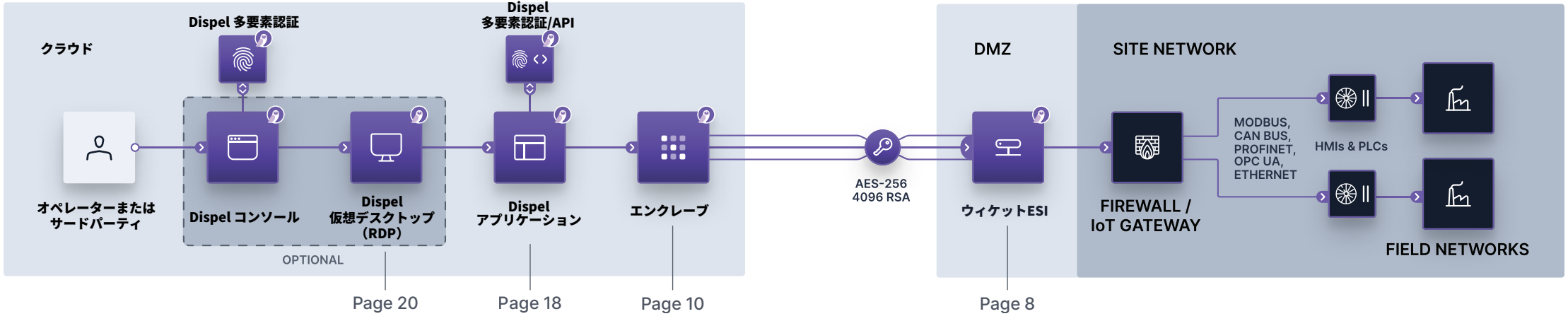
# 産業用制御システム（ICS）向け リモートアクセス

DISPEL.io


クラウド
Dispel 多要素認証
Dispel
多要素認証/API
オペレーターまたは
サードパーティ
Dispel コンソール
Dispel
仮想デスクトップ
(RDP)
OPTIONAL
Dispel
アプリケーション
エンクレーブ
AES-256
4096 RSA
DMZ
ウィケットESI
SITE NETWORK
FIREWALL /
IoT GATEWAY
MODBUS,
CAN BUS,
PROFINET,
OPC UA,
ETHERNET
HMIs & PLCs
FIELD NETWORKS
Page 20
Page 18
Page 10
Page 8

# 目次



## 本書について

**本書の目的は2つあります。（1）Dispel社のリモートアクセスプラットフォームの様々なコンポーネントを技術に深い理解を与えること、そして（2）導入計画の段階で、お客様がネットワーク要件、クラウドへの影響、および接続プロセスについて十分な理解を得られるようにすることです。**

– Dispel

# 各コンポーネント

# ウィケットESI

## ウィケットESIとは？

ウィケットESIは、既存の産業用制御システムにソフトウェアをインストールすることなく、チームがリモートで産業用制御システムに接続できるようにするオンプレミスのコンポーネントです。

## ハードウェアとソフトウェアのどちらですか？

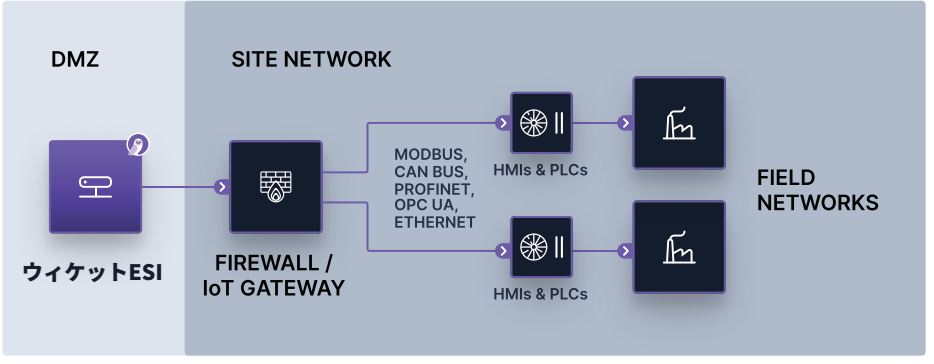
ウィケットESIは、ハードウェアまたは、仮想アプライアンスとして提供されます。OSはUbuntuを使用しています。

## 何をするものですか？

(1)エンクレーブへの暗号化接続を確立します。（P.10）
(2)内部のホワイトリストで許可されている産業用制御系のデバイスへの接続を有効化します。

## 自動化されていますか？

はい、自動化されています。Wicket ESIは、エンクレーブへの暗号化接続を（再）確立するために主体的に通信を試みます。Wicket ESIを並列で配置することで、冗長性をもたせることもできます。




FIREWALL RULES

```
OUTBOUND 1194  [ENCRYPTED TUNNEL TO ENCLAVE]
OUTBOUND 443   [HTTPS - FOR CREDENTIAL MANAGEMENT]
OUTBOUND 22    [SSH - INSTALLATION/REMOTE SUPPORT]
```

# Dispelエンジン

## Dispelエンジンとは？

Dispelエンジンはエンクレーブや仮想マシン、その他の仮想コンポーネントを構築します。エンジンには3つの部品があります。(1)ビルドAPI、(2)コンソール、(3)アイデンティティ・コントローラーです。

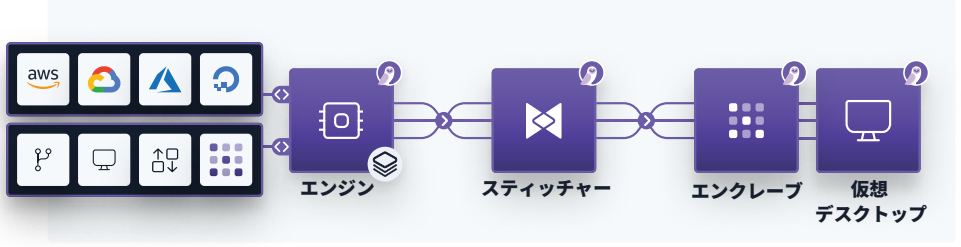
## エンジンはどこに配置されますか？

Dispelは、お客様の敷地内にハードウェアデバイスとして、またはパブリッククラウドやプライベートクラウドにホスティングされた仮想アプライアンスとして、エンジンを展開することができます。

**ビルドAPI**：クラウドプロバイダーからVMをリースし、ビルドスクリプトやアップデートを適用し、ネットワークの構築とメンテナンスを監督します。

**コンソール**：システムを管理し、ユーザーのアクセスを制御するためのウェブインターフェースです。

**アイデンティティ・コントローラー**：ユーザーの認証情報を検証する機能です。LDAPやActive Directoryとの連携機能も含まれます。




| | | | |
|---|---|---|---|
| FIREWALL RULES | BI-DIRECTIONAL | 443 | [CLOUD APIS & USERS] |
| | OUTBOUND | 22 | [APPLY BUILD SCRIPTS TO VMS] |
| | INBOUND | 22 | [INTRA-ENGINE COMMUNICATION] |

# エンジンのクラウド環境への導入

## クラウドへの導入

エンジンは、Dispelのクラウド環境、またはお客様のクラウド環境のいずれかに導入することができます。後者の場合は、別途エンジンライセンスが必要です。

## 仮想マシンのハードウェア要件

仮想マシンのハードウェア要件は、同時構築の要件によって異なります。標準的な展開では、8 vCPU、32 GB RAM、500 GB以上のSSDディスクを推奨します。

| クラウドへの導入メリット | |
|---|---|
| 短時間での導入 | ✓ |
| シングルテナントオプション | ✓ |
| 暗号化キーの制御 | ✓ |
| 堅牢なSLAオプション | ✓ |
| 迅速な障害復旧 | ✓ |
| 世界150のデータセンターに設置 | ✓ |



# エンジンのオンプレミス環境への導入

## オンプレミスでの導入

Dispel エンジンはオンプレミスでの導入も可能です。このオプションは、オンプレミスのリソースをお持ちで、現在クラウドへの移行を希望されていないお客様に適しています。

## 仮想マシンのハードウェア要件

標準的な展開では、4つのvCPU、16GBのRAM、250GB以上のSSDディスクスペースを備えたマルチサーバー（3サーバー）構成を推奨します。

| オンプレミスへの導入メリット | |
|---|---|
| シングルテナント | ✓ |
| オンプレミスの暗号化キー | ✓ |
| 迅速な障害復旧 | ✓ |
| レギュレーションの対応 | ✓ |
| 既存のセキュリティフレームワークに統合 | ✓ |

# エンジンのハイブリッド環境への導入

## ハイブリッド環境の詳細

ユーザーがコンソールにアクセスするためには、コンソールはすべての HTTPS トラフィックを受信できなければなりません。

攻撃対象をできるだけ小さくしたい場合は、Build APIとIdentity Controllerを自社内に配置し、Consoleをパブリッククラウドに配置することをお勧めします。

この構成では、オンプレミスのエンジン・コンポーネントは単一の接続を受信するだけになります。

| ハイブリッド環境への導入メリット | |
|---|---|
| シングルテナント | ✓ |
| オンプレミスの暗号化キー | ✓ |
| ファイヤーウォールルールのコロケーション | ✓ |
| レギュレーションの対応 | ✓ |
| 堅牢なSLAオプション | ✓ |

# セッション録画

## セッション録画

ユーザーが仮想デスクトップ上で何をしているのか、何をしたのかを正確に把握することができます。

## ストレージオプション

セッション録画のデータはエンクレーブ内のクラウドサーバに保存したり、オンプレミス環境にて長期保存したりすることができます。

**セッション録画に必要なディスク容量**
（ユーザー数）×（日数）×（~2.4GB）

| | 30日 | 60日 | 120日 |
|---|---|---|---|
| 10ユーザー | 720GB | 1.44TB | 2.88TB |
| 50ユーザー | 3.6TB | 7.2TB | 14.4TB |
| 100ユーザー | 7.2TB | 14.4TB | 28.8TB |
| 200ユーザー | 14.4TB | 28.8TB | 57.6TB |

**セッション録画とライブビューの特長**

| | | | |
|---|---|---|---|
| 仮想デスクトップユーザーの操作ををすべて録画 | ✓ | 接続にセッション録画を必須設定 | ✓ |
| 効率的なRDP専用ストレージ | ✓ | 可変速再生 | ✓ |
| バックアップの設定 | ✓ | ライブストリーミング | ✓ |
| 機能の上書き不可を設定 | ✓ | アイドルタイムを素早く判別 | ✓ |
| 冗長化オプション | ✓ | わかりやすい管理画面 | ✓ |

Scan to see a video of our session recording functionality.
https://dispel.io/remote-access-recording

# 接続までの流れ

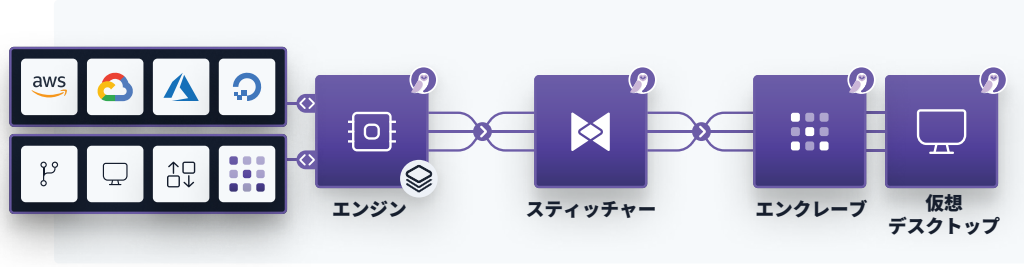
# 1 エンジンによって作成されるエンクレーブ

### 1.1: 管理者によるエンクレーブの起動

管理者は、エンクレーブの地理的な位置と構成コンポーネントを決定します。このリクエストはビルドAPI に送信され、サブコンポーネントの“スティッチャー”を起動してビルドスクリプトを適用し、エンクレーブの内部ネットワークをつなぎ合わせます。

### 1.2: 管理者によるユーザーの追加

管理者は、適切なユーザーをエンクレーブに追加します。Active Directoryと統合されている場合、ユーザーは招待フィールドに自動参照されます。Active Directory以外のユーザーの招待は、電子メールで要求されます。




Components:
[Traffic] Hub Entry Exit
[Desktop] Linux Windows Logging

# 2 ウィケットESIからエンクレーブへの接続

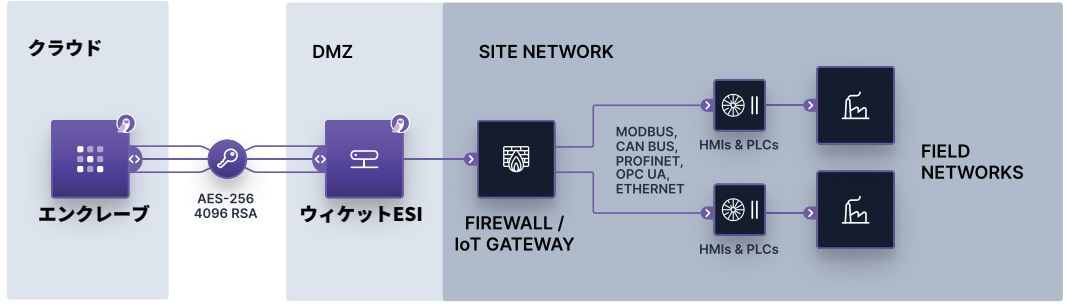
## 2.1: ウィケットESI認証

ウィケットは、割り当てられたエンクレーブの接続情報をフラグメントと呼ばれる特殊なアプレットに通信します。各フラグメントは、アイデンティティ・コントローラーによって定期的に更新されます（プッシュのみ）。

ウィケットESI は接続情報を受け取ると、エンクレーブとの認証を行うためにアクセスします。

## 2.2: ウィケットによる接続の確立

ウィケットESI は、エンクレーブのエンドツーエンド暗号化トンネルを確立し、自らをエグジットポイントとして登録します。



3a

信頼できるユーザーとデバイスによる

# ICSへのアクセス

### 3a.1: ユーザーのアプリケーションログイン

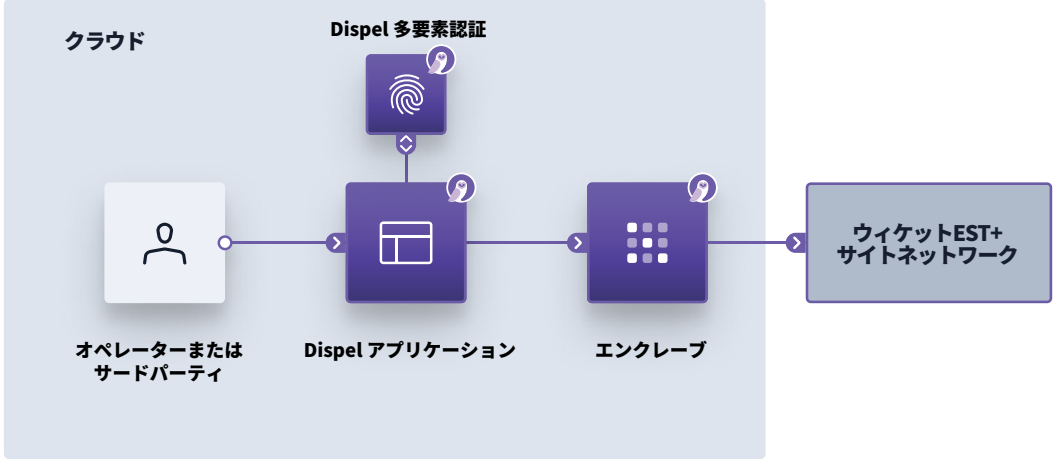
ユーザーはDispelアプリケーションにログインし、認証情報/MFAを入力します。

### 3a.2：ユーザーの ウィケット ESI 接続

ユーザーは、アクセスしたいエンクレーブを選択し、次にアクセスしたいウィケットESIを選択します。

### 3a.3: ユーザーのICSへの接続

ICSネットワークへのトンネルを利用して、ユーザーはウィケットESIによってホワイトリストに登録されたICSデバイスに、お客様のファイアウォールで許可されたプロトコルで接続することができます。
（ユーザーは適切なPurdue Model Layers 3 & 4を選択）



# 3b 標準的なICSへの接続

### 3b.1: ユーザーのコンソールへのログイン

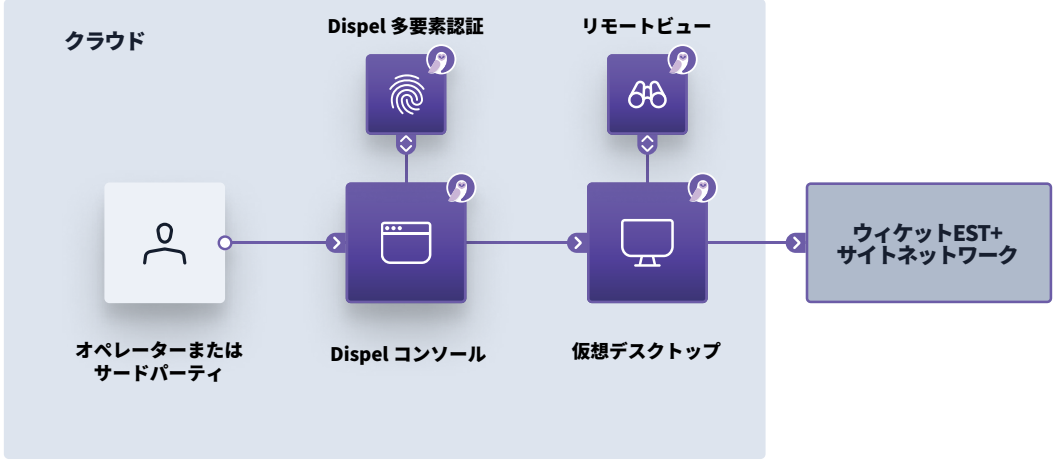
ユーザーは、電子メール、パスワード、多要素認証トークンを使ってDispelコンソールにログインします。

### 3b.2: ユーザーが接続先のウィケットESIを選択

ユーザーは、アクセスを許可されたウィケットESIのみを表示するリストから、接続する必要のあるウィケットESIを選択します。

### 3b.3: ユーザーによるICSへの接続

ユーザーには、RDP接続可能な仮想デスクトップが表示されます。
仮想デスクトップからは、ウィケットESIにアクセス許可されているICSデバイスにアクセスできます。
ユーザーの操作はすべて録画され、必要であれば、管理者にライブストリーミングされます。



# 3c 信頼されていないデバイスからの接続

### 3c.1: ユーザーのアプリケーションログイン

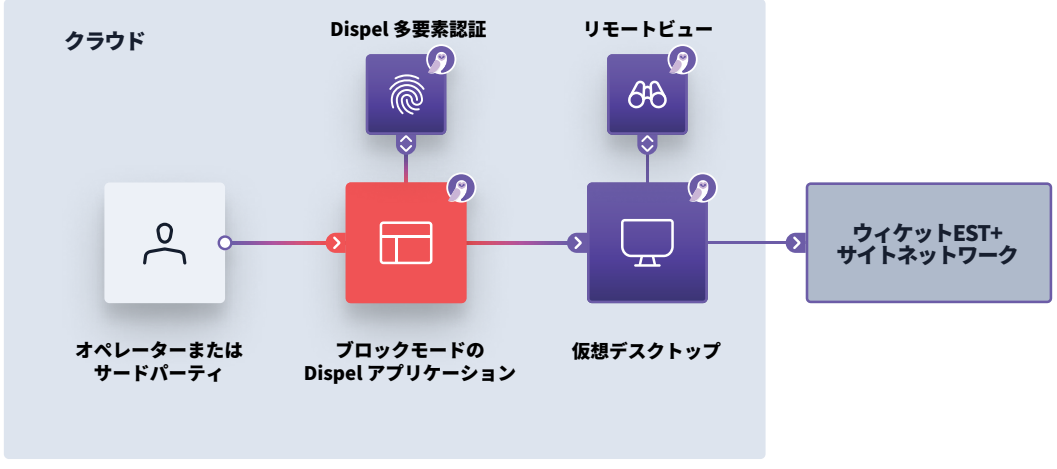
ユーザーはDispelアプリケーションにログインし、認証情報/MFAを入力します。ICSに接続されている間、遠隔地のハッカーが信頼されていないデバイスにアクセスするのを防ぐため、アプリケーションは、接続されているエンクレーブからのトラフィック以外のすべてのインバウンドトラフィックをブロックします。

### 3c.2: ユーザーが接続先のウィケットESIを選択

ユーザーは、アクセスを許可されたウィケットESIのみを示すリストから、接続する必要のあるウィケットESIを選択します。

### 3c.3: ユーザーによるICSへの接続

ユーザーには、RDP接続可能な仮想デスクトップが表示されます。
仮想デスクトップからは、ウィケットESIにアクセス許可されているICSデバイスにアクセスできます。
ユーザーの操作はすべて録画され、必要であれば、管理者にライブストリーミングされます。



# 導入メリット

# 主要なメリット

| 主要なメリット | | | |
|---|---|---|---|
| シンプル、セキュアなログイン | ✓ | セッション録画 | ✓ |
| 高速て安定したインストール | ✓ | 強固なエンドツーエンド暗号化 | ✓ |
| Moving Target Defence | ✓ | 多要素認証 | ✓ |
| ネットワークレベルのアクセスコントロール | ✓ | 運用、メンテナンスコストの削減 | ✓ |
| あらゆるクラウドプラットフォームに対応 | ✓ | わかりやすい権限とスケジュール管理 | ✓ |



# ケーススタディ

ConnecticutWater

## プロジェクト概要

Dispel社は、CT Water社と契約し、同社のICS（SCADA）環境へのリモートアクセスソリューションを導入しました。

## 導入効果

Dispelは現在、会社のHMIやPLCで作業するCT Water社のオペレーターにリモートアクセスを提供しています。さらに、CT Water社は従来のVPNをDispelに置き換え、Dispelの仮想デスクトップを介してベンダーやサードパーティがアクセスできるような環境を構築しています。

| CT Water社の導入メリット | |
|---|---|
| オペレーターログインを87%高速化 | ✓ |
| 980,000ドル相当のコスト削減 | ✓ |
| 10〜15倍の費用対効果 | ✓ |
| Active Directoryに統合 | ✓ |
| 完全冗長化されたシステム | ✓ |
| サードパーティによるセッション録画 | ✓ |

# 競合分析

| 競合分析 | |
|---|---|
| グローバルに展開可能 | ✓ |
| Moving Target Defence | ✓ |
| 柔軟な連携 | ✓ |
| オペレーターの迅速なログイン | ✓ |
| ポスト量子暗号 | ✓ |
| 拠点ネットワーク間の干渉ゼロ | ✓ |

## グローバルに展開可能

Dispelのエンクレーブと仮想デスクトップは、150以上のグローバルデータセンターまたは顧客が管理するプライベートクラウドに導入することができます。

## Moving Target Defense

エンクレーブとVDIは、スケジュールやオンデマンドで破壊・再構築することができ、常に変化するネットワークを構成します。この常に変化する構成によって、攻撃の足がかりを作ろうとする攻撃者を妨げることができます。攻撃の足がかりを作らせず、攻撃が到達できる可能性自体を低下させるため、どんな攻撃に対しても有効な仕組みです。

## 柔軟な連携

Dispelのシステムは、Active Directory、PAMシステム、データダイオード、その他のセキュリティ対策と素早く統合することができます。

## オペレーターの迅速なログイン

Dispelのシンプルなログイン方法はオペレーターやサードパーティに喜ばれています。多くのユーザーが慣れ親しむVPNスタイルのログインと身の回りのスマートフォンによるMFAなど、Dispelはシンプルさとスピードを犠牲にすることなく、セキュリティを提供します。

## ポスト量子暗号

エンクレーブ内のすべての接続は、初期の鍵交換に独立した4096ビットのRSA鍵を用いたカスケード暗号のAES-256-CBCの2層によって暗号化されています。

## 拠点ネットワーク間の干渉ゼロ

ウィケットESIを拠点ネットワークの外部に配置することで、Dispelのリモートアクセスソリューションはダウンタイムのリスクを生じることなく動作します。


enterprise@dispel.io | dispel.io