データシート

Symantec Endpoint Threat Defense for Active Directory

Active Directory を起点とするドメイン侵害

Microsoft Active Directory は、社内リソース（サーバー、エンドポイント、アプリケーション、ユーザー）を管理するために世界中で 10 社に 9 社の割合で使用されているネットワークドメインサービスです[1]。AD（Active Directory）は、ドメインに接続しているすべてのユーザーに対してオープンな仕様です。つまり、企業ネットワーク上のすべての ID とリソースが可視化されており、そのため AD は攻撃者に最も狙われる標的となっています。

企業ドメインに接続されたエンドポイントが 1 つ侵害されるだけで、企業全体が危険にさらされてしまうのです。

- 機密データがどこに保存されているのか
- 管理者がどこにいるのか
- 標的とする環境をどうすれば所有できるのか

Microsoft Active Directory を使えばすべてがわかります。

ドメインに接続されたエンドポイントへの足掛かりをつかんだ攻撃者は、AD データベースを偵察して、すべての企業リソースを可視化します。エンドポイントにローカル保存されている、または他のリソースにリモート保存されているドメイン資格情報の窃取です。盗み出した資格情報を使用することで、攻撃者は気付かれることなく企業内のすべてのサーバー、アプリケーション、コンピュータへの完全なアクセス権を取得します。最終的な目標はデータの窃取または暗号化です。

攻撃者は、信頼されているアプリケーションと組み込みのツールを利用して侵入後の活動を行います。悪質なバイナリではなく、信頼されているアプリケーションと組み込みのプロトコルを使用することで、ステルス性の高い攻撃の検出、フォレンジック追跡、捜索はほぼ不可能になります。

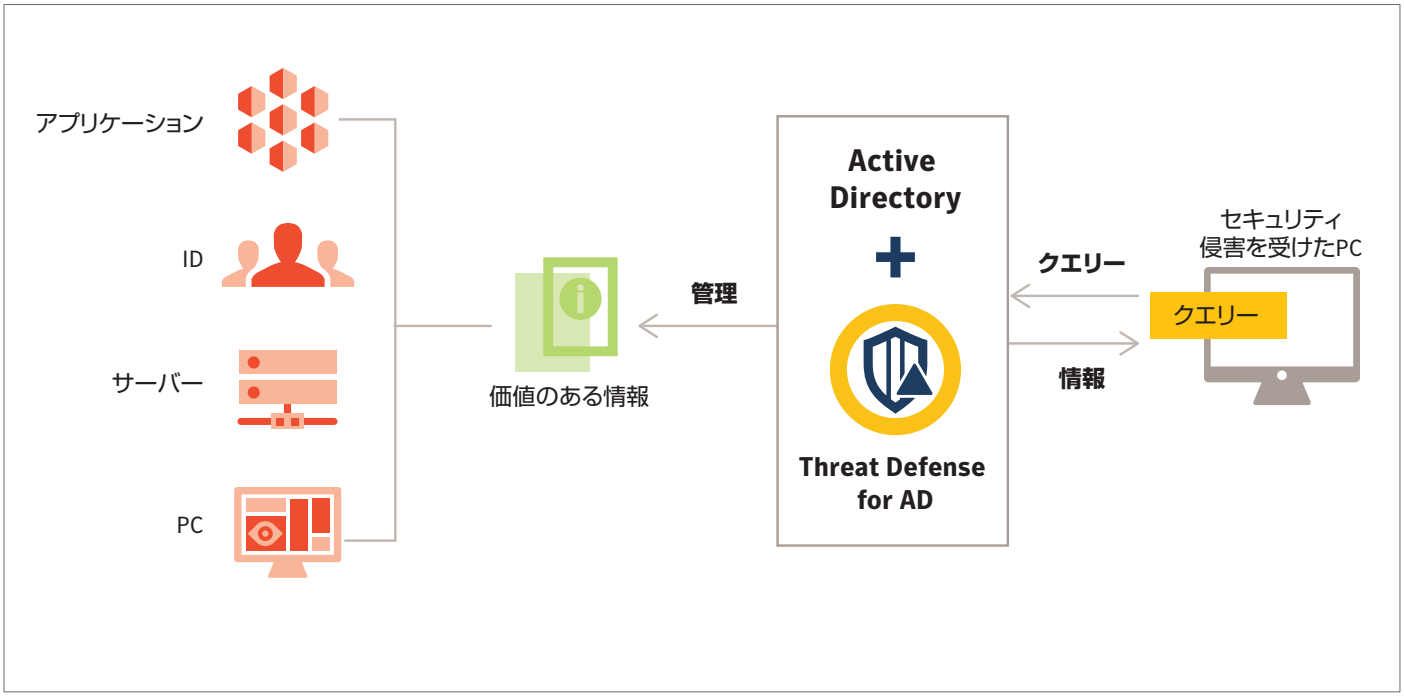
Active Directory の強化による標的型攻撃の封じ込め

Symantec Endpoint Threat Defense for Active Directory（Threat Defense for AD）は、エンドポイントから AD を効果的に防御することでステルス性の高い攻撃や標的型攻撃に対応するようにシマンテックのエンドポイントセキュリティソリューションを進化させ、自動的なセキュリティ侵害の封じ込め、インシデント対応、ドメインセキュリティ評価を実現します。

エンドポイントのセキュリティが侵害された後、攻撃者がドメインで攻撃を続ける前に直ちに封じ込める唯一のセキュリティソリューションです。偵察活動を妨げ、攻撃者が AD を利用して他の資産へと横感染するのを阻止します。Threat Defense for AD は、昨今のネットワークにおいて最も弱い攻撃対象を保護します。これにより、セキュリティ侵害の開始地点つまりエンドポイントでのセキュリティ侵害の検出と封じ込めに関連する時間、労力、エラーが大幅に削減されます。

Threat Defense for AD は、AI による自然言語処理、高度な難読化技法、高度なフォレンジック手法を適用して、セキュリティ侵害を迅速に検出し封じ込めます。

[1] 『An Overview of Active Directory（Active Directory の概要）』、Philippe Beraud 氏、Microsoft Corporation、2016 年



難読化によって Active Directory を攻撃から防御

Threat Defense for AD は、セキュリティ侵害を受けたことにより企業の内部リソース（すべてのエンドポイント、サーバー、ユーザー、アプリケーション、ローカル保存された資格情報）が攻撃者へどのように見えるかを効果的に制御します。このソリューションは、企業の AD 構造全体（サーバー、エンドポイント、アプリケーション、ユーザー、支店、命名規則、設定、属性など）を自動で学習し、そのデータに基づいて確実かつ無制限に難読化します。エンドポイントでのプロセス、コンテキスト、AD アクティビティの実行時評価により、難読化を有効にする必要性の有無を判断します。ドメインに接続しているセキュリティ侵害を受けた資産の全体像が、難読化されたかたちで攻撃者に表示されます。攻撃者は、Threat Defense for AD が見せている資産を操作したりドメイン管理者資格情報の使用を試みたりしているうちに正体を現します。この時点で、信頼性の高い警告がトリガされ、攻撃は自動的にブロックされます。

リアルタイムでのセキュリティ侵害の可視化と攻撃の自動的な封じ込め

攻撃が検出されると即座にエンドポイントから警告がトリガーされ、オンデマンドスキャンによって攻撃に関連するフォレンジック情報が収集されます。攻撃が検出された場合にだけフォレンジックプロセスの自動化と適切な情報のスキャンを行うことにより、優先度の高い正規の警告だけが表示され、警告処理の負担が軽減されます。

企業の AD ドメイン環境向けの独自のインシデント対応手法を使用するこのソリューションは、攻撃者が実行した実際の偵察、資格情報の窃取、横感染フェーズを把握するフォレンジックレポートをリアルタイムで提供します。攻撃チェーンは、攻撃元を特定するために最初に感染したコンピュータまでさかのぼって文書化され、攻撃がローカルインシデントか大規模な攻撃の一部かを評価します。自動修復によってエンドポイント上の悪質なプロセスを停止してセキュリティ侵害をリアルタイムで封じ込めることにより、さらなるプロセスの量産、メモリの別の部分の上書き、偵察コマンドの実行、ネットワーク外への通信を阻止します。

継続的な Active Directory 評価による攻撃対象領域の縮小

企業による AD の導入が拡大するにつれ、設定が適切に維持されない、セキュリティ強化が行われてない、ドメインおよび AD サービスに脆弱性が現れ始めるといった状況が発生します。攻撃者はそこを悪用してくる可能性があるのです。攻撃者はさらに、後でいつでも戻って来られるように、バックドアや永続性を維持するためのフックを残します。Threat Defense for AD は、ドメインの設定ミス、脆弱性、永続性を継続的に調べ、攻撃者の観点でのドメインを AD 管理者に提示し、すぐにリスクを緩和して攻撃対象領域を縮小できるようにします。

自動評価プロセスは攻撃シミュレーションを使用して、ドメインの設定、特権アカウント、セキュリティ設定、GPO、エンドポイント、ドメインコントローラ、Kerberos に関する詳細情報を収集します。次に、ドメインおよび AD 構造のあらゆるコンポーネントを自動的に分析して、設定ミスや攻撃者が残したバックドアの有無を調べます。これらの設定ミスやバックドアを継続的に特定し、ドメインへのリスクを削減することが重要です。設定ミスやバックドアが特定されると、修復に関する規範的な推奨事項を含む警告が中央コンソールに送信されます。

Symantec Endpoint Threat Defense for Active Directory について詳しくは、こちらをご覧ください:
http://www.go.symantec.com/threat-defense-for-ad

シマンテックについて

シマンテックコーポレーション（NASDAQ: SYMC）はサイバーセキュリティ業界をリードする世界的企業です。さまざまな場所に保管されている大切なデータを守るため、企業や政府機関、個人のお客様を支援しています。エンドポイントからクラウド、インフラまでを高度な攻撃から守るため、世界中の企業がシマンテックの戦略的統合ソリューションを選択しています。また、世界中で 5 千万以上の個人やご家庭が、自宅などで使用するデバイスそしてデジタルライフを守るために、ノートンと LifeLock 社の製品を使用しています。シマンテックのサイバーインテリジェンスネットワークは民間が運営するネットワークとしては世界最大規模を誇ります。このネットワークが、先進的な脅威をいち早く発見し、お客様を守ります。詳しくは www.symantec.com/ja/jp をご覧ください。

〒107-0052 東京都港区赤坂1-11-44 赤坂インターシティ | www.symantec.com/ja/jp

19C199995_DS_SEP_THREAT_DEFENSE_AD_JP