ジャストインタイム特権による Active Directoryの保護

One Identityジャストインタイム特権

攻撃者がActive Directory（AD）を狙っていることは明らかです。ADは、ほとんどの組織のほぼすべての重要なリソースのアクセスに関連および制御しています。ADが攻撃者によって侵害されると、アクセスできるあらゆるものが制御、破壊、あるいは身代金要求の対象となります。ほとんどのハッカーの目的は、できる限り中に入り込み、多くは基幹業務のユーザ資格情報を侵害することによって、管理レベルにまで権限を昇格させることです。攻撃者のコミュニティでは「DA（ドメイン管理者）を獲得しろ」というフレーズがよく使用されます。

特権アカウントの侵害は、いくつかの異なる方法で行うことができます。

特権資格情報を侵害する一般的な方法として、残存するハッシュの使用があります。このハッシュは、標準ユーザであっても、特権ユーザであっても、ユーザがシステムにログインしたときに残されるものです。特権ユーザの残存するハッシュを使用して特権を昇格させることで、最上位の管理者としてActive Directory内を移動することができます。これをどのように防ぐことができるのでしょうか?

セキュリティの強化

One Identity Active Rolesは、ADにおける広範な権限の必要性を排除するように特別に設計されており、One Identity Safeguardは、特権資格情報を保存するように設計されています。これらの連携により、Active Directoryのセキュリティと一般的なセキュリティが強化されます。

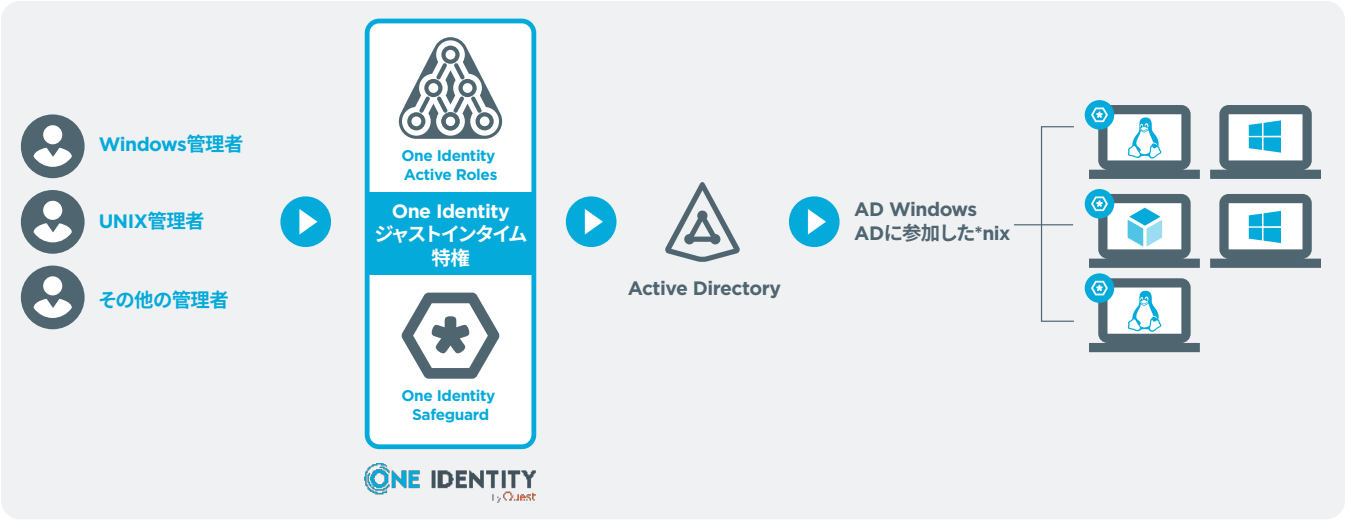
要旨

One Identityジャストインタイム特権ソリューションは、資格情報のチェックアウト時に権限を自動的に割り当て、タスクが完了すると直ちに特権アクセスを排除し、アカウントのパスワードをリセットします。

ジャストインタイム特権

One Identityジャストインタイム（JIT）特権ソリューションを使用すると、特権アカウントは必要になるまで特権を持つことができません。**One Identityジャストインタイム特権ソリューション**により、資格情報のチェックアウト時に特権を割り当てることができます。機能の実行（ドメイン管理など）のために特権が必要なADアカウントは、そのアカウントがOne Identity Safeguardでチェックアウトを承認されると適切なグループに追加されます。これは、パスワード要求とセッション要求の両方に適用されます。

この処理を行うには、**「特権の割り当て対象」**のユーザアカウントを必要に応じて適切なグループに追加し、タスクが完了して特権アクセスが不要になったときにそのアカウントを排除します。



使用できないアカウント

これはどのようなセキュリティを追加するのでしょうか。**One Identityジャストインタイム特権ソリューション**が監視しているこれらのいずれかのアカウントが、パスワードの盗難や残っている資格情報（ハッシュ）などにより侵害された場合、そのアカウントは使用できなくなります。

このようなアカウントには権限がなく、アクセス権はどこにも昇格されません。実際に、Active Directoryの他のどのユーザよりもアクセス権は少なくなります。

当社の統一IDプラットフォーム

One Identityは、あらゆる規模の企業が、統一されたIDセキュリティソリューションを使用することでそのシステムとデータを保護できるよう尽力しています。**One Identityジャストインタイム特権ソリューション**は、One Identity Active Rolesの強力なAD管理機能とOne Identity Safeguardの比類のないパスワード管理機能を組み合わせることで、特権アカウントに対するサイバー攻撃のリスクを劇的に軽減します。

GitHubで利用可能

One Identityジャストインタイム特権ソリューションには、One Identity Active Roles、One Identity Safeguard for Privilege Passwords、One Identity Safeguard Privilege Sessions、およびGitHubで利用可能なプラグインが必要です。詳細について、または利用を開始するには、One Identity GitHubリポジトリをご覧ください。

One Identityについて

当社の統一IDプラットフォームは、クラス最高のIDガバナンスと管理（IGA）、アクセス管理（AM）、特権アクセス管理（PAM）、およびActive Directoryの管理（AD Mgmt）の機能を統合し、組織がIDセキュリティに対して、断片的なアプローチから包括的なアプローチに移行できるようにします。One Identityは世界中の5,000超の組織で2億5千万を超えるIDを管理し、全世界の実績と信頼を得ています。

詳細については、www.oneidentity.com/jp-ja/をご覧ください。

ONE IDENTITY by Quest