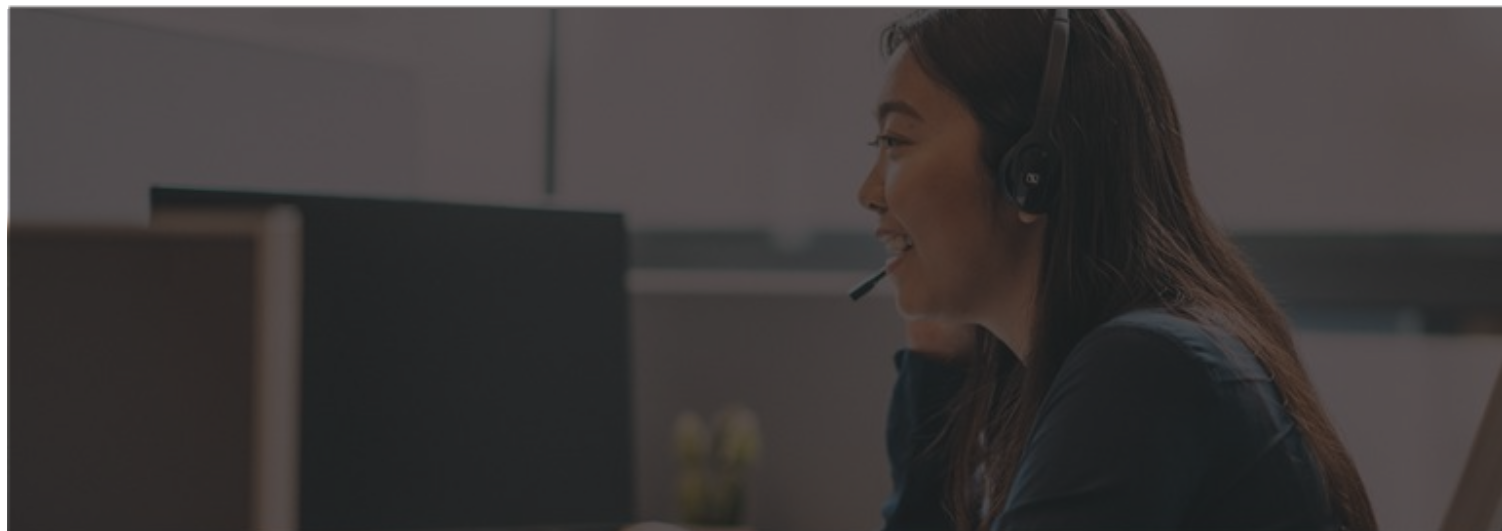




REMOTE SUPPORT BUYER'S GUIDE

貴社ヘルプデスクに最適なソリューションを選定するための
ベンダーと製品の評価基準



目 次

1. 序章	2
2. リモートサポートの定義	3
3. リモートアクセスにおけるセキュリティ	4
4. 貴社の理想のリモートサポートソリューションとは	5
5. このガイドの使い方	6
6. 完全なリモートサポートソリューションの 6つの主要コンポーネント	7
1. 幅広いプラットフォームのサポート	7
2. コラボレーション	8
3. 連携と統合	9
4. セキュリティ、監査、コンプライアンス	10
5. ブランディングとカスタマイズ	12
6. 柔軟な導入オプション	12
1つのサポートソリューションに統合するメリット	13
7. BeyondTrust Remote Support	14
8. 付録:Remote Support 選定チェックリスト	15

1 序章

適切なリモートサポートソフトウェアの選択は、サービスデスクの生産性とセキュリティ面で極めて重要

IT ヘルプデスクはますます複雑化するサポート対象環境に直面しており、厳格なセキュリティ要件に対応し、拡張、適応、そして継続的で柔軟なリモートサポート方法の選択肢が必要です。小規模な IT ビジネスオーナーでも、大企業の技術サポートチームのメンバーでも、適切なリモートサポートソフトウェアを選択することは、サービスデスクの生産性とセキュリティの面で極めて重要です。

組織内のリモートサポートツールを監査すると、次に挙げるような多様なサポートシナリオで使用されているリモートアクセス製品の混在が顕在化する場合があります。

- ▶ 従来の考え方でのネットワーク境界の内外にいるユーザーを支援
- ▶ サーバーやワークステーション、その他の無人システムにリモートでアクセスする
- ▶ ネットワークデバイス（スイッチ、ルーターなど）の保守
- ▶ Windows、Linux、Mac 上のシステムを含む、多くのプラットフォームをサポート
- ▶ iOS や Android で動作する多様なモバイルデバイスのサポート
- ▶ ベンダーその他のサードパーティによるリモートアクセスを受け入れる用意
- ▶ ロボット、マシン、その他のインターネット接続のないデバイス等の、ネットワーク外のデバイスの修正

リモートサポートにおいては、少ないほどベター

多くのサービスデスクでは、リモートサポートに複数のツールを使い分けていますが、技術者が多様なタスクでツールを切り替える際にそれが妨げとなる場合があります。一部のツールは、限られたシステムまたはプラットフォームの組み合わせのみサポートし、高度な統合機能はありません。こうした例では、統合時の課題を危惧するテクノロジーやアプリケーション、管理上の負担の増大、サイバーリスクやコンプライアンスの侵害の増大などの要因で、サポートツール・エコシステムが実際にイノベーションを抑制し、より良いシステムへのアップグレードや、新しいエンタープライズ向け技術の導入から組織を遠ざける可能性があります。

簡単に言うと、組織は、サービスデスク全体での使い勝手を向上させながら、広範な使用用途のリストをカバーできるリモートサポートソリューションを必要としています。

2 リモートサポートの 定義

リモートサポートソフトウェアを使用すると、インターネット接続を介して、1 台のコンピューターから別のコンピューターまたはデバイスの画面にリモートでアクセスして表示できます。

リモートサポート用のソフトウェアは、1 台のコンピューターからインターネット接続で別のコンピューターその他のデバイスにリモートでアクセスして画面を表示することができ、特にサポート用途の機能を提供できます。これらのツールは、SaaS かライセンス形態でのソフトウェア、そして物理アプライアンスか仮想アプライアンスとして導入できます。

リモートサポートソリューションを用いることで、IT サポートスペシャリストは、Web にアクセスできる大半のコンピューターやモバイルデバイスからリモートでシステムを制御できるようになり、PC ベースおよび Mac ベースのデスクトップ、モバイルデバイス、さらにサーバーや POS システムなど、その他のネットワーク資産のサポート業務が可能になります。

リモートサポートソリューションは、サポート技術者のアクセスに、サポート対象のマシンにクライアントソフトウェアを事前にインストールする必要がある場合と、ない場合があります。また、接続の確立に仮想プライベートネットワーク (VPN) やオープンポートを使用する必要もありません。

有人及び無人セッション

リモートサポートは、対象のマシン側が有人または無人のいずれかの場合でのセッションでも提供できます。最も一般的な方法である有人セッションは、サービスを受けるユーザー（社内または社外）にリアルタイムでヘルプが提供されるサポートセッションです。無人リモートサポートセッションとは、サポート技術者がデバイスまたはシステムに接続する際、サポート対象のデバイスまたはシステムの側に別の人間がいる必要がないセッションを指します。無人セッションは、技術者がエンドポイント（デスクトップ、サーバー、モバイルデバイスなど）のアプリケーションやシステムの状態を把握したり、1 つまたは複数のエンドポイント、アプリケーション、またはシステムの更新や保守業務の実施を支援します。

3 リモートアクセスに おけるセキュリティ

従来のリモート接続方法は、詐取された資格情報とセッションハイジャックを介して容易に悪用される可能性あり

今やリモートサポートツールはハッカーと CISO 双方にとって“レーダー”の対象になりました。

リモートアクセスツールとその経路は、エンドユーザーや企業組織の IT 環境へのバックドアとしてサイバー攻撃にますます悪用されており、企業組織はセキュリティを意識したアプローチでリモートサポート/リモートアクセスソリューションの評価する必要があります。

VPN などの従来からのリモート接続方法や無料のリモートアクセスツールなどには、きめ細かなアクセス管理制御がなく、詐取された認証情報やセッションの乗っ取りを通じて簡単に悪用される可能性があります。一般的にこれらの方法には、きめ細かな権限設定オプションがなく、ファイアウォール設定が弱体化され、リモートサポートセッションをログをとったり記録する機能がありません。

攻撃者にとっては、サービスデスク用のマシンで正当なリモートサポートツールを使用することも効果的です。たとえば、攻撃者は MSP や MSSP を含む多くの IT サービスプロバイダーの従業員用デバイスにあるリモートサポートその他のリモートアクセスツールを悪用し、ツールをバックドアとして使用して、サービスプロバイダーの顧客に第三者としての攻撃を仕掛けてきました。組織全体で一元化できる安全なリモートサポートソリューションに標準化すると、こうしたツールをブラックリストにまとめやすくなり、不正なリモートアクセスソフトウェアや shadowIT の可能性を減少できます。

Is Your Help Desk Vulnerable?

ヘルプデスクの技術者はソーシャルエンジニアリング攻撃を検知する訓練を受けていないことが多いことから、セキュリティ専門家はヘルプデスクを企業の最大のセキュリティ脆弱性と呼ぶことがよくあります。彼らは単に、訓練を受けたこと、即ちユーザーの問題を解決することを遂行することに貢献しますが、彼らヘルプデスク担当者は、頻繁にフィッシング活動のターゲットにされています。ヘルプデスク部門は通常技術者の監視を充分にできておらず（コールログの追跡、認証の変更の記録など）、ハッカーにとっては引き続きヘルプデスクのフィッシング詐欺は都合のよいターゲットです。

リモートサポートツールが組織のセキュリティ、柔軟性、信頼性、および評判にどのように影響するかを慎重に検討する必要があります。

4 貴社の理想のリモートサポートソリューションとは

リモートサポートには多様な使用形態がありますが、リモートサポート技術のユーザーは、誰が何をサポートするかに関わらず、使いやすく信頼性が高く安全なソリューションを求めます。

適切なリモートサポートソリューションによって、ユーザーは、世界中のどこであっても、任意のプラットフォームで稼働するほぼすべてのリモートデバイスにすばやくアクセスして問題を是正できます。また、内部および外部のリモートアクセスについて完全な可視性と制御、管理対象資産への安全な接続、そして完全で歪みのない監査証跡とコンプライアンス準拠を提供する必要があります。

適切なソリューションは世界中で稼働する任意のプラットフォームのほぼすべてのリモートデバイスにすばやくアクセスして問題を是正することを支援

適切なリモートサポートソリューションが結果をもたらす

- ▶ 顧客満足度と FCR（First Call Resolution、一次解決率）の向上
- ▶ インシデントの処理時間の短縮
- ▶ サポートスタッフの生産性と仕事の満足度の改善
- ▶ プロセスの合理化と既存のワークフローの改善
- ▶ ITSM や CRM など、既存の他のサービスデスクツールの価値向上
- ▶ セキュリティ課題の対応とリスクの軽減

このホワイトペーパーは詳細な情報を提供し、業務に適したリモートサポートソリューションを選択するためのガイドとして役立ちます。

5 このガイドの使い方

このガイドは、最新の技術を利用したサービスデスク環境を実現する上で不可欠と考えられる機能に焦点を当てます。

リモートサポートの選定者は、成熟して機能が豊富な製品を探す必要がありますが、正確にはどういう事でしょうか。このバイヤーズガイドでは、組織が中小企業、大企業、IT サービスのいずれかであっても、最新のサービスデスク環境を実現するために不可欠と考えられる機能に焦点を当てていきます。

リモートサポートソリューションの評価プロセス全体を通じて、下記の要件を留意してください。

▶ 総所有コスト（TCO）

導入によって、（手動プロセスを自動化に置き換える等）時間を節約でき、他の任務にリソースを割り当てができるようになりますか。

▶ 価値実現までの時間

サービスデスクのパフォーマンスを測定可能なレベルでの改善に至るまで、どのくらい早く役立ちますか。ソリューション導入の最終的な目標の達成にどのくらいかかりますか。

▶ 統合

既存の ITSM エコシステムの他の部分とどのように統合できますか。スタンドアロンまたはポイントソリューションとしてのみ機能し、限られた範囲の使用形態の範囲でのみ機能する場合は、長期的なソリューションとしては現実的ではない可能性があります。一方でソリューションに他のサービスデスクツールとの相乗効果がある場合は、既存の IT 投資を向上するのに役立ちます。

▶ 長期的展望

ソリューションベンダーはあなたと共に成長しますか、それともサービスデスクの有効化を通じて成長に向かって推進を続けますか。ベンダーは、将来の新しい使用形態に対応するために、機能を進化させ、機能の豊富さを深めるようにリソースを割り当てていますか。組織が拡大するにつれて、ソリューションの適用範囲も拡大するはずです。

最も重要な要件に対応することは、サービスデスクの強化につながります。

6 完全なリモートサポートソリューションの6つの主要コンポーネント

リモートサポートソリューションは、サービスデスク全体をより強力で、より効率的で、より効果的なものにできる必要があります

何よりもまず、リモートサポートソリューションは、サービスデスク全体をより強力で、より効率的で、より効果的なものにできる必要があります。このセクションでは、リモートサポートソリューションで検討する必要がある6つのカテゴリの主要機能について説明します。

1. 幅広いプラットフォームのサポート

こんにちのリモートサポートソリューションは、サポート技術者がプラットフォームやエンドユーザーのプラットフォームに関わらずサポートを提供できるようにする必要があります。サポート技術者が外出中の場合、モバイルデバイスを介してシームレスにサポートを提供する必要があります。サポート技術者は、ChromeなどのWebブラウザを通して速やかに接続できる必要がある場合があります。このような場合、HTML 5 ベースのコンソールの使用は特に効果的です。

プラットフォームサポートの範囲が広いほど、統一されたツールの使用でサポートを標準化し、インシデントの処理時間と技術者の生産性を向上させ、その他も含む全体の効率を向上させることができます。

サポートすべき主要プラットフォーム

- ▶ Windows
- ▶ Mac
- ▶ Linux
- ▶ Android
- ▶ iOS
- ▶ Chrome OS
- ▶ ネットワーク内外のその他デバイス、キオスク端末、マシン

ベンダーに確認したい事項

- ▶ どのプラットフォームがサポート対象か
- ▶ それらはすべて基本費用に含まれているか、それともモバイルサポートなどの追加料金が必要か
- ▶ それらにはエンドユーザー側のプラットフォームのみのサポートなのか、それともそれらプラットフォームからのサポート提供も可能か



このカテゴリの機能は、カスタマーサポート・エクスペリエンスの核であり、インシデントの解決を迅速化するのに役立ちます。

2. コラボレーション

チャットサポート、リモートカメラ共有、インテリジェントコラボレーション、その他このカテゴリの機能は、カスタマーサポート・エクスペリエンスの中心であり、インシデントの解決を迅速化します。

コラボレーションと効率化に関する上位機能

- ▶ ワークフローの合理化
 - 上位の人材へのエスカレーションパスを定義して、インテリジェントなコラボレーションを可能にし、適切な人材にリモートサポートセッションの迅速な転送
 - リモートデスクトップやサーバーに対してパッチやインストーラーを実行するために使用可能な事前にセットするスクリプトの提供
 - コマンドラインへのセキュアなアクセスを、ネットワークのトラブルシューティングや、システム診断またはネットワークデバイスのサポートでのコマンドの記録をセキュリティと監査のために提供
 - VPN トンネリングやファイアウォール設定変更を必要としないリモートネットワークでの安全な使用の実現
 - 顧客向けとサポート技術者の両方へのアンケートの管理
- ▶ マルチプラットフォームのサポートとチャット
 - 貴社のウェブサイトからのサポート技術者の効率的なサポート提供
 - Android および MacOS モバイルデバイスの画面共有
 - リモートカメラ共有を使用による、ハードウェアや周辺機器など、ユーザーが目視できる事の共有
 - チャットやその他のリモートサポートツール
 - AR(拡張現実)機能を提供し、技術者はユーザーが見ているものをリアルタイムで正確に把握でき、ライブストリームを介して注釈を付けることを実現
- ▶ スケーラビリティ
 - サポート部門が数百、数千のシステムへの無人アクセスを管理できるようにする
 - サポートスタッフ側と無人エンドポイント双方の展開用インストーラパッケージの生成
- ▶ 高度な機能
 - Intel vPro テクノロジーを利用したリモート PC の電源のオン/オフ、BIOS の再起動、リモートコンピューターの再イメージ化、およびリモートデスクトップへのアクセスにより、OS のより下層のトラブルシューティングを実現
 - ユーザーとのリモートセッションの中断や、画面共有セッションを必要としない Windows PC のリモートレジストリエディターへのアクセス
 - プロセスの強制終了、サービスの開始、停止、一時停止、再開、再起動をリモートで実行や、リモート PC またはモバイルデバイス上のプログラムのアンインストール

3.連携と統合

トラブルシューティングとエンドユーザーのリクエストをより効率的に管理のためのサービスデスクやサポートセンターのソリューションにすでに投資しているかもしれません。リモートサポートソフトウェアは、環境にシームレスに適合してこその他のソリューションとの相乗効果を引き出します。

主要な ITSM、CRM、およびシステム管理ソリューションとすぐに連携して使用できるリモートサポートソリューションは、管理の負担を軽減します。

強力なリモートサポートと ITSM 統合で、サービスをより効率的に提供し、運用の負担を減らし、プロセス、ワークフロー、そしてサービスエクスペリエンスを管理できます。

シームレスなインシデントの解決と管理プロセスのために、サポート技術者は、サポートチケットまたは変更記録から直接リモートサポートセッションを起動し、サポートセッションの詳細でチケットを自動的に更新し、チャットの記録とセッションの記録をチケットに追加する必要があります。これには、リモートサポートツールをインシデントおよびケース管理システムと統合する必要があります。

相互運用性が高く、リモートサポートとサービスデスクの他の部分との統合が強いほど、サービスデスクの技術者とその顧客の両方のエクスペリエンスが向上します。

リモートサポートとサービスデスクの他の部分との統合が強ければ強いほど、サービスデスクの技術者と顧客の両方のエクスペリエンスが向上します。

リモートサポートとサービスデスクの他の部分との統合が強ければ強いほど、サービスデスクの技術者と顧客の両方のエクスペリエンスが向上します。

ITSM 連携のための主要な機能

- ▶ ITSM、CRM、ServiceNow、Cherwell Software、Remedy、Salesforce などの主要なシステム管理ソリューションとのプリセットされた設定オプション
- ▶ LDAP、Active Directory、RADIUS、SAML などの外部ディレクトリとの連携で、既存の管理プロセスを使用したユーザー、グループ、MFA 認証、および権限を管理し、シングルサインオン (SSO) のサポート
- ▶ カスタム連携機能と堅牢な API
- ▶ ITSM ツールからの直接チャットやリモートサポートセッションを開始する機能
- ▶ チャットからリモートサポートセッションへのワンクリックでの昇格
- ▶ 完了時のセッション後調査を含むリモートサポートセッションの詳細を追記するインシデントレコードの自動入力
- ▶ 着信リモートサポート要求にたいして手の空いている技術者への自動割当て

ベンダーに確認したい事項

- ▶ 連携関連の機能はどのくらいの頻度で更新されるか
- ▶ 連携のための設定は簡単か
- ▶ カスタム連携のための API は提供されているか
- ▶ 新しいユーザーと資産の登録の自動化に役立つ API があり、統合環境にアクセスして容易に設定可能か
- ▶ サポートされている機能の詳細は何か



4.セキュリティ、監査、コンプライアンス

リモートでの作業が増えるにつれ、pcAnywhere、RDP、VNCなどのポイントツーポイントのリモートアクセスツールや無料のセキュアとは言えないアクセスツールに関するデータ侵害の数も増えています。これらのツールの限られた使用用途では、安全で効率的範囲を超えて拡大することが多く、特にセキュリティ機能（またはその欠如）は危険信号です。これらのツールの問題は多種多様です。最も差し迫った欠点は、リモートアクセスセッションの可視性の欠如と、アクセスに最小権限の原則を適用できないことです。

サービスデスクの技術者は、サポートの問題を解決するために、昇格された管理者権限の資格情報を使用する必要があることがよくあります。特権アカウントの資格情報は一般的にハッカーのターゲットになりますが、資格情報管理の本来のベストプラクティスは、トラブルを迅速に解決するために犠牲になりがちです。実際、多くのサービスデスクチームは資格情報を共有し、プレーンテキストで保存しています。資格情報管理のベストプラクティスを常に実施しながら、ITシステムへの迅速なアクセスに必要な資格情報と認証を、サポート技術者に提供できることが不可欠です。

今日の脅威環境と規制により、企業は、リモートアクセスアクティビティに関わる誰が、何を、どこで、いつかを特定し、記録できることが求められています。これらは、エンタープライズクラスの最高のリモートサポートツールだけが対応できる質問です。しかし、エンタープライズツールの中でも、セキュリティの成熟度と機能の完全性に実質的な違いがある場合があります。

堅牢で統合された「パスワード金庫」を有効にすると、IT サービスデスクによる特権資格情報の使用を安全に保存、共有、追跡可能

PCI、HIPAA、ISO、GDPR、NIST、CJIS、FFIEC、またはその他の厳しい規準の対象であるかどうかにかかわらず、適切なソリューションは、詳細な認証レポートを簡単に作成してコンプライアンスを証明するのに役立ちます。これらの対策をサポートするセキュリティ機能には、高度な暗号化、最小権限の適用、機密データ（PII など）へのアクセスのきめ細かい制御、監査ログ、およびすべてのセッションの記録が含まれます。

セキュリティ、監査、コンプライアンス関連の上位機能

セキュリティに関しては、サービスデスクは非常に脆弱な場合があります。リモートアクセスツールとその経路は、サイバー攻撃でエンドユーザーと顧客環境へのバックドアとしてますます利用されています。検討中のリモートサポートツールは、これらのリスクを軽減する必要があります。

▶ 安全なアーキテクチャ

- すべてのセッション接続での SSL の使用など堅牢な暗号化を実施し。理想的には、TLSv1.2 を使用した転送中のすべてのデータを暗号化し、必要に応じて暗号スイートを構成（有効化、無効化、並べ替えなど）可能にする
- SSL 証明書を使用が可能
- VPN トンネリングなしでファイアウォールを越えた操作が可能で、ネットワーク境界セキュリティを変更なしで使用
- TCP ポート 443 のアウトバウンドのみのセッショントラフィックを使用（ポートの露出を最小限に抑えることで潜在的に存在する攻撃面を削減）
- シングルテナント環境に各リモートサポート顧客をセグメント化して、データが他の顧客データとの混同を回避

▶ 監査証拠とレポート

- 全セッションのログと、顧客とサポート技術者間のアクセス許可、チャットの記録、システム情報、および技術者が行ったその他のアクションが含むやり取りの監査とレビュー

- 完全なセッションログを改ざん不可能な形式で最大 90 日間保存
- 画面共有セッションを通したエンドポイント画面に表示されるユーザーインターフェイスのセッションビデオを記録し、メタデータを含めて、どの時点でもマウスとキーボードを制御しているユーザーを特定可能
- ▶ 認証と許可
 - 有人および無人のリモートサポートに関する多様なポリシーの定義と適用
 - LDAP などの外部ディレクトリとのシームレスな連携による安全な認証
 - ネイティブな二要素認証か既存のソリューションとの二要素認証連携
 - ローカルスマートカードまたは Common Access Card (CAC) の資格情報をリモートコンピュータに送信
 - パスワード保管庫との連携で、IT サービスデスクによる特権資格情報を安全に保存、共有、使用の追跡

リモートアクセスツールと経路はサイバー攻撃によってますます利用されており、検討中のリモートサポートツールはこのリスクを軽減するはずです。

資格情報保管庫の役割

理想的なパスワード管理ソリューションは、盗まれた資格情報とパスワードに関連するサービスデスクの脅威を軽減しながら、サービスデスクのワークフローにシームレスに適合できるものです。

追求すべき主な機能は次のとおり：

- ▶ リモートサポート用の資格情報を検出して登録
- ▶ プレーンテキストのパスワードをマスクして、エンドユーザーや顧客に対してマスク
- ▶ 資格情報の定期ローテーション
- ▶ アクセスが必要なシステム、アプリケーションなどに資格情報を自動で入力
- ▶ アクセスが必要で、認証が満たされている場合、安全な保管庫からパスワードをチェックアウトし、セッションの期限が切れると、パスワードを保管庫に返却（チェックイン）
- ▶ 最小権限ときめ細かいアクセス許可の適用で、必要なユーザーに適切なレベルのアクセス権を正確に付与



ベンダーに確認したい事項

- ▶ 二要素認証に追加費用が発生するか
- ▶ 保存データは暗号化されるか
- ▶ クラウドサービスでのデータ保存時に暗号化されるか
- ▶ 改ざん防止監査ログはあるか
- ▶ ソリューションは FIPS またはその他のセキュリティ認定を受けているか
- ▶ サービスデスクで一般的に使用される特権アカウントの使用を追跡可能か

ブランドと個別にカスタマイズされたサポートサービスがエンドユーザーからの信頼感の醸成に寄与

5.ブランディングとカスタマイズ

サポート対象のお客様は、自分のデバイスへのリモート接続の許可について心配になる事もあります。サポートを提供する部門や組織の積極的なブランド認知の強化によって信頼を育む重要な方法の一つは、ユーザーのサポートエクスペリエンスをブランド化できるようにカスタマイズすることです。リモートサポートソリューションは理想的には、サポート対象の顧客、グループ、製品ごとなどでカスタムポータルを作成できることが望まれます。

ブランディングとカスタマイズに関する上位機能

- ▶ ログ等の設定機能を使用したポータルのブランド化
- ▶ サポートの招待メールのカスタマイズ
- ▶ 透かしの使用
- ▶ 公開サイト、契約とメッセージ、顧客クライアント、事後調査を含む複数のカスタマイズ要素
- ▶ Active Directory からのサポート技術者の写真のインポートによるパーソナライズ



ベンダーに確認したい事項

- ▶ サポートリクエストをどのようにウェブに誘導できるか
- ▶ 複数の顧客企業をサポートする場合、顧客ごとにユーザーエクスペリエンスを設定可能か
- ▶ サポート契約とメッセージはカスタマイズ可能か
- ▶ チャットウィンドウのカスタマイズ可否

導入とライセンスオプションは多様な選択ができ、貴社のニーズに沿ったものを選べるべき

6.柔軟な導入オプション

貴社の要望と要件に最適な導入オプションとライセンスオプションが提供されるソリューションを探します。導入オプションは一般的にクラウドサブスクリプションに加えて、物理および仮想アプライアンスが選択できます。一部のベンダーは単一のオプションのみしか提供しない場合もあれば、いくつかのオプションを提供している場合もあります。ただし、同じベンダーでも多様な展開シナリオ間で提供されている機能が異なる場合があるため、選択する展開モデルに期待する機能が含まれていることを確認してください。

さらに、もし連邦政府機関やその他特別に厳格なセキュリティと規制のニーズがある組織で使用する場合は、連邦情報処理標準出版物（FIPS）の検証に適合しているソリューションを検討してください。

考慮すべき導入オプション

- ▶ 物理又は仮想アプライアンス
- ▶ ホステッドクラウド / SaaS
- ▶ AWS、Azure、VMWare ESXi、Microsoft Hyper-V を含む自社環境内の IaaS



ベンダーに確認したい事項

- ▶ セットアップの容易性
- ▶ ファイアウォールを設定変更の必要性の有無
- ▶ サポートされている仮想プラットフォーム
- ▶ 導入モデル間での機能の差異
- ▶ クラウドベースのサービスの有無とシングル・マルチテナンシーの区分
- ▶ 要件変更時のある展開方法から他の展開方法への移行可否

一種のサポートツールに統合することは時間とコストの節約につながる

1つのサポートソリューションに統合するメリット

リモートサポートを安全に提供するための包括的な統合アプローチを提供するベンダーを選定する必要があります。

使用する製品を一つにすることで、重複するコストを排除できます。複数のツールのインストール、保守、トラブルシューティング、または管理に費やしてきた時間の多くをインシデント解決に使えるようになります。

統合することのメリット

- ▶ サポートツールの実装の直接的なコスト削減
- ▶ スタッフの生産的に使うべき時間の節約
- ▶ オンサイトでのサポート訪問の減少
- ▶ ツールの種類の増加とセキュリティリスクの低減
- ▶ 監査とレポートの簡素化

7

BeyondTrust
Remote Support

BeyondTrust Remote Support は、サービスデスク全体をよりよく運営できるように構築されています。BeyondTrust のソリューションは、選択可能な範囲で最も堅牢なリモートアクセスセキュリティを実装した、最も広範なリモートサポートの使用シナリオをカバーしています。実際に、BeyondTrust は、FIPS 140-2 レベル 2 の厳しい要件を満たす唯一のリモートサポートソリューションを備えています。ローカルネットワーク内、インターネットなどあらゆる場所に接続して、多様なプラットフォームの多様なデバイスをサポートすると同時に、主なサービスデスク統合システムと強力な相乗効果を発揮します。

効率を高めながら既存の IT 投資を最大化するには、BeyondTrust Remote Support が貴社にとって最適な選択肢です。また、BeyondTrust のリモートサポートソリューションは、業界最高の契約更新率を誇っています。



エンタープライズ組織が世界のどこからでも、あらゆる
デバイスやシステムに安全にアクセスしてサポートするための、
#1 のソリューション

8

付録:
Remote Support
選定チェックリスト

コラボレーションと効率性	BeyondTrust	A 社	B 社
チャット	✓		
インテリジェントなコラボレーション (定義されたエスカレーションパス、 リクエストルーティング)	✓		
iPhone、iPad、Android の画面共有	✓		
既定のスクリプト	✓		
数百または数千のシステムにアクセスするための スケーラブルなリモートサポート	✓		
リモートカメラ共有	✓		
埋め込みチャットとアプリのサポート	✓		
コマンドラインセッション	✓		
OS の状態に関係なく、Intel vPro テクノロジー を利用してリモートデスクトップにアクセスする ことで、OS より下層のトラブルシューティング	✓		
拡張現実	✓		
リモートレジストリエディター	✓		
セッション後の調査	✓		

付録:
Remote Support
選定チェックリスト

サポートされているプラットフォーム	BeyondTrust	A 社	B 社
Windows	✓		
Mac	✓		
Linux	✓		
Android	✓		
iOS	✓		
Chrome OS	✓		
ネットワーク上、またはネットワーク外のリモートコンピューターやデバイスへのアクセスと制御	✓		

付録:
Remote Support
選定チェックリスト

ITSM 統合	BeyondTrust	A 社	B 社
ITSM ソリューション用の事前設定された統合	✓		
LDAP、Active Directory、RADIUS、SAML、SSO などの外部ディレクトリとの事前設定された統合	✓		
カスタム統合機能と堅牢な API	✓		
ITSM ツールからの直接チャットまたはサポートセッションの開始	✓		
チャットから完全なリモートサポートセッションまでワンクリックで昇格	✓		
インシデントレコードへのリモートサポートセッションの詳細の自動入力	✓		

付録:
Remote Support
選定チェックリスト

セキュリティ、監査、コンプライアンス	Beyond Trust	A 社	B 社
ファイアウォールを介して (VPN トンネリングなしで) 動作することで、ネットワーク境界セキュリティを変更せずに維持	✓		
TCP ポート 443 経由のアウトバウンドのみのセッショントラフィック	✓		
シングルテナント環境を介して各リモートサポート顧客をセグメント化	✓		
有人および無人のリモートサポートセッションに対して異なるポリシーを定義および適用する機能の提供	✓		
堅牢で詳細な権限を適用した、技術者、顧客、およびリモートシステムの相互作用の定義	✓		
管理者がローカルスマートカードまたは共通アクセスカード (CAC) の資格情報をリモートコンピューターに渡すことの許可	✓		
LDAP などの外部ユーザーディレクトリとのシームレスな統合による、安全なユーザー認証	✓		
2 要素認証のネイティブな提供か、既存のソリューションからの 2FA 統合のサポート	✓		
検出、ローテーション、自動化されたワークフローなどの、より高度な機能を含む、特権資格情報の使用を保存、共有、追跡するためのパスワード保管庫	✓		
最小限の特権と詳細なアクセス許可を適用して、必要なユーザーに適切なレベルのアクセス権を正確に付与	✓		
必要に応じてエンドユーザーへのプロンプトを開始し、サポートを受けているユーザーによる特定の操作の承認	✓		

付録:
Remote Support
選定チェックリスト

すべてのセッション接続に SSL を使用するなど 堅牢な暗号化	✓		
すべてのセッションをログに記録し、すべての ユーザーとサポート担当者のやり取りの完全な 監査とレビューを実現。ログに記録されるセッ ションデータには、関係する担当者、お客様から 付与された権限、チャットの記録、システム情 報、および担当者が行ったその他の操作を含む	✓		
完全なセッションログを改ざんできない形式で 最大 90 日間保持	✓		
画面共有セッション全体のエンドポイント画面 の可視ユーザーインターフェイスのセッション 記録。記録には、いつでも誰がマウスとキーボ ードを制御しているかを識別するメタデータを含 める必要あり。	✓		
SSL 証明書を使用する機能	✓		

付録:
Remote Support
選定チェックリスト

ブランディングとカスタマイズ	Beyond Trust	A 社	B 社
ロゴやその他のオプションを使用したサポートサイトのブランディング	✓		
カスタマイズされたサポート招待	✓		
カスタム透かしの使用	✓		
契約とメッセージ、顧客クライアント、出口調査のカスタマイズ	✓		
技術者の写真のアップロードー手動または Active Directory から	✓		

付録:
Remote Support
選定チェックリスト

導入オプション	Beyond Trust	A 社	B 社
物理アプライアンス	✓		
仮想アプライアンス	✓		
ホステッドクラウド/SaaS	✓		
AWS、 Azure、	✓		
VMWare ESXi、 Microsoft Hyper-V	✓		

Remote Support について

BeyondTrust Remote Support の導入で、ヘルプデスクチームが単一のソリューションで、あらゆるプラットフォームのあらゆる場所にあるリモートデバイスに迅速かつ安全にアクセスして修正できます。

BeyondTrust は、組み込みこまれたセキュリティ機能に基づいたリモートでのサポートのシナリオの最大数を実現すると共に、主要なサービスデスク統合製品との強力な相乗効果を発揮します。内部および外部のリモートアクセスを完全に可視化、制御、そして管理下の資産への安全な接続を確立し、完全で改ざんできないコンプライアンスのための監査証跡を生成します。あらゆる規模の組織で、ヘルプデスクサポートを統合および標準化することで、サービスデスクの生産性、効率、セキュリティをより向上させることができます。

BeyondTrust について

BeyondTrust は、特権アクセス管理 (PAM) の世界的なリーダーであり、組織が特権全体での保護と管理を実現します。

当社の統合された製品とプラットフォームは、業界で最も先進的な PAM ソリューションを提供し、クラウド環境とハイブリッド環境全体で攻撃面を迅速に縮小できるようにします。

BeyondTrust Universal Privilege Management アプローチは、パスワード、エンドポイント、およびアクセス全体の特権使用を保護し、リスクの軽減、コンプライアンスの達成、および運用パフォーマンスの向上に必要な可視性と制御を組織にもたらしめます。当社はフォーチュン 500 の 70% を含む 20,000 人の顧客、およびグローバルパートナーネットワークから Trust(信頼)されています。

