KEEPER®
CONNECTION MANAGER

Datasheet: Accesso remoto per DevOps e team IT

Accedete all'istante alla vostra infrastruttura remota con la sicurezza zero-trust

Keeper Connection Manager fornisce ai team DevOps e IT accesso senza problemi a RDP, SSH, database ed endpoint di Kubernetes attraverso il browser web.

L'accesso facile e protetto a tutta l'infrastruttura interna è sempre stata una sfida. Di solito, concedere l'accesso a un sistema è un'operazione che, una volta configurata, ce ne dimentichiamo facilmente. Col tempo le richieste aumentano e finite per ritrovarvi con un numero indefinito di persone che hanno accesso a questi sistemi fondamentali.

Apportare modifiche o verificare le autorizzazioni è una sfida. Se qualcosa va storto, spesso è impossibile sapere cosa è stato fatto nel sistema dopo l'accaduto.

Alcune soluzioni provano a risolvere la cosa con agenti, client, server bastion distribuiti o una combinazione dei tre. Tale tipo di approcci aumentano la complessità del sistema, riducono il livello di sicurezza e compromettono l'adozione su larga scala.

Keeper Connection Manager risolve la complessità e il dilemma della sicurezza con una soluzione moderna e senza agente che fornisce quella sicurezza, facilità e velocità richieste dagli odierni ambienti di lavoro distribuiti e in remoto.

Perché scegliere Keeper Connection Manager per i vostri team IT e DevOps?

- Integrazione pronta all'uso con Keeper Secrets Manager. Gestite le credenziali per i collegamenti ai sistemi con privilegi nella cassetta di sicurezza di Keeper.
- Supporta l'autenticazione passwordless ai server remoti tramite tutte le soluzioni di autenticazione più diffuse con o senza una soluzione IdP.
- Accesso istantaneo alla sessione della console dei tuoi sistemi privilegiati. L'accesso fisico a un dispositivo non è richiesto, pertanto i costi di assistenza sono ridotti.
- Per ottenere e rimanere la condizione di conformità secondo SOX, HIPAA, RPGD, FINRA e altri regolamenti di settore, gli amministratori possono registrare le sessioni con privilegi e conservare registri dettagliati.
- Funzionalità all'avanguardia e avanzate supportano l'accesso multiutente, la condivisione multisessione, più sessioni aperte e il passaggio rapido tra le sessioni.
- L'accesso ai sistemi critici può essere chiuso completamente, in modo che non esistano punti d'ingresso ignoti o non autorizzati.
- Attenuate o riducete il rischio nei confronti di fornitori e collaboratori esterni di terze parti concedendo un accesso protetto, temporaneo e monitorato verso dispositivi e macchine autorizzati.

COHERENTIA
CYBERSECURITY

KEEPER
CONNECTION MANAGER

Scheda tecnica
Accesso remoto per DevOps e team IT

Un collegamento rapido, semplice e protetto con la vostra infrastruttura remota. Sostenuto dalla sicurezza zero-trust e zero-knowledge e da un servizio di assistenza di prim'ordine.

Cosa rende Keeper Connection Manager di gran lunga più sicuro rispetto alle tradizionali soluzioni per desktop remoti?

- Tutto il traffico passa attraverso un gateway protetto e autenticato. La sessione remota non è mai visibile nell'Internet pubblico.
- Secondo i principi del modello zero-trust, vengono consentiti solo i collegamenti autorizzati e autenticati.
- Tutte le funzioni remote 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**.