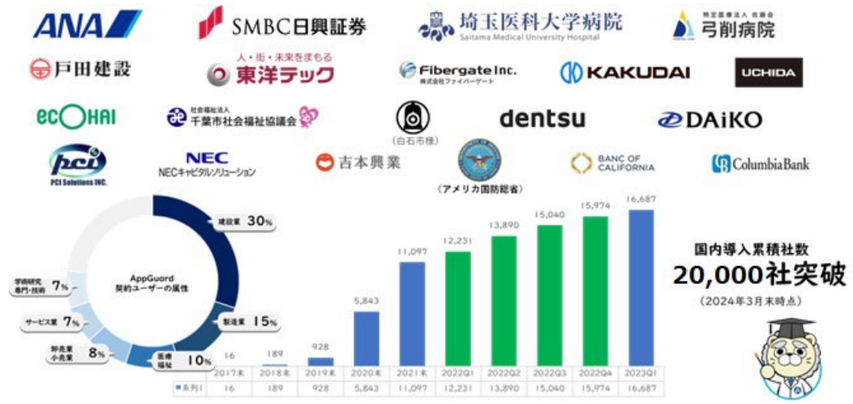
●App Guard 導入事例　※国内2万社以上が導入し、被害を受けた実績は１社も有りません



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下QRコードから閲覧する事が出来ます

Cutting Edge!! カッティングエッジ!!
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@ctg-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2025年8月です。

Blue Planet-works
Safety for the Connected World

日本の技術、金融資産、公共インフラを守る究極で最強のサイバー攻撃対策ソリューション
侵入され感染しても、許可しない行為を阻止
米国ペンタゴン向けに開発され、24年間１度も破られた事が無い

ゼロトラスト型エンドポイントセキュリティ
APPGUARD

米国政府関連での導入実績

1ライセンス年額わずか¥7,500(税別)、安心のサイバー保険付

Cutting Edge!! カッティングエッジ!!

米国国防総省(ペンタゴン)で使うために開発されたAPP GUARDは、許可されたアプリケーションしか起動をさせない、究極のサイバーセキュリティツール。政府、公共インフラ、ハイテク企業、銀行、大学、病院等国内２万社以上が導入しています。

個人や中小企業はサイバー攻撃を受けないと考えていませんか？

ハッカー集団がマルウェア等で盗んだ情報を出品するマーケットプレースと言う商談の場があります。2024年5月1日から1か月間に、日本人の情報が2,883人台出品されており、銀行情報、クレジットカードのID、パスワード、実名、写真、住所を含んだ様々な詳細な情報が販売されております。その多くは、下記個人の端末から侵入した事が分かりました。

1. フェースブック　885台（31%）
2. DMM　748台（26%）
3. Discord　662台（23%）　※ゲーム用アプリ
4. インスタグラム　626台（22%）
5. アダルトサイト　422台（15%）

しかし、情報を盗まれた本人は何も気付いておりません。

サイバー攻撃者は、簡単に侵入出来る個人や中小企業のパソコンから攻撃を行い、感染と同時に大きな被害をもたらすランサムウェアや、マルウェアを送り、そこから勤務先のサーバーに侵入します。さらにサプライチェーン等の大手企業のサーバーに到達して、重要な資産を盗みます。つまり、個人や中小企業のパソコンが最も狙われ易いターゲットとなります。

感染したらどうなる？

・端末、サーバーを乗っ取られ、機能不全となり、リモートコントロールされる
・感染した端末の持ち主の名前で、Word等添付メールを社内/社外/友人に配布し、周りの端末を全て感染させる
・パスワード、クレジットカード情報、銀行情報、個人情報、企業秘密情報、資産情報、技術情報等が盗まれ売却される
・情報を暗号化し、身代金を数日以内に支払う様要求される（最近の身代金平均額約16億円　※1千万ドル）
・データが改ざんされたり、破壊される
・PCのカメラとマイクから持ち主の顔、声をコピーし、本人になりすましたAI 画像やAI 音声を作り、犯罪に使われる
・最近現れたInfo Stealerと言うマルウェアは、本人に盗まれた事を気付かれない様に情報を盗み販売する怖い攻撃。

App Guardの大きな特長と機能

1. マルウェア起動阻止機能
なりすましメールやランサムウェア等のマルウェアの起動を阻止、侵入されても発症させず、未知の脅威から守ります。

2. 改ざん処理防止機能
悪用される可能性があるアプリに対して不正アクセスをさせません。侵害されてもシステムへの改ざん行為を制御します。

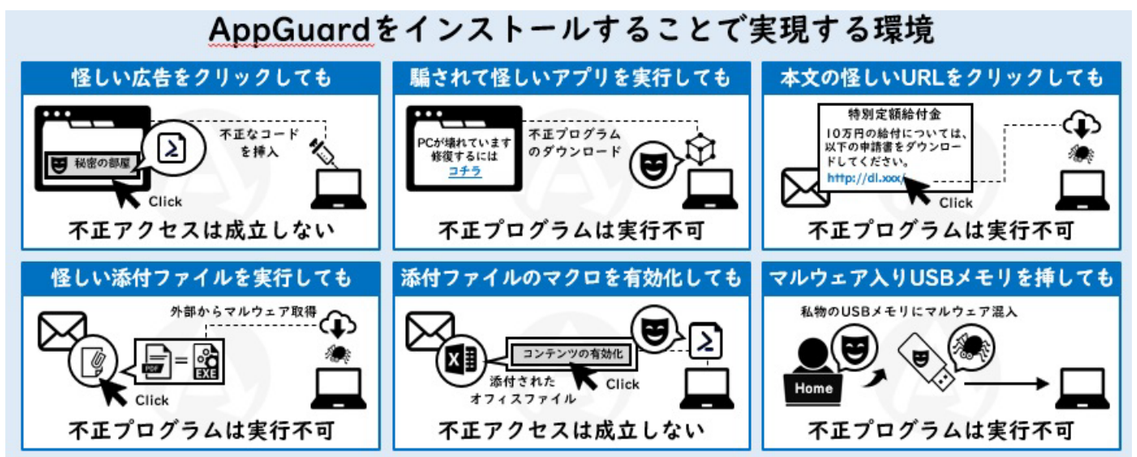
3. プライベートフォルダ
個人情報や機密情報の格納されたフォルダを、サイバー攻撃からのアクセスを遮断し守ります。

4. ファイル更新・アップデートが不要
従来のウイルスソフトとは異なり、ファイルの更新やAI/機械学習エンジンのアップデートは不要です。

5. 運用管理の簡素化とコストダウン
インストールするだけで、継続的にシステムの安全性を維持し、EDR方式の様に専門知識は不要で、ウイルスソフトの経費・人的負荷軽減が可能です。

6. 現在使用中のセキュリティ製品との併用が可能
App Guardは、プラスアルファのセキュリティ対策として現在使用中のウイルスソフトと併用してお使い出来ます。

7. 1年間、1ライセンスわずか￥7,500（税別）、会社1社当たり最大1億円のサイバー保険も付いており、非常に安心です。



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
マルウェア検知	×	○
マルウェア駆除	×	○
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には約3週間掛かります。そ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、許可されたアプリケーションだけしか起動させない究極の方法を取っており、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、プログラムを起動する事が出来ません。攻撃者の行動の自由を奪い、目的を達成させない理想的なツールです。新旧、種類、攻撃手法に関係無く、どの様なサイバー攻撃にも対応が可能です。**

Microsoft365に無料で付属の**ディフェンダー**が、時間とともに、ウイルスを検知され、駆除します。

App GuardとEDRの大きな違い

製品	App Guard	EDR
目的	予防	事後対応
機能	アプリケーションとプロセスのゼロトラスト化	NIST SP800-171に基づく防御、検知、対処
手法	攻撃の成立を阻止	脅威の検知・相関関係整理
成果	「やって良い事」が実践されているかの検証	侵害中又は侵害された痕跡とデータの照合
機能のタイミング	攻撃実行前	攻撃実行後
コスト	安い (¥5,500～¥7,500 / 年)	非常に高い(人件費+諸経費)
未知の脅威、環境寄生型攻撃、未知の脆弱性	App Guardは、マルウェアの発症、不正アクセスに因る侵害を成立出来ない状態にするため、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たい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、攻撃を受けた時の防御、検知、対処を行うツールで、専門教育を受けた担当者数人を24時間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アプリケーションをインストールするだけで、特に専門知識も専門担当者も不要です。許可され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、動く事も悪さをする事も何も出来ません。そのため、何も気づかないうちに、裏側では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。**

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。