JEDR / JMDR

powered by Acronis

24時間
365日緊急対応

Acronis 社の提供する Cyber Protect Cloud サービスを
株式会社ジインズがサポートするセキュリティサービス
としてお客様に提供致します。

- JEDR　：EDR
- JMDR　：EDR＋SOC（24 時間 365 日電話メール対応）

JEDR JMDR のココがスゴい！

1. **AI 技術**による高度な脅威検証と分析能力
2. クラウドから組織全体の**ライセンスを一元管理**
3. 導入＋ランニングが**低コスト**

EDR(Endpoint Detection and Response)

エンドポイント（パソコンやサーバー、スマートフォンなど）へのマルウェアの侵入を防ぎ、**内部へ侵入した脅威も検出・通知・根絶するシステム**です。
従来のセキュリティは侵入を防ぐことが主な目的で、近年それだけでは防ぎきれないサイバー攻撃が増加しています。
JEDR はエンドポイントへ配置したエージェントプログラムにより、常時監視を行います。

MDR(Managed Detection and Response)

セキュリティの専門業者が組織の**セキュリティ監視を行う運用サービス**です。
エンドポイントへ侵入した脅威は SOC がいち早く検知・通報し、的確な対応をサポートします。
マルウェアの脅威を根絶した後は脅威を追跡し、侵入元や原因の追及を行います。
JMDR では EDR＋SOC によりエンドポイントにおける脅威の検知・対応・予防までをまとめて実現いたします。

SOC(Security Operation Center)

組織のセキュリティに関連する活動を監視・管理する部門または組織です。
主な役割はセキュリティ監視やサイバー攻撃の検知、インシデント分析・対応、脅威情報の収集・対策・分析・追跡等が挙げられます。
インシデントへの素早く的確な対応には SOC の存在が不可欠です。しかし、セキュリティの専門知識が必要なため、外部の業者へ委託することが多いです。

株式会社 ジインズ
Japan Info Net Service

JEDR/JMDR 共通機能

Security	＃CyberFit スコア（セキュリティ診断）
	脆弱性診断
	ランサムウェア対策機能 Acronis Active Protection
	アンチウイルス / アンチマルウェア保護：クラウド シグニチャベースのファイル検出
	アンチウイルス / アンチマルウェア保護：AI ベースの実行前ファイルアナライザ、振る舞い検知のサイバーエンジン
Data Loss Prevention	デバイス制御
Cyber Protection Management	デバイスのグループ管理
	保護計画の集中管理
	ダッシュボードとレポート
	ハードウェア インベントリ
	リモートディスクトップ及びリモート支援

エージェントのインストールや
管理コンソールの利用は無償
(ライセンス数のみ課金)

標準機能

- セキュリティ
- マネジメント

拡張機能

- バックアップ
- オートメーション

SOC の疑問お答えします!

監視ってどうやってするの？常駐してくれるの？

自施設内のSOCでない限り、通常はクラウド経由でリモートでの監視を行います。

業務が復旧するまで対応してくれるの？

SOCには業務運用知識はなく、また、あっても業務には一切立ち入らないというのが前提です。業務復旧判断はあくまでもお客様側でのご判断となります。

24 時間 365 日どれぐらいで初動対応してくれるの？

遅くとも検知してから 30 分～ 1 時間程度で初動対応が行われます。現実的には、初動対応時点で自動的に脅威が隔離・根絶までされていて、既に全ての処理が完了していることが多いです。

JINS Japan Info Net Service

お問い合わせ
TEL 03-6380-9917
http://www.jins.co.jp/
Mon-Fri 9:00～18:00

会社HP

株式会社ジインズ
●本社
〒406-0846
山梨県笛吹市境川町三椚301
TEL: 055-225-3471

●東京事業所
〒101-0047
東京都千代田区内神田1-6-6
MIFビル9階
TEL: 03-6380-9917