KEEPER®
CONNECTION MANAGER

Scheda tecnica: Desktop remoto e accesso ai server

Accesso sicuro e senza problemi a desktop e macchine remoti senza una VPN

Proteggete l'accesso ai vostri sistemi ovunque vi troviate, su qualsiasi dispositivo, tramite qualsiasi browser per web.

Per lavorare in remoto a lungo termine, le organizzazioni hanno bisogno di un modo sicuro, affidabile e scalabile per fornire ai propri dipendenti accesso rapido a desktop e applicazioni.

Le reti private virtuali (VPN) sono spesso preferite, ma per certi aspetti si dimostrano limitate. Sono costose e notoriamente difficili da configurare e manutentare da parte del personale IT, nonché da utilizzare da parte degli utenti finali. Soffrono di problemi di latenza, affidabilità e disponibilità.

Se implementati correttamente, i desktop remoti sono un'ottima alternativa alla VPN.

- Il carico amministrativo per la distribuzione, il supporto e la manutenzione di un ambiente di desktop remoto standardizzato è notevolmente inferiore a quello per il supporto di dispositivi fisici distribuiti e utilizzati dagli utenti finali.
- Finché la soluzione di desktop remoto non richiede un agente sugli endpoint, i dipendenti possono utilizzare fondamentalmente qualsiasi macchina per accedere, incluso il PC portatile personale e lo smartphone.
- Raramente ci sarà l'esigenza di accedere fisicamente al dispositivo di un utente finale, pertanto si riducono in generale i costi di assistenza per gli asset aziendali.
- I desktop remoti rafforzano la sicurezza del personale che lavora in remoto rendendo possibile l'adozione di un'architettura zero-trust, impossibile con la maggior parte delle VPN.
- Le azioni che i team distribuiti svolgono tramite desktop remoto sono protette dal firewall aziendale. Di conseguenza, godono della stessa protezione dei sistemi di sicurezza aziendali di cui usufruirebbero se lavorassero fisicamente in ufficio.
- I desktop remoti incoraggiano gli utenti a conservare i dati nella rete aziendale invece che sulle macchine locali. La protezione del firewall aziendale è più forte perché i dati possono essere facilmente protetti facendone un backup. Inoltre, è molto meno probabile spostare erroneamente i dati e molto più facile condividerli con altri.
- I desktop remoti sono altamente scalabili, soprattutto quando non è necessario mettere un agente sugli endpoint. Le immagini possono essere facilmente standardizzate e gli aggiornamenti del desktop e delle applicazioni possono essere automatizzati, poiché non è necessario accedere ai dispositivi personali.

Caso di un cliente che usa Keeper Connection Manager: settore manifatturiero

Keeper Connection Manager può andare oltre la mera fornitura di desktop remoti al personale che lavora da casa. Poiché è molto scalabile, sicuro e facile da usare, molte organizzazioni lo utilizzano per fornire desktop per ambienti di laboratorio e di formazione.

Un produttore di dispositivi consumer leader del settore configura laboratori di formazione per i suoi uffici in tutto il mondo. Fornire accesso diretto ai desktop era un'operazione difficile da sostenere a livello di manutenzione e confondeva gli utenti.

Keeper Connection Manager ha semplificato i sistemi interni per l'aggiornamento, la protezione e la fornitura di accessi al proprio team affinché potesse ricevere formazione sui desktop remoti per le attività di laboratorio. La sicurezza e la velocità hanno trasformato l'ambiente di formazione del produttore. Ai partecipanti alla formazione serviranno solo un browser web, un URL e le credenziali di accesso.

KEEPER CONNECTION MANAGER

Scheda tecnica

Desktop remoto e accesso ai server

Un'esperienza di desktop remoto completa ovunque si trovino i vostri utenti. Sostenuto dalla sicurezza zero-trust e zero-knowledge e da un servizio di assistenza di prim'ordine.

Cosa rende più sicuro Keeper Connection Manager rispetto alle tradizionali soluzioni di desktop remoto?

- Tutto il traffico passa attraverso un gateway protetto e autenticato. I desktop non sono mai visibili nell'Internet pubblico. Secondo i principi del modello zero-trust, vengono consentiti solo i collegamenti autorizzati e autenticati.
- Tutte le funzionalità del desktop sono protette dal firewall aziendale. Gli utenti in remoto godono della stessa protezione, come se stessero lavorando in ufficio all'interno della rete aziendale.
- Per una maggiore sicurezza è possibile richiedere i certificati dei client e l'autenticazione multifattoriale.
- Keeper Connection Manager è progettata per funzionare secondo il principio dei privilegi minimi. I diritti di accesso sono concessi con prudenza tramite utenti e gruppi, che vengono creati in automatico dai pacchetti di Keeper Connection Manager e tramite rigide autorizzazioni ai file.
- Gli utenti finali comunicano con i desktop remoti tramite una sessione protetta all'interno del browser. È un modo semplice ed efficace di crittografare il traffico tra gli utenti finali e il gateway senza intaccare le prestazioni.
- L'accesso a sistemi con privilegi può essere concesso senza rendere visibili le credenziali di accesso all'utente finale.
- Funziona con gli endpoint RDP, SSH, VNC, K8s e MySQL.

Caso d'uso	Keeper Connection Manager
Accesso web	✓
Autenticazione multifattoriale	✓
Accesso senza agente	✓
Più spazi di archiviazione per dati	✓
Protezione a zero-knowledge	✓
Framework zero-trust	✓
Registrazione sessioni	✓
Autenticazione passwordless	✓
Supporto multiprotocollo	✓
Integrazione con Keeper Secrets Manager	✓

Informazioni su Keeper Security, Inc.

Keeper Security, Inc. (Keeper) è l'apprezzata piattaforma di sicurezza informatica leader del mercato per la prevenzione delle violazioni dei dati legate alle password e delle minacce digitali. Il software di sicurezza e crittografia zero-trust e zero-knowledge di Keeper è apprezzato da milioni di persone e migliaia di aziende in tutto il mondo. Keeper è stata nominata Miglior gestore di password dell'anno e Scelta della redazione da PC Magazine, Scelta della redazione da PCWorld e ha vinto diversi premi come Miglior software secondo G2. Keeper è certificata SOC-2 e ISO 27001 ed è inclusa nell'elenco di utilizzo del governo federale degli Stati Uniti tramite il System for Award Management (SAM, sistema di gestione dei riconoscimenti). Maggiori informazioni alla pagina https://keepersecurity.com.