SecureSeed Plus EPDR with Watch Guard

万全のセキュリティ EPPとEDRで 安心の端末保護

近年のサイバー攻撃は、より高度で複雑になっています。
従来のウイルスの特徴をもとに検知するシグネチャベースのアンチウイルスソフトでは
既知のウイルスは検知できますが、未知のウイルスは検知できません。
さらに、LOTL攻撃や非実行型マルウェアなどの痕跡を残さない攻撃も存在するため
「感染前」のみならず「感染後」の対策も重要となっています。

SecureSeed Plus EPDR には EPPとEDRの機能があります

2つのエンドポイントセキュリティ機能

感染前

EPPソリューション
Endpoint Protection Platform

高い検知率で大幅に感染リスクを低減！
シグネチャとヒューリスティック分析で
マルウェア感染を予防・検知する。

感染後

EDRソリューション
Endpoint Detection and Response

少ない労力で感染後のリスクを低減！
収集情報を基に攻撃予兆や端末ステータスを
可視化し不正を自動で対処。

それぞれの特性を組み合わせて、エンドポイントを守ります。

EDRとEPPが
統合的に搭載されていることで
両方からの情報を相関的に分析し
エンドポイントを保護します！

株式会社 南日本情報処理センター MIC は SecureSeed Plus シリーズで

貴社の情報漏洩対策・セキュリティ対策をトータルサポートいたします。

■ 製品特徴

従来のEDR製品	異常を検知 ▶	検知アラートを確認後、手動で対処
SecureSeed Plus EPDR	異常を検知 ▶	収集した情報を相関分析し、自動で対処

EDRでは専門知識が必要でしたが、EPDRでは端末エージェントが自動で実行します。

管理負担を軽減する
プラットフォームを標準装備

リアルタイムで
- **端末ステータス**
- **ライセンス**
- **保護状況**

を可視化します

リアルタイム性

エンドポイントでの活動をリアルタイムで監視し、異常な挙動や潜在的な脅威を迅速に検知します。サイバー攻撃が発生した際には即座に対応し、被害を最小限に抑えることが可能です。

詳細な分析

攻撃の詳細なログを収集し、インシデント分析を行うための強力なツールを提供します。これにより、攻撃の原因や手法を深く理解し、将来の防御策を強化することができます。また、フォレンジック調査を通じて法的な証拠を確保することも可能です。

自動化された対応

脅威を検知した際には、自動化された対応を行うことができます。感染したエンドポイントを隔離したり、悪意のあるプロセスを停止したりすることで、攻撃の拡散を防ぎます。修復機能を備えている場合、システムの回復を迅速に行い、業務への影響を最小限に抑えることができます。

■ 動作環境

対応OS	
Windows	Windows 10 および Windows 11
macOS	macOS 10.10 Yosemite 以降
Linux	AlmaLinux 8.3以降, Ubuntu 22.04以降, Fedora 42以降, Debian 11以降, RedHat 7以降, CentOS Stream 9.x以降, LinuxMint 21以降, SuseLinux Enterprise 15 SP3以降, Oracle Linux 8.0以降, RHEL 8.6 およびRockyLinux8.3以降
Android	Android 12 以降

■ 提供価格

課金単位		価格
初期費用（環境構築、初期導入支援）		50,000 円
月額費用	運用サポート費用	5,000 円 ～
	ユーザー利用料（１ユーザーあたり）	1,000 円 ～

導入・環境構築から
毎月の運用サポートまで
お任せください

株式会社南日本情報処理センター https://www.kk-mic.jp

本社 〒891-0115　鹿児島県鹿児島市東開町4-104
TEL 099-269-9711　FAX 099-269-9718

東京支社 〒140-0013　東京都品川区南大井6-16-4 戸浪大森ビル8 F
TEL 03-6436-8686　FAX 03-6388-9450

宮崎支社 〒880-0806　宮崎県宮崎市広島2-5-16 興亜宮崎ビル5F
TEL 0985-29-9900　FAX 0985-29-9127

お問い合わせ先

202506