

ZSCALERとONELOGIN、 最初にアイデンティティを入力



Zscaler用OneLoginは、企業が複数の内部ディレクトリを容易に接続し、オフィス内または外出先でシングルサインオンを利用し、多要素認証を強制することを可能にします。

ZscalerとOneLoginは、パートナーとなって、クラウドアプリケーションを使用する企業にシームレスな認証とセキュリティを提供しています。それにより、ユーザーはAD認証情報を使用してZscalerにログインすることができ、ADグループのメンバーシップはZscalerに同期されます。

インスタントオン

OneLoginは完全なクラウドベースであり、起動から実行までを数分以内に行うことが可能です。インストールするソフトウェアも、アプライアンスも、ファイアーウォールの変更もありません。

シングルサインオン

OneLoginは、ユーザーがZscalerにサインインするために、SAML 2.0を使用します。標準ベースのSAMLプロトコルは、アイデンティティプロバイダーとアプリケーションの間の信頼確立にデジタル署名を使用し、ユーザー管理のパスワードやフィッシングのリスクを排除します。また、SAMLは、ユーザーが、所属組織独自の認証ポリシーを使用して、OneLoginにより認証された後でなければアクセスできないことを必須とすることも可能です。

ONELOGIN MOBILE

多くのWebアプリケーションにはネイティブなモバイル版はなく、モバイル版は往々にして削減された機能セットしか提供しません。OneLoginはそのことをすべて変えます。そのため、ワンクリックだけでクラウドやファイアーウォールの背後にあるWebアプリにアクセスすることができます。

多要素認証

複数の認証要素は、保護の追加レイヤーをもたらします。そのため、犯罪者は単にユーザーのパスワードを推測するだけでは、データにアクセスすることはできません。OneLoginのスマートフォン用アプリ、もしくは、RSA、SafeNet、Symantec、またはVASCOの統合済みサードパーティーソリューションを使用します。

ACTIVE DIRECTORYとLDAPの統合

OneLoginのActive Directory Connectorは、数分でインストールでき、サーバーの再起動やファイアーウォールの変更は必要ありません。1つまたは複数の組織単位 (OU) を視覚的に選択し、ユーザーをActive Directoryからインポートすれば、すべて完了です。OneLoginはユーザーをリアルタイムで同期し、そのことにより、ユーザーが組織を去る場合のために、ユーザーキルスイッチをIT部門に提供します。OneLoginのAD統合は、高可用性モードで構成することができ、ドメインコントローラーごとに複数のAD Connectorを活用します。

セキュリティと可用性

OneLoginは、世界でも最も要求が厳しい、何社かの株式会社の複雑なディレクトリインフラストラクチャをサポートします。冗長型データセンター、冗長型DNS、DDoS保護、ISECパートナーによる四半期ごとのセキュリティ審査、そして、1日24時間、週7日間の監視により、安心してご利用いただけます。99.99%のアップタイムを保証します。

使用可能

