企業が今すぐEDRを導入しなくてはならない5つの訳

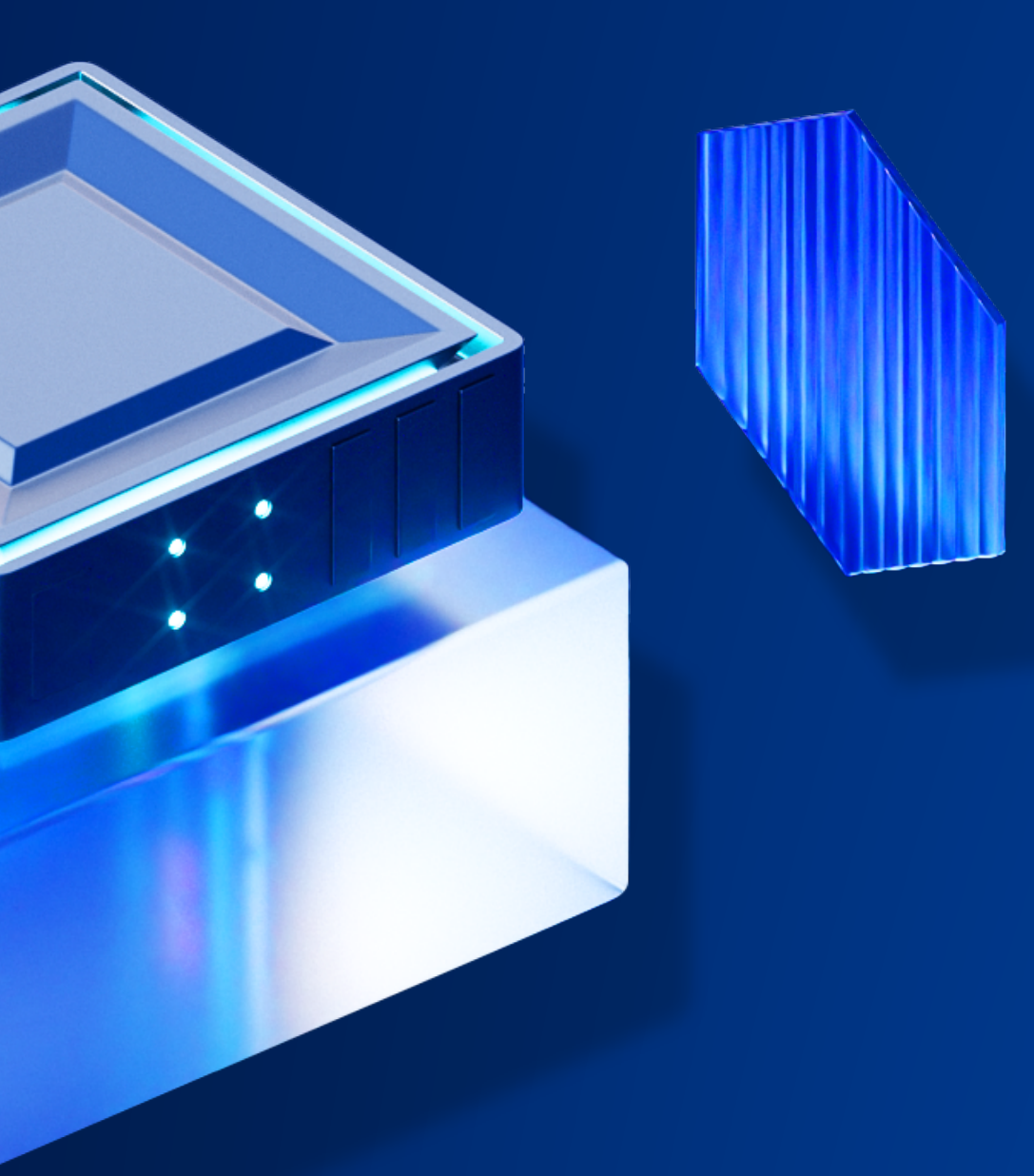
Acronis

01.

デジタルリスクの増大によって 予防第一のアプローチが 求められている

2023年、データ侵害による被害は過去最高となりその被害額は445万ドルに上りました。これは2022年から2.3%増加しています。

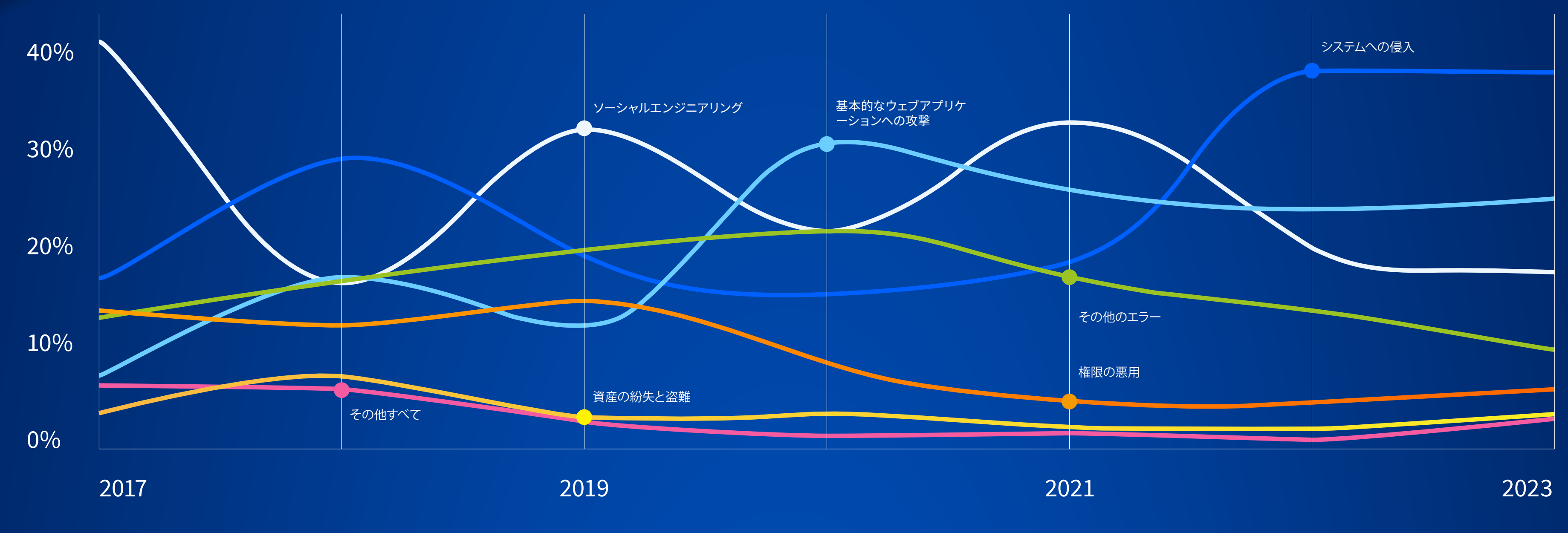
出典: 2023年データ侵害被害額レポート、Ponemon InstituteおよびIBM Security



02.

高度な攻撃に対する防御の確保

攻撃はますます巧妙になっているため、保護にはEDRのようなより高度なセキュリティコントロールが必要です。



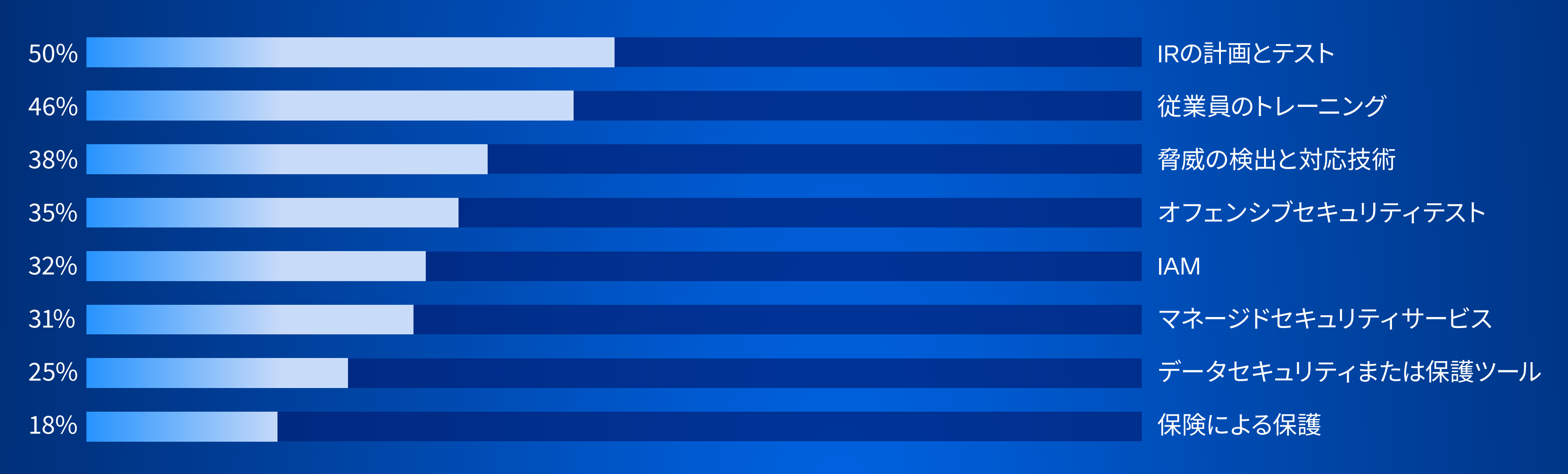
出典: 2023年Verizonデータ侵害調査レポート（DBIR）

03.

素早いインシデント対応と情報に富む分析

51%の組織はデータ侵害の結果としてセキュリティへの投資を増やすことを計画しています。追加投資の上位にはインシデント対応（IR）の計画とテスト、従業員のトレーニング、脅威の検出と対応技術などがあげられています。

データ侵害後のセキュリティへの追加投資の中で最も一般的な投資



出典: 2023年データ侵害被害額レポート、Ponemon InstituteおよびIBM Security

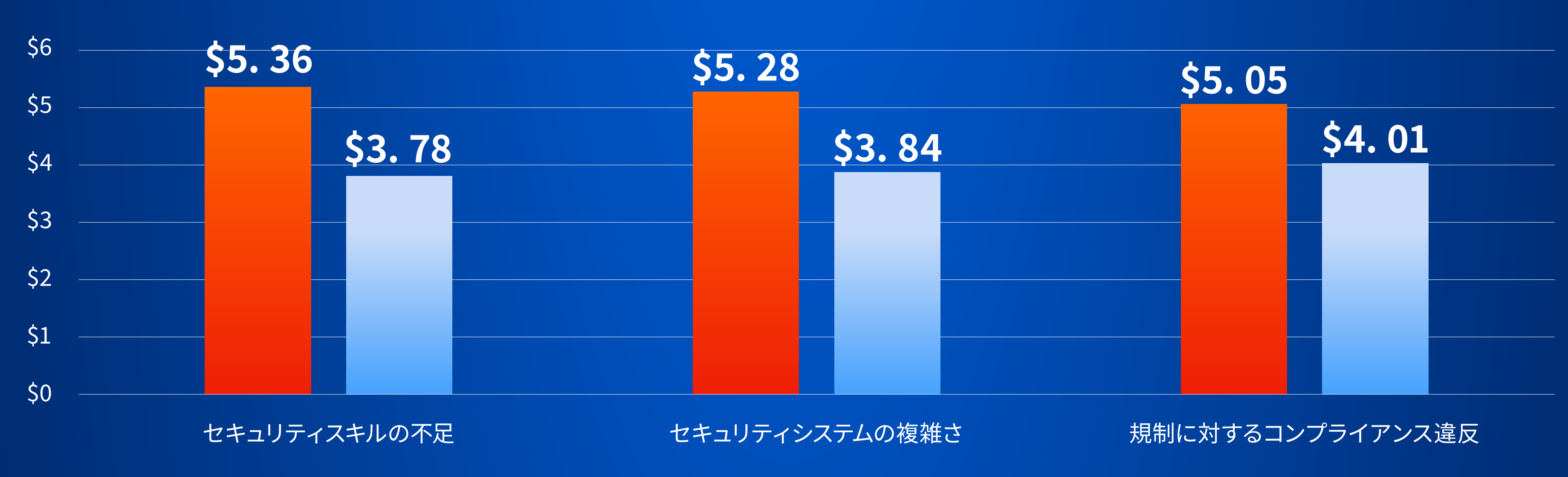
04.

既存の規制要件および今後予想される規制要件へのコンプライアンス対応

米国クラスA企業は、CISOが合理的に同等またはより安全な補完的制御方法の使用を書面で承認していない限り: (1) ラテラルムーブメントを含むがこれに限定されない異常なアクティビティを監視するためのエンドポイントでの検出と対応（EDR）ソリューションを実装しなければなりません。

出典: NY州DFS

27の要因のうちデータ侵害による被害額を最も増加させた要因



出典: 2023年データ侵害被害額レポート、Ponemon InstituteおよびIBM Security

05.

サイバーセキュリティ保険の要件

出典: 連邦取引委員会（https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/cyber-insurance）

ベストプラクティスに含まれるもの:

- 機密データの暗号化
- 脆弱性診断とパッチ管理
- EDR
- プログラムによるバックアップとDR計画
- 多要素認証（MFA）と権限（最小特権管理）に関する厳格なポリシー
- 振舞い検知のマルウェア対策機能
- セキュリティ意識向上トレーニング
- インシデント対応計画

ビジネスレジリエンスを確保する総合的なサイバープロテクション

今すぐ購入　今すぐ試用

Acronis

acronis.com