

2022年サイバー脅威防御レポート

ITセキュリティ専門家が現在最も懸念しているサイバー脅威とは？
2022年の最優先セキュリティ技術とは？

CyberEdge Groupは世界中のITセキュリティに関する意思決定者と実務経験者1,200名を対象に調査を実施し、直面している課題やアプリケーションとデータ保護に関するさまざまな技術の評価に関する知見をお届けしています。

重要なポイント:

ATO攻撃に対する懸念が高まっています。 アカウント乗っ取り (ATO) やクレデンシャルスタッフィング攻撃に対する懸念の水準がこの1年で急上昇しました。調査で追跡しているすべての脅威の中で、マルウェアに続き2位になっています。

その他のWeb攻撃も顕著です。 調査回答者は個人情報漏洩、カード不正利用／支払い不正攻撃、Magecartなどのデジタルスキミング攻撃を挙げました。

API保護とWAFが頼みの綱です。 60%以上の企業がAPI保護とWebアプリケーションファイアウォール (WAF) 技術をインストールしています。

アプリケーションセキュリティとデータセキュリティ技術を統合することで効果が発揮されます。 クラウドセキュリティ体制の改善、インシデント調査の向上、顧客サポート体験の拡充などのメリットがあります。

ネットワークベースのサイバー脅威

ITセキュリティチームは、最大の懸念事項として次のようなネットワークベースのサイバー脅威を挙げました。



アカウント乗っ取り／クレデンシャルスタッフィング攻撃

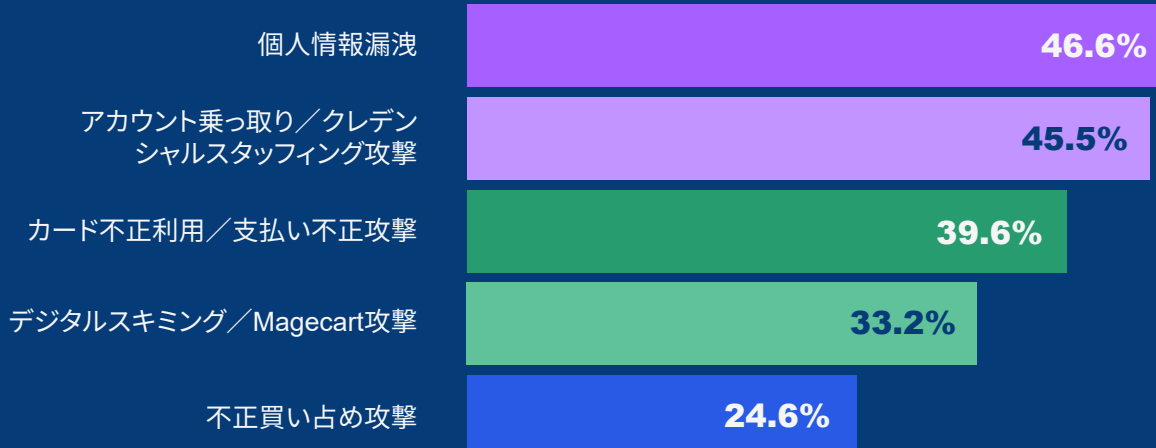


サービス妨害攻撃



Webアプリケーション攻撃

最も懸念すべきWebアプリケーションとモバイルアプリケーションの攻撃



アプリケーションセキュリティとデータセキュリティの基盤...

10社のうち6社がこの技術を導入済み



APIゲートウェイ／保護



Webアプリケーションファイアウォール (WAF)



データベースファイアウォール

...期待が高まっている技術

今年最も多く導入が予定されているアプリケーションセキュリティとデータセキュリティの技術。



ボット管理



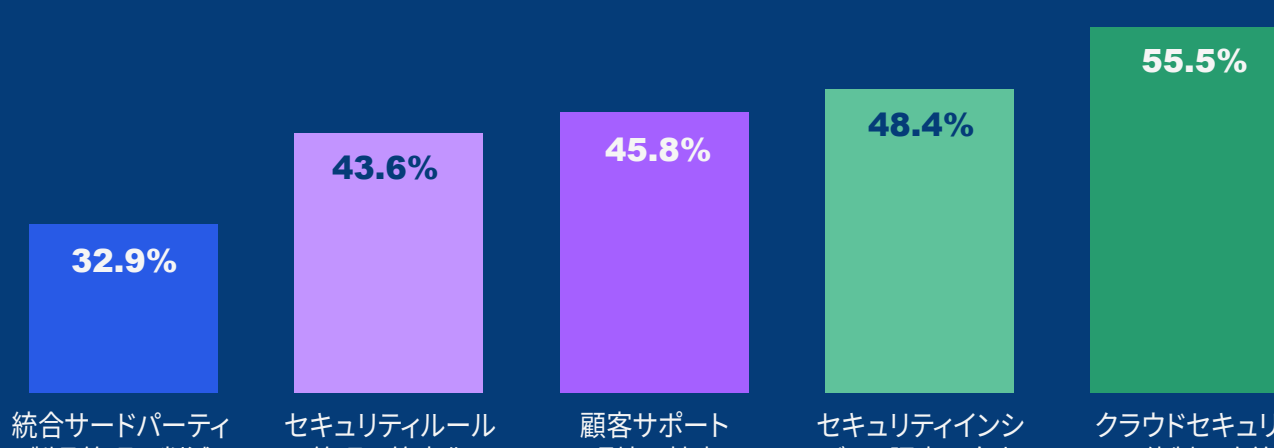
高度セキュリティアナリティクス



データアクティビティ監視 (DAM)

アプリケーションとデータのセキュリティを一元化する利点

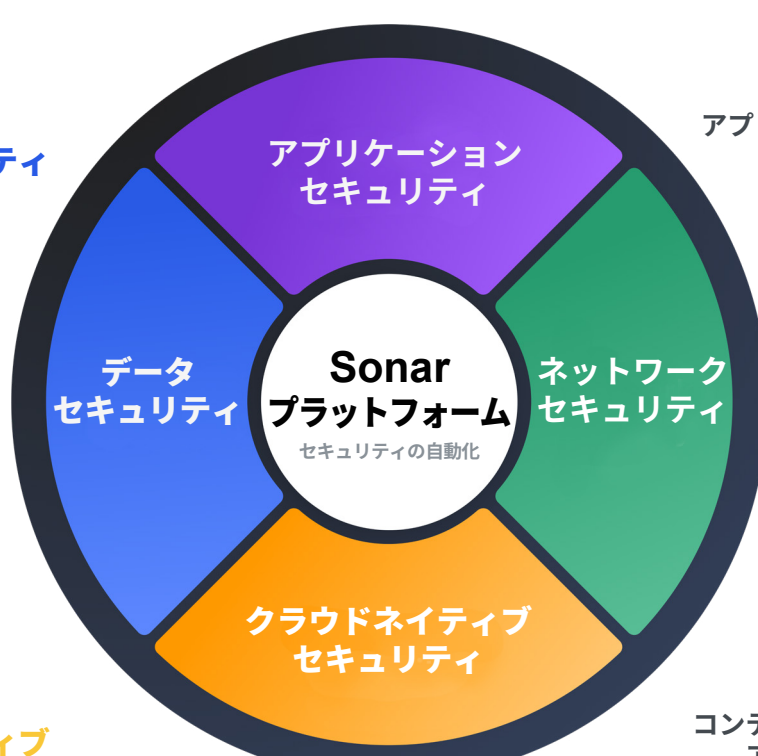
アプリケーションセキュリティとデータセキュリティの防御 (WAF、DDoS防御、RASP、APIセキュリティ、データリスク分析、データベースセキュリティなど) を1つのプラットフォームに一元化することで得られる利点。



あらゆる場所でワークロードとデータを保護

エッジやAPIから重要データまで保護。

データセキュリティ
保存場所を問わずデータを保護。



レポート全文は<http://www.imperva.com/ja/cdr2022>からダウンロードできます
ライセンス先: IMPERVA, INC.