BeyondTrust

Choisir le bon logiciel de support technique à distance est essentiel pour assurer la productivité et la sécurité de votre service desk

Remote Support Buyer's Guide

TABLE DES MATIÈRES

Introduction

Les services help desks IT sont confrontés à un environnement de plus en plus complexe qui requiert des options de support à distance flexibles capables d'évoluer, de s'adapter et de continuer à répondre à des exigences de sécurité rigoureuses. Que vous soyez propriétaire d'une petite entreprise du secteur IT ou que vous fassiez partie de l'équipe du support technique d'une grande entreprise, choisir le bon logiciel de support à distance est essentiel pour assurer la productivité et la sécurité de votre service desk.

Un audit des outils de support à distance utilisés dans votre organisation est susceptible de révéler un ensemble de produits d'accès distant utilisés pour différents scénarios, y compris :

- aide apportée aux utilisateurs à l'intérieur et à l'extérieur du périmètre réseau traditionnel ;
- accès à distance aux serveurs et aux postes de travail, ainsi qu'à d'autres systèmes autonomes ;
- entretien des périphériques réseau (commutateurs, routeurs, etc.) ;
- prise en charge d'un certain nombre de plates-formes, y compris Windows, Linux et Mac ;
- prise en charge d'une grande variété de dispositifs mobiles comme iOS et Android ;
- possibilité d'accès à distance pour les fournisseurs et autres tiers ;
- support des périphériques hors réseau, tels que les robots, les machines et tout autre appareil non connecté à Internet.

Avec Remote Support, la simplification est synonyme d'avantages

De nombreux services desks utilisent plusieurs outils pour le support à distance, mais les équipes techniques peuvent être limitées lorsqu'elles passent d'un outil à un autre pour différentes tâches. Certains outils ne prennent en charge qu'un ensemble restreint de systèmes ou de plates-formes et manquent de fonctionnalités d'intégration avancées. Dans de telles situations, votre écosystème d'outils de support peut en réalité nuire à l'innovation, empêchant votre organisation de passer à de meilleurs systèmes. La peur suscitée par les défis liés à l'intégration, au respect des conformités, ainsi qu'à l'augmentation de la charge administrative et des cyberrisques peut freiner l'intégration de nouvelles technologies et applications d'entreprise.

En termes simples, les organisations ont besoin de solutions de support à distance capables de couvrir une longue liste de cas d'usages, tout en améliorant l'expérience de votre équipe.

> *Un logiciel de support distant permet à un ordinateur d'accéder à distance à un autre ordinateur ou appareil et d'en visualiser l'écran via une connexion Internet.*

Définition du support à distance

Un logiciel de support distant permet à un ordinateur d'accéder à distance à un autre ordinateur ou appareil et d'en visualiser l'écran via une connexion Internet, en particulier pour fournir des fonctionnalités en la matière.

Les solutions de support à distance doivent permettre aux spécialistes du support IT de contrôler des systèmes depuis presque n'importe quel ordinateur ou appareil mobile pouvant accéder au Web, ce qui leur permet de prendre en charge des PC et des Mac, des appareils mobiles et d'autres ressources du réseau, telles que des serveurs et des systèmes de point de vente (POS).

Les solutions de support à distance peuvent nécessiter ou non l'installation préalable d'un logiciel client sur la machine bénéficiant du support afin que l'équipe technique puisse y accéder. Elles ne doivent pas non plus nécessiter que des réseaux privés virtuels (VPN) ou des ports ouverts soient utilisés pour établir la connexion.

Sessions autonomes et non autonomes

Le support à distance peut être effectué via des sessions autonomes ou non autonomes. Les sessions non autonomes, la méthode la plus typique, consistent en un support fourni en direct au client (soit en interne, soit en externe). Les sessions de support à distance autonomes sont celles au cours desquelles l'équipe technique se connecte à un appareil ou à un système sans que la présence d'une autre personne soit nécessaire. Les sessions autonomes sont un moyen non intrusif permettant aux équipes techniques d'évaluer à distance l'état de santé des endpoints (ordinateurs de bureau, serveurs, appareils mobiles, etc.), des applications et des systèmes, ainsi que d'effectuer des mises à jour et des opérations de maintenance sur un ou plusieurs endpoints, applications ou systèmes.

Gestion de la sécurité des accès à distance

Les outils de support à distance sont désormais considérés par les pirates et votre CISO. Les outils et les chemins d'accès à distance sont de plus en plus exploités par les cyberattaquants comme des portes dérobées dans les environnements des utilisateurs finaux et des clients, de sorte que les organisations doivent adopter une approche prenant en compte la sécurité afin d'évaluer toutes les solutions d'accès/de support à distance.

Les méthodes traditionnelles de connectivité à distance, telles que les VPN ou les outils d'accès à distance gratuits, manquent de contrôles granulaires de gestion des accès et peuvent être facilement exploitées via le vol d'identifiants et le piratage de session. Elles ne disposent généralement pas d'options suffisantes de configuration granulaire des autorisations, il n'est pas possible de consigner ou d'enregistrer des sessions de support à distance et leur utilisation affaiblit le fonctionnement des pare-feu.

> *Les méthodes traditionnelles de connectivité à distance peuvent être facilement exploitées via le vol d'identifiants et le piratage de session.*

Les attaquants ont également tiré parti d'outils de support à distance légitimes sur les machines du service support. Par exemple, les attaquants ont exploité le support à distance et d'autres outils d'accès à distance sur les appareils des employés d'un certain nombre de fournisseurs de services IT (y compris des MSP et MSSP) et les ont utilisés comme portes dérobées pour lancer des attaques tierces contre les clients de ces fournisseurs de services. La standardisation d'une solution de support à distance hautement sécurisée dans l'ensemble de l'entreprise facilitera la création d'une liste de blocage générale pour les autres outils de ce type, ce qui réduira le risque lié aux logiciels d'accès à distance malveillants et au « shadow IT ».

Votre service support est-il vulnérable ?

Les experts en sécurité désignent souvent les services support comme étant le point le plus vulnérable d'une entreprise, car les équipes techniques qui y travaillent sont souvent mal formées pour identifier les attaques d'ingénierie sociale. Ils font simplement ce pour quoi ils ont été formés : aider à résoudre les problèmes des utilisateurs. Les représentants du service support sont souvent des cibles pour les campagnes de phishing. Étant donné que les services support ne surveillent généralement pas leurs équipes (suivi des journaux d'appels, enregistrement des changements d'authentification, etc.), il est fort probable que les pirates continueront à exploiter de manière opportuniste leurs stratagèmes de phishing via le service support.

Vous devez examiner attentivement l'impact des outils de support à distance sur la sécurité, la flexibilité, la fiabilité et la réputation de votre organisation.

Quelle est votre solution idéale pour le support à distance ?

Il existe de nombreux cas d'usages du support à distance, mais peu importe qui ou ce que vous prenez en charge, les utilisateurs de telles technologies veulent une solution facile à utiliser, fiable et sécurisée.

La bonne solution de support à distance permet aux utilisateurs d'accéder rapidement à presque n'importe quel périphérique distant et d'apporter un support, où qu'il se trouve et quelle que soit la plate-forme qu'il exécute. Elle doit également offrir une visibilité et un contrôle absolus sur les accès à distance internes et externes, sécuriser la connectivité aux ressources gérées et fournir une piste d'audit complète et irréprochable pour assurer la conformité.

La bonne solution de support à distance est efficace en :

- améliorant la satisfaction client et la résolution dès le premier appel (FCR) ;
- réduisant le délai de traitement des incidents ;
- optimisant la productivité des représentants et la satisfaction au travail ;
- rationalisant les processus et en améliorant les workflows existants ;
- tirant plus de valeur de vos autres outils du service support, tels que les solutions ITSM et CRM ;
- résolvant les problèmes de sécurité et en atténuant les risques.

Ce livre blanc fournit des informations détaillées et sert de guide pour choisir la solution de support à distance la mieux adaptée à votre entreprise.

La bonne solution de support à distance permet aux utilisateurs d'accéder rapidement à presque n'importe quel périphérique distant et d'apporter un support, où qu'il se trouve et quelle que soit la plate-forme qu'il exécute.

Comment utiliser ce guide

Les acheteurs de Remote Support recherchent un produit mûr et riche en fonctionnalités. Qu'est-ce que cela signifie exactement ? Ce buyer's guide se concentre sur les caractéristiques et fonctionnalités que vous devriez considérer comme essentielles pour mettre en place un environnement de service support moderne.

Tout au long du processus d'évaluation des solutions de support à distance, gardez à l'esprit ces exigences professionnelles :

Coût total de possession

Cela vous permet-il de gagner du temps (par exemple en remplaçant des processus manuels par une automatisation) et de redéployer des ressources en faveur d'autres initiatives ?

Rapidité de constatation des bénéfices

Dans quel délai cela vous permet-il d'améliorer de manière mesurable les performances de votre service support ? Combien de temps vous faudra-t-il pour atteindre vos objectifs avec la solution ?

Intégrations

Comment cela s'intègre-t-il au reste de votre écosystème ITSM ? Si la solution fonctionne correctement seulement en tant que solution autonome ou ponctuelle et pour une gamme limitée de cas d'usages, ce n'est probablement pas viable en tant que solution à long terme. D'autre part, si la solution présente des synergies avec vos autres outils du service support, cela vous aidera à maximiser les investissements IT existants.

Longévité

Le fournisseur de votre solution évoluera-t-il avec vous ? Ira-t-il jusqu'à vous accompagner dans l'optimisation de votre service support ? Le fournisseur dispose-t-il des ressources nécessaires pour faire évoluer les fonctionnalités et enrichir ces dernières afin de répondre aux cas d'usages futurs ? Au fur et à mesure que votre organisation se développe, votre solution doit se développer avec vous !

Répondre aux exigences les plus essentielles optimise votre service support.

Les cinq composants clés d'une solution complète de support à distance

Tout d'abord, votre solution de support à distance doit permettre à votre service desk d'être plus puissant, plus efficace et plus efficient. Cette section couvre les principales fonctionnalités à prendre en compte dans cinq catégories pour une solution de support à distance.

1. VASTE PRISE EN CHARGE DES PLATES-FORMES

Les solutions modernes de support à distance devraient permettre aux équipes techniques de fournir un support quelle que soit leur plate-forme ou celle de l'utilisateur final. Lorsque les équipes techniques sont en déplacement, elles doivent être en mesure de fournir un support en toute facilité via leur appareil mobile. Parfois, les équipes techniques doivent se connecter rapidement via un navigateur Web, tel que Chrome. Dans ces cas, avoir une console basée sur HTML 5 peut être particulièrement avantageux.

Plus la prise en charge de la plate-forme est étendue, plus vous pouvez standardiser le support en utilisant un outil unique afin d'améliorer le délai de traitement des incidents et la productivité des équipes, le tout en bénéficiant d'une efficacité accrue.

Principales plates-formes prises en charge

- Windows
- macOS
- Linux
- Android
- iOS
- Chrome OS
- Autres périphériques, kiosques ou machines, connectés ou non à un réseau

Votre solution de support à distance doit permettre à votre service desk d'être plus puissant, plus efficace et plus efficient.

Questions à poser au fournisseur

- Quelles plates-formes prenez-vous en charge ?
- Tout cela est-il inclus dans le produit de base, ou devons-nous payer un supplément, par exemple pour le support mobile ?
- Cela inclut-il la prise en charge de la plate-forme de l'utilisateur final uniquement, ou puis-je aussi assurer un support à partir de ces plates-formes ?

2. COLLABORATION

Des fonctionnalités telles que le support par chat, le partage de caméra à distance, la collaboration intelligente et d'autres appartenant à cette catégorie sont essentielles à l'expérience support client et contribuent à accélérer la résolution des incidents et la productivité tout en offrant d'autres gains d'efficacité.

Principales fonctionnalités axées sur la collaboration et l'efficacité

Flux de travail rationalisés

- Définissez des chemins de remontées vers des ressources compétentes pour permettre une collaboration intelligente et transférer rapidement des sessions de support à distance de façon pertinente
- Fournissez des scripts prédéfinis qui peuvent être utilisés pour exécuter des correctifs ou des programmes d'installation sur des postes de travail et des serveurs distants
- Accordez un accès sécurisé à la ligne de commande pour le support réseau, les diagnostics système ou le support de périphériques réseau avec un enregistrement des sessions de ligne de commande à des fins de sécurité et d'audit
- Mettez en place une utilisation sécurisée sur les réseaux distants, sans nécessiter de tunnellisation VPN ou de modifications du pare-feu
- Créez et administrez des enquêtes destinées aux clients ainsi qu'aux équipes support.

Prise en charge et chat multiplateforme

- Permettez aux équipes support de fournir efficacement de l'aide à partir de votre site Web
- Activez le partage d'écran des appareils mobiles Android et macOS
- Procurez un support pour tout ce que votre client peut voir, y compris le matériel et les périphériques, en partageant à distance la vue de la caméra
- Intégrez des fonctions de chat et d'autres outils de support à distance dans votre application
- Fournissez des fonctionnalités de réalité augmentée qui permettent aux équipes support de voir exactement ce que le client voit en temps réel et d'effectuer des annotations via un flux en direct

Mise à l'échelle

- Activez un support pour gérer l'accès autonome à des centaines ou des milliers de systèmes
- Créez des packages d'installation en masse pour les consoles des équipes support et les endpoints non surveillés

Fonctionnalités avancées

- Assurez un support sous le système d'exploitation en tirant parti de la technologie Intel vPro pour allumer/éteindre à distance un ordinateur, redémarrer le BIOS, réimager un ordinateur distant et accéder à des postes de travail distants, quel que soit l'état du système d'exploitation
- Fournissez un accès à l'éditeur de registre distant sur des ordinateurs Windows sans interrompre le client distant et sans nécessiter une session de partage d'écran.
- Soyez en mesure de mettre fin à des processus ; démarrez, arrêtez, mettez en pause, reprenez et redémarrez des services ; et désinstallez des programmes sur des ordinateurs ou des appareils mobiles distants.

Les fonctionnalités dans cette catégorie sont essentielles à l'expérience du support client et contribuent à accélérer la résolution des incidents.

Plus l'intégration du support à distance avec le reste de votre service desk est forte, meilleure est l'expérience de vos équipes et de vos clients.

3. INTÉGRATIONS

Vous avez déjà investi dans des solutions pour votre service support afin de suivre plus efficacement les incidents et les demandes des utilisateurs finaux. Votre logiciel de support à distance doit s'intégrer parfaitement dans votre environnement et provoquer des synergies avec les autres solutions de votre écosystème.

Les solutions de support à distance fournies avec des intégrations prêtes à l'emploi pour les principales solutions ITSM, CRM et de gestion des systèmes réduisent la complexité administrative.

De puissantes intégrations de support à distance et de solutions ITSM permettent aux entreprises de fournir des services plus efficacement, de réduire les demandes opérationnelles et de gérer les processus, les flux de travail ainsi que les expériences de service. Afin de résoudre et de gérer les incidents sans heurt, vos équipes doivent pouvoir lancer une session de support à distance directement depuis le ticket de support ou le registre des modifications, de mettre à jour automatiquement les tickets avec les informations provenant de la session de support, et d'inclure la transcription du chat et l'enregistrement de la session dans le ticket. Pour ce faire, il faut intégrer vos outils de support à distance avec vos systèmes de gestion des incidents et des dossiers.

Plus l'interopérabilité et l'intégration du support à distance avec le reste de votre service desk sont fortes, meilleure est l'expérience de vos équipes et de vos clients.

Principales fonctionnalités d'intégration des solutions ITSM

- Intégrations prédéfinies avec des solutions ITSM, CRM et de gestion de systèmes, telles que ServiceNow, Salesforce, etc.
- Intégrations avec des annuaires externes, tels que LDAP, Active Directory, RADIUS et SAML, afin de pouvoir gérer les utilisateurs, les groupes, l'authentification MFA et les autorisations au moyen de processus administratifs existants, et prendre en charge l'authentification unique (SSO)
- Fonctionnalités personnalisées d'intégration et API robustes
- Capacité à démarrer un chat ou une session de support à distance directement depuis n'importe quel outil ITSM
- Passage en un clic du chat à une session complète de support à distance
- Remplissage automatique des dossiers d'incidents avec les détails de la session de support à distance, y compris l'enquête post-session, le cas échéant
- Acheminement automatique des demandes de support à distance entrantes vers le technicien le moins occupé

Questions à poser au fournisseur

- À quelle fréquence les intégrations sont-elles mises à jour ?
- À quel point est-il facile d'accéder à l'intégration et de la configurer ?
- L'application fournit-elle des API pour des intégrations personnalisées ?
- Des API sont-elles disponibles pour aider à automatiser l'intégration de nouveaux utilisateurs et ressources ?
- Quelles fonctionnalités sont prises en charge ? Demandez les détails !

4. SÉCURITÉ, AUDIT ET CONFORMITÉ

L'augmentation du télétravail a entraîné celle du nombre de violations de données via des outils d'accès à distance point à point tels que RDP, VNC et des outils d'accès non sécurisés gratuits. Les cas d'usages limités de ces outils sont souvent étendus au-delà de ce qui est sûr ou efficace, et leurs fonctionnalités de sécurité (ou leur absence) devraient constituer un signal d'alerte. Les problèmes posés par ces outils sont multiples. Les failles demandant une attention immédiate sont le dangereux manque de visibilité des sessions d'accès à distance et l'incapacité d'appliquer le principe du moindre privilège aux accès.

> *La mise en place d'un coffre-fort de mots de passe intégré et robuste permet à votre entreprise de stocker, partager et suivre en toute sécurité l'utilisation des identifiants à privilèges par le service support IT.*

Les équipes du service support doivent souvent utiliser des identifiants admins avec des privilèges élevés pour résoudre les incidents. Bien que les identifiants de comptes à privilèges soient une cible courante pour les pirates, les meilleures pratiques de gestion des identifiants sont souvent sacrifiées sur l'autel de la résolution rapide des problèmes. En effet, de nombreuses équipes de support partagent et stockent les identifiants en texte brut. Il est essentiel de fournir aux équipes techniques les identifiants et les moyens d'authentification dont ils ont besoin rapidement pour accéder sans délai aux systèmes IT, tout en appliquant les meilleures pratiques de gestion des identifiants.

L'environnement de menaces et les réglementations actuelles exigent des entreprises qu'elles soient en mesure d'identifier et d'enregistrer le qui, le quoi, le où et le quand en ce qui concerne les activités d'accès à distance. Ce sont des questions auxquelles peuvent répondre uniquement les meilleurs outils professionnels de support à distance puisqu'ils ont été conçus pour cela. Pourtant, même parmi les outils d'entreprise, il peut y avoir des différences substantielles en ce qui concerne la maturité des fonctions de sécurité et l'exhaustivité des fonctionnalités.

Que vous soyez régi par des réglementations telles que le PCI, l'HIPAA, les normes ISO, la RGPD, le NIST, les CJIS, le FFIEC ou d'autres, la bonne solution doit vous aider à produire facilement les rapports d'attestation détaillés pour prouver votre conformité. Les fonctions de sécurité, qui prennent en charge ces mesures, incluent le cryptage avancé, l'application du principe du moindre privilège et le contrôle granulaire de l'accès aux données sensibles (telles que les informations permettant une identification personnelle), les journaux d'audit et les enregistrements de toutes les sessions.

Principales fonctionnalités en matière de sécurité, d'audit et de conformité

Le service support peut être extrêmement vulnérable sur le plan de la sécurité. Les outils et les chemins d'accès à distance sont de plus en plus exploités par les cyberattaquants comme des portes dérobées dans les environnements des utilisateurs finaux et des clients. Tout outil de support à distance envisagé doit pouvoir remédier à ces risques.

Architecture de sécurité

- Applique un cryptage robuste, y compris l'utilisation du protocole SSL pour chaque connexion de session. Dans l'idéal, toutes les données devraient être cryptées en transit à l'aide du protocole TLSv1.2, et vous devriez être en mesure de configurer (activer, désactiver, réorganiser, etc.) les suites de cryptage selon vos besoins
- Possibilité d'utiliser des certificats SSL
- Capable de fonctionner à travers les pare-feu sans tunnellisation par VPN, de sorte que la sécurité de votre périmètre demeure intacte.
- Utilise le trafic de session sortant uniquement via le port TCP 443. En limitant l'exposition des ports, vous réduisez considérablement la surface d'attaque potentielle de votre site de support.
- Segmente chaque client du support à distance via des environnements à locataire unique, de sorte que vos données ne soient jamais mélangées avec d'autres données clients

Les outils et les chemins d'accès à distance sont de plus en plus exploités par les cyberattaquants. Tout outil de support à distance envisagé doit pouvoir remédier à ces risques.

Pistes d'audit et rapports

- Enregistre les détails de chaque session, permettant l'audit complet et l'examen de toutes les interactions entre le client et le support, y compris les autorisations accordées par le client, les transcriptions du chat, les informations système et toute autre action effectuée par l'équipe technique
- Conserve les journaux de session complets dans un format non modifiable jusqu'à 90 jours
- Enregistre des vidéos de la session en capturant l'interface utilisateur visible de l'écran du endpoint pendant toute la durée du partage d'écran, y compris les métadonnées pour identifier qui contrôle la souris et le clavier à chaque instant

Authentification et autorisations

- Possibilité de définir et d'appliquer différentes règles pour les sessions de support à distance autonomes ou non
- Authentification sécurisée grâce à une intégration harmonieuse avec les annuaires d'utilisateurs externes, tels que LDAP
- Authentification native à deux facteurs ou via l'intégration 2FA depuis une solution existante
- Transmission d'identifiants sur carte à puce locale ou carte d'accès commun (CAC) vers un ordinateur distant
- Les coffres-forts de mots de passe intégrés permettant aux équipes techniques de stocker, partager et suivre en toute sécurité l'utilisation des identifiants à privilèges par le service IT

Le rôle des coffres-forts d'identifiants

La solution idéale de gestion des mots de passe doit s'intégrer parfaitement au flux de travail de votre service support, tout en atténuant les menaces potentielles liées au vol d'identifiants et de mots de passe qui pourrait l'affecter. Les fonctionnalités clés comprennent :

- La découverte et l'intégration de tous les identifiants du support à distance
- La possibilité de masquer les mots de passe en texte brut afin qu'ils ne soient jamais révélés à l'utilisateur final ou au client
- La rotation fréquente des identifiants
- L'injection automatique des identifiants dans le système, l'application, etc., où l'accès est nécessaire
- L'extraction du mot de passe du coffre-fort sécurisé lorsque l'accès est nécessaire et que les critères d'authentification sont remplis et renvoi du mot de passe (archive) dans le coffre-fort lorsque la session a expiré
- L'application du principe du moindre privilège et des autorisations granulaires de sorte qu'un accès dimensionné soit accordé à ceux qui en ont besoin

Questions à poser au fournisseur

- Le 2FA est-il inclus sans frais supplémentaires ?
- Prenez-vous en charge le chiffrement des données au repos ?
- Les données sont-elles cryptées au repos dans l'offre cloud proposée ?
- Existe-t-il un journal d'audit inviolable ?
- La solution a-t-elle obtenu une certification FIPS ou d'autres certifications de sécurité ?
- Puis-je suivre les comptes à privilèges couramment utilisés dans le service support ?
- La solution masque-t-elle les mots de passe en texte brut aux utilisateurs ?
- Existe-t-il une rotation automatique ou manuelle des mots de passe après chaque utilisation ?
- Puis-je exporter des enregistrements de session ? Dans quel format ?

5. STRATÉGIE DE MARQUE ET PERSONNALISATION

Les clients du support peuvent être réticents à l'idée d'autoriser une connexion à distance à leurs appareils. Un moyen efficace pour les entreprises de support de renforcer la notoriété positive de leur marque et de favoriser la confiance passe par la personnalisation de l'expérience de support pour leurs clients. Idéalement, votre solution de support à distance devrait vous permettre de créer des portails personnalisés pour chaque client, groupe et/ou produit pris en charge par vos utilisateurs.

Principales fonctionnalités en matière de stratégie de marque et de personnalisation

- Offre la possibilité de personnaliser le portail avec votre logo et d'autres caractéristiques
- Permet de personnaliser les invitations au support
- Permet l'utilisation d'un filigrane personnalisé
- Offre plusieurs éléments de personnalisation, y compris pour les sites publics, les accords et les messages, les enquêtes de sortie des clients, etc.
- Permet l'importation de photos des équipes techniques à partir d'Active Directory pour personnaliser l'expérience de support

Questions à poser au fournisseur

- Comment pouvons-nous envoyer des demandes de support via le Web ?
- Si je procure mes services de support à plusieurs clients, puis-je créer une expérience utilisateur personnalisée pour chaque entreprise cliente ?
- Puis-je personnaliser les accords et les messages relatifs au support ?
- Puis-je personnaliser la fenêtre du chat ?

Avantages de la consolidation vers une solution de support unique

Les acheteurs doivent rechercher un fournisseur qui propose une approche complète et intégrée pour sécuriser la prestation du support à distance.

Grâce à l'utilisation d'un seul produit, une entreprise de support élimine les coûts redondants. La majeure partie du temps passé à installer, entretenir, supporter ou gérer plusieurs outils peut désormais être utilisée pour résoudre les incidents.

Avantages de la consolidation

- Économies directes dans le provisionnement du support IT
- Gain de temps en termes de productivité pour les employés
- Moins de visites sur site pour le support
- Réduction de la prolifération des outils et des risques pour la sécurité
- Audits et rapports simplifiés

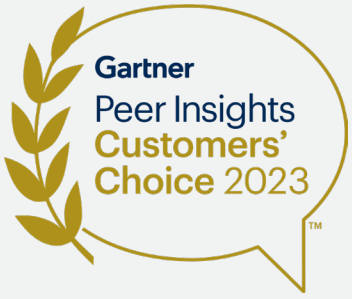
> *La consolidation vers un seul outil de support permet d'économiser du temps et de l'argent*

Remote Support de BeyondTrust

Remote Support de BeyondTrust est la meilleure solution pour accéder et supporter en toute sécurité n'importe quel appareil ou système, quel que soit le lieu, et permet aux services IT de se concentrer sur la résolution des problèmes des utilisateurs, tout en maintenant les plus hauts niveaux de sécurité.

En effet, BeyondTrust dispose de la seule solution de support à distance qui répond aux exigences rigoureuses de la norme FIPS 140-2 niveau 2. Remote Support optimise l'efficacité du service support, comble les failles de sécurité liées à l'accès à distance et simplifie les audits de conformité au moyen d'un journal de session centralisé, optimisant ainsi la valeur avec une solution unique.

Planifiez une démo ou lancez un essai gratuit sur beyondtrust.com/remote-support



Remote Support de BeyondTrust a également été désigné comme le **choix des clients 2023 dans l'étude Gartner® Peer Insights™ pour le Remote Desktop Software**.

Vous pouvez accéder au rapport en cliquant ici.

Nous pensons que cette reconnaissance confirme une fois de plus Remote Support de BeyondTrust en tant que solution leader dans sa catégorie. Sur la base des enquêtes réalisées par BeyondTrust, nous sommes fiers d'annoncer que plus de 70 % de nos clients Remote Support ont réduit les temps de traitement des incidents grâce au produit, tandis que 85 % ont amélioré les résolutions au premier appel et enregistré des scores de satisfaction client (CSAT) en hausse en utilisant cette solution.

*Vous pouvez aussi consulter ce que nos clients Remote Support pensent de nous sur la plate-forme Gartner® Peer Insights™, en cliquant **ici**.*

Annexe : Checklist de Remote Support

Collaboration et efficacité	BeyondTrust	Fournisseur A	Fournisseur B
Chat	✓		
Collaboration intelligente (chemins d'escalade définis, acheminement des demandes)	✓		
Partage d'écran sur iPhone, iPad et Android	✓		
Scripts prédéfinis	✓		
Support à distance adaptable pour accéder à des centaines de milliers de systèmes	✓		
Partage de caméra distante	✓		
Chat et support intégrés pour vos applications	✓		
Sessions de ligne de commande	✓		
Support sous le système d'exploitation en tirant parti de la technologie Intel vPro pour accéder à des postes de travail distants, quel que soit l'état du système d'exploitation	✓		
Réalité augmentée	✓		
Éditeur de registre distant	✓		
Enquêtes d'après-session	✓		

Plates-formes prises en charge	BeyondTrust	Fournisseur A	Fournisseur B
Windows	✓		
macOS	✓		
Linux	✓		
Android	✓		
iOS	✓		
Chrome OS	✓		
Accédez à tout ordinateur ou appareil distant et contrôlez-le, sur le réseau ou en dehors	✓		

Fonctionnalités d'intégration aux solutions ITSM	BeyondTrust	Fournisseur A	Fournisseur B
Intégration prête à l'emploi pour vos solutions ITSM	✓		
Intégration prête à l'emploi avec des annuaires externes tels que LDAP, Active Directory, RADIUS, SAML et/ou SSO	✓		
Fonctionnalités personnalisées d'intégration et API robustes	✓		
Lancement de sessions de chat ou de support directement à partir de l'outil ITSM	✓		
Élévation en un clic d'une session de chat à un support à distance complet	✓		
Remplissage automatique des dossiers d'incidents avec les détails de la session de support à distance	✓		

Sécurité, audit et conformité	BeyondTrust	Fournisseur A	Fournisseur B
Fonctionne à travers les pare-feu sans tunnellisation par VPN, de sorte que la sécurité de votre périmètre demeure intacte	✓		
Trafic de session sortant uniquement via le port TCP 443	✓		
Segmente chaque client du support à distance via des environnements à locataire unique (single tenant)	✓		
Offre la possibilité de définir et d'appliquer différentes règles pour les sessions de support à distance autonomes ou non	✓		
Applique des autorisations robustes et granulaires pour définir la manière dont les équipes techniques, les clients et les systèmes distants interagissent	✓		
Permet aux admins de transmettre des identifiants sur carte à puce locale ou carte d'accès commun (CAC) vers un ordinateur distant	✓		
Authentifie de façon sécurisée les utilisateurs grâce à une intégration harmonieuse avec les annuaires d'utilisateurs externes, tels que LDAP	✓		
Fournit nativement une authentification à deux facteurs ou prend en charge l'intégration 2FA depuis une solution existante	✓		
Propose un coffre-fort de mots de passe pour stocker, partager et suivre l'utilisation des identifiants à privilèges, ce qui comprend des fonctionnalités plus avancées telles que la découverte, la rotation et l'automatisation des flux de travail	✓		
L'application du principe du moindre privilège et des autorisations granulaires de sorte qu'un accès dimensionné soit accordé à ceux qui en ont besoin	✓		
Affiche des notifications de sorte que l'utilisateur bénéficiant du support doit approuver certaines actions	✓		

Sécurité, audit et conformité	BeyondTrust	Fournisseur A	Fournisseur B
Applique un chiffrement robuste, y compris l'utilisation du protocole SSL pour chaque connexion à une session	✓		
Enregistre les détails de chaque session, permettant l'audit complet et l'examen de toutes les interactions entre le client et l'équipe de support. Les données de session enregistrées doivent inclure les équipes impliquées, les autorisations accordées par le client, les transcriptions du chat, les informations sur le système et toute autre action entreprise par l'équipe technique	✓		
Conservation des journaux de session complets dans un format non modifiable jusqu'à 90 jours	✓		
Enregistrement de la session de l'interface utilisateur visible sur l'écran du endpoint pour toute la session de partage d'écran. L'enregistrement doit également inclure des métadonnées pour identifier qui contrôle la souris et le clavier à tout moment	✓		
Capacité d'utiliser des certificats SSL	✓		

STRATÉGIE DE MARQUE ET PERSONNALISATION	BeyondTrust	Fournisseur A	Fournisseur B
Personnalisation du site de support avec votre logo et d'autres options	✓		
Invitations personnalisées au support	✓		
Utilisation d'un filigrane personnalisé	✓		
Personnalisation des accords et des messages, des enquêtes de sortie des clients, etc.	✓		
Chargement de la photo des techniciens — manuellement ou depuis Active Directory	✓		

À PROPOS DE REMOTE SUPPORT

Remote Support de BeyondTrust permet aux équipes support d'accéder rapidement et en toute sécurité à n'importe quel appareil distant, sur n'importe quelle plate-forme, et de résoudre des incidents, grâce à une solution unique. BeyondTrust permet le plus grand nombre de cas d'usages de support à distance avec ou sans surveillance, possède les fonctions de sécurité intégrées les plus robustes et débloque de puissantes synergies grâce à des intégrations clés du service desk. Bénéficiez d'une visibilité et d'un contrôle absolus sur les accès à distance internes et externes, sécurisez la connectivité aux ressources gérées et créez une piste d'audit complète et irréprochable pour assurer la conformité. Les organisations de toutes tailles peuvent améliorer leur productivité, leur efficacité et leur sécurité en consolidant et en normalisant leur service support avec BeyondTrust.

À PROPOS DE BEYONDTRUST

BeyondTrust est le leader mondial de la gestion intelligente des identités et de la sécurisation des accès, permettant aux organisations de protéger les identités, de contrer les menaces et de fournir un accès dynamique. Nous sommes à la pointe de l'innovation en matière de sécurisation des identités et bénéficions de la confiance de 20 000 clients, dont 75 font partie du classement Fortune 100, ainsi que d'un écosystème mondial de partenaires.

Pour en savoir plus, rendez-vous sur **beyondtrust.com/fr**