KEEPER®
CONNECTION MANAGER

Datasheet: Remote Desktop and Server Access

# Secure, effortless access to remote desktops and machines without a VPN

**Secure access to your systems from anywhere, on any device, through any web browser.**

For remote work to succeed long-term, organizations need a secure, reliable and scalable way to provide employees with fast access to desktops and applications.

Virtual private networks (VPNs) are a common choice, but they fall far short in several areas. They're expensive and notoriously difficult for IT personnel to configure and maintain – as well as for end-users to use. VPNs also suffer latency, reliability and availability problems.

When properly implemented, remote desktops are a compelling alternative to VPNs.

- The administrative burden for deploying, supporting and maintaining a standardized remote desktop environment is significantly less than it is for supporting distributed physical devices used by end-users.
- As long as the remote desktop solution doesn't require an agent on endpoints, employees can use essentially any machine for access, including their personal laptop and smartphone.
- There is rarely any need to physically access an end-user's device, which reduces overall support costs for company assets.
- Remote desktops harden security for distributed workers by making it possible to adopt a zero-trust architecture, something that's not possible with most VPNs.
- Actions that distributed teams perform via remote desktops are executed behind the enterprise firewall. As a result, they enjoy the same protection from corporate security systems that they would if they were working in a physical office environment.
- Remote desktops encourage users to store data on the enterprise's network instead of local machines. Protection is stronger inside the firewall because data can be properly backed up and secured. Additionally, data is far less likely to be misplaced and much more easily shared with others.
- Remote desktops are highly scalable, especially when they don't require an agent on endpoints. Images can be easily standardized, and updates to desktops and applications can be automated, since there's no need to access individual devices.

## Keeper Connection Manager Customer Story: Manufacturing Sector

Keeper Connection Manager can do more than provide remote desktops to people working from home. Because it's so scalable, secure, and easy to use, many organizations use it to provide desktops for labs and training environments.

A leading consumer device manufacturer set up training labs in its global offices. Providing direct access to desktops was difficult to maintain and confusing for users.

Keeper Connection Manager simplified internal systems for updating, securing and providing access for its team to train on lab-based remote desktops. The security and speed transformed the manufacturer's training environment. Trainees only required a web browser, a URL and login credentials.

KEEPER
CONNECTION MANAGER

Data Sheet
Remote Desktop and Server Access

# A fully remote desktop experience wherever your users are. Backed by zero-trust, zero-knowledge security and world-class support.

## What makes Keeper Connection Manager more secure than traditional remote desktop solutions?

- All traffic passes through a secure, authenticated gateway. Desktops are never exposed to the public Internet. Following zero-trust principles, only authorized and authenticated connections are allowed.
- All desktop functions are executed behind the corporate firewall. Remote users enjoy the same protection as if they were working inside an office on the corporate network.
- Client Certificates and Multi-Factor authentication can be enforced for even stronger security.
- Keeper Connection Manager is designed to operate on the Principle of Least Privilege. Access rights are carefully delegated through users and groups, which are automatically created by the Keeper Connection Manager packages and through strict file permissions.
- End-users communicate with remote desktops via a secure session from their browser. It's a simple and effective way to encrypt traffic between end-users and the gateway without hindering performance.
- Access to privileged systems can be granted without exposing login credentials to the end-user.
- Works with RDP, SSH, VNC, K8s and MySQL endpoints.

| Use Case | Keeper Connection Manager |
|---|---|
| Web-Based Access | ✓ |
| Multi-Factor Authentication | ✓ |
| Agentless Access | ✓ |
| Multiple Data Stores | ✓ |
| Zero-Knowledge Security | ✓ |
| Zero-Trust Framework | ✓ |
| Session Recording | ✓ |
| Passwordless Authentication | ✓ |
| Multi-Protocol Support | ✓ |
| Integration with Keeper Secrets Manager | ✓ |

## About Keeper Security, Inc.

Keeper Security, Inc. (Keeper) is the market-leading, top-rated cybersecurity platform for preventing password-related data breaches and cyberthreats. Keeper's zero-trust, zero-knowledge security and encryption software is trusted by millions of people and thousands of businesses globally. Keeper has been named PC Magazine's Best Password Manager of the Year & Editors' Choice, PCWorld's Editors' Choice and is the winner of multiple G2 Best Software Awards. Keeper is SOC-2 and ISO 27001 Certified and is also listed for use by the U.S. federal government through the System for Award Management (SAM). Learn more at https://keepersecurity.com.