

リモートアクセスをオンデマンドで拡張

長期的なアクセスから短期的なイベントまで、あらゆるセキュアリモートアクセスを実現

企業：某化学工業メーカー

業種：化学工業

世界的に展開をしている某化学工業メーカーでは、2つのパターンのリモートアクセスを並行して実行するため、Dispelを導入されました。

【パターン①】 デバッグやメンテナンスを行うベンダーやオペレーターの日常的なリモートアクセス

【パターン②】 コミッショニング、検証用に短期間で集中するイベント的なリモートアクセス

Dispelを選択した理由

- 標準化されたベンダーアクセス
- 試運転時のセキュアなアクセスの拡張性
- シンプルなオペレータアクセスと中央管理
- サードパーティのシステムインテグレータ経由のワークフローを許可

Dispelで解決した課題

リモートアクセスを行う外部のベンダーにノートPCの発送して管理を行っていたケースでは、下記のような課題が起きていました。

【拡張性】 ベンダーが増えるたびに新しい端末を購入する必要がある。

【安全性】 工場内のネットワークへ直接アクセスされる。

【監査】 ベンダー行動履歴やログが保存できない。

【分散型】 シンプルな中央管理の仕組みがない。

【管理】 発送したノートPCの管理に膨大な手間と費用が発生。

費用対効果分析

■ベンダーのリモートアクセス

- セキュアリモートアクセス費用
- 施設全体でのリモートアクセス運用費用

Dispel導入前と比較⇒3.5倍～7倍の効果

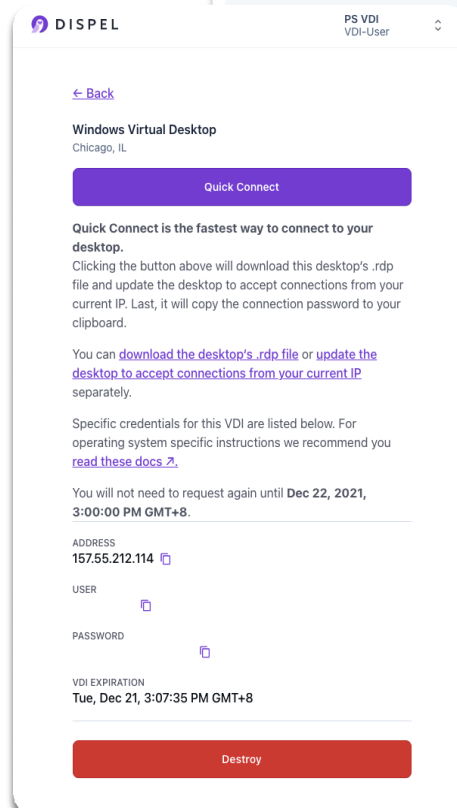
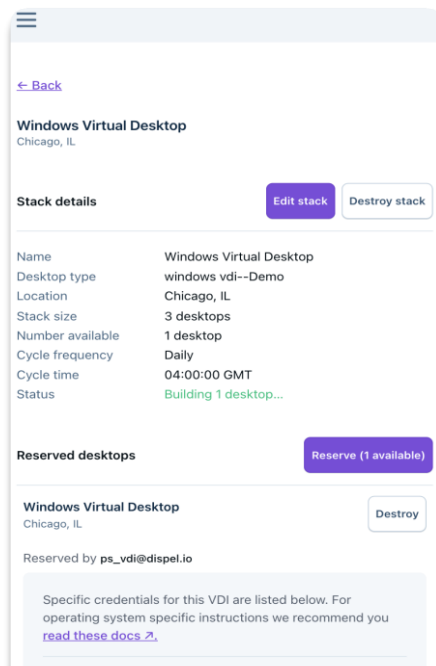
■コミッショニング・検証イベント

- 短期間で発生するセキュアリモートアクセス費用
- 50社/2週間分のセキュアリモートアクセス費用

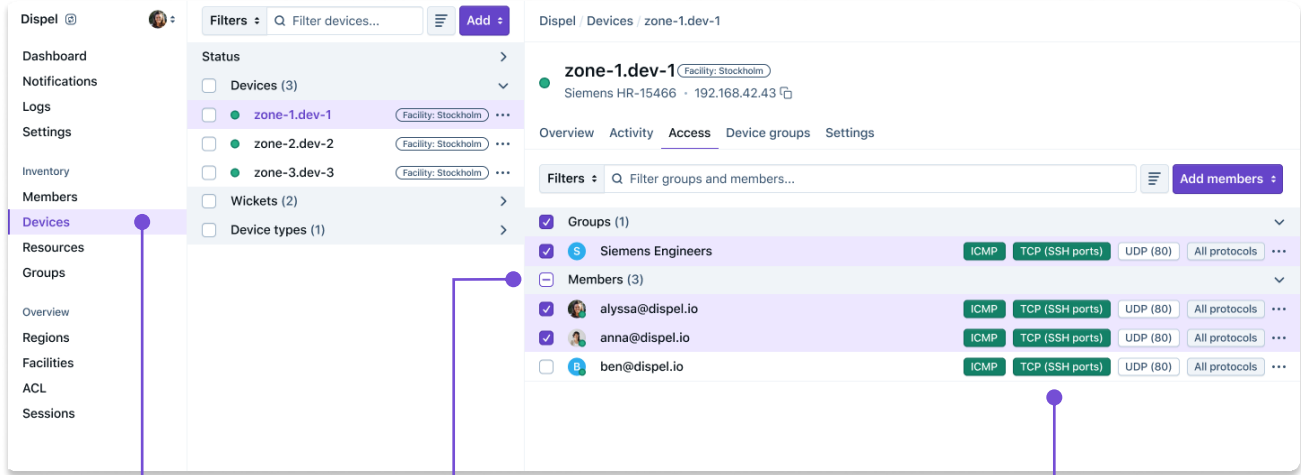
Dispel導入前と比較⇒5倍～10倍の効果

■より高い費用対効果を実現

- 在庫管理の低減
- 管理およびメンテナンス費用の節約
- 各プロセスに関連するサイバーリスクの低減
- 監査性、コンプライアンスの向上



ユーザー、端末、プロトコルレベルでアクセス制御



すべての端末の一覧をすばやく確認、端末のアクセスコントロールリストを更新するためにフィルタリングすることができます。

アクセス制御ルールを1人、または複数のユーザーに同時に適用可能な一括アクション

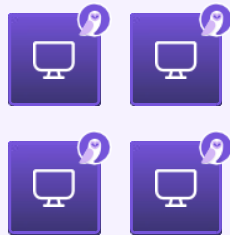
各端末の特定のポートにのみユーザーごとのアクセスを許可することで、最小特権を維持することができます

オンデマンドでスケーラブルなセキュアソリューション

Dispelは、長期的なアクセスから短期的なイベントまで、あらゆるリモートアクセス、プロジェクトに対応する費用対効果の高いスケーラブルなオプションを提供します。

短期間のイベントであれば数十人、数百人の契約社員で対応し、プロジェクト終了後は規模を縮小することも可能です。

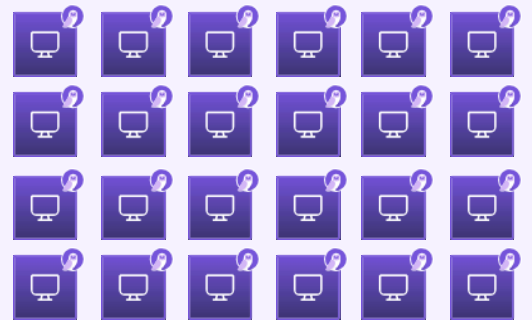
通常のリモートアクセス



Standard Facility
Virtual Desktop Stack



短期間で集中するイベント的なリモートアクセス



Built on-demand, scalable capacity,
without full-year commitments

Dispelの導入効果

ナレッジを伝達する録画セッション

このケースでは、録画セッション機能を使用することで、トラブルシューティングや技術関連でのベンダー依存を低減することができました。また、これらの録画は、新入社員の研修資料としても活用されています。

企業ネットワークとSCADAネットワークに対応

企業ネットワークとSCADAネットワークの両方にDispelを導入することで、あらゆるネットワークへのアクセスセッションを一元的に可視化し、グローバルなベンダーアクセスを一元的に管理することが可能になりました。

ユーザー階層ごとのカスタム仮想デスクトップイメージ

このケースでは、ベンダー用と社内メンバー用の2つのカスタム仮想デスクトップイメージを設定しました。これらのイメージには、お客様のセキュリティポリシーに準拠したカスタムGPOが設定されています。