事例研究

KKB

KKB(トルコの信用調査会社)が情報セキュリティ部門ランキングでForeScout CounterACT®を「第一位」に評価

業種

金融

導入環境

厳重な規制環境で300名の従業員が400台のデバイスを使用

課題

- ネットワークに接続されているすべてのノートパソコンとワークステーションが、正規の社内ユーザーによって使用されることを保証する
- セキュリティコントロールを自動化し、リスクを軽減してセキュリティインシデントへの対応を促進する
- ビジネス業務の中断を避けて生産性を維持

ソリューション

- ユーザー操作を最小限に抑えた、使いやすいエージェントレスソリューション
- Arubaのワイヤレスアクセスポイントと Cisco®スイッチを使用し、非侵入型で迅速な導入によりKKBのネットワークに簡単に統合
- セキュリティ機密情報の共有と、エンドポイントの緩和・修復措置アクションの自動化を可能にする、ForeScout CounterACTプラットフォームでのFireEye®とArcSight™プラグインの統合
- 信頼性の高いネットワークセキュリティソリューション(ミラー化されたトラフィックをCounterACTに転送)

導入成果

- ネットワーク上のエンドポイントに対するリアルタイムの可視化と継続的モニタリングが可能になり、既知の脆弱性を介したサイバー攻撃の可能性が低下
- リモートワーカーのデバイスに対するローカル管理者パスワード管理を自動化し、従業員の年間労働時間を数週間短縮
- 「Pass to Hash」攻撃に対する予防的なコントロール
- 情報セキュリティバンキング規制に対するコンプライアンスの向上

概要

トルコで最初の、そして唯一の信用調査機関KKB (Kredi Kayit Burosu)は、1995年トルコの大手銀行9行によって創設されました。銀行、レンタカー、賃貸、家財を含む数多くの分野で財務リスクを削減するKKBのインターネットポータルでは100万人の会員が定期的に利用しており、2014年度は5億件の信用照会を行いました。

ビジネスにおける課題

慎重な扱いを要する金融および個人情報に関するコンプライアンスとサイバーセキュリティは、サービスプロバイダーとしてのKKBの信用に直接影響を及ぼします。このため300名の従業員と400台のエンドポイントに対して、ネットワークの完全な可視化とコントロールを提供するソリューションが必要とされていました。

ForeScoutが選ばれた理由

KKBはネットワークの可視性とセキュリティコントロールを高めるソリューションを調査すべく、情報セキュリティのコンサルティングパートナーSymturkに近づきました。SymturkはForeScout CounterACT®を推奨し、KKBの情報セキュリティ/リスク管理部門の主任アリ・クトルハン・アクタス氏に、オンサイトのPoC(概念実証)を提案しました。Cisco ISEも同時に検討されました。

評価の要件には、迅速なインストレーション、異なるテクノロジー(Arubaのワイヤレスアクセスポイントおよびシスコのスイッチ)が混在するITインフラのサポート、ビジネス業務を中断しないソリューション、自動化アクションとコンプライアンスコントロールなどが含まれました。KKBは、それぞれ製品のデータシートや導入先の評判を検討して選定を行いました。

アクタス氏は、「当社はCisco NACではなくForeScoutを選定した。Cisco製品だけでなく、異なるテクノロジーが混在するITインフラをサポートすることも理由の一つだが、インストールが迅速で簡単なソリューションを求めていた。ForeScoutは条件を満たしていた。さらに、優れた統合能力を備えたユニークなプラットフォームCounterACTの存在もある。FireEye、ArcSight、CyberArk®などの他社製セキュリティ製品との統合が簡単だったことにより、さまざまな製品による混在型のセキュリティ環境を構築して活用することで、KKB内での可視性とサイバーセキュリティ保護を向上させることができた」とコメントしています。

ビジネスへの影響

デバイスおよび脆弱性のリアルタイムの可視化

ForeScout CounterACTを導入してから、KKBはネットワーク上のエンドポイントに対してはるかに高い可視性が得られるようになり、各デバイスのセキュリティ状態を継続的に確認できるようになりました。アクタス氏は、「以前は、悪意のある活動の可能性についてネットワークでポートスキャンを実行すると、結果を知ることができるのはスキャン終了後だったが、ForeScoutの導入により、検出、確認、ブロックをすべて同時に行うことができるようになった。加えて、CounterACTはセキュリティ脆弱性が発生すると同時に警告を発し、エンドポイントに対する緩和・修復措置を自動的に行うことができ、これによりヒューマンエラーの発生確率を下げることができる」と、語っています。

「当社には、業務を中断するリスクを侵すことなく迅速に展開できるNACソリューションが必要だった。加えて、ArubaやCiscoの製品が混在するITインフラをサポートする必要もあった。ForeScout CounterACTはこれらの要件をすべて満たすだけでなく、既存のFireEyeおよびArcSightセキュリティツールとの優れた統合能力など、ほかにも多く優れた機能を提供していた。さらに、複数の自動化セキュリティチェックやコンプライアンスコントロールを最も効果的な方法で実現することから、当社ではCounterACTを当社情報セキュリティ部門の「スイス・アーミーナイフ」と呼んでいる」

ー アリ・クトルハン・アクタス氏、情報セキュリティ/リスク管理部門主任、KKB

ポリシーの作成と施行

アクタス氏は、CouterACTを使用して同社が策定したカスタムセキュリティポリシーのいくつかについて次のように説明しています:

- 「当社はForeScout、ArcSight、CyberArkを統合しており、コンピューターまたはラップトップがネットワークに接続された際に、ForeScoutソリューションによってそのデバイスのローカル管理期間が確認され、45日以上経過している場合はそのデバイスの名前を含むCEFメッセージがArcSightに送信される。ArcSightはこのメッセージをカスタムルール内で相対的に関連付け、CyberArkサーバーにインストールされているエージェント上でスクリプトを実行する。このスクリプトを使って、CyberArkでパスワード変更のプロセスが開始され、パスワードが適切に変更される。これは、特に社外のオフサイトで勤務する従業員にとって、非常に重要なセキュリティ対策となっている」
- 「当社は、ForeScout CounterACTを使用して、クライアントマシン上でドメイン管理資格情報ハッシュをチェックし、ワークステーションでドメイン管理ログイン/資格情報ハッシュを検出した場合は、そのマシンをネットワークから隔離する。これは「Pass to Hash」攻撃に対する予防的なコントロールとなる。また、ワークステーション上でローカル管理特権についてもチェックし、ヘルプデスクがスタッフに未承認のローカル管理特権を与えた場合、それを検出して当該エンドポイントを隔離する」
- 「CounterACT経由でデータ損失防止サービスをチェックし、実行されていない場合は、サービスを実行するためのコマンドを3回送信する。それでも実行されない場合、またはサービスが完全にアンインストールされている場合は、そのデバイスを隔離する。さらに、ディスク暗号化、p2pプログラム、怪しい動作やアンチウィルスによるスキャン頻度など、その他のさまざまなアイテムについてもチェックする」

人件費の削減

KKBの選定条件の一つに、自動化セキュリティコントロールの最適化による、人件費およびリスクの削減という課題がありました。アクタス氏は、「ForeScoutソリューションの導入前は、従業員の退職時などノートパソコンやワークステーションのパスワードは手動で変更する必要があり、とても時間がかかっていた。CounterACTの導入により、ForeScout、ArcSight、CyberArkをリンクするカスタムポリシーを作成することで、パスワード変更のプロセスを自動化できた。これにより資金を節約し、情報セキュリティを向上させることができた。このプロセスを積極的に自動化することで、従業員の年間労働時間を数週間程度短縮できると見積もっている」とコメントしています。

セキュリティ製品の統合

ForeScoutのControlFabric®テクノロジーにより、CounterACTとその他のITシステム間で情報を共有し、さまざまな問題に対処することが可能になりました。KKBはこれを機会ととらえ、FireEyeおよびArcSightソリューションをCounterACTに統合して最大限に活用しています。

ForeScoutとFireEyeの統合により、コンプライアンスに適合しない、またはウイルスなどに感染しているエンドポイントによる企業全体のリスクに対するリアルタイムのモニタリングおよび緩和・復旧措置が可能になりました。分散環境およびBYOD環境におけるAPT(持続的標的型攻撃)、ボットネット、伝播するマルウェアは瞬時に識別、検証、隔離されます。

ArcSight SIEM(セキュリティ情報およびイベント管理)に対するForeScoutソリューションの相互運用性により、エンドポイントのセキュリティ状態に関する詳細が提供されているため、エンドポイントに関するセキュリティリスクおよびコンプライアンス違反について、より良い、より早い、より多くの情報に基づいた意思決定を行うことができます。

ForeScoutソリューションの強み

KKBの全体的な成功に寄与した主な差別化要因:

- ControlFabricアーキテクチャを介したセキュリティ製品の統合
- マルチベンダー環境での実装の容易さ/相互運用性
- セキュリティ脅威およびサイバー攻撃に対する継続的モニタリングおよび緩和・復旧措置
- ネットワーク上のデバイスに対するリアルタイムの可視化
- セキュリティおよびコンプライアンスコントロールの自動化と、それに伴う人件費の削減

詳細については
www.ForeScout.com
をご覧ください。

ForeScout®

ForeScout Technologies, Inc.
900 E. Hamilton Avenue #300
Campbell, CA 95008 USA

米国内フリーダイヤル 1-866-377-8771
国際電話番号 +1-408-213-3191
サポート 1-708-237-6591
Fax 1-408-371-2284