alle esigenze del cliente e le risorse aggiuntive per le singole macchine virtuali possono essere scalate da noi. Un aumento delle risorse comporta un adeguamento corrispondente della tariffa mensile. In questo modo si garantisce un'ottimizzazione delle prestazioni delle applicazioni e una gestione dinamica del fabbisogno di risorse.

**Nessun costo di licenza aggiuntivo:** tutte le licenze necessarie per il sistema operativo (Windows o Linux), la protezione degli endpoint e il sistema di backup sono incluse nella prestazione. Ciò riduce la complessità e garantisce l'assenza di costi nascosti.

**Licenze per applicazioni:** le licenze per applicazioni di terze parti, software o servizi specifici utilizzati dal cliente non sono incluse nelle prestazioni e devono essere acquistate e licenziate separatamente dal cliente.

**Responsabilità del cliente:** il cliente è responsabile dell'acquisto di tutte le licenze applicative necessarie e deve garantire che esse siano correttamente installate e utilizzate all'interno dell'ambiente.

**Alta disponibilità:** garantiamo la disponibilità delle macchine virtuali e dell'infrastruttura cloud secondo quanto previsto nel nostro SLA (Service Level Agreement).

**Basato sul contratto:** la garanzia di disponibilità dettagliata, inclusi i tempi di inattività massimi consentiti e i tempi di risposta in caso di interruzioni, è documentata in un SLA formalizzato, che costituisce la base per la collaborazione.

## Gestione della sicurezza

**Massima protezione dei dati:** dati di telemetria minimizzati secondo le possibilità tecniche per una migliore protezione della privacy.

**Protezione degli endpoint gestita con Managed Detection and Response (MDR):** rilevamento e difesa automatizzati delle minacce, attivi 24 ore su 24, 7 giorni su 7.

**Security Operations Center (SOC) 24x7:** monitoraggio continuo da parte di un team di esperti per rilevare e fermare gli attacchi informatici. Powered by Kaspersky NEXT Complete Security

**Architettura firewall ridondante:** per garantire un'alta disponibilità, adottiamo un'architettura ridondante. Se un firewall dovesse fallire, l'altro subentra senza compromettere la sicurezza.

**Protezione del traffico internet in ingresso e in uscita:** il traffico in uscita è protetto da un proxy web, mentre il traffico in ingresso è monitorato e protetto da un Web Application Firewall (WAF) contro gli attacchi alle applicazioni web.

**Backup online:** effettuiamo il backup giornaliero delle vostre macchine virtuali e dei dati per garantire un rapido ed efficiente ripristino del sistema in caso di guasto o interruzione. Il backup giornaliero è incluso di default nel servizio. Opzioni aggiuntive, come il backup continuo, possono essere definite nel contratto SLA e sono a pagamento.

**Backup offline:** oltre alla protezione giornaliera, viene effettuato un regolare trasferimento offline dei backup in un repository separato e sicuro. Questa misura protegge contro la perdita dei dati dovuta ad attacchi informatici o disastri, garantendo che i dati vengano conservati in una posizione sicura esterna.

**Crittografia completa:** tutte le trasmissioni di dati tra macchine virtuali e altri sistemi sono protette da protocolli sicuri come TLS, mentre tutti i backup vengono crittografati per impedire l'accesso non autorizzato, anche in caso di vulnerabilità fisiche nella sicurezza.

**Accesso sicuro:** per proteggere l'accesso al vostro ambiente virtuale, utilizziamo l'autenticazione a più fattori (MFA). Ciò richiede che gli utenti si autenticino non solo con una password, ma anche con un secondo fattore di sicurezza (ad esempio, un codice generato sullo smartphone).

## Automazione IT e manutenzione

**Aggiornamenti automatizzati:** eseguiamo aggiornamenti regolari e installazioni di hotfix per garantire che il vostro ambiente virtuale rimanga sempre aggiornato e sicuro. La selezione e l'esecuzione degli aggiornamenti vengono gestiti da noi e comprendono i sistemi operativi, gli aggiornamenti di sicurezza e il software applicativo gestito da noi. Non esiste un diritto su un ciclo di aggiornamenti specifico. I cicli di aggiornamento personalizzati sono opzionali e a pagamento.

**Minimizzazione dei tempi di inattività:** tutti gli aggiornamenti vengono eseguiti in modo tale che l'impatto sulla disponibilità e sulle prestazioni delle VM sia minimo. I clienti senza operazioni 24 x 7 hanno una finestra di manutenzione predefinita fissa dalle 23:00 alle 01:00 (ogni giorno). Le operazioni di manutenzione pianificate verranno comunicate con adeguato anticipo.

**Monitoraggio in tempo reale:** monitoriamo il vostro ambiente 24 ore su 24, 7 giorni su 7, per rilevare anomalie e problemi di performance. I nostri sistemi identificano automaticamente potenziali problemi prima che possano influire sull'esperienza dell'utente.

**Tempi di risposta rapidi:** il nostro team risponde prontamente agli allarmi e agli incidenti per adottare misure immediate e ridurre al minimo i tempi di inattività. Il supporto è disponibile in qualsiasi momento per risolvere rapidamente eventuali disservizi.

**Microsoft Windows Server Datacenter o Linux OS:** potete scegliere tra diversi sistemi operativi da eseguire sulle vostre macchine virtuali. Offriamo sia Microsoft Windows Server Datacenter che sistemi basati su Linux, a seconda delle esigenze delle vostre applicazioni.

**Compatibilità:** entrambi i sistemi sono completamente compatibili con le applicazioni cloud comuni e offrono la flessibilità di integrare diverse soluzioni software.

## Supporto e facilità d'uso

**Opzioni di accesso flessibili:** gli utenti possono accedere all'ambiente cloud privato da qualsiasi luogo e con qualsiasi dispositivo (portatile, smartphone, ecc.). Ciò è reso possibile da connessioni VPN sicure e tecnologie Single Sign-On (SSO), che offrono un'esperienza utente fluida garantendo al contempo elevati standard di sicurezza.

**Controllo degli accessi:** la gestione dei diritti e degli accessi degli utenti avviene in modo centralizzato. Solo gli utenti autorizzati hanno accesso alle risorse critiche.

**Combined Service Desk Silber:** supporto durante l'orario d'ufficio come indicato sul nostro sito web. I servizi di supporto sono fatturati separatamente. Per informazioni dettagliate sui livelli di servizio e le prestazioni, consultare la descrizione dei servizi per il Servicedesk.

**Si applicano anche le condizioni generali di terzi:** per determinati componenti e soluzioni software, si applicano le condizioni generali dei fornitori terzi.

## Combined SECUREsafe

Un luogo sicuro per tutti i vostri dati. Un sistema assolutamente sicuro per sincronizzare tutti i vostri dati su tutti i dispositivi desiderati. Tutti i dati rimangono sul vostro server virtuale personale. Combined SECUREsafe in combinazione con Combined SECUREworkplace è la soluzione più sicura in Svizzera per proteggere il vostro oro digitale.

Basato su Nextcloud, la piattaforma self-hosted più diffusa per la condivisione di file e la collaborazione sul web.

L'offerta include tutti i servizi di **combined.swiss SECUREdatacenter** oltre a:

**Sincronizzazione sicura e indipendente dal dispositivo:** accedete ai vostri file in modo sicuro da qualsiasi dispositivo.

**Accesso ai file offline:** accedete ai vostri dati tramite client desktop anche senza connessione internet.

**App mobili:** accesso e sincronizzazione dei file tramite smartphone e tablet.

**Sincronizzazione locale:** sincronizzate solo file o cartelle specifiche sui vostri dispositivi.

**Autorizzazioni di accesso personalizzate:** gestite i diritti dettagliati per utenti e gruppi.

**Versioni e recupero:** ripristinate facilmente i file a versioni precedenti, se necessario.

## Combined SECUREmail

Combined SECUREmail riunisce in modo efficiente tutte le esigenze della comunicazione e collaborazione digitale moderna. Ciò include la gestione indipendente da dispositivi e sistemi operativi di dati sensibili come e-mail, contatti, calendari, chat, videoconferenze e molto altro.

Basato su tecnologia open source e su sistema Linux, Combined SECUREmail è scalabile e soddisfa i più elevati requisiti di sicurezza.

Basato su grommunio, la più avanzata soluzione open source alternativa nel campo della comunicazione e della collaborazione.

L'offerta include tutti i servizi di **combined.swiss SECUREdatacenter** oltre a:

**E-mail, contatti, calendario e attività:** una soluzione completa per la comunicazione e la collaborazione.

**Chat e videoconferenza:** queste funzionalità sono disponibili in modo opzionale e possono essere implementate a pagamento.

**Sincronizzazione indipendente dal dispositivo:** accesso e sincronizzazione senza interruzioni su tutti i dispositivi (Outlook, iOS, Android, Thunderbird e altri).

**Gateway e-mail ridondante:** gestione di una soluzione gateway e-mail centrale con protezione avanzata.

**Certificato SwissSign E-Mail Silver:** incluso per una comunicazione sicura e affidabile.

**Crittografia SEPPmail:** crittografia e firma e-mail incluse per una comunicazione e-mail protetta.