MOXTRA

Business Security

A MOXTRA WHITE PAPER

- 日本語訳 -

Contents

イントロダクション

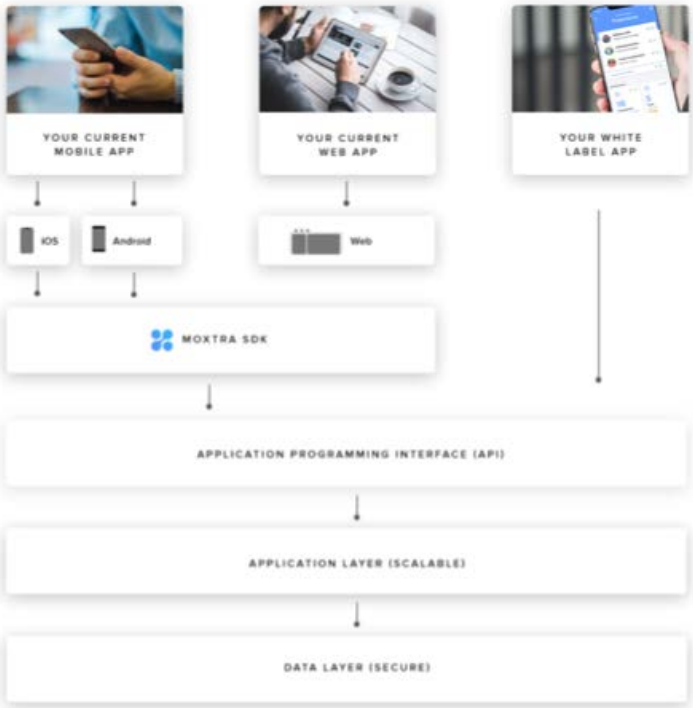
Moxtraはセキュリティと安全性について真剣に受け止め、顧客データの機密性、完全性、可用性を保護します。 私たちはセキュリティをシステムの重要な側面として認識しています。 Moxtraでは、最新のテクノロジーとセキュリティのベストプラクティスを使用して、安全なサービスを提供しています。

これを行うために、アカウント管理者が独自のポリシーをカスタマイズできる高度なインフラストラクチャを作成しました。このホワイトペーパーでは、Moxtraを安全な作業ツールにするために確立したポリシーと、管理者が利用できるオプションについて詳しく説明します。

サービス

Moxtraは、デジタルビジネスを強化するためのワンストップクライアントアプリを提供します。 企業はMoxtraを使用して会話、資料共有、会議、取引などを通じてクライアントと交流します。
Moxtraは企業に独自のホワイトラベルアプリを提供するか、完全に機能が網羅されたSDKを通じて既存アプリにサービスを埋め込むことができます。

すべてがオープンAPI形式に基づいて構築されているため、既存のツールやサービスと統合できます。 これらはすべて、Moxtraの安全なクラウドインフラストラクチャに接続します。これにより、さまざまなレベルの情報が複数のサービスレイヤーに分散され、セキュリティが強化されます。



アーキテクチャ

Moxtraのサービスは、サービスレイヤーフレームワーク上に構築された、非常にスケーラブルで効率的なバックエンドによって支えられています。 これによりシステムの冗長性、データ/ロジックの分離、および安全なデータ交換が実現します。 環境の変化に対応し、最新のベストプラクティスを反映するために、製品とアーキテクチャを継続的に進化させています。 Moxtraのデータおよびアプリケーションレイヤーアーキテクチャは、このアプローチを強調しています。

データ永続化レイヤー 永続化レイヤーは、データファームからのデータの保存と取得を処理します。

キャッシュレイヤー キャッシュレイヤーはサーバーの中心部分として機能し、データの非常に高速な読み取りと書き込みを提供し、ビジネスロジックのルールに従ってデータを処理します。

リアルタイムサービス 当社のリアルタイムサービスには、音声、公衆交換電話網（PSTN）、ビデオ、デスクトップ共有、リアルタイムチャットサービスが含まれます。当社の音声サービスは、VoIPテクノロジーとMoxtraの安全なネットワークを活用しています。 Hosted Voiceは、PBXなしでPBXのような音声機能を提供します。 つまり、ユニファイドコミュニケーション機能の完全なセットを活用することができます。

メールエンジン メールエンジンは、すべての受信メールを処理します。 電子メールを解析し、それに応じてそれぞれのバインダーにデータを投稿します。

検索ファーム 検索ファームは、高速で正確な検索結果を提供する責任があります。

ネットワークセキュリティ

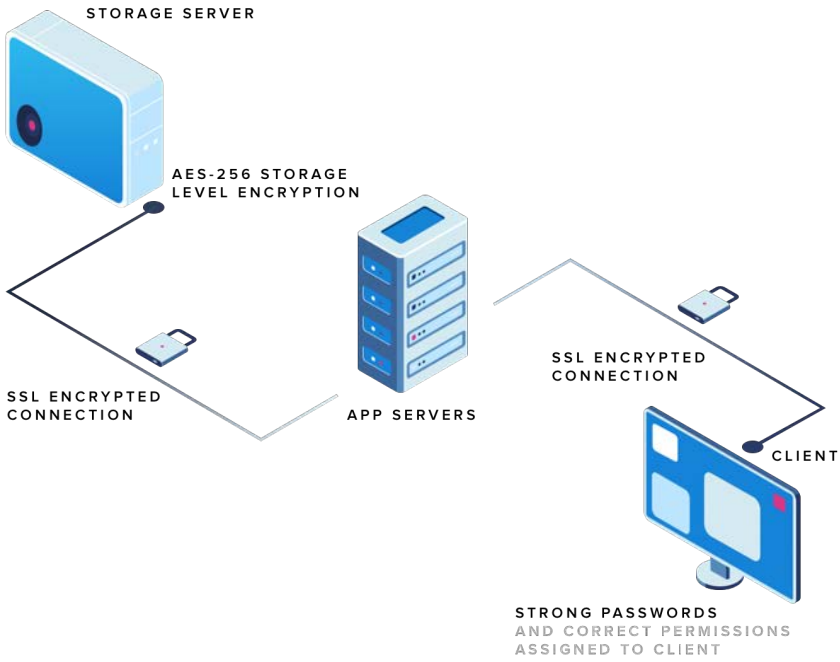
Moxtraは、バックエンドネットワークのセキュリティを維持します。 Moxtraは、専用の内部セキュリティチームとサードパーティのセキュリティスペシャリストによる定期的なアプリケーション、ネットワーク、およびその他のセキュリティテストと監査により、リスクを特定して軽減します。これらのテストは潜在的なセキュリティの脆弱性とバグを特定してパッチを適用できること、すべての通信がTLSやHTTPSなどの適切な証明書に基づいています。

Moxtraの内部プライベートネットワークは、使用状況とリスクレベルに応じてセグメント化されています。主なネットワークは、インターネットに面したDMZ、VPNフロントエンドDMZ、本番ネットワーク、企業ネットワークです。

稼働環境へのアクセスは、許可されたIPアドレスのみに制限されています。アクセス可能なIPアドレスは、企業ネットワークまたは承認されたMoxtra担当者に関連付けられています。承認されたIPアドレスは四半期ごとにレビューされ、安全な運用環境を確保します。 IPアドレスリストを変更するためのアクセスは、許可された個人に制限されています。

Moxtraの内部ネットワークと公衆インターネットの間には厳格な制限が維持されています。本番ネットワークとの間のすべてのインターネット行きのトラフィックは、専用のプロキシサービスを介して慎重に制御され、それらは制限的なファイアウォールルールによって保護されます。

Moxtraは、業界のセキュリティアラートを常にチェックしており、業界のセキュリティ標準およびガイドライン（OWASP）に従い、他の業界グループおよびセキュリティリサーチコミュニティを活用して、アプリケーションの安全を確保します。



データセキュリティ

Moxtraで交換されるすべてのデータは、最高のセキュリティプロトコルとエンドツーエンドの暗号化によって保護されています。つまり、企業は、Moxtraで共有されるすべてのメッセージ、ファイル、会議、その他の情報が非公開で安全であることを確信できます。以下では、この約束を果たすために実行する手順について詳しく説明します。

転送中のデータ

Moxtraは転送中のデータを保護するために、データ転送にSecure Sockets Layer（SSL）/ Transport Layer Security（TLS）を使用して、128ビット以上のAdvanced Encryption Standard（AES）暗号化によって保護された安全なトンネルを作成します。 Moxtraクライアント（現在はデスクトップ、モバイル、API、またはWeb）とホストされているサービスの間で転送されるデータは、常にSSL / TLSを介して暗号化されます。私たちが制御するエンドポイント（デスクトップおよびモバイル）と最新のブラウザーでは、強力な暗号を使用し、完全転送秘密をサポートしています。個々のセッションは、ログイン時に作成された一意のトークンを使用して、トランザクションごとに識別および再検証されます。

保存されたデータ

Moxtraは、Amazon S3を使用してサービスをホストします。これは、Amazon S3が提供する保管データのセキュリティの概要です。AmazonS3サーバー側暗号化（SSE）は、Amazon S3に保管されているデータを暗号化するために使用されます。 Amazon S3サーバー側暗号化は、強力な多要素暗号化を採用しています。各オブジェクトは一意のキーで暗号化されます。追加の安全策として、このキー自体は定期的にローテーションされるマスターキーで暗号化されます。 Amazon S3サーバー側暗号化は、利用可能な最も強力なブロック暗号の1つである256ビットAdvanced Encryption Standard（AES-256）を使用してデータを暗号化します。

信頼性

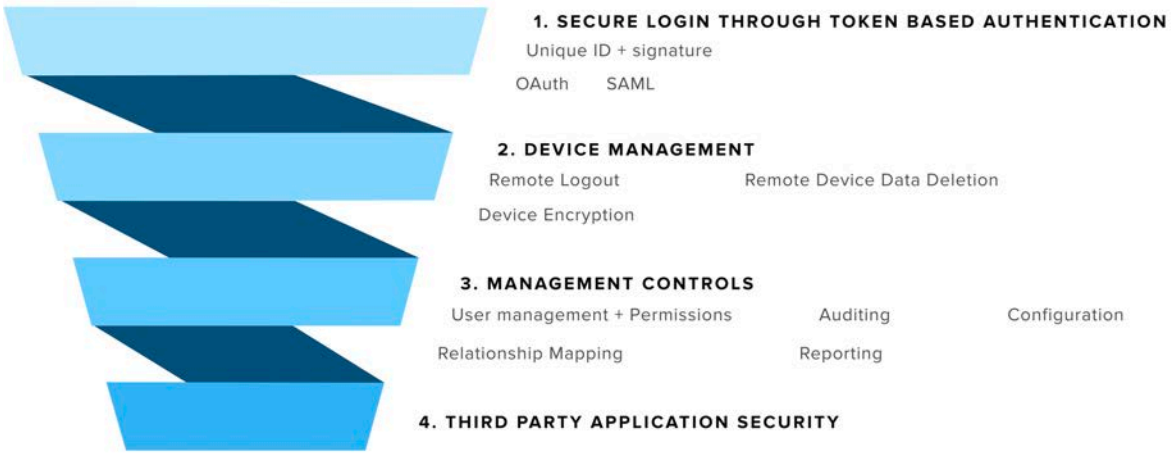
コミュニケーションとコラボレーションのシステムは、信頼性が高いほど優れています。そのために、データの損失を防ぎ、可用性を確保するために、多層の冗長性を持つMoxtraを開発しました。 メタデータの冗長コピーは、N + 2可用性モデルのデータセンター内の独立したデバイスに分散されます。 すべてのメタデータに対して、1時間ごとの増分バックアップと毎日の完全バックアップが実行されます。

この機能は、ユーザーデータの保護を超えて、Moxtraサービスの高可用性を提供します。 Moxtraのサービスへの接続が失敗した場合、接続が再確立されると、クライアントまたはフロントエンドサーバーは正常に動作を再開します。 複数のサーバー間での負荷分散により、冗長性と一貫した通信エクスペリエンスがエンドユーザーに保証されます。

アクセス制御

Moxtraのサービスへのアクセスは4レベルのセキュリティコントロールによって保護されており、適切な人だけが適切なシステムから適切なデータにいつでもアクセスできるようになっています。

コンテンツをMoxtraに追加する前に、ユーザーは次の4つの安全な方法のいずれかを使用してMoxtraアカウントにログインする必要があります。



トークンベースの認証による安全なログイン

ユーザー名とパスワード Moxtraのすべてのパスワードは一方向ハッシュ（SHA256）を使用して保存され、クリアチャネルを介して交換されることはありません。

一意のID +署名 この方法は、アプリケーションにMoxtraへのシングルサインオン（SSO）を許可し、Moxtra SDKおよびAPIを使用する簡単な方法を提供します。このオプションを使用すると、アプリケーションまたはバックエンドは、一意のID（ユーザーごとに一意の文字列）+署名（MoxtraクライアントID、クライアントシークレット、および現在のタイムスタンプを使用して生成されたエンコード文字列）を使用してユーザーをMoxtraにSSOします。

OAuth Moxtraは、承認のための業界標準プロトコルであるOAuthを使用して、ユーザーがアカウント認証情報を公開することなく、アプリにアカウントアクセスを許可できるようにします。

すべてのAPIリクエストを認証するためにOAuth 2.0をサポートしています。

SAML 2.0 セキュリティアサーションマークアップ言語（SAML）は、当事者間で認証および承認データを交換するためのXMLベースのオープンスタンダードです。Moxtraは、SAML（セキュリティアサーションマークアップ言語）2.0プロトコルを使用したフェデレーション認証をサポートし、さまざまなIDプロバイダーおよびクラウドSSOプロバイダーとの統合を簡単に可能にします。

これにより、組織はIDプロバイダーと信頼関係にあるMoxtraの間で安全に認証および承認できます。

端末管理

セキュリティレイヤーの更なる強化のために、デバイス上のすべてのデータは暗号化され、各ユーザーはWebページ上で操作することで、すべてのデバイスからログアウトできます。また管理ユーザーは、ユーザーを非アクティブ化し、非アクティブ化されたユーザーをすべてのデバイスからログアウトさせることもできます。ユーザーがログアウトすると、すべてのユーザーデータがデバイスから消去されます。

3rd アプリケーションによるセキュリティ

Moxtraと統合するサードパーティのアプリケーションは、ユーザーからの承認を必要とし、Moxtraとサードパーティのアプリケーション間の通信は、HTTPS接続を使用してポート443経由で行われます。

管理者の制御

Moxtraは、企業がユーザーがアクセスできる機能とデータを制御できる管理ポータルを提供します。また、プラットフォーム上のすべてのアクティビティを完全に把握できます。コントロールの完全なリストを以下に示します。

ユーザー管理 ユーザーアカウントの追加、編集、無効化、削除

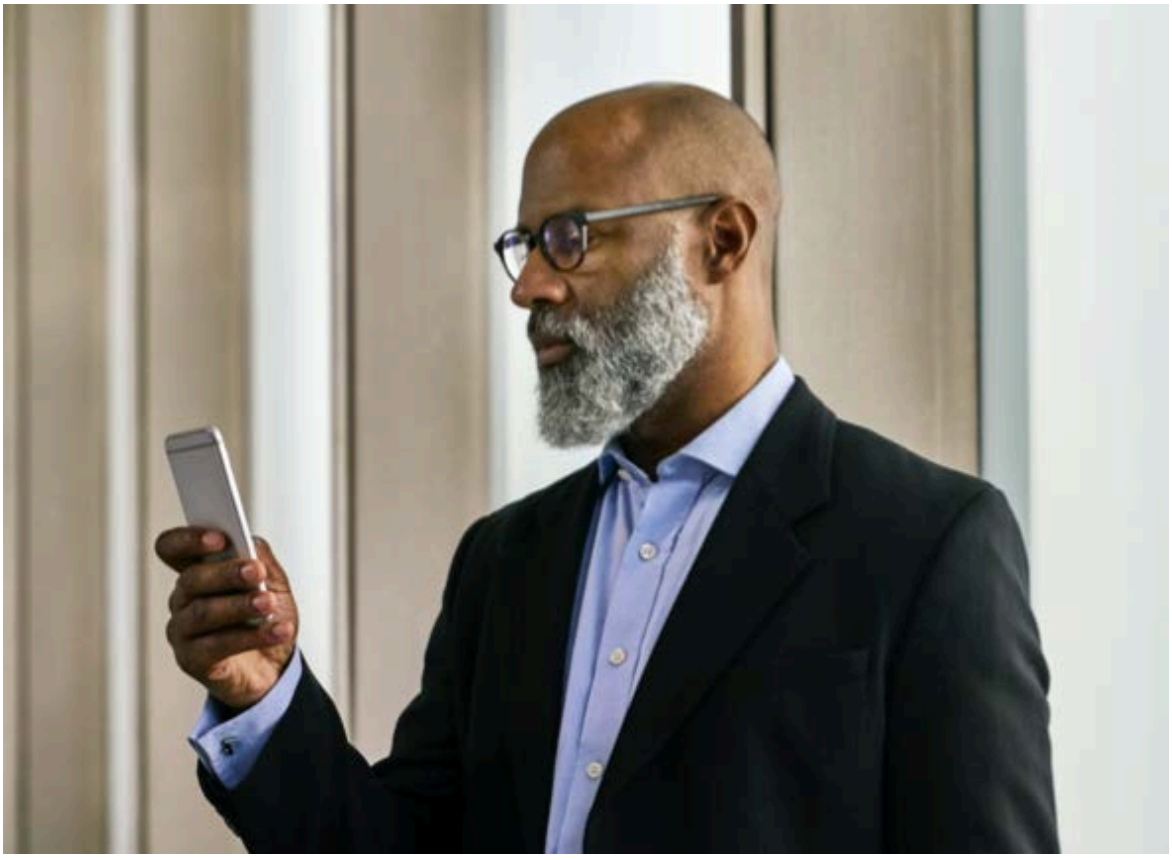
ユーザー権限 プラットフォームのすべての機能をユーザーごとにオン/オフが可能

関係マッピング プラットフォーム上の誰と通信できるかを制御可能

報告 プラットフォームの使用とエンゲージメントの監視

監査 すべてのメッセージ、ファイル、会議、アクティビティが追跡され、タイムスタンプが付けられ、検索可能

構成 さまざまなビジネスで機能をオン/オフが可能



情報セキュリティ

Moxtraは、情報セキュリティフレームワークを確立し、セキュリティポリシーを定期的に確認および更新し、セキュリティトレーニングを提供し、アプリケーションとネットワークのセキュリティテストを実行し、セキュリティポリシーの遵守を監視し、内部および外部のリスク評価を実施しています。これらのポリシーは、少なくとも年に1度レビューおよび承認され、すべての従業員、インターン、および請負業者には、必要に応じて追加のトレーニングを受ける更新が通知されます。

ポリシー

情報セキュリティ デバイスセキュリティ、認証要件、データとシステムのセキュリティ、従業員によるリソースの使用ガイドライン、潜在的な問題の処理などの主要な領域を含む、ユーザーとMoxtra情報に関するポリシー

物理的セキュリティ Moxtraで人と財産の安全な環境を維持する方法（下記の「物理的セキュリティ」セクションを参照）

インシデント対応 評価、通信、および調査手順を含む、潜在的なセキュリティインシデントへの対応に関する当社の要件

論理アクセス 企業および本番環境へのアクセス制御をカバーするMoxtraシステム、ユーザー情報、およびMoxtra情報を保護するためのポリシー

物理生産アクセス 人員の管理レビューおよび解雇された人員の許可解除を含む、物理的な生産ネットワークへのアクセスを制限するための当社の手順

変更管理 承認された開発者による、アプリケーションのソースコード、システム構成、および製品リリースへのセキュリティに影響を与える変更のコードレビューおよび管理のポリシー

サポート アカウントの表示、サポートの提供、またはアクションの実行に関するサポートチームのユーザーメタデータアクセスポリシー

従業員のアクセス

Moxtra環境への従業員のアクセスは中央ディレクトリによって維持され、強力なパスワード、パスフレーズで保護されたSSHキー、およびOTPトークンの組み合わせを使用して認証されます。リモートアクセスの場合、2要素認証を使用したVPNの使用が必要であり、特別なアクセスはすべてセキュリティチームによってレビューおよび検査されます。

従業員のオンボーディングおよびオフボーディングポリシーには、バックグラウンドチェック、セキュリティポリシーの確認、セキュリティポリシーの更新の伝達、および機密保持契約が必要です。従業員が会社を辞めたとき、すべての従業員のアクセスは即座に削除されます。

プライバシー

ユーザーのプライバシーとビジネスデータのプライバシーを保護することは私たちが真剣に取り組んでいることなので、不正アクセスからユーザー情報を保護するために努力しています。

Moxtraは、技術的なアクセス制御と内部ポリシーを使用して、従業員がユーザーファイルに任意にアクセスすることを禁止し、ユーザーのアカウントに関するメタデータやその他の情報へのアクセスを制限しています。エンドユーザーのプライバシーとセキュリティを保護するために、Moxtraのコアサービスの開発を担当する少数のエンジニアだけが、ユーザーデータが保存されている環境にアクセスできます。

ネットワーク間のアクセスは、最小限の従業員とサービスに厳しく制限されています。たとえば、本番ネットワークへのアクセスはSSHキーベースであり、職務の一環としてアクセスを必要とするエンジニアリングチームに制限されています。ファイアウォール構成は厳しく制御され、少数の管理者に制限されています。

さらに、当社の内部ポリシーでは、SSH秘密鍵の作成と保存に関するベストプラクティスを遵守することを、本番環境と企業環境にアクセスする従業員に要求しています。

物理的アクセス

企業施設への物理的なアクセスは、承認されたMoxtra要員に制限されています。企業サーバーを含む領域へのアクセスは、許可された担当者に制限されています。企業環境および本番環境への物理的アクセスが承認された許可された個人のリストは、少なくとも四半期ごとに見直されます。

本番システムが存在する施設への物理的なアクセスは、職務を遂行するために必要な場合、Moxtraによって承認された担当者に制限されます。本番環境設備への追加のアクセスを必要とする個人は、適切な管理者による明示的な承認を通じてアクセスを許可されます。

アクセス要求、正当化、および承認の記録は管理者によって記録され、アクセスは適切な個人によって許可されます。承認を受けると、インフラストラクチャチームの責任者が適切なサブサービス組織に連絡して、承認された個人のアクセスを要求します。サブサービス組織はユーザーの情報を独自のシステムに入力し、承認されたMoxtra担当者のバッジアクセスと、可能であれば生体認証スキャンアクセスを許可します。承認された個人にアクセスが許可されたら、アクセスが許可された個人のみに制限されるようにするのは、データセンターの責任です。

変更管理

正式な変更管理ポリシーがMoxtraエンジニアリングチームによって定義され、すべてのアプリケーション変更が本番環境に実装される前に確実に承認されます。ソースコードの変更は、Moxtraのアプリケーションまたはサービスを拡張したい開発者によって開始されます。すべての変更は、自動化された品質保証（QA）テスト手順を実行して、セキュリティ要件が満たされていることを確認する必要があります。 QA手順が正常に完了すると、変更が実装されます。 QA承認済みの変更はすべて、本番環境に自動的に実装されます。コードの変更は、QAおよび手動のセキュリティコードレビュープロセスを介して、潜在的なセキュリティ問題についてスクリーニングされます。

本番環境にリリースされたすべての変更はログに記録されてアーカイブされ、アラートはMoxtraエンジニアリングチームの管理に自動的に送信されます。

Moxtraインフラストラクチャへの変更は、許可された担当者のみに制限されます。 Moxtraのセキュリティチームは、インフラストラクチャのセキュリティを維持し、サーバー、ファイアウォール、およびその他のセキュリティ関連の構成が業界標準で最新に保たれるようにする責任があります。ファイアウォールルールセットと本番サーバーにアクセスできる個人は定期的に見直されます。

サマリー

Moxtraは、企業が必要とするセキュリティを犠牲にすることなく、企業にクライアントと従業員のためのワンストップなデジタルビジネスポータルを提供する使いやすいツールを提供します。 Moxtraは、堅牢なバックエンドインフラストラクチャ、エンドツーエンドのデータセキュリティ、ネットワーク保護、アクセス制御、および一連のセキュリティポリシーを組み合わせた多層セキュリティフレームワークを採用しています。 セキュリティに対する私たちのアプローチは、GDPR、SOC II、クラウドセキュリティアライアンス、EU-USプライバシーシールドなどの主要なプライバシーおよびセキュリティ認証機関への準拠に翻訳されています。