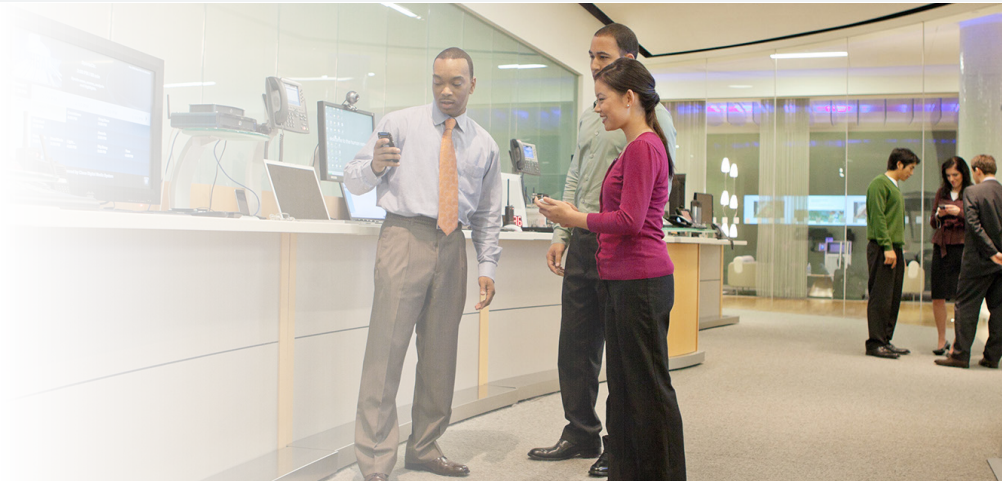
ブランド価値の保護と強化

小売業のためのリスク管理



メリット

- 小売店向けにカスタマイズされたエンドツーエンドの保護を実現
- 複数のチャネル全体で顧客データ、従業員データ、クレジット カード データを保護
- 実際の店舗、顧客、従業員、資産のセキュリティを確保
- サイバー攻撃の発生前、発生中、発生後もブランドと資産を保護
- 管理の複雑さを緩和

セキュリティは顧客ロイヤルティ獲得の第一歩

モバイル デバイス、分散型サービス、顧客からの高まる期待、仮想化システム、ビジネス目標の変化などのさまざまな要素によって、小売ブランドに脆弱性が生じてしまいます。実際、90 % を超える消費者は、買い物をする店舗に常に最先端の財務セキュリティ テクノロジーを利用することを期待しています。[1]

脆弱なセキュリティは、ブランドへのロイヤルティに深いダメージを与えるだけでなく、顧客の信頼にも深刻な悪影響を及ぼす可能性があります。

革新的な小売業者は、リスク管理を単にリスクを緩和する手段ではなく、カスタマー エクスペリエンスと収益機会の一部であると認識しています。こうした企業は、サイバーセキュリティへの備えを、コスト要因ではなく競合優位性に変える方法を見出しています。

たとえば、セキュリティ侵害が発生した小売業者に対しては、買い物客が個人情報の共有に消極的になることがあります。その結果小売業者は、買い物客が期待するような、分析に基づいて高度にパーソナライズされたエクスペリエンスを、実店舗やオンラインで提供できなくなります。すると買い物客は、安全なデータを利用してさらに優れたカスタマー エクスペリエンスを提供できる別の小売業者に乗り換えることになります。

窃盗や不正行為の防止

商品逸失は、あらゆる小売業者に影響する慢性的な根強い問題です。商品逸失の一部は顧客によるものですが、それ以外は店舗内部者によって発生しています。ビデオ監視を通じた分析手法を導入することで、両方のタイプの脅威に一次的な防御を講じることができます。顧客、従業員、資産の動きをリアルタイムで追跡するビデオを利用することで、脅威が発生しうる場所での異常を検証できます。

[1] PSFK Labs/MasterCard

「私たちの最大のサイバーセキュリティ侵害の懸念は、財務への直接的な影響よりも、評判にどのような影響が及ぶかということです。お客様が当社は信頼に値しないと判断し、離れてしまったらどうなるのでしょうか」

— Stein Mart CFO
Greg Kleffner 氏

物理的資産と情報（データ）資産の保護

アクセス制御を通じて価値の高い領域へのアクセスを制限することで、物理的な脅威からの資産保護に役立てることができます。しかし、さらに大きな脅威が m（モバイル）-コマース、e-コマース、店舗での支払といったデジタル要素から発生しており、物理施設への侵入者による脅威の割合は減少しています。たとえば、英国の小売業者は、2013 年にハッカーによって 8 億 5000 万ドル以上の損失が発生したことを報告しています。[2]エンドツーエンドのセキュリティ アーキテクチャを導入すると、物理的侵害と仮想的侵害の両方を緩和し、ブランドの信頼性低下に関わるコストも削減できます。

法規制とプロセスへのコンプライアンスを容易に達成

コンプライアンス リスクが高い産業である小売業に属する企業は、競合優位性を確立して成功を収めるために、内部および外部のコンプライアンス リスクを把握するための戦略を立てる必要があります。たとえば、決済カード業界（PCI）は、コンプライアンス違反のリスクをなくして最前線でデータを保護することを小売業者に求めています。シスコのソリューションとサービスを利用すると、ネットワークをセグメント化するアプローチを通じて容易に PCI コンプライアンスを達成できます。

シスコの小売業のためのリスク管理は、柔軟性に優れており、機能の構成も可能なため、既存のソリューションを排除することなく即座にメリットを享受できます。また、すべての買い物客、従業員、チャネル、アプリケーションが、データとビジネスを保護する非常に安全な単一の統合プラットフォームを活用できます。

今すぐ顧客の保護を開始

エンドツーエンドのリスク管理計画の立案はシスコにお任せください。詳細については、小売業のためのリスク管理を参照してください。

[2] Intel

C45-737261-01　04/17