



マネージドXDRソリューション

エンドポイントからプラットフォームに及ぶ企業全体のセキュリティ運用を統合、生産性を高めて検出と対応を強化

パロアルトネットワークス社の Cortex XDR をマネージドサービスでご提供します。ネットワーク、エンドポイント、クラウドにわたる豊富なデータを AI が学習し、優れた検出結果と共にセキュリティ運用業務の削減と強化を実現します。

● ソリューションの特長

特長1 SASEと連携することでプラットフォーム全体を保護

Global SASE with IIJ Omnibus と組み合わせることでサイロ化されていたセキュリティ管理を統合し、デバイスからプラットフォームまで包括的な可視化と対応を実現します。

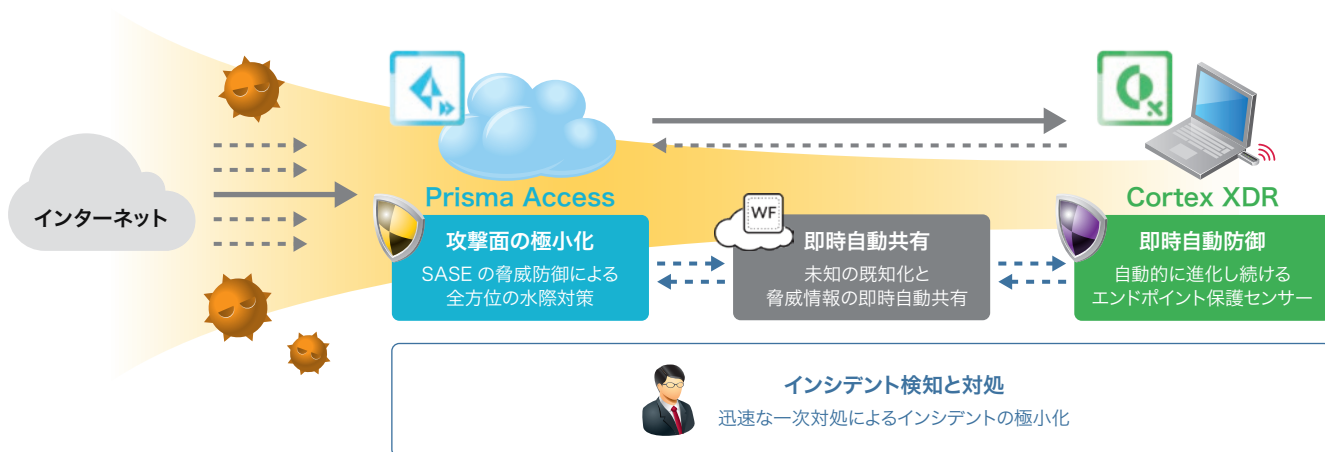
特長2 機械学習を活用した最高峰の脅威検出と対応が可能

様々なデータソースを利用することで、既知および未知のマルウェア、ファイルレス攻撃、エクスプロイトをブロックする多層型防御によりデバイスを保護します。

特長3 インシデントの検出から初動対応までを能動的に実施

アラートによる検知と通知だけでなく、セキュリティチームによるインシデントの判断から通信の遮断と端末の隔離までを実施します。

● ご提供イメージ



プラットフォームからエンドポイントまで一貫した保護

脅威情報の自動連携で相互にブロック

端末の振る舞いを学習し不審デバイスも検出可能

迅速なインシデント対応でセキュリティ運用負荷を軽減

複数のデータソースを統合し、単独のセキュリティ製品では不可能な脅威を検出し、調査、対応を自動化・迅速化します。



● マネージドXDRソリューションの利用メリット

クラウド提供により 定常運用業務の負荷を低減

ウイルス管理サーバのハードウェア/OS
メンテナンス不要でバージョンアップも
完全自動化を実現

様々なデータソースを利用した クラス最高の検出と防御

エンドポイントとネットワークの双方向
からデータを取得し、複雑な脅威を検
出して防御

迅速なインシデント対応による 影響の最小化

感染後の自動対応に加えて、インシデ
ントの検知と初動対応として端末隔離ま
で実施

● ソリューションメニュー

基本機能

マネージドXDRソリューション

エンドポイント保護(EPP)/エンドポイントの検出と対応(EDR)/ユーザの行動分析(UBA)/
ネットワークトラフィック分析(NDR)/インシデント検出・通知・初動対応

オプション機能

拡張ハンドリング初動代行

初動対応後のトリアージ(調査)・一次対応

連携ソリューション

Global SASE with IIJ Omnibus連携

非管理デバイスの可視化・不審端末の通信遮断

● 基本機能一覧

XDR標準機能	Prevent	Pro per Endpoint	Pro per TB
機能概要	EPP	EPP + EDR	NDR
対象	エンドポイント	エンドポイント	ネットワーク機器、ファイアウォール等
マルウェア防御	○	○	-
WildFireによる解析	○	○	-
デバイス制御、ディスク暗号化	○	○	-
感染時の隔離	○	○	-
ログ保管(アラート)	○	○	-
ログ保管(アクティビティログ)	-	○	-
不正デバイスの検出	-	○	○
行動分析テクノロジー	-	○	○
感染時の調査ツール・端末修復・スクリプト実行	-	○	○
ライセンス購入単位	デバイス数	デバイス数	解析容量(TB単位)
ライセンス最小購入数	200	200	5TB
運用メニュー	内容		
統合セキュリティ監視	セキュリティ統合監視(24時間365日有人監視)、インシデント通知、解析結果・必要な対応連絡、ネットワークフロー監視、相関分析		
統合運用	障害監視・障害対応(リモートのみ)、稼働監視、設定変更、遮断設定、チューニング、バージョンアップ		
Webポータルサイト	チケット管理、インシデント情報、稼働統計情報、セキュリティアラート統計情報、シグネチャ検索、最新脆弱性情報		



IIJ Global

お問い合わせ

株式会社IIJ グローバルソリューションズ
E-Mail : info@iijglobal.co.jp
URL : www.iijglobal.co.jp

※ 本内容は、予告なく変更することがあります。(2022年3月作成)
※ 記載されている企業名あるいは製品名は、一般に各社の商標または登録商標です。