●App Guard 導入事例　※国内2万2千社以上が導入し、過去1度も被害を受けた実績は有りません

航空：ANA
通信：DAIKO XTECH
旅行：JTB
医療：埼玉医科大学
建設：戸田建設
運送サービス：ecoHAI
製造：JFE / Pentel / KAKUDAI
地方自治体：越前市 / （白石市様）
教育：日病学園
福祉サービス：社会福祉法人 千葉市社会福祉協議会
医療：津山中央病院 / 柏澤病院 / 弓削病院 / 名寄市立総合病院
公益財団法人 日米医学医療交流財団
専門サービス：Deguchi
特殊団体：公益財団法人 日本テニス協会
証券業：SMBC日興証券
警備サービス：東洋テック
その他：アメリカ国防総省

米国政府関連での導入実績

App Guardは、日本病院共済会推奨製品となりました

近年、医療機関を標的としたサイバー攻撃は増加の一途をたどり、攻撃手法の巧妙化も進んでいます。現実に病院がランサムウェアの被害により診療を長 期間停止した事例も多く発生しており、医療機関が一層強固なセキュリティ対策が求められています。「AppGuard」は、2023年6月、日本病院共済会から、日本病院会会員病院をサイバー攻撃から守る最適な製品とのご評価を頂き業務提携を致しました。



組込みシステム用サイバー攻撃対応
App Guard Industrial

ある精密機器メーカー実例
課題
1機器にサイバー対策機能追加の要望が増加
2ウイルスソフトのセキュリティが担保出来ない
ウイルスソフトの課題
1製品仕様において、自社開発プログラムを全て登録する導入プロセスに 障壁を感じる。また既に機器にマルウェアが潜伏している場合、そのプロセスもホワイトリスト(WL)化しリスク回避できない。
2WL型ではファイルレス攻撃から機器を守る事が出来ない
3ソフトウェア更新の際に個々に設定が必要で手間
製品選考時の機能要求
1CPU負荷が低く機器の生産性を劣化させない
2機器メーカーの定めるプロセス以外の動作を禁じる機能が有る
3機器内プログラム修正等に大きな影響を受けず高い運用性を有する
4未知・既知問わずマルウェアの攻撃を阻止可能
実検証の結果、AppGuardが選ばれた理由
1CPU負荷は非常に小さく生産能力に影響無し
2動作制限の機能要件を満たしている
3AppGuardの「自動継承機能 ※特許機能」が制御プログラム修正の影響を最小化できる
4防御機構上、非常に高い防御力と判断 ※実検体を使いペンテストを実施
5海外での組込み実績
App Guard Industrial導入開始済み、及び検証中の実例
精密機器メーカー、大手物流マテリアルハンドリングメーカー、大手機械製造会社、大手機械製造会社、大手食品原料加工メーカー、大手包装容器メーカー、
大手コンビニチェーン全店舗のPoS、Kiosk端末

App Guardを短時間で理解する事が可能な動画をQRコードから閲覧する事が出来ます

CUTTING EDGE

正規販売代理店 カッティングエッジ株式会社
〒101-0044 東京都千代田区鍛冶町1-9-6
TEL / FAX：03-6822-5613
https://cuttingedge-tech.jp/
sales@cut-edge.jp

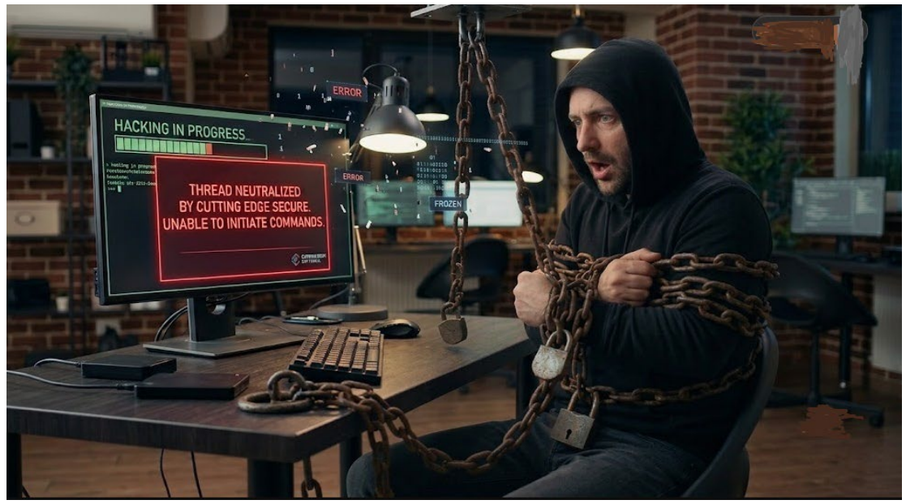
お問い合わせ先はこちら

●カタログの内容は予告無く変更する場合がありますので、ご了承願います。　●カタログの写真や色は印刷により若干異なる場合が有ります。　●このカタログの制作は2026年11月です。

ゼロトラスト型エンドポイントセキュリティ APPGUARD

CUTTING EDGE

AIサイバー攻撃が、脆弱性の有る穴から侵入しても、悪い事を何もさせない！
ウイルス感染したUSBを挿しても、怪しい添付ファイルを実行しても、
不正プログラムの実行は不可能！許可されたアプリケーションしか起動させない。
専門知識も、専門担当者も、24時間/365日監視も不要！
米国政府、米国ペンタゴン、日本政府、防衛省等国内導入23,000社を突破！
26年間1度も破られた事の無い、サイバー攻撃を無力化し阻止するソリューション















CUTTING EDGE

サイバー攻撃が脆弱性の穴から侵入して来ても、攻撃を無力化し、許可したアプリケーションしか起動をさせない！
米国国防総省(ペンタゴン)で使うために開発され特許取得の、26年間1度も破られた事の無い究極のサイバー攻撃阻止ソリューション

App Guardの大きな特長



※ フィッシング詐欺には対応しません
フィッシング詐欺とは、大手通販会社、宅配業者等のなりすましメールを送りつけ、貼り付けたリンクをクリックさせて偽のホームページに誘導し、クレジットカード番号やアカウント情報（ユーザID、パスワードなど）などの重要な情報を盗み出す詐欺のことです。フィッシング詐欺は、サイバー攻撃とは異なり、自らが重要情報を入力してしまうため、対策としては十分に注意をするしか有りません。

App Guardとアンチウイルスソフトの大きな違い

製品	App Guard	アンチウイルス
目的	悪い事をさせない	悪い奴を見つける
ウイルス検知	×	○
ウイルス駆除	×	○
マルウェア生成阻止	○	×
マルウェア起動阻止	○	×
端末乗っ取り	○	△

アンチウイルスソフトは、被害情報に基づいたウイルスだけを特定して検知し駆除する方法を取っており、対策アップデートが配布される迄の間に攻撃者が常に先手を取るため、攻撃をくい止める事が出来ず、ウイルスソフトでは未知の攻撃に対して効果が全く有りません。

一方App Guardは、システムに害を与えるOSの重要領域へのアクセスや不審な処理を、構造的に一切許可しない（アイソレーション技術）という手法を採用しております（特許）。許可したアプリケーションだけしか起動させない方法を取っており、侵入した攻撃者のアプリケーションは許可されていないためフリーズさせ、プログラムを起動させません。攻撃者の行動の自由を奪い、目的を達成させません。新旧、種類、攻撃手法に関係無く、どの様な侵入攻撃にも対応が可能です。
App Guardには駆除機能が有りません。しかしMicrosoft365を使用している場合、無料付属の**ディフェンダー**が機能し、ウイルスを検知し、駆除しますので、ディフェンダーと同時併用するとアンチウイルスソフトの機能も使うことが出来、大きな効果を出す事が可能です。

App GuardとEDRの大きな違い

製品	App Guard	EDR
目的	攻撃の成立を阻止	侵入される事を前提として、侵入後の迅速な対処を支援
導入と作業	PCやサーバーにインストールし許可するアプリを選択するだけ	専門教育を受けた技術者が常時監視とログ収集し、通信、プロセス実行などの挙動データを常に記録・蓄積
手法	許可しない動作を阻止	脅威の検知・相関関係整理、分析
専門技術者	不要　※導入時に外部から管理し調整	24時間365日監視する専門技術者人数：6～10人
年間コスト	①ライセンス年間費用: ¥7,200／端末 + 管理費約¥3,000 ②導入管理費: 企業規模に因るが、80～300万円(初年度のみ)	①専門技術者6～10人の人件費: 5000～8000万円以上 ②ライセンス他経費 : 年間500万円～1,000万円以上
外部委託サービス	無し	①サービス導入時の社内人員: 1～2人 ②年間1.5～3万円/ライセンス + 監視費 ③運用費: 年間150～1000万円以上
未知の脅威、環境寄生型攻撃、未知の脆弱性	マルウェアの発症、不正アクセスに因る侵害を成立させない。脅威の新旧や種類、攻撃手法に依存しない。	EDRの特性上、新しい脅威や攻撃に対しては新しい検知モデルが必要であり、最終的には利用者側の対処スキルに大きく依存する

EDRは、侵入されることを前提として、侵入後の迅速な対処を支援する手法で、攻撃を受けた時の防御、検知、対処を行うための専門教育を受けた担当者数人を24時間／365日体制で監視させる必要が有ります。そのため、人件費、スキルアップのための教育コスト等非常に大きな経費が掛かります。
また、攻撃を受けた際の防御方法、対処方法等が担当者のスキルや判断に因るため、相関関係整理が重要となります。
一方、App Guardは、パソコンやサーバーにソフトウェアをインストールし、許可するアプリケーションを選択するだけで、専門知識も担当者も不要です。許可したアプリケーションしか開く事が出来ないため、マルウェア等はフリーズした様な状態となり、起動する事が出来ません。そのため、気づかないうちに、裏側でApp Guardがサイバー攻撃をストップさせて守ってくれています。

