KEEPER CONNECTION MANAGER

Datenblatt: Remote-Desktops und Serverzugriff

Sicherer, bequemer Zugriff auf Remote-Desktops und Rechner ohne VPN

Sicherer Zugriff auf Ihre Systeme von allen Geräten und Webbrowsern.

Für einen langfristigen Erfolg des Homeoffices benötigen Unternehmen eine sichere, zuverlässige und skalierbare Möglichkeit, um Mitarbeitern schnellen Zugriff auf Desktops und Anwendungen zu gewähren.

Virtuelle private Netzwerke (VPNs) sind eine gängige Wahl, aber bislang in mehreren Bereichen weit hinter den Erwartungen zurückgeblieben. Sie sind kostspielig, für IT-Mitarbeiter schwierig zu konfigurieren und zu warten und für Endbenutzer kompliziert zu bedienen. Bei VPNs hapert es zudem bei der Latenz, Zuverlässigkeit und Verfügbarkeit.

Mit einer ordnungsgemäßen Implementierung sind Remote-Desktops eine überzeugende Alternative zu VPNs.

- Der Verwaltungsaufwand für die Bereitstellung, Unterstützung und Wartung einer standardisierten Remote-Desktop-Umgebung ist erheblich geringer als bei verteilten Firmengeräten.
- Sofern für die Remote-Desktop-Lösung kein Agent an Endpunkten erforderlich ist, können Mitarbeiter praktisch jeden Computer verwenden, d. h. auch ihre persönlichen Laptops und Smartphones.
- Nur in den seltensten Fällen muss vor Ort auf das Gerät eines Endbenutzers zugegriffen werden, was den Vorteil mit sich bringt, dass Supportkosten deutlich gesenkt werden können.
- Remote-Desktops erhöhen die Sicherheit für Homeoffice-Mitarbeiter, da sie über eine Zero-Trust-Architektur laufen können. Dies ist mit den meisten VPNs nicht möglich.
- Befehle und Vorgänge, die Homeoffice-Mitarbeiter über Remote-Desktops ausführen, sind durch die Unternehmens-Firewall geschützt. Dadurch genießen sie die gleichen Sicherheitssysteme des Unternehmens wie in einer physischen Büroumgebung.
- Mit Remote-Desktops werden Benutzer automatisch bestärkt, Daten im Unternehmensnetzwerk zu speichern, und nicht etwa auf ihrem lokalen Computer. Der Schutz innerhalb der Firewall ist stärker, da Daten ordnungsgemäß gesichert und geschützt werden können. Darüber hinaus ist es weitaus unwahrscheinlicher, dass Daten verloren gehen. Sie können zudem viel einfacher mit anderen Mitarbeitern geteilt werden.
- Remote-Desktops sind sehr gut skalierbar, insbesondere wenn keine Agents an Endpunkten benötigt werden. Bilder lassen sich einfach standardisieren und Updates für Desktops und Anwendungen automatisieren, da kein Zugriff auf einzelne Geräte erforderlich ist.

Keeper Connection Manager Kundenbericht: Fertigungssektor

Keeper Connection Manager kann mehr als nur Remote-Desktop-Lösungen für Menschen anbieten, die von Zuhause aus arbeiten. Da die Anwendung sehr skalierbar, sicher und benutzerfreundlich ist, wird sie von vielen Organisationen verwendet, um Desktops für Labore und Schulungsumgebungen bereitzustellen.

So richtete zum Beispiel ein führender Hersteller von Verbrauchergeräten in seinen weltweiten Niederlassungen Schulungslabore ein. Die Bereitstellung eines direkten Zugriffs auf Desktops war einst schwierig zu verwalten und für Benutzer etwas verwirrend.

Mit Keeper Connection Manager konnte das Unternehmen interne Systeme zum Aktualisieren, Sichern und Bereitstellen des Zugriffs für das Team vereinfachen. So konnten Schulungen auf laborbasierten Remote-Desktops durchgeführt werden. Die Sicherheit und Geschwindigkeit verbesserten die Schulungsumgebung des Herstellers. Die Auszubildenden benötigten nun lediglich einen Webbrowser, eine URL und Zugangsdaten.

© 2022 Keeper Security, Inc.

KEEPER CONNECTION MANAGER

Datenblatt

Remote-Desktops und Serverzugriff

Ein komplettes Remote-Desktop-Erlebnis – unabhängig vom Standort Ihrer Benutzer. Unterstützt durch Zero-Trust-, Zero-Knowledge-Sicherheit und erstklassigen Support.

Was macht den Keeper Connection Manager sicherer als herkömmliche Remote-Desktop-Lösungen?

- Der gesamte Datenverkehr wird über ein sicheres, authentifiziertes Gateway geleitet. Desktops sind niemals dem öffentlichen Internet ausgesetzt. Gemäß den Zero-Trust-Prinzipien werden nur autorisierte und authentifizierte Verbindungen zugelassen.
- Alle Desktop-Funktionen werden hinter der Unternehmens-Firewall ausgeführt. Homeoffice-Benutzer genießen den gleichen Schutz, als würden sie in einem Büro im Unternehmensnetzwerk arbeiten.
- Client-Zertifikate und Multi-Faktor-Authentifizierungen lassen sich bei Wunsch nach einer verstärkten Sicherheit erzwingen.
- Keeper Connection Manager wurde entwickelt, um nach dem Prinzip der geringsten Berechtigung zu arbeiten. Zugriffsrechte werden sorgfältig durch Benutzer und Gruppen delegiert, die automatisch von den Keeper Connection Manager-Paketen und durch strenge Dateiberechtigungen erstellt werden.
- Endbenutzer kommunizieren mit Remote-Desktops über eine sichere Sitzung von ihrem Browser aus. Dies ist eine einfache und effektive Möglichkeit, um den Datenverkehr zwischen Endbenutzern und dem Gateway zu verschlüsseln, ohne dabei Abstriche bei der Leistung in Kauf nehmen zu müssen.
- Der Zugriff auf privilegierte Systeme kann gewährt werden, ohne dass dem Endbenutzer die Zugangsdaten offengelegt werden.
- Funktioniert mit RDP-, SSH-, VNC-, K8s- und MySQL-Endpunkten.

Anwendungsszenarien	Keeper Connection Manager
Webbasierter Zugriff	✓
Mehr-Stufen-Authentifizierung	✓
Agentunabhängiger Zugriff	✓
Mehrere Datenspeicher	✓
Zero-Knowledge-Sicherheit	✓
Zero-Trust-Framework	✓
Sitzungsaufzeichnung	✓
Passwortlose Authentifizierung	✓
Unterstützung mehrerer Protokolle	✓
Integration mit Keeper Secrets Manager	✓

Über Keeper Security, Inc.

Keeper Security, Inc. (Keeper) ist die führende Lösung zum Schutz vor passwortbezogenen Datenpannen und Cyberbedrohungen. Auf die Zero-Trust-, Zero-Knowledge-Sicherheit und Verschlüsselungssoftware von Keeper vertrauen Millionen von Menschen und Tausende von Unternehmen aus aller Welt. Keeper wurde vom PC Magazine zum besten Passwort-Manager des Jahres und Editors' Choice ernannt. Von PCWorld wurde es ebenfalls zum Editors' Choice gewählt. Außerdem hat Keeper mehrere G2 Best Software Awards erhalten. Keeper ist nach SOC-2 und ISO 27001 zertifiziert und wird über das System for Award Management (SAM) auch von der US-Regierung verwendet. Nähere Infos unter **https://keepersecurity.com**.

© 2022 Keeper Security, Inc.