

Boost Bank：セキュリティとオブザーバビリティの統合により、デジタルバンクのセキュリティとレジリエンスを向上

主な課題

マレーシア初の国産デジタルバンクとして先駆的な組み込み型バンキング機能を提供するBoost Bankでは、ハイブリッドクラウドでの高速な取引の監視、コンプライアンスの維持、監査に対応したログの記録、競争の激しい市場での信頼構築が必要になっていました。

主な成果

リアルタイムの可視化と高度な分析を取り入れて、プロアクティブなセキュリティ態勢に移行するとともにオブザーバビリティを構築して、意思決定を迅速化し、カスタマーエクスペリエンスを全体的に向上させました。



業種：金融サービス

ソリューション：プラットフォーム、オブザーバビリティ

製品：[Splunk Enterprise](#)、[Splunk Observability Cloud](#)

機能：SIEM/セキュリティ分析、統合セキュリティ運用、セキュリティインシデント対応、インフラ監視とトラブルシューティング、インシデント対応と自動化、オブザーバビリティのログ

デジタルファーストバンクにセキュリティとコンプライアンスを組み込む

Boost Bankは、最高水準のセキュリティ、レジリエンス、規制コンプライアンスを維持しながら、これまでサービスが十分に行き届かなかった地域にシームレスで包括的な金融サービスを提供するという明確な使命のもとで設立されました。

同行は当初から、信頼こそがデジタルバンキングの基盤だと認識していました。規制の厳しい環境で事業を行い、常時アクセスを求める消費者や中小企業にサービスを提供するために、ハイブリッドクラウド環境全体をリアルタイムで可視化し、脅威をプロアクティブに検出して、監査に対応した統制を確立できるテクノロジープラットフォームを必要としていました。

さらに、デジタルバンクを立ち上げるということは、従来型の金融機関を転換することとは根本的に異なります。同行は、ハイブリッドクラウド環境全体で複雑かつ高速なデジタル取引を監視すると同時に、サイバーリスクと運用リスクをリアルタイムで検出して対応する必要がありました。また、マレーシア国立銀行の「テクノロジーにおけるリスク管理(RMiT)」要件を含む厳格な規制要件を満たすとともに、設立当初から、監査に対応したログ、トレーサビリティ、運用レジリエンスを確保する必要もありました。

Boost Bankは、サービス開始後に事後対応型のツールを導入するのではなく、セキュリティ、オブザーバビリティ、レジリエンスを事前に組み込むという慎重な判断を下しました。

同行のCEOであるFozia Amanulla氏はこう述べています。「さまざまなソースのデータを統合して、ITとセキュリティの運用状況をリアルタイムで一元的に把握できる堅牢なプラットフォームが必要でした。同じように重要だったのは、利用者が増加し、エコシステムの統合が拡大したときに、組織の成長に合わせて拡張でき、規制要件にも対応できたことでした」

これらの要求を満たすためにBoost Bankがセキュリティとオブザーバビリティ戦略の基盤として選択したのが、[Splunk Enterprise](#)と[Splunk Observability Cloud](#)です。

成果

- **プロアクティブなセキュリティ管理とオブザーバビリティ**
- **自動化による効率向上**
- **包括的な可視化による意思決定の迅速化**

Splunkによる一元的なセキュリティとオブザーバビリティ

Boost Bankは、2024年に予定されていたアルファ版のリリース前にSplunk EnterpriseとSplunk Observability Cloudを導入しました。早い段階で導入したおかげで、サービスを提供する顧客層を拡大する前に、インフラのレジリエンス、セキュリティ、完全なオブザーバビリティを確保することができました。

まず、Splunk EnterpriseとSplunk Observability Cloudを組み合わせ、アプリケーション、インフラ、セキュリティシステムを横断する一元のかつイミュータブル(不変)なログ管理を実現し、ダッシュボードによってハイブリッド環境全体をフルスタックでリアルタイムに可視化できるようにしました。また、自動アノマリ検出やインテリジェントなアラートによって手動での監視を減らすとともに、高度な分析機能やドリルダウン機能を取り入れてインシデントの調査と解決にかかる時間を短縮しました。

この統合的なアプローチにより同行では、事後対応的なトラブルシューティングから脱却し、状況をプロアクティブに把握する運用へ転換することができました。

Amanulla氏はこう説明します。「Splunkを導入することで、場当たりのインシデント対応から、体系的でプロアクティブな監視へと移行できました。異常なパターンや、システムの性能低下、潜在的なリスクを、お客様に影響が及ぶ前に特定できるようになりました」



Splunkを導入したことで、セキュリティを強化し、運用のレジリエンスを向上させ、インシデントの検出と調査に対するプロアクティブなアプローチを確立できました。これらは、デジタルバンクに不可欠な基盤です。

Boost Bank、CEO、
Fozia Amanulla氏

セキュリティを強化し、対応を迅速化して、成果を向上

Boost Bankでは、Splunkを使用して、アプリケーションのパフォーマンスだけでなく、APIの動作、取引の流れ、インフラの健全性もリアルタイムで継続的に監視しています。その結果、セキュリティや運用に関するインシデントをよりすばやく検出および解決し、自動化を通じて手作業を減らして、MTTD (平均検出時間)とMTTR (平均解決時間)を短縮することにより、取引ピーク時の信頼性が向上しました。

Splunkでは、セキュリティだけでなく、トラフィックの多いサービス、ユーザーの行動、パフォーマンスのボトルネックの初期兆候など、運用についても深いインサイトを獲得できます。

規制コンプライアンスと監査への対応がBoost Bankの運用モデルの中核に

Splunkの導入により、Boost Bankでは、強力なガバナンス、透明性、アカウントビリティが確保されていることを証明できるようになりました。これは、マレーシア国立銀行のRMiTセキュリティポリシーの遵守に役立っています。

Splunkを活用することで、イミュータブル(不変)で検索可能なログを蓄積し、システムアクセス、トランザクション、イベントの明確な追跡可能性や、データ保持とアクセス制御の検証可能性を確保し、規制審査や内部保証のための監査に対応した証拠を収集することが容易になりました。

その結果、監査時だけでなく、日常業務の一環としても、強力なガバナンス、透明性、アカウントビリティを実証できるようになりました。

さらに、同行にとってセキュリティとオブザーバビリティは、単なるリスク管理ではなく、カスタマーエクスペリエンスを直接支える取り組みにもなっています。Splunkで状況を包括的に可視化することにより、顧客接点に影響を及ぼす可能性のある問題を迅速に検出して解決できます。

これは、サービスの信頼性向上、デジタルジャーニーの中断の低減、顧客の信頼と顧客維持率の向上にもつながります。Amanulla氏はこう述べています。「可視性が向上したことで、組織の最優先事項であるカスタマーエクスペリエンスが向上しました。一貫性と信頼性によって顧客の信頼が築かれるデジタルバンキングにおいて、これは極めて重要なことです」

長期的な成長を見据えた戦略的パートナーシップ

Boost Bankは、Splunkチームの対応力と専門知識を高く評価しています。Splunkによるサポートとベストプラクティスのガイダンスは、プラットフォームへの投資効果を最大化するために役立っています。同行は将来を見据えて、Splunkダッシュボードのユーザーを技術系のチームだけでなく経営幹部や上級管理層にまで拡大し、組織全体にわたってデータ主導のより迅速な意思決定を実現することを目指しています。

Splunkは引き続き、デジタルレジリエンスの確保、セキュリティ態勢の強化、不正検出や顧客に関するインサイト獲得のための高度な分析を通じて、Boost Bankのテクノロジーロードマップにおいて重要な役割を果たしていきます。

Amanulla氏はこう締めくくります。「Splunkを導入したことで、当行は先進的な組織としての地位を確立できました。Splunkが組織の成長を支え、セキュリティ基盤を強化してくれるので、進化し続ける規制や顧客の期待に自信を持って対応できるのです」

Splunkを無料でダウンロードするか、[Splunk Cloudの無料トライアル](#)をお試ください。Splunkは、クラウドかオンプレミスか、また組織の規模の大小などにかかわらず、お客様のニーズに最適な展開モデルでご利用いただけます。



お問い合わせはこちら：
https://www.splunk.com/ja_jp/talk-to-sales.html

[www.splunk.com/ja_jp
jp_marketing_splunk@cisco.com](https://www.splunk.com/ja_jp/jp_marketing_splunk@cisco.com)