政府・軍基準を搭載した新方式の
統合型セキュリティスィート

PC Matic PRO

EPP:エンドポイント保護

EDR:エンドポイント検出応答

RMM:端末運用管理

Performance:パソコン快適化

Application Whitelisting (NIST SP 800-167)

従来のエンドポイント保護でマルウェアを完全防御できたか?

既知のマルウェア検体を分析した上でのシグネチャーを用いた仕組みであり、ヒューリスティックエンジンも完全には防御できていないため、感染が起きている。

このため、感染後の分析手法としてEDR/XDRが重宝されているが、犯罪者を特定するためのツールであり防御能力ではない。

エンドポイント保護は限界論

Copyright © 2023 Bluestar Corporation.

政府が用いるホワイトリスト方式は?

- バージョンアップの度にホワイトリストを作成する手間
- アプリに脆弱性が発見される事により、侵入を許してしまっている
- スクリプト形式など新しい脅威が生まれ保護できていない

使い勝手の悪いホワイトリスト方式は過去のもの?

Copyright © 2023 Bluestar Corporation.

政府機関は理論上感染しない利便性の高いものを要求

- 新しい利便性の良い強固なエンドポイント保護が必要ではないか。

- そのような課題に国土安全保障省(DHS)、国防総省(DoD)、連邦捜査局(FBI)、サイバーセキュリティ・社会基盤安全保障庁(CISA)が中心となり研究を行っていた。

Copyright © 2023 Bluestar Corporation.

一方、マルウェアに悩まされるパソコンメーカー

- パソコンメーカーは、マルウェアやソフト的にOSを破壊するフリーソフトウェアなどに悩まされていた。
- 顧客は、「パソコンが壊れた」とサポートに連絡してくるからである。

- マルウェアに感染せず、不具合のあるドライバーなどを更新できる良い顧客サポートの仕組みは実現できないものだろうか。(サポート費用抑制)

Copyright © 2023 Bluestar Corporation.

両者の悩みは偶然にも同じ方向へ

- 世の中にあるすべての実行可能ファイルを信頼しない(ゼロトラスト)
- 信頼しないアプリケーションは絶対に実行させない(SP 800-167)
- バイナリー形式、スクリプト形式の両方をアプリケーションと定義し、セキュリティ制御下に置く
- 脆弱なアプリケーションは顧客に判断を仰がずに自動更新(SP 800-40)

パソコンに悪影響があるファイルを実行させないという方向性が、政府機関とパソコンメーカーで偶然にも一致していた。

マルウェアを実行しようとしても
感染しない仕組み
+
専門家が許可しないと実行不可

脆弱性が発見されても
悪用されない仕組み
+
脆弱性対策のため自動更新

- ゼロトラトセキュリティモデル(NIST SP 800シリーズ)という新しいセキュリティフレームワーク策定へつながる
- アプリケーション・ホワイトリスティング方式(Application Allowlisting)へと繋がる。

Copyright © 2023 Bluestar Corporation.

従来製品のマルウェアへの対処方法

- COVID-19 と同様にマルウェアもセキュリティソフトを回避するため、原種から変異を繰り返し亜種が生み出される。
- 新種COVID-19にはワクチンがないのと同様に、まったく新しいマルウェアも定期的に作成される。

- ワクチンは、原種だけでなくオミクロン種にも対応した二価ワクチンが提供されたのと同様に、セキュリティソフトにも亜種に対応したワクチンを定義ファイルという形で配信し対処する。

- 2022年に新規検出されたマルウェアは1460億個。新種は1.2億個

- この方法は、クラウドAI監査の次世代エンドポイント保護(NGAV)やEDR/XDRでも同様で、過去の知見に基づいて対処が行われる。

↓

- 新種発見時には、誰かが感染してしまうということ

Copyright © 2023 Bluestar Corporation.

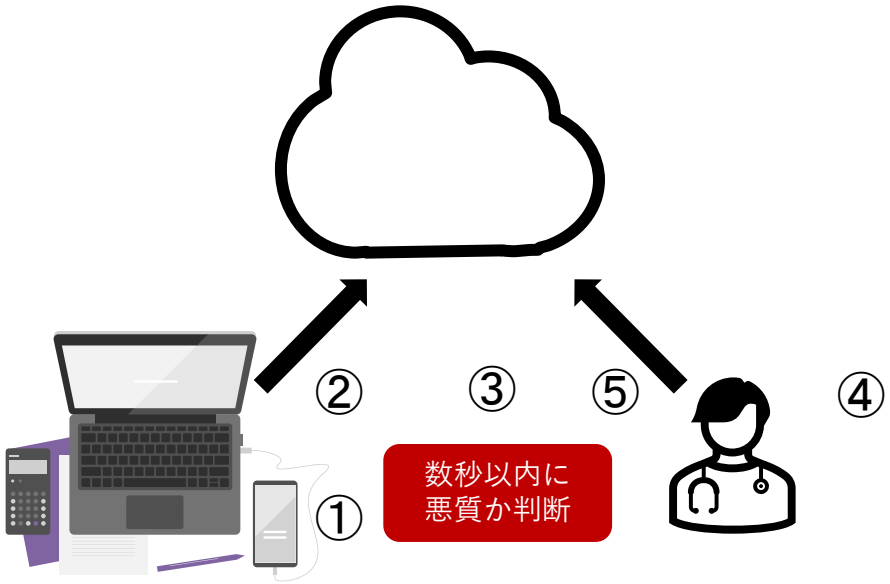
従来製品の課題

- クラウドAI監査の次世代エンドポイント保護、EDR製品も過去の知見により「マルウェア」や悪質通信が判定される
- 全く新しく開発されたマルウェア・ランサムウェアに関し、過去の知見がないため感染を許してしまうこととなる
- 新たな感染により、新たな知見が得られ他者を守るのが今までのセキュリティ対策の考え方
- 脆弱性を抱えたアプリケーションは起動許可される(=リスク)
- NIST CMMC レベル3として規定された保護水準となる
- NGAVやEDRは、知見に基づくためZero Trustではない

Copyright © 2023 Bluestar Corporation.

概念図

他社　EPP,EDR,XDRの仕組み



①ワクチンにてマルウェアであるかの判断を数秒で実施(端末,クラウド判定)
②感染時および、感染の嫌疑がある検体をサーバへ転送
③サーバにて過去の知見に基づきAI分析しスコアリング
④マルウェア分析官がマルウェアであるかを調査し、マルウェアの場合はワクチンを作成
⑤ワクチンやAIサーバがマルウェアと判定できるようになり防御される

過去の知見に基づくため感染者により他者を守る仕組み

毎日たくさんの犠牲者により他者を保護

Copyright © 2023 Bluestar Corporation.

どうすれば、被害者ゼロにできるのか

- マルウェアは、人が作成した悪意あるプログラムやスクリプト
- これはOSがプログラムやスクリプトに対して実行可能なAPIを提供しているから実行可能となっている

↓

- OSから全てのAPIを標準オフにしたら、マルウェアは活動できない
(Default Denyや標準拒否と呼ばれている考え方)

↓

- 善良なプログラム、もしくはマルウェアを新種も含めてどう判断したら良いのか。過去の知見、サンドボックスでは発見できない新種マルウェアはどうやったら見つけられるのか。

↓

- 経験豊かなマルウェア分析官が全件、人手によるデジタルフォレンジックを実施しないと難しいのではないかとの結論。ソースコード分析が基本となる。

Copyright © 2023 Bluestar Corporation.

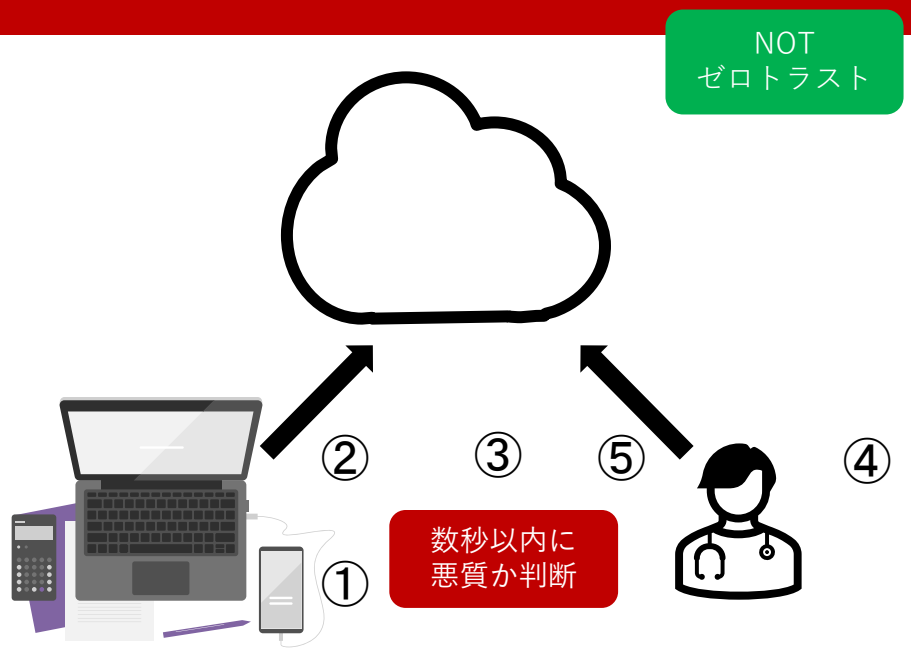
What’s PC Matic?

- OSから実行可能ファイル、スクリプト、サービスなど全てを標準ロック
- マルウェア分析官による手作業でのデジタルフォレンジック(科学捜査)を経た上でなければ、ロックが解除されない(=起動許可は与えられない)
- マルウェア分析官は、送信された検体をAIの力を借りて効率的に分析ができるようダッシュボードなどを利用。怪しい検体は起動保留が継続され、複数の分析官による判定を経る
- 過去の知見のないマルウェアや通信でも、一人も被害者を出さない仕組み
- 判定結果は全世界の顧客で共有される(1億3千万件の善良リスト※2023/09時点)
- 脆弱性を抱えたアプリケーションは起動許可されない(=安全)NIST SP 800-40
- 使い勝手は、既存エンドポイント保護と遜色ない (だから個人版も販売)
- NIST CMMC レベル5として規定された保護水準となる

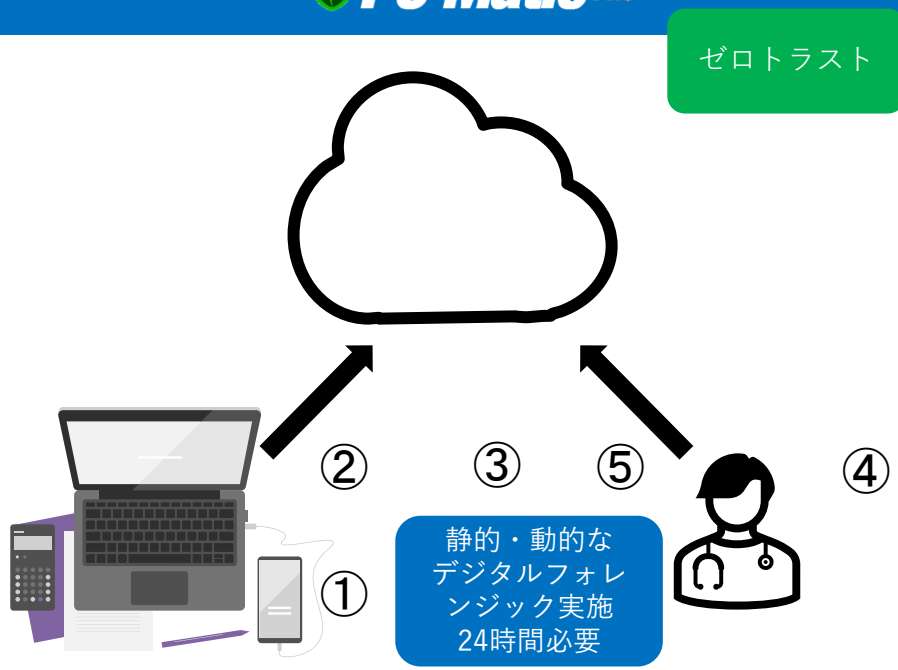
Copyright © 2023 Bluestar Corporation.

過去の知見によるものはゼロトラストではない

他社　EPP,EDR,XDRの仕組み



PC Matic PRO



国家予算でサイバー兵器としてのマルウェアが年間1460億個も
作成されているのに秒で判断できると本気で思いますか?

①ワクチンにてマルウェアであるかの判断を数秒で実施(端末,クラウド判定)
②感染時および、感染の嫌疑がある検体をサーバへ転送
③サーバにて過去の知見に基づきAI分析しスコアリング
④マルウェア分析官がマルウェアであるかを調査し、マルウェアの場合はワクチンを作成
⑤ワクチンやAIサーバがマルウェアと判定できるようになり防御される

①バイナリー、スクリプト形式の実行ファイルは全てデフォルト拒否
②サーバへ実行是非をリクエスト
③グローバルリストの中で善良と判定していれば起動許可
④マルウェア分析官によるデジタルフォレンジックが実施されていなければ、
２４時間以内に判定を実施し、起動のロック解除などを判断する
⑤全世界の顧客でグローバルリストが共有される

過去の知見に基づくため感染者により他者を守る仕組み

全実行ファイルに対してデジタルフォレンジックを実施

毎日たくさんの犠牲者により他者を保護

感染ゼロ

Copyright © 2023 Bluestar Corporation.

私たちが考える真のゼロトラスト

- そして、PC Maticの考え方
- ウイルスや細菌に免疫力がない人がクリーンルームで過ごしているのと同様
- PC Maticはゼロトラストを基本とし、脆弱性を抱えているプログラムも起動拒否
- NGAV/EDR/XDRは、過去の知見に依る自動判定であるためゼロトラストではない
- 境界(信頼されたイントラ網)はあってもよいが、境界内も信頼がないことを前提とした仕組みがゼロトラスト
- この考えが、米国・豪州政府の基本方針と近年定められた。

Copyright © 2023 Bluestar Corporation.

2021年5月12日のバイデン大統領令(EO) 14028

ゼロトラスト・アーキテクチャ(ZTA)、エンドポイントでの検知及び対応(EDR)、データの暗号化並びに多要素認証(MFA)の更なる普及推進

Copyright © 2023 Bluestar Corporation.

Executive Order on Improving the Nation’s Cybersecurity骨子

- EDR、保存された情報の暗号化、多要素認証(MFA)に加え、大きなポイントが「利用可能アプリケーションの限定化」

- DHS(国土安全保障省)が主導し、全省庁とその傘下組織で利用するアプリケーションの認証を取る

  推測されている認証内容
  - 米国内製ソフトウェア (開発した人材の国籍含む)
  - 脆弱性を抱えていないか (利用後、脆弱性発見により対処版へ即座に差し替え)
  - 組織や役職によりアクセスできる情報範囲の規定

- フリーソフトウェア、市販ソフトであっても組織内で利用許可がだされていないアプリケーションやスクリプト・マクロは利用できない。

州政府や米国企業へも、このセキュリティガイドラインを推奨

Copyright © 2023 Bluestar Corporation.

EPPはアプリケーション・ホワイトリスティング方式

- 米国防総省、豪政府はエンドポイント保護をアプリケーション・ホワイトリスティング方式による運用とNIST CMMC Level 4,5で定めています。

- 最高レベルの保護はホワイトリスト型でなければならなず、Default Denyのクラウド型AI監査型であっても機械分類による製品は、レベル3迄しか認められていません。

- CMMC（Cybersecurity Maturity Model Certification：サイバーセキュリティ成熟度モデル認証）は、米国の防衛産業基盤（DIB）企業がサイバーセキュリティ対策について定めた統一規格です。

FedRAMP

連邦政府調達には、
FedRAMP認証取得が必要

Copyright © 2023 Bluestar Corporation.

米国政府によるゼロトラスト・フレームワークの推進

背景

従来のセキュリティ方法は、安全・危険の境界防御に重点を置いてい。ネットワーク境界の内側に入ったユーザーは「信頼」され、多くの場合、多くの企業リソースへの幅広いアクセスが許可される。しかし、悪意のある行為者は境界の内外から侵入する可能性があり、近年、いくつかの著名なサイバー攻撃により、境界ベースのモデルの論拠が崩れつつあります。さらに、クラウドコンピューティングやモビリティの拡大、現代の労働力の変化など、いくつかの要因により、境界はあまり意味を持たなくなってきている。

ゼロトラストは、サイバーセキュリティ戦略であり、境界ベースの防御を、広範で静的な境界から、企業のリソースがどこにあるかに関係なく、狭範で動的なリスクベースのアクセス制御に移行することに重点を置いています。ゼロトラスト・アクセス制御は、アイデンティティやエンドポイントの健全性など、多くの属性に基づいて行われます。

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Copyright © 2023 Bluestar Corporation.

ゼロトラスト・アーキテクチャ(ZTA)策定への協力ベンダー

Technology Collaborators		
Appgate	IBM	Ping Identity
AWS	Ivanti	Radiant Logic
Broadcom Software	Lookout	SailPoint
Cisco	Mandiant	Tenable
DigiCert	Microsoft	Trellix
F5	Okta	VMware
Forescout	Palo Alto Networks	Zimperium
Google Cloud	PC Matic	Zscaler

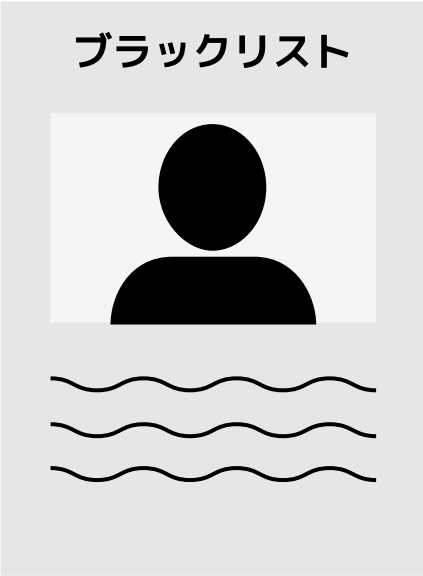
PC Matic, Inc.は、NIST CCoE構成企業の一社

現在、このNCCoE構成企業内で製品の連携により、ゼロトラスト・フレームワークを強靭化する連携策が進行しています。
PC Maticは、EPPにてアプリケーション・ホワイトリスティング方式を担う中核です。

Copyright © 2023 Bluestar Corporation.

アプリケーション・ホワイトリスティング方式

- アプリケーション・ホワイトリスティング方式は、業務上必要なアプリケーションとスクリプトのみ実行可能とする施策。NIST SP 800-167として規定。
- 脆弱性を抱えたものは起動を保留し、最新版へ強制的に差し替えられる。(SP 800-40)
- ゼロトラスト・フレームワークの中核をなす。



指名手配レベル

CMMC level 2

空港保安レベル

CMMC Level 3

軍事レベル

CMMC Level 5

Copyright © 2023 Bluestar Corporation.

WHY ZERO TRUST: デフォルト拒否と多重防護壁

- アプリケーション・ホワイトリスティング方式
  - デホルト拒否で未知のものは実行不可。すべてクラウド監査
  - クラウド上で徹底監査し、高度に難読化されているものをコードスキャニング
  - 実在するPCのBIOSなどに偽装したサンドボックス
  - 特定GWアドレスのサンドボックスを作成
  - 悪意あるC&Cサーバのブラックリスト
- ゼロデイ前提での設計思想
  - wsf,bat,ps1等のスクリプトによる暗号化、ファイル転送などを標準拒否
- 確認外APIコール、ポートの拒否
  - クラウド監査にて得られたAPIや通信ポートのみ許可
- ブラックリスト認証局判定
  - 不正の多い認証局はデジタル署名を信頼しない
- 強制自動更新ポリシー
  - 新たな脅威へ事前対応するためPC Maticのエンジンを随時更新
  - 著名アプリを強制自動更新し、脆弱性を早期に塞ぐ
- など多数の防護壁で多段防御

Copyright © 2023 Bluestar Corporation.

UNIQUE: 新方式アプリケーション・ホワイトリスティング

アプリケーション・ホワイトリスティング:後出しジャンケン方式

- パソコンにて未知のファイルは全てPC Maticサーバへ問い合わせ
- マルウェア分析官により善良と確認済は起動許可
- 世界中顧客が遭遇していないファイルはデジタルフォレンジック
- PC Matic側でリバースエンジニアリング等を行い善悪に分類
- 万が一、悪質なものを善良と誤判断してしまったら・・
  端末内EDRエンジンが未許可機能コールとして実行不許可

連続1900日以上
感染ゼロ

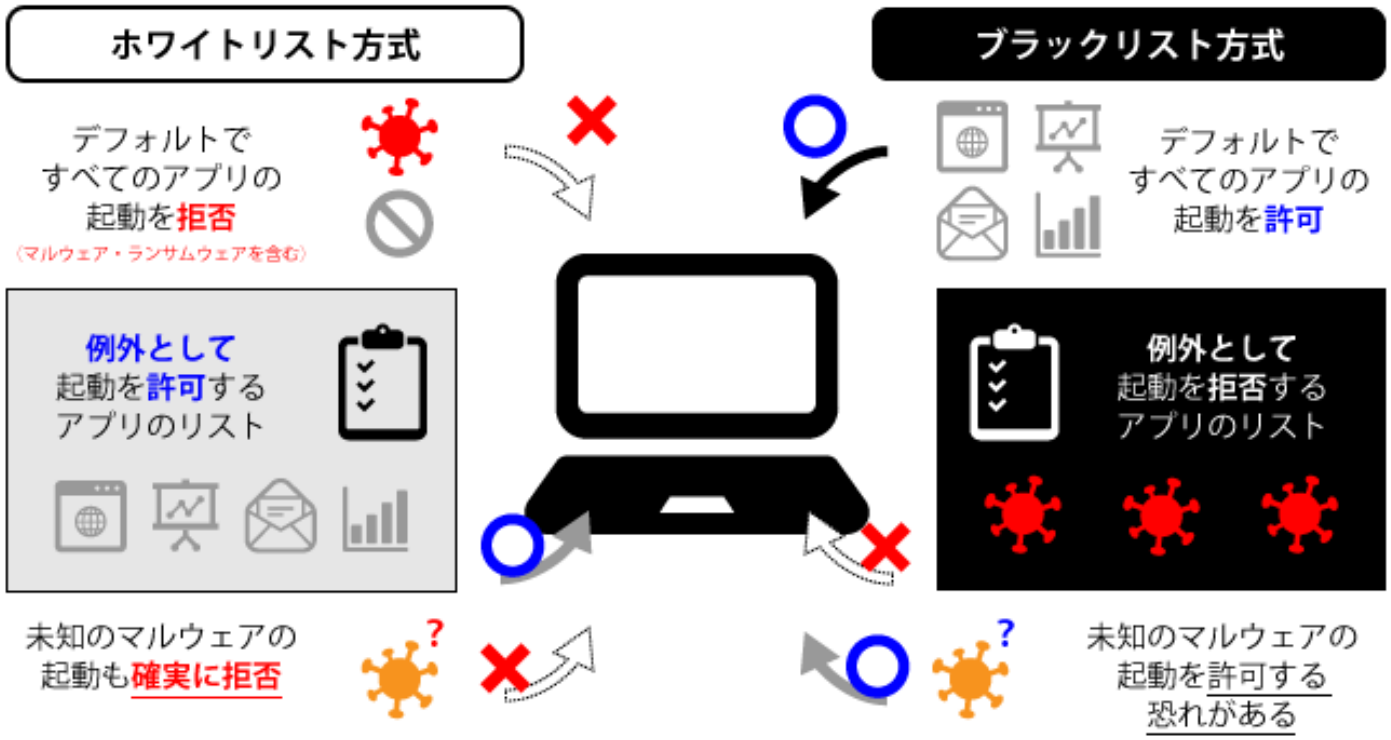
元FBIサイバー捜査官を含むマルウェア分析チームが判断

次世代エンドポイント:未知のウイルスに遭遇したら感染リスクあり

- 悪質かの判断をパソコンにて数秒で判定
- 起動許可し、ウイルスらしい活動をしないか監視
- 悪質な動き(=感染)を検知したら停止。(検知できない場合も多数)
- 悪質な検体をセキュリティ会社のサーバへ転送
- セキュリティ会社がAIの手助けでワクチンを生成
- ワクチンをシグネチャファイルにし、同種の活動を阻止

毎日
数百件の感染

クラウド上のAIが過去の知見に基づきリアルタイムで脅威を検知



アメリカCISA、ランサムウェア対策に同方式を推奨

https://www.cisa.gov/stopransomware

すべての資産に対し、アプリケーションのホワイトリストやエンドポイント検出と応答（EDR）ソリューションを使用して、承認されたソフトウェアのみが実行可能であり、すべての未承認のソフトウェアがブロックされるようにします。

※「初期アクセスベクトル: 前駆体マルウェア感染」セクションより

TLP:CLEAR

2024年現在、米英豪加新の5ヵ国が連名で推奨

Copyright © 2023 Bluestar Corporation.

PC Matic とは

1. PC Matic は、必要に応じて既存のセキュリティ層へオーバーレイし運用が可能です (blacklist AV, EDR/XDR, Firewall, etc.)。

2. PC Matic の常駐プログラムは、端末負荷をほぼかけず、かつ少しのメモリ資源しか消費しません。

3. PC Matic は、日本の唯一同盟国であるアメリカ国内でアメリカ人により100%開発・運用されています。

4. 昔のホワイトリスト方式からいくつもの改善がされています。

   - ゼロトラスト設計施策の導入
   - 善良なファイルとプロセスの管理
   - ローカル例外処理に関するガバナンス

Copyright © 2023 Bluestar Corporation.

PC Matic ゲームチェンジャー

① 新種による被害者がゼロ

従来製品は、過去のマルウェア情報を元にワクチンを作成するため、新種の場合はすり抜け感染してしまう。PC Maticは、全実行ファイルをマルウェア分析官による人手での監査を経て善良としたものしか起動させないため、新種を見逃さない

② グレーゾーンを起動保留

疑わしきは罰せずが従来製品。PC Maticは、ホワイトリストであるため善良のみで疑わしいものも起動させない

③ 深刻な脆弱性を持つ場合起動せず

実行することでセキュリティ上の脅威が発生するアプリをPC Maticは起動保留。従来製品は起動許可。

④ 脆弱性自動更新とCVE通知

悪意ある者に悪用されやすい著名アプリを最新版へ自動更新。また脆弱性を含むアプリの起動をCVE番号付きで管理者へ通知

⑤ 多層保護

複数のホワイトリスト保護方式を多層実装し、いくつかをパスしてしまっても他層で阻止される安心設計

⑥ 膨大なサーバーリソース

膨大なサーバーリソースで、静的及び動的に分析を行い、多数のスコアリングにてマルウェア分析官により最終判定

⑦ 同盟国製品

日本の同盟国であるアメリカ国内で研究開発し運用されている唯一の製品。国家安全保障のため、一切オフショアなし。

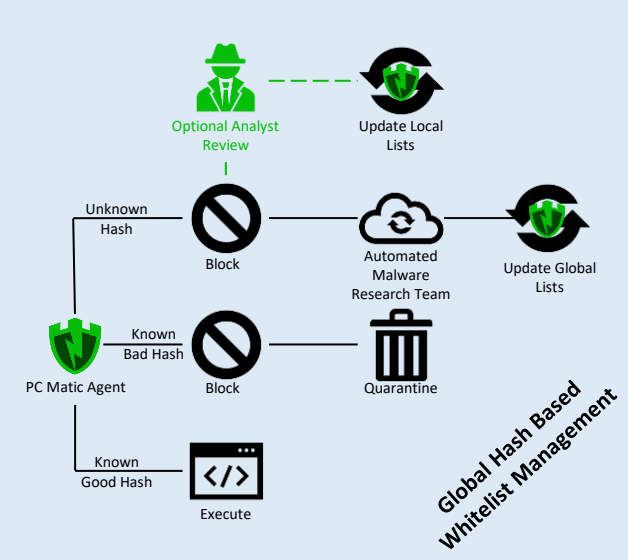
Copyright © 2023 Bluestar Corporation.

アプリケーション・ホワイトリスティング

- アプリケーション・ホワイトリスティングは、ネットワーク上で実行されようとしているものを特定し、実行するために認証を必要とするものです。
- ファイルやプロセスが不明またはマルウェアと判定された場合、実行前にブロックされます。したがって、アプリケーション・ホワイトリスティング方式は新種マルウェアやランサムウェアを防ぐための**唯一の方法**です。
- 従来のブラックリストによるセキュリティソリューションとは異なり、対処療法ではなく予防を目的としたセキュリティ方式です。
- アプリケーションホワイトリスティングは、ソフトウェア資産管理の一種です。

Copyright © 2023 Bluestar Corporation.

グローバル・ホワイトリスティング



- 従来のアプリケーション・ホワイトリストティングは、製品が正しく動作するために、ユーザーが自分のローカルリストを一から構築することに依存していました。リスト作成には、膨大な労力が必要でした。

- 従来のアプリケーション・ホワイトリスティング製品とは異なり、PC Maticは、すべての導入端末に適用可能な統合化されたグローバル・ホワイトリストを備えています。管理者は、自分で作成したローカルリストに依存することなく、ゼロトラストのセキュリティを即座に得ることができます。

- 購入、またはダウンロードが可能な場合、PC Maticのグローバル・ホワイトリストに登録されています。

- PC Maticのグローバルリストは、最初に導入ソフトウェアを列挙したり、善悪を検証する必要性をなくし、野放しにされているソフトウェアを発見しても慌てる必要を亡くすことができます。

- PC Maticのグローバル・ホワイトリストには、2600万以上のファイルとプロセスが含まれています。

  - アプリケーション、デジタル証明書、スクリプトのホワイトリストで構成されています。
  - 誤検出の可能性を最小限に抑えます。
  - PC Maticの100%アメリカ国内のマルウェア分析官により、連邦政府推奨基準で毎日更新されます。

Copyright © 2023 Bluestar Corporation.

グローバル・ホワイトリスティング

- 未知分類の起動阻止が発生した場合、管理者はPC Maticのマルウェア分析官による分類を任せるか、ローカルリストに例外的起動を追加するかのいずれかを選択できます。

- PC Maticは、ポータル管理者が個々のエンドポイントから企業全体まで、多くのユーザーに対して、ホワイトリストの追加を展開することを可能にします。

- 従来のアプリケーション・ホワイトリスティング方式とは異なり、PC Maticのローカル・ホワイトリストの追加は、導入端末の総数に関係なく、すべて数秒以内に有効になります。

PC Matic社にて用意される
グローバルリストへは、
１億個の実行ファイルが登録済です。
これにより、ブラックリスト製品のような
使い勝手を実現しました。

自分たちの業務アプリケーションは、
ローカルリストへ追加することで、
即座にロックが解除され使用可能に。
リアルタイム配信で端末に触れる必要はありません。

Copyright © 2023 Bluestar Corporation.

スクリプト・ホワイトリスト

- PC Maticは、全顧客で共有されるグローバル・スクリプティング・ホワイトリストを持つ**唯一の製品**です。

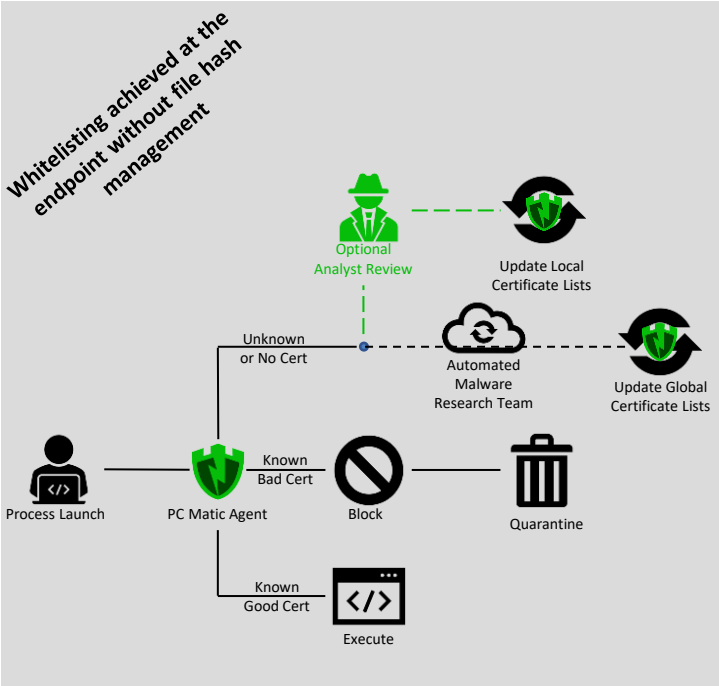
- powershellなどのスクリプトプログラムは、ランサムウェアを実行するためによく悪用されます。

- これは、応答性の高いセキュリティ製品の検出を回避するために、隠しスクリプトコマンドやオフィスマクロなどを使って行われます。

- PC Maticのグローバル・スクリプティング・ホワイトリストは、ファイルレスでマルウェアが展開される新時代に、例外を許さない保護を提供します。

Copyright © 2023 Bluestar Corporation.

デジタル署名ホワイトリスト



Custom and homegrown software can be added by digital code signing certificates or by file hash.

- PC Maticは、グローバルとローカルの両レベルでデジタル証明書のホワイトリスト機能を備えています。
- ローカル・ホワイトリストに電子証明書を採用するのは簡単で、その特定の証明書で署名された過去と未来のすべてのファイルを自動的にホワイトリストに登録します。
- PC Maticは、デジタルコードサイニング証明書の取り扱い方法に関する特許を取得しています。

Copyright © 2023 Bluestar Corporation.

様々なホワイトリスト方式を併用した多層防御

グローバル・ホワイトリスト

世界中の利用者が検知したアプリケーションから善良なものを共通リスト化したものです。世界中のPC Matic顧客へ即時提供し、善良確認済のアプリ・スクリプトのみ起動を許可します。
NIST SP 800-167準拠

ローカル・ホワイトリスト

アプリケーション・ホワイトリスティングを補完するため、お客様が独自のアプリケーションを指定端末・組織・企業全体に適用することができます。

署名ホワイトリスト

自社開発したデジタル署名済みのアプリケーションは、デジタル署名により包括的に許可され、アプリケーション毎にホワイトリストへ登録する必要がありません。

スクリプト・ホワイトリスト

ランサムウェアはOS標準機能のスクリプトを介して展開されるため、当社は業界唯一のスクリプティングホワイトリストを作成し実装しました。

Windows RDP 認証ホワイトリスト

ハッカーはRDPを利用して端末を乗っ取ります。PC Matic PROは、このセキュリティを強化するため、利用端末へ様々な追加認証の仕組みを提供しています。

端末認証ホワイトリスト

Windows RDP接続端末のペアを限定する機能を提供。しかも接続時に追加の接続認証は不要としました。

Microsoft Office ホワイトリスト

マルウェアは、Officeのマクロを介して活動を開始することがあります。このため、Office専用に別途起動可能なマクロやスクリプトのホワイトリストを多段実装しました。

ファイル拡張子ホワイトリスト

マルウェアは、危険なファイル拡張子を使って実行されます。悪意あるファイル拡張子によるアプリケーションの起動を無効化するホワイトリストを装備しています。

ローカルディレクトリ・ホワイトリスト

特定ディレクトリをホワイトリストに登録することができ、社内アプリケーションを開発、試験、配布とその利用許可を容易に行うことができます。

PC Maticは、様々なホワイトリスト方式を併用し、強固な保護を実現。

ファイルレス・スクリプト攻撃へ完全対応

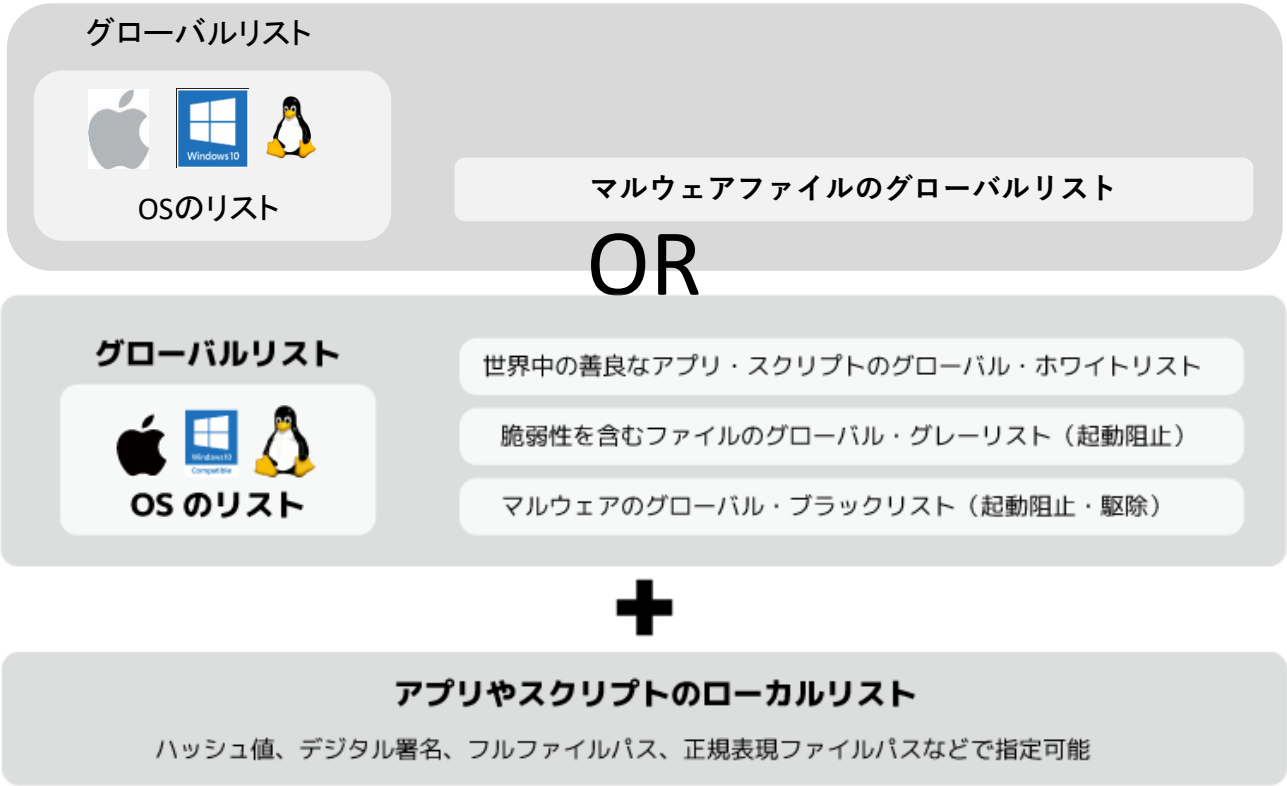
ホワイトリストを活用し、社内利用アプリケーションを起動阻止させず即座に利用可能

Copyright © 2023 Bluestar Corporation.

グローバルリストとローカルリスト

Automatically provided Global list and customer local lost

- PC Maticマルウェア分析官によるデジタルフォレンジックが実施された善良なアプリケーションリストである「グローバル・ホワイトリスト」が１億個分提供され、ブラックリスト方式製品と遜色のない使い勝手を実現
- 自社開発アプリケーションなどはローカル・ホワイトリストへ追加することで、運用の容易性を実現



グローバルリストは、「OSのみ」か「OS+豊富なリスト」の2つのモードから選択可能。

Copyright © 2023 Bluestar Corporation.

グローバルリストとローカルリスト

アプリケーション・ホワイトリスティング方式

グローバルリスト(PC Matic社が分類)

グローバル・ホワイトリスト

マルウェア分析官により、デジタルフォレンジック済のOS構成ファイル、善良なアプリとスクリプト

グローバル・グレーリスト

マルウェア分析官により、マルウェア嫌疑が濃厚、セキュリティホールがあるもの、分類が困難なファイル

グローバル・ブラックリスト

マルウェア分析官により、デジタルフォレンジックにてマルウェア、PUP、諜報ツールと判定したファイル

ローカルリスト(顧客が分類)

ローカル・ホワイトリスト

お客様が起動を許可したファイル

ローカル・ブラックリスト

お客様が起動を拒否したファイル

Copyright © 2023 Bluestar Corporation.

全ての脅威から保護するホワイトリスト方式

ランサムウェア

サイバー犯罪者にとって新しい手法のランサムウェアは、データを暗号化するだけではなく、公開や流出したくなければ身代金を払えと要求してきます。

ポリモーフィック型ウイルス

ポリモーフィック型ウイルスは、リアルタイムに自分自身や挙動自体を変更し、既知を前提とした一般的なセキュリティツールを回避します。

時限爆弾

ウイルスが即座に活動を始めるとは限りません。一般的なセキュリティツールで検知されないように顰み、突然活動し感染を広げます。企業にとって深刻な危機管理上の対応が必要になります。

クリプトマイニング

パソコンやサーバに常駐し、気がつかないうちに暗号資産を採掘する新しいウイルス。特にシステム管理者が不在な企業は、機器の性能を保持するために、感染に気がつきにくいこのウイルスを阻止する必要があります。

ゼロデイ攻撃

未発見の新たなマルウェアには検知シグネチャが存在しないため、既知を前提としたセキュリティツールはゼロデイマルウェアの影響を受けます。

ファイルレス感染

OSがもつ機能やオンメモリベースの攻撃は、スキャンや実行ファイルを制御する一般的なセキュリティツールを回避してしまいます。

キーロガー

キーロガーやその他の認証情報を盗むマルウェアは、取得した情報を悪用して様々なアカウントへ侵入。あなたの情報を利用したり、ダークウェッブ上で公開します。

スパイウェア／アドウェア

悪意のレベルには達していないものの、端末資源を消費したりデータを流出させるPUA（Potentially Unwanted Applications）を停止する必要があります。

Copyright © 2023 Bluestar Corporation.

一般的なエンドポイント保護製品では対象外の脅威

- 脆弱性(セキュリティホール)
  - 著名アプリケーションの脆弱性はサイバー攻撃によく利用される
  - 発見から対応されるまでの間のゼロデイ攻撃
  - 未発見で国家情報機関が保有する脆弱性情報(=サイバー兵器)

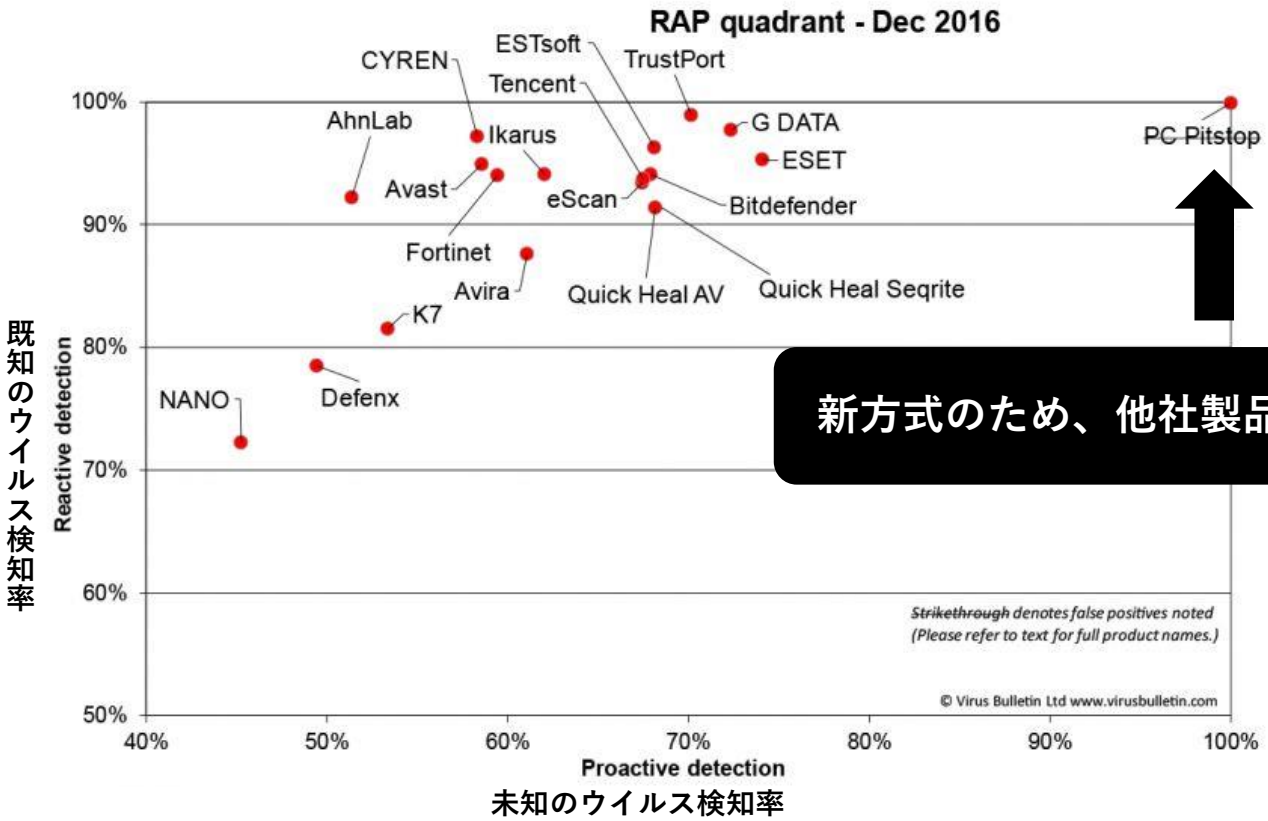
- ブラウザースクリプト攻撃
  - 仮想通貨マイニングスクリプト（日本では無罪判決。現在法整備検討中）
  - バンキング情報諜報スクリプト（クレジットカード番号や銀行取引情報を盗む）

- 国家情報機関が作成したスパイウェア
  - セキュリティベンダーが発売している国の情報機関製スパイウェアをマルウェア判定することは難しい。Microsoft製品は特にスパイウェアを検知しない。

PC Maticは、すべてに対応

Copyright © 2023 Bluestar Corporation.

TOP OF LINE:未知のウイルス検知率１位を獲得



新方式のため、他社製品と圧倒的な差がある

高い性能を誇っているのは、旧共産圏国の製品ばかりですが、**西側諸国製品として、PC Maticは圧倒的な防御力**です。

Copyright © 2023 Bluestar Corporation.

ROAD TEST:現状唯一の実稼働テスト PC Magazine

複数のAV製品を実稼働させ、最新の悪質URLクリックやウイルス感染を試みる手法
調査サンプル数は少ないものの、実運用状態に唯一近い性能評価です。

厳しい利用者試験で最高評価

Copyright © 2023 Bluestar Corporation.

TOP LINE:悪質URL防御力試験で世界1位を獲得

Malware Protection Tests ▲ High scores are best ▼ Low scores are best **Bold** type denotes top score	Suite	Free	Malware Detection		Malicious URL Blocking
			score ▲	% ▲	% ▲
PC Pitstop PC Matic With Super Shield			10.0*	100%*	100%*
Emsisoft Anti-Malware 2017			9.4	100%	94%
IObit Malware Fighter 5 Pro			8.7	89%	79%
ThreatTrack Vipre Advanced Security	Y		8.4	89%	86%
TotalAV			7.7	86%	88%
Kaspersky Free		*Y*	*7.2*	*79%*	*67%*
Bitdefender Antivirus Plus			**7.1**	**75%**	**91%**
Microsoft Windows Defender Security Center		Y	6.5	67%	86%
Reason Core Security			4.8	61%	12%
TESTED WITH PREVIOUS MALWARE COLLECTION					
Webroot SecureAnywhere AntiVirus (2016)			**10.0**	**100%**	84%
Comodo Antivirus 10			10.0	**100%**	37%
G Data Antivirus 2017			9.8	**100%**	78%
Ashampoo Anti-Virus 2015			9.8	**100%**	88%
F-Secure Anti-Virus (2017)			9.8	100%	78%
Symantec Norton AntiVirus Basic			9.7	97%	98%
Avast Pro Antivirus 2017			9.7	97%	87%
Trend Micro Antivirus+ Security (2017)			9.7	97%	89%
ESET NOD32 Antivirus 10			9.5	97%	89%
AVG Internet Security - Unlimited (2017)	Y		9.5	97%	73%
WinPatrol WinAntiRansom			9.2	97%	78%*
McAfee AntiVirus Plus (2017)			9.2	94%	85%
Panda Antivirus Pro (2017)			9.2	94%	48%
BullGuard Antivirus (2017)			9.0	94%	88%
K7 Anti-Virus Plus 15			9.0	97%	59%
Avira Antivirus Pro 2017			8.9	97%	95%
Check Point ZoneAlarm PRO Antivirus + Firewall 2017			8.7	87%	74%
Quick Heal AntiVirus Pro 17			8.5	94%	92%
TrustPort Antivirus Sphere (2017)			8.5	87%	70%
Check Point ZoneAlarm Free Antivirus+ 2017		Y	8.5	87%	62%
Qihoo 360 Total Security Essential 8.6		Y	8.1	84%	76%
adaware antivirus pro 12			8.1	87%	67%
Malwarebytes 3.0 Premium			7.2	77%	55%

RED denotes Editors' Choice.

米パソコン誌 PC Magazineの悪質URL防御力テスト結果が2017年9月に発表され、PC Matic SuperShieldがトップスコアを記録しました。試験者は「PC Maticは100.00%のスコアで競合を引き離しました」 とコメントしています。

標的型攻撃やランサムウェアの主要侵入方法である**ドライブ・バイ・ダウンロード攻撃に対しても高い防御力**でした。

電子メールの添付メールを開いたら感染するのか。

左図の検査数値左側「Malware Detection」が100%でなければ、添付ファイルによる、標的型攻撃やランサムウェアを防ぐことはできません。

つまり**この数値は100%でなければ、エンドポイントセキュリティを導入している意味はありません。**

Copyright © 2023 Bluestar Corporation.

COMPARISON:他社製品 比較

従来エンドポイントセキュリティ製品

エンドポイントセキュリティ(EPP)

ブラックリスト
ヒューリスティック

＋

EDR (別途オプション)

PC Matic PRO　PC Matic MSP

エンドポイントセキュリティ(EPP)
エンドポイント検出(EDR)
パソコン快適化
クライアント遠隔管理(RMM)

統合
製品

FedRAMP

FedRAMP認証取得済

	従来EPP製品	PC Matic 法人版
運用体系	オンプレ/クラウド	クラウド
初期投資	サーバ・初期導入費	不要
防御方式	ブラック・ヒューリスティック	アプリケーション・ホワイトリスティング
監査方式	パソコン内監査ロジック	ニューラルネットワーク型人工知能

Copyright © 2023 Bluestar Corporation.

管理者の手間が不要なアプリケーションホワイトリスト

	PC Matic	Airlock Digital	Threat Locker	AppLocker	Carbon Black	Comodo
Default-Deny Security	✓	✓	✓	✓	✓	✓
Global Allow List	✓					
Lightweight Security	✓					
Good Process Monitoring	✓	✓	✓	✓		
Realtime Admin Exceptions	✓	✓				
Integrated Remote Tools	✓				✓	✓
100% Made In The USA	✓					

FR
FedRAMP

Copyright © 2023 Bluestar Corporation.

PC Matic vs　従来のホワイトリスト製品

	PC Matic	他社ホワイトリスト製品
方式名	アプリケーション・ホワイトリスティング　NIST SP 800-167 準拠(製品と運用)	ホワイトリスト
ホワイトリスト制御対象	バイナリー形式 & スクリプト形式	バイナリー形式
ホワイトリスト	1億件以上の登録済グローバル・ホワイトリスト とローカル・ホワイトリストによる制御	管理者がホワイトリスト作成
制御ホワイトリスト	機器毎に異なる暗号化ファイル (改竄・差替不可能)	プレーンテキストファイル (改竄・差替可能)
起動許可指定	ファイルパス、ハッシュ、デジタル署名、スクリプト	ファイルパス、ハッシュ、デジタル署名
ファイルレス攻撃防御能力 Windows内部コマンド+Script	あり	なし = 感染リスク (別途AV機能購入)
マルウェア監査ロジック	EDRヒューリスティックエンジン(挙動振る舞い)、 AIプリプロセス後に最終マルウェア分析官➡GlobalList	なし = 感染リスク (別途AV機能購入)
外部デバイス制御 USBメモリやCD-ROM接続等	あり	あり
プロセス稼働ログ	EDR (端末,Syslog or クラウド), プロセス稼働管理と制御	動作ログのみ
Microsoftセキュリティソフト認定	認定取得済	対象外
脆弱アプリ対策　NIST SP 800-40	あり	なし = 脆弱性による権限昇格リスクあり
Windows RDP接続制御	時間帯制限, 接続元限定, 接続履歴ほか	なし
遠隔運用管理	コマンドプロンプト, ファイルマネージャ,管理者用独自リモートデスクトップほか	なし
ソフトウェア資産管理 ハードウェア資産管理	あり	なし
インストール時ネット環境	必須	不要
管理者用Webダッシュボード	あり	一部製品にあり
ライセンス期限	【個人版】1年, 50年 【法人版】毎月, 年次(1～5年)。 【PC Matic PRO embedded】年次, 製造時一括 無期限	無期限

Copyright © 2023 Bluestar Corporation.

PC Matic vs 従来のエンドポイント保護

	アプリケーション・ホワイトリスティングの PC Matic SuperShield保護（個人版・法人版）	一般的なセキュリティソフト NGAVや PC Matic ブラックリスト保護（個人版）
方式名	アプリケーション・ホワイトリスティング(NIST SP 800-167) **プロアクティブ型（予防療法）**	ブラックリスト & ヒューリスティック方式 **リアクティブ型（対処療法）**
NIST基準	NIST CMMC Level **5（最高）** 迄対応可	NIST CMMC Level **3（中程度）** 迄対応可
悪意ある者 への優位性	じゃんけん後出し 勝ち	じゃんけん先出し 負け
監査エンジン 実装箇所	クラウド監査	原則端末内
基本とする制御対象	バイナリー形式 & スクリプト形式 実行ファイル	バイナリー形式 実行ファイル
防御・駆除対象	マルウェア、ランサムウェア、スパイウェア、PUA(迷惑アプリ)、 悪質なブラウザ拡張機能、悪質JavaScript、その他プライバシー侵害	一般的にマルウェア、ランサムウェアのみ。 PC Maticではスパイウェア、PUA含む
未知の攻撃手法	マルウェア分析官による判断待ちにより不許可	許可し感染
新しい実行ファイル検出時	起動保留、検体をPC Maticに転出し、多数のAIがスコアリングおよび コードへ分解。マルウェア分析官がそれらのデータにより、科学捜査を行い悪意あるコードがなければ24時間以内に起動許可	端末内で検査し、過去悪意あるコードに類したものがなければ、即座に起動許可
マルウェア監査ロジック	AIプリプロセス、最終的に全件マルウェア分析官が判断	全て機械処理で問題発生時に分析官が対処
深刻なセキュリティ 欠陥持つアプリ利用	利用不可 (NIST SP 800-167準拠) 自動更新を実施	利用可能
著名アプリ欠陥対策 NIST SP 800-40	あり（著名アプリケーション自動更新機能）	なし
自己製品へのパッチ	自動更新。ユーザ対処不要	利用者がダウンロードし手動適用
ファイルレス攻撃防御能力 Windows内部コマンド+Script	デフォルト拒否	シグネチャーにて後日対処
プロセス稼働ログ	EDR (端末,Syslog or クラウド), プロセス稼働管理と制御	動作ログのみ
ブラウザー保護機能 による詐欺対策	あり	原則なし
動画再生中 動画広告スキップ	あり	なし
管理者用Webダッシュボード	あり	一部製品にあり
サブスクリプション 期限	【個人版】1年, 50年 【法人版】毎月, 年次(1～5年)。 【PC Matic PRO embedded】年次, 製造時一括 無期限	年次, 端末ライフサイクル

Copyright © 2023 Bluestar Corporation.

ALL IN ONE:端末運用統合ソリューション

EPP:エンドポイント保護

- ゼロトラスト・アプリケーション型エンドポイント保護
- 想定外挙動検知応答ヒューリスティックエンジン
- OS API,各種スクリプト,通信ソケットの標準拒否
- ファイルレス・マルウェア制御
- エクスプロイト攻撃防御
- Java 有効/無効 制御
- 起動阻止情報のsyslogサーバ送信
- トラッキングcookie削除
- ブラウザー保護 拡張機能(Edge,Firefox,Chrome対応)
  - ・詐欺広告、バナー広告、動画広告スキップ機能
  - ・WEBスキミング阻止
  - ・仮想通貨マイニングスクリプト阻止
  - など

EDR:Endpoint Detection & Response

- (予防:記録) ドライバ自動更新と実施記録
- (予防:記録) 著名アプリケーション自動更新と実施記録
- (記録) 起動アプリケーション稼働ログ(クラウド記録24h+端末内7日)
- (記録) 端末導入済サービス一覧取得
- (記録) 端末導入済プロセス一覧取得
- (記録) 稼働プロセスのスナップショット取得
- (記録) セキュリティ状況モニター
- (記録:制御) Windows RDP接続制御・接続ログ
- (記録:制御) 全稼働プロセス詳細把握(端末/日時等)と稼働制御
- (制御) ファイルレス・ランサムウェアが利用するOS内部暗号機能制御
- (制御) 各種スクリプト言語によるファイル外部送受信制御
- (制御) USBストレージ装置利用可否
- (制御) Windowsアカウントロック制御
- (制御) 組織別のホワイトリスト/ブラックリスト管理
- (記録:駆除) アドウェアや迷惑アプリ削除
- (記録:駆除) 悪質なブラウザアドオン削除
- (記録:駆除) 悪質ファイル検索・駆除

RMM:端末運用管理

【端末情報】

- ソフトウェア資産管理 (SAM)
- ハードウェア資産管理 (HAM)
- CPU負荷状況、RAM・ストレージ利用率監視
- リソース・セキュリティ関連 アラート通知
- 世界ランクによる端末陳腐化評価
- SIEM連携API (IBM BigFix,Syslog等)
- 運用状況レポートのPDF自動送信
- Windows Server稼働監視

【端末操作】

- 管理者用リモートデスクトップ (管理→遠隔)
- ファイルマネージャー (遠隔←→管理)
- コマンドプロンプト (管理→遠隔)
- Windows RDP 機能 オン・オフ
- 再起動
- スリープ制御 (常時オン維持)
- 管理者端末 2FA (Google,Microsoft Authenticator等)

【端末快適化】 Windowsのみ

- レジストリ最適化
- TCP/IPパケット長 最適化
- 不要スタートアップ削除
- 一時ファイル削除

対応OS・リソース

- Microsoft Windows 11 / 10 / 8.1 / 8 / 7
- 上述のWindows Embedded 各版
- Windows Server 2022/2019/2016/2012R2/2012/2008R2 (Server版対応)
- macOS 10.13.2以降 (Intel, Appleシリコン)
- Chrome OS
- iOS 13以降
- iPadOS 13以降
- Linux (Red Hat, Debian, Ubuntu, OpenSUSE)
- ハードディスク容量 : 150 MB 以上
- セキュリティ対策エージェントメモリ使用量 : 50 MB
- インターネット回線 : ブロードバンド・インターネット

社内端末管理に必要なものがすべて標準装備

PC Matic PRO	EPP+EDR遠隔運用管理(RMM)が統合した法人向けエンドポイント保護スイート製品
PC Matic MSP	PC Matic PROのマルチテナント版 事務機器販売店、大企業向け製品
PC Matic FEDERAL	政府・軍隊向けオンプレミス型エンドポイント保護スイート製品 FedRAMP
PC Matic Embedded PRO	PC Matic PROの産業機器組込版 オフライン・オンライン両対応

Copyright © 2023 Bluestar Corporation.

PC Matic 認証と準拠

●認証
- FedRAMP 認証済
  - アメリカ合衆国政府によるリスクおよび認証管理プログラム(政府向け)
- NMSDC 認証

●準拠
- NIST CMMC Level 5(最高値)
- NIST SP 800 シリーズ準拠
- HIPAA
- PCI DSS
- FIPS 140-2 Compliant
- MITRE ATT&CK Compliant
- CISA指針
  - アプリケーションホワイトリスト方式によるセキュリティ運用指針
- オーストラリア Cyber Security Centre (ACSC) Essential Eight Compliant
- CIS Controls Compliance

●メンバー
- NIST NCCoE
  - アメリカ合衆国政府によるゼロトラスト・フレームワーク策定企業メンバー
- CISA (アメリカ合衆国サイバーセキュリティ・社会基盤安全保障庁)
  - アドバイザリー・メンバー

Copyright © 2023 Bluestar Corporation.

AWARD WINNER

世界中の評価機関や雑誌社から高い評価を得た次世代製品

Copyright © 2023 Bluestar Corporation.

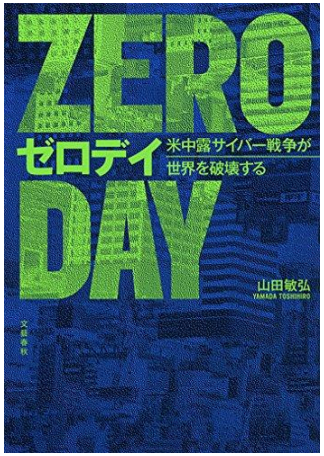
KEY FACTS: 同盟国　米国内開発品

- 米国生まれの米国人正社員のみで開発
- オフショア開発などは一切なし
- 西側諸国のみで発売のため情報機関の諜報ツールを徹底排除

現在、すでに国家間のサイバー戦争は始まっています。
セキュリティ製品は、あなたの会社そして**事業を守る防衛装備品**。

エンドポイントセキュリティ製品は、OSの深部で稼働するため、諜報ツールにも容易に変化します。この製品でなくとも同盟国製品の選択を検討してください。

Made in the USA



関連図書:ゼロデイ
現在起きているサイバー攻撃と各国の取り組みなどが解説されています。
セキュリティに携わる方はご一読されることをお勧めします。

Copyright © 2023 Bluestar Corporation.

YOU ARE SECURED:ファイルは何も考えずに利用可

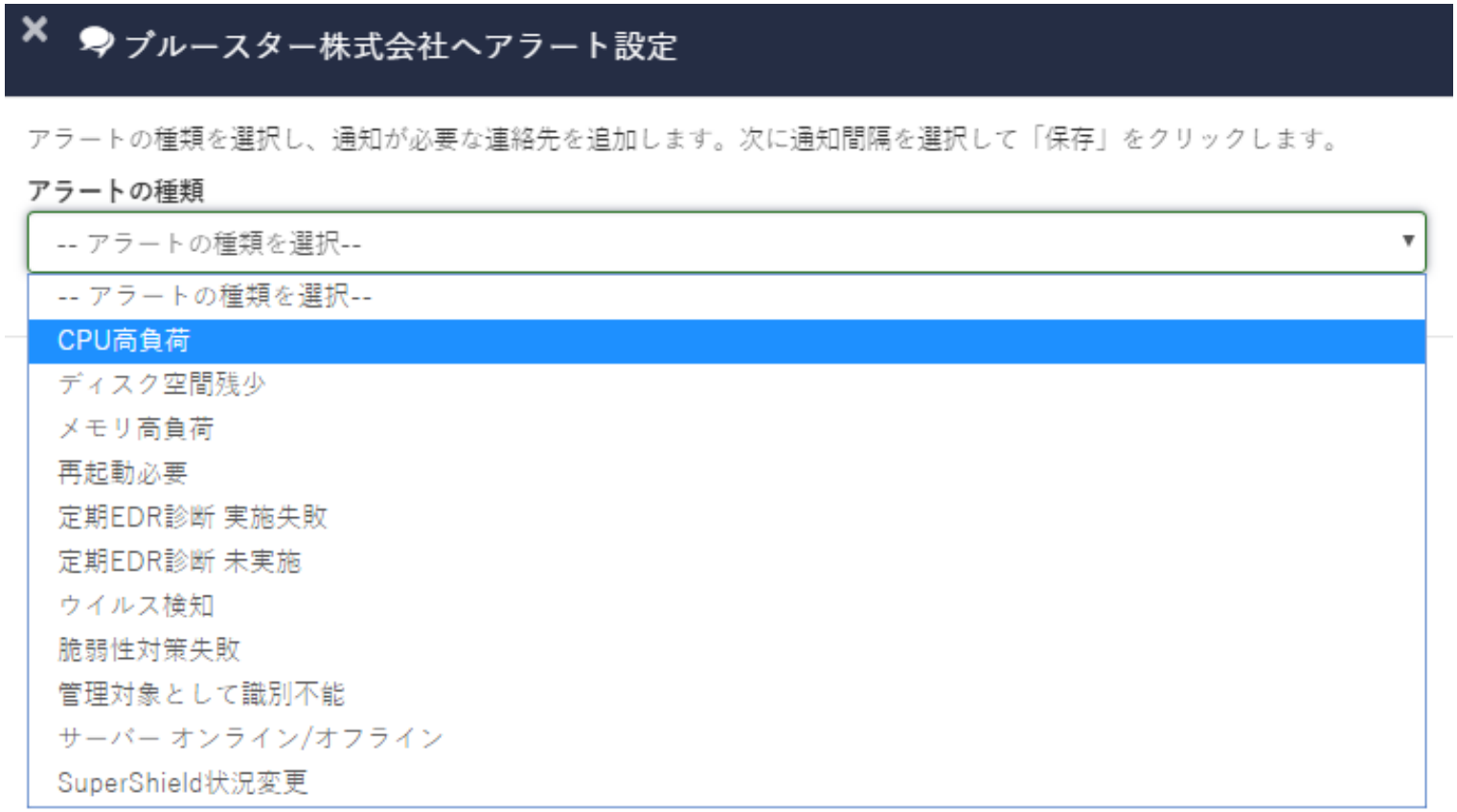
ExcelやWordファイルを開く前に感染有無をチェックし、有害なものは自動的に無害化処理をし、利用者は特別な対処は不要です。

他社の次世代セキュリティソフトが感染を許した、emotetもPC Maticは阻止を確認しています。

後出しジャンケン方式だから、添付ファイルも考えずに開いて大丈夫！

Copyright © 2023 Bluestar Corporation.

LET ME KNOW:使いやすい！　アラート機能



パソコンがウイルス感染した際やハードディスク残量が少なくなった際など多様なアラート通知もマイページで設定いただけます。

高いCPU負荷率、HDD空き容量不足、脆弱性パッチ適用失敗など運用しやすく設定しやすい！

Copyright © 2023 Bluestar Corporation.

EDR（Endpoint Detection and Response）

EPPによる防御に加え、パソコン内のファイルを低負荷状態の場合および、スケジュールにて設定された間隔で検索をし、悪質なファイルをMD5にて検索・照合します。

パソコン内に導入されている全アプリケーション一覧をスケジュール設定された間隔で取得することができ、脆弱性を抱えるアプリケーションを強制的にアップデートすることが可能です。

EDR:(予防:記録) ドライバ自動更新
EDR:(予防:記録) 著名ソフトウェア自動更新
EDR:(記録) 起動アプリケーションログ記録
EDR:(記録) 稼働サービス一覧取得
EDR:(記録) 稼働プロセス一覧取得
EDR:(記録:駆除) アドウェアや迷惑アプリ(PUA)削除
EDR:(記録:駆除) 悪質なブラウザアドオン削除
EDR:(記録:駆除) 悪質ファイル(Virus,Spyware)検索
EDR:(回復)　　バックアップとリストア

Copyright © 2023 Bluestar Corporation.

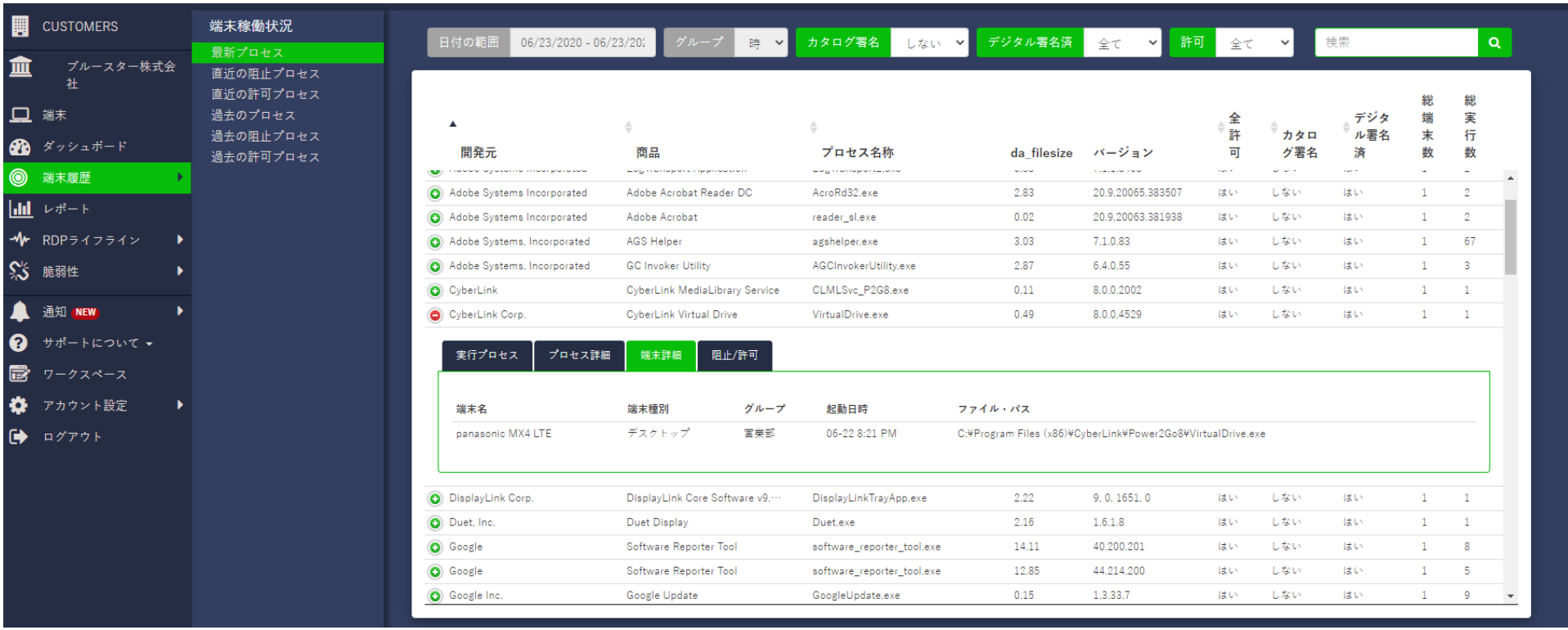
EDR:スナップショットが取得可能。サポートに強い

顧客対応の必要があるMSP事業者様においては、顧客が指定した間隔もしくはサポートにてオンデマンドにてパソコンのスナップショット記録が可能です。スナップショットによって取得される情報は以下のとおりです。これを利用して、顧客に発生している問題点を突き止め、解決に結びつけることができています。

- 稼働中のサービス
- 稼働中のプロセス
- 導入済ドライバ一覧
- 導入済アプリケーション一覧
- 悪質なファイル検査(ウイルス検査、PUP、悪質ブラウザプラグイン)
- 脆弱な著名アプリケーション(Java, Flash,FileZillaなどの古い版)
- パソコン製造元、モデル、BIOSバージョン、搭載メモリ･･･
- CPU負荷率、メモリ使用率、Cドライブ空き容量、etc･･･

Copyright © 2023 Bluestar Corporation.

EDR:組織内全稼働プロセスの把握

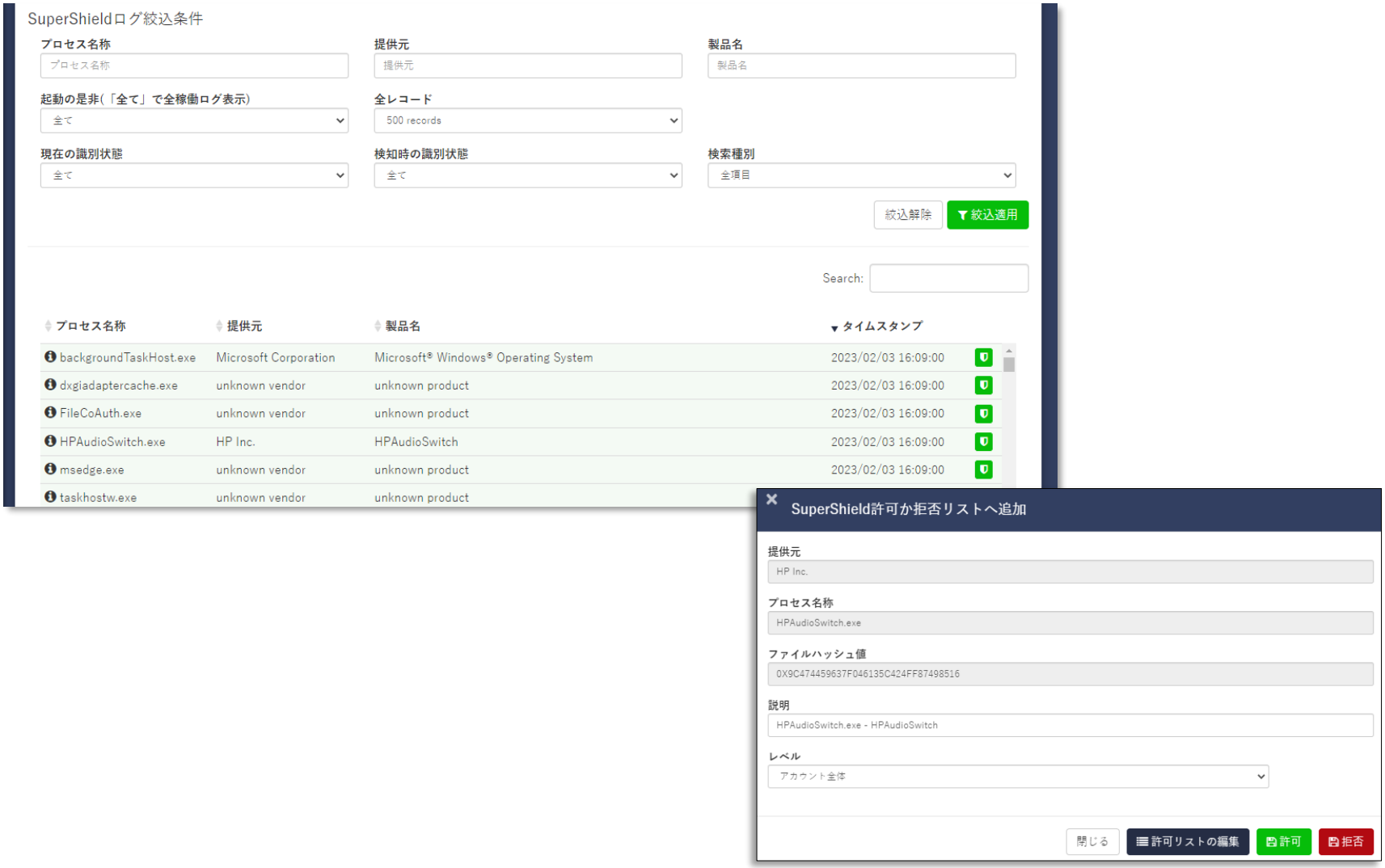


本機能は、企業・グループ・端末ごとに利用されている全プロセスを把握することが可能です。3カ月分記録・保持されます。この情報を利用し、**許可しないアプリケーションを把握し、それを従業員が勝手に利用させない制御が可能**です。

導入済アプリケーション一覧よりも正確な情報を把握することが可能です。

Copyright © 2023 Bluestar Corporation.

EDR:起動ログでウイルス感染時の分析が可能



どのようなウイルスによる影響を受けたのか、また起動を阻止されたファイルが何であるかを的確かつ即座に把握可能です。クラウド上に保管されます。
社外であっても社内同様に端末管理が可能です。

Copyright © 2023 Bluestar Corporation.

WebShield:強力なブラウザー保護

エンドポイント保護(EPP)やEDRでは防ぎきれないブラウザー内の脅威が急増しています。

ホームページを閲覧するだけで、警告音がして「ウイルスに感染しました」と至急電話を促す画面が表示されたり、仮想通貨をマイニングするなど、ブラウザーを通じた様々な悪質行為が散見されるようになりました。しかしこれらは、Windows標準では防止されませんし、一般的なセキュリティソフトでも対象外となっています。

また、正規のECサイトがハッキングされクレジットカード情報などをスキミング行為を行うよ「Webスキミング」なども流行しています。これらは、ブラウザー内で完結するため、パソコンに常駐するセキュリティソフトでは対処できません。

Chrome, Edge, Firefoxへブラウザ拡張機能を提供し、悪質なものを非表示や防御しています。

- バナー広告非表示
- 動画再生中の動画広告スキップ
- テクニカルサポート詐欺サイトへの誘導阻止
- 不正広告ネットワークによるアダルト・違法広告非表示
- 金融機関や有名ECサイトに似せた詐欺サイトへの誘導阻止
- 不正侵入防止
- 不正スクリプト実行阻止
- プライバシー侵害スクリプト阻止
- 仮想通貨マイニングスクリプト実行阻止
- スクリプト型Webスキミング防止

など

Copyright © 2023 Bluestar Corporation.

資産管理(RMM)もできる

PC Maticで管理しているパソコンの情報をパソコンいつでもどこでもご覧頂けます。

パソコン資産管理、アプリケーションやドライバの更新状況、ウイルス感染の有無や、レジストリクリーニング状況など多岐にわたる詳細な情報や、CPU負荷状況、ハードディスク使用状態、インターネット速度なども把握することができ、離れた場所にいる両親や友達のパソコンであっても管理しているパソコンの情報を手に取るように把握していただけます。

- 顧客別専用インストーラの生成
  インストールすると顧客コード・部署コードが自動的にアサインされます
- PC Matic Supershield
  ADを通じての一斉インストール、稼動状況把握、ホワイトリストの定義
- 脆弱性対策
  アプリケーションアップデート、ドライバアップデート
- ＰＣチューニング（最適化）の実施・休止の全体・個々への詳細定義
  ディスク最適化、マルウェアスキャン、システム復元ポイントの最適化、不要な一時ファイル削除、レジストリ最適化、インターネット設定最適化、パフォーマンス最適化、サービス最適化、不必要なスタートアップの休止
- パソコン稼動状況の把握
  CPU処理速度、CPU負荷率、メモリ利用率、ディスク空容量率
  利用中のドライバ、稼働中のサービス一覧
- USBメモリ、SDカード、外付けHDDの利用制御
- パソコンの再起動
- パソコンへの遠隔操作
  顧客サポートに有効
- IT資産管理
  ベンダー名、モデル、CPU型番、搭載メモリ量、搭載メモリ仕様(DDR3L等)、搭載ディスク量など

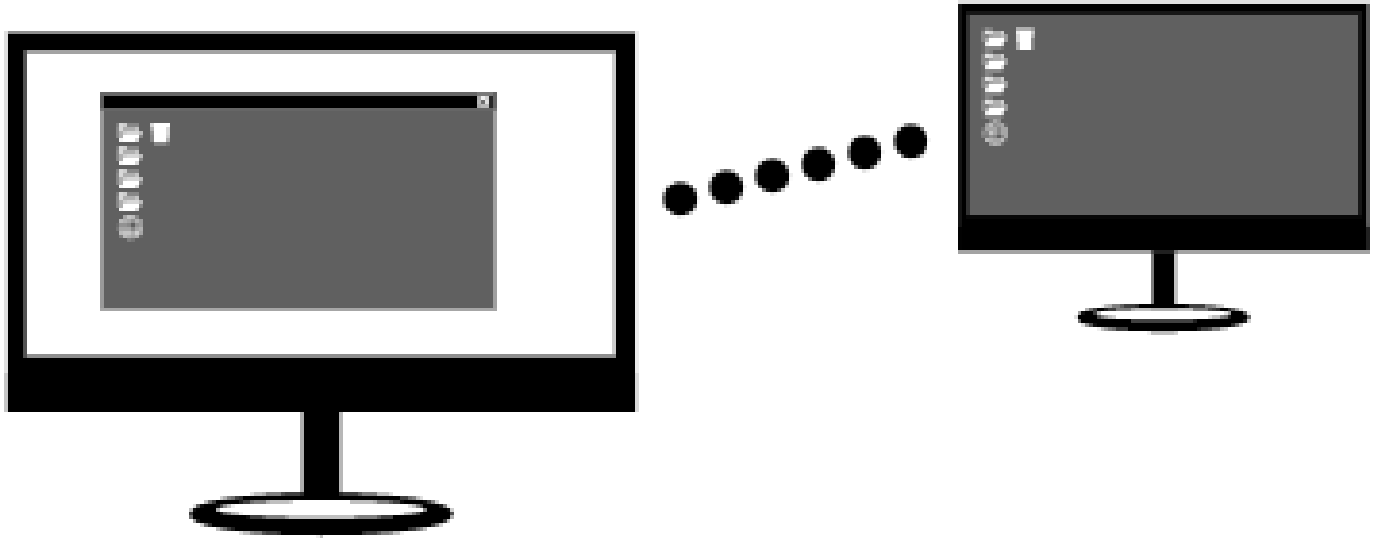
Copyright © 2023 Bluestar Corporation.

クラウド越しで詳細な状況把握

シングルダッシュボードで管理PCの状況把握、操作がすべて可能

Copyright © 2023 Bluestar Corporation.

OWN RDP:管理者用リモートデスクトップ機能



法人版はゼロタップ型リモートデスクトップ機能を搭載しています。
顧客PCの運用保守管理を行う事業者様には心強いツール

※リモートディスクトップ機能はインストールしないことも可能です。

Copyright © 2023 Bluestar Corporation.

FILE MANAGER:ファイル転送

管理対象端末との間でファイル転送や削除が可能です。

Copyright © 2023 Bluestar Corporation.

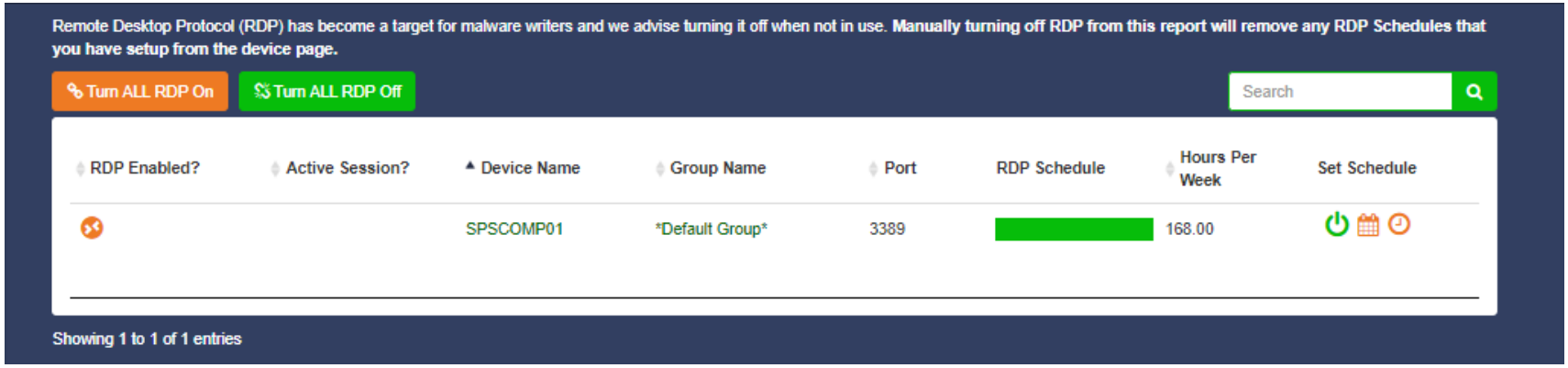
COMMAND:コマンドプロンプト実行

コマンドプロンプトによる柔軟かつ迅速な対応が可能です。
データ通信量も少なく様々なシーンでご利用いただけます。

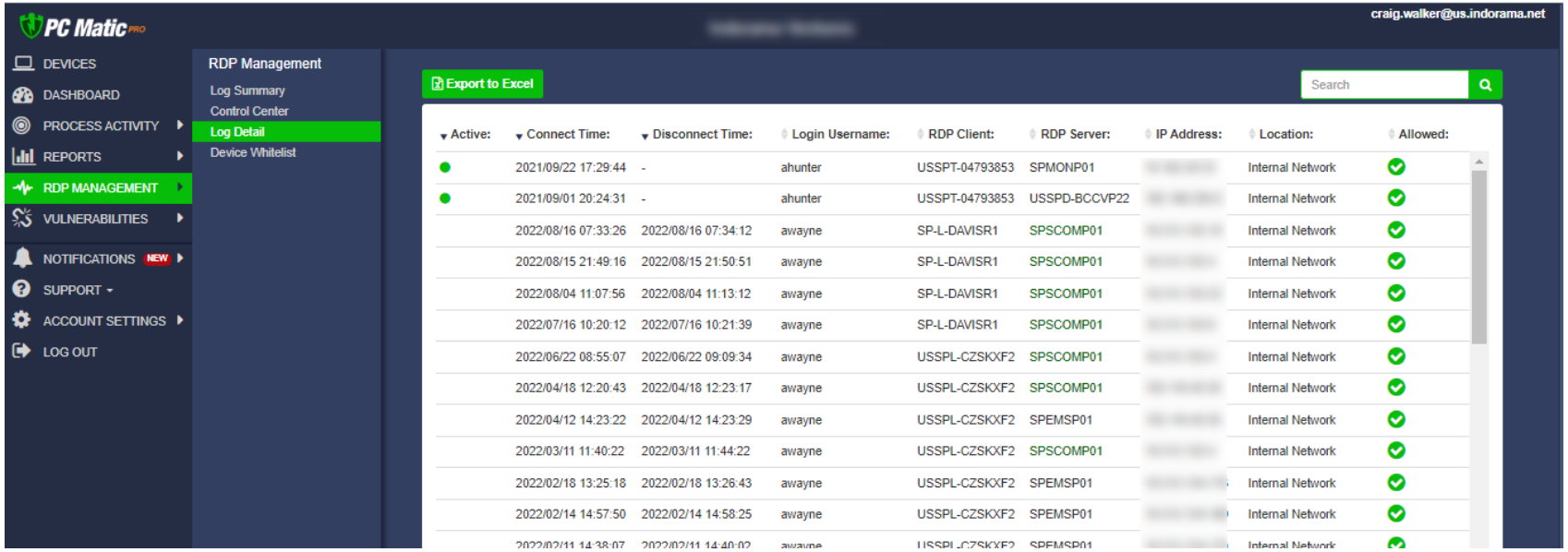
Copyright © 2023 Bluestar Corporation.

Windows RDP詳細制御・接続ログ

接続可能な曜日時間帯、接続可能端末、利用者制限が可能



接続ログの詳細な記録



Copyright © 2023 Bluestar Corporation.

USBメモリ等の大容量外部デバイスを制御可能

ATTACK SURFACE: 著名アプリとドライバ自動更新

脆弱性を抱えやすい著名なアプリケーションやドライバの自動更新機能も装備し、セキュリティ防御能力を高め、パソコンの安定性を向上させます。脆弱性対策が万全であればファイアーウォール機能はWindows標準のもので十分です。NIST SP 800 - 40準拠

ドライバ

ネットワーク: Intel, Broadcom, Atheros, VIA, Realtek
ディスプレイ: Nvidia, Intel, AMD (ATI), VIA
無線ＬＡＮ: Intel, Atheros, Broadcom, Realtek TP-Link
他ドライバ： サウンド、プリンタ、カードリーダ等

著名なアプリケーション

Adobe: Flash Player, Air, Reader, Shockwave
Oracle: Java
Browser: Chrome, Firefox, Opera
7-Zip, FileZilla, Foxit Reader, iTunes, Sea Monkey, Thunderbird, Open Office, Quick Time, Real Player, Skype, WinRAR, WireSharkほか多数

Copyright © 2023 Bluestar Corporation.

ソフトウェア資産管理・ハードウェア資産管理

ソフトウェア資産管理

Name		Quantity
7-Zip 22.00 (x64)	1	1
7-Zip 22.01 (x64 edition)	1	1
Adobe Acrobat (64-bit)	1	1
Adobe Illustrator CS5	1	1
Adobe Photoshop Elements 11	1	1
Adobe Refresh Manager	1	1
Alcorlink PCIE Card Reader Driver	2	1
ALPS Touch Pad Driver	1	1
AMD Chipset Software	1	1
AMD PSP Driver	1	1
AMD Ryzen Balanced Driver	1	1
AMD SBxxx SMBus Driver	1	1
AMD_Chipset_Drivers	1	1
ASUS Wireless Router Device Discovery Utility	1	1
Bing Wallpaper	1	1
BTup Service	2	1
Chrome Remote Desktop Host	2	1
Common Components for Panasonic PC	3	1
Common Components for Panasonic PC (x64)	4	2
CrystalDiskMark 8.0.4	1	1
CyberLink Power2Go 8	1	1
CyberLink PowerDVD 10	1	1
D3DX10	1	1
Dashboard for Panasonic PC	2	2
Definition Update for Microsoft Office 2010 (KB3115475) 32-Bit Edition	1	1
DREAMHIVE DH-APPLI GrepReplace!	1	1
Dropbox	1	1
Dropbox Update Helper	1	1
e-Taxソフト(WEB版) 事前準備セットアップ (Windows利用者向け)Ver1.22.1	1	1
Elements 11 Organizer	1	1
Energy Star	1	1
FileZilla 3.62.2	1	1
Google Ads Editor	1	1
Google Chrome	7	6
HOLDモード設定ユーティリティ	2	2
Hotkey 設定	2	1
HP AC Power Control	1	1

ハードウェア資産管理

Platform	Manufacturer	Model	Quantity
Desktop	BESSTAR TECH LIMITED	JB95	1

Computer Name	Alias	Serial	OS Version	BIOS Date	PC Matic Date	Group Name
DESKTOP-8IVS1ER	前田皇帝PC	Default string	Windows 11 Professional x64	2021/09/22	2021/12/15	営業部門

Desktop	Default string	Default string	1

Computer Name	Alias	Serial	OS Version	BIOS Date	PC Matic Date	Group Name
DESKTOP-NKK2QMD	VOYO	Default string	Windows 10 x64	2015/12/24	2021/07/05	人事部門

Desktop	Fanless Mini PC	Quieter 3C	1

Computer Name	Alias	Serial	OS Version	BIOS Date	PC Matic Date	Group Name
DESKTOP-TC7D1K1	前田デスクトップ	Default string	Windows 11 Professional x64	2022/07/14	2023/01/30	営業部門

Desktop	LENOVO	11A9CTO1WW	1

Computer Name	Alias	Serial	OS Version	BIOS Date	PC Matic Date	Group Name
THINKCENTRE	坂本	PC1DLWA0	Windows 11 Professional x64	2020/08/24	2022/12/17	営業部門

Desktop	MeLE Computer	Quieter2	1

Computer Name	Alias	Serial	OS Version	BIOS Date	PC Matic Date	Group Name
MELE	会議室	Default string	Windows 11 Professional x64	2021/04/01	2022/12/13	営業部門

Laptop	HP	HP ENVY Laptop 13-ad1xx	1

Computer Name	Alias	Serial	OS Version	BIOS Date	PC Matic Date	Group Name
ENVY13		5CG7516CKR	Windows 11 Professional x64	2019/04/22	2023/02/03	企画部門

Laptop	LENOVO	20309	1

Computer Name	Alias	Serial	OS Version	BIOS Date	PC Matic Date	Group Name
SECPOINT		QB07131607	Windows 10 x64	2013/07/31	2019/05/08	開発部門

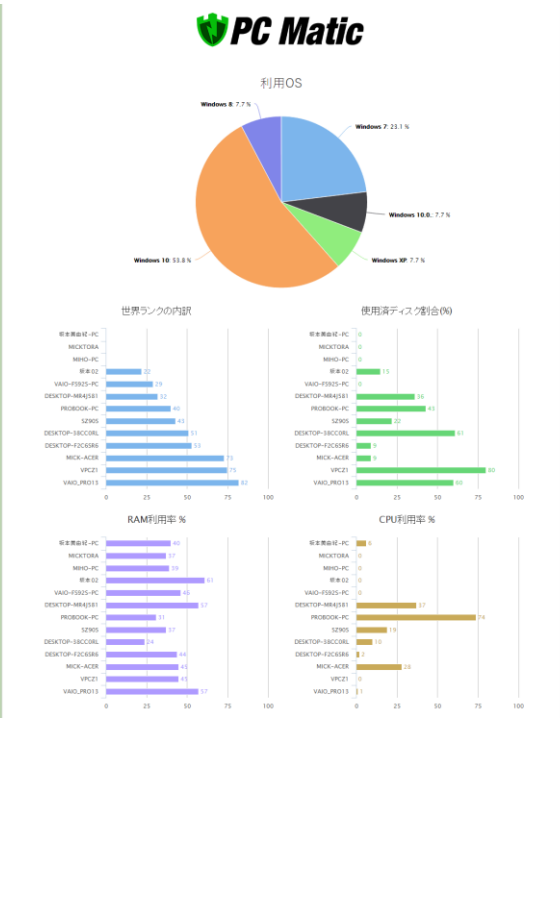
Laptop	Panasonic Corporation	CFMX4-1	1
Laptop	Panasonic Corporation	CFRZ4-1L	1

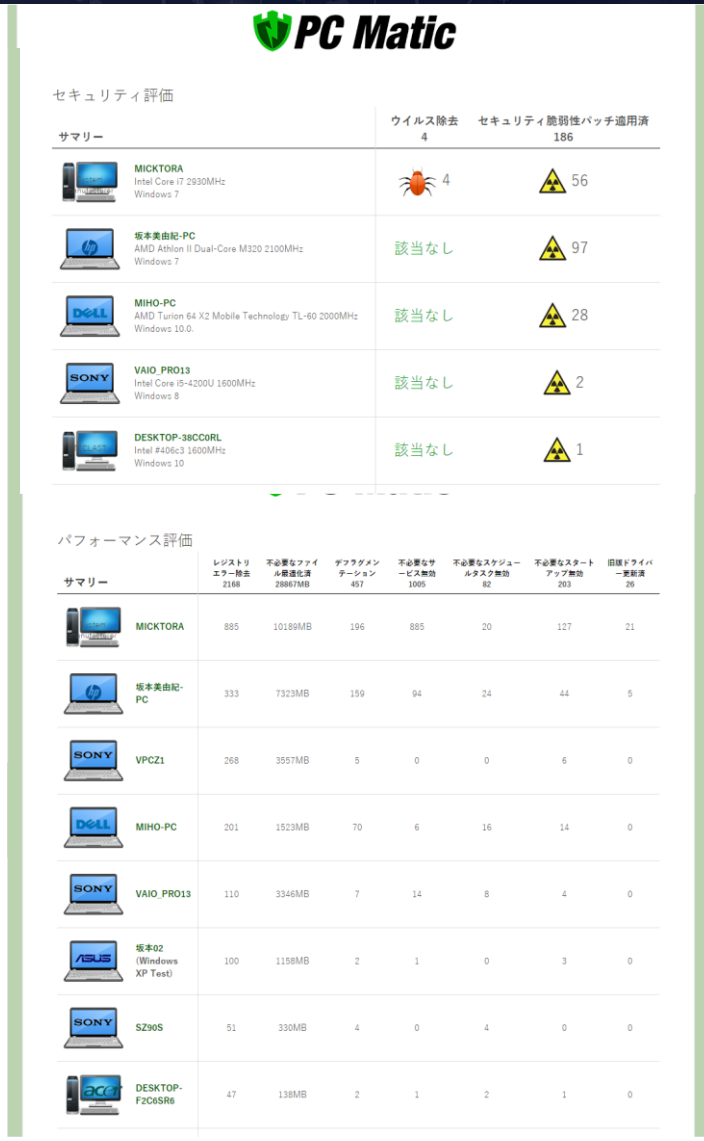
Showing 1 to 9 of 9 entries

組織単位で導入済ソフトウェアやハードウェアを把握でき、一覧をEXCEL形式でダウンロードも可能

Copyright © 2023 Bluestar Corporation.

GRANCE:強力かつ表現豊かな稼働状況レポート



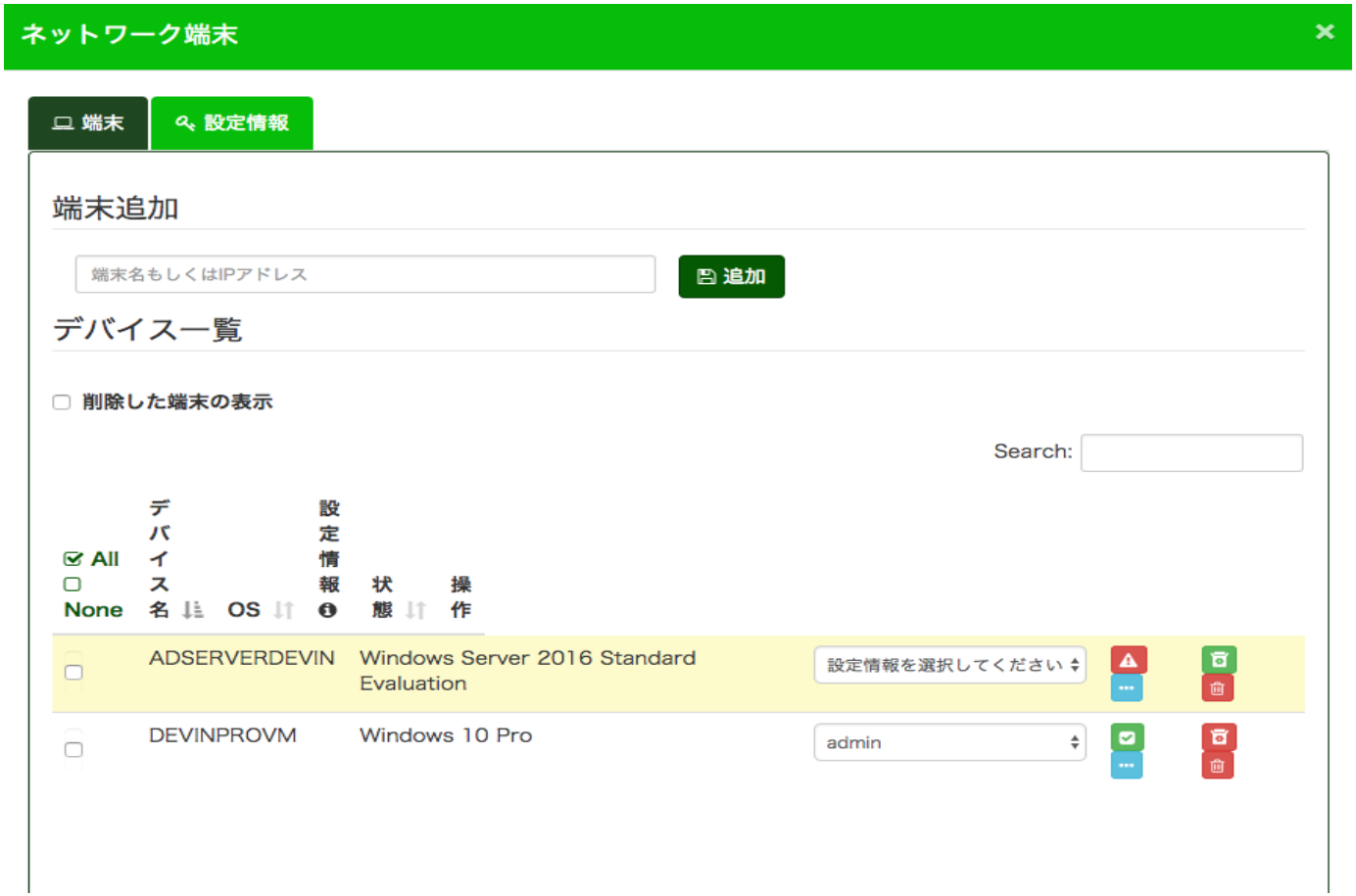


機種情報、機種別パスォーマンス状況、ウイルス駆除状況、レジストリ最適化実施状況、ドライバ自動更新数などをPCやスマートフォンよりご覧頂けます。

PDF出力可能なので、顧客へそのまま報告できます。

Copyright © 2023 Bluestar Corporation.

EASY TO DEPLOY: Active Directory連携で一斉導入



ActiveDirectory連携によるPC Maticの強制インストールが可能

Copyright © 2023 Bluestar Corporation.

HCL BigFix, Syslog連携

BIGFIX

BigFix端末へFixletsを用いてデプロイができ、BigFixと連携を行うことでエンドポイント管理の範囲が大きく拡張されます。

BigFix管理コンソールより、PC Matic PROの主要機能を操作することができます。

Syslog

TCP/UDP 514 (RFC 3164)などを用いて端末のsyslogを特定のサーバーへ送信することができます。

Copyright © 2023 Bluestar Corporation.

悪質なファイル簡易分析サービス

PC Matic 法人版のお客様へは、悪質と思われるファイルの個別分析を個別対応させて頂きます。

提出検体を分析

お客様にて入手された悪質と思われるファイルをA4で1枚程度で簡単な分析を日本人セキュリティエンジニアが行います。調査費用は、難易度に関わらず一律5万円+消費税です。感染した場合、感染元ファイルを分析するサービスになります。

PC Maticでは、原則24時間以内にブラック・ホワイトの分類を自動的に行いますので、自動的な処理に関して無償で管理画面より取得して頂けます。誤検知疑いの調査依頼はもちろん無償対応致します。

有償分析サービスの内容一例

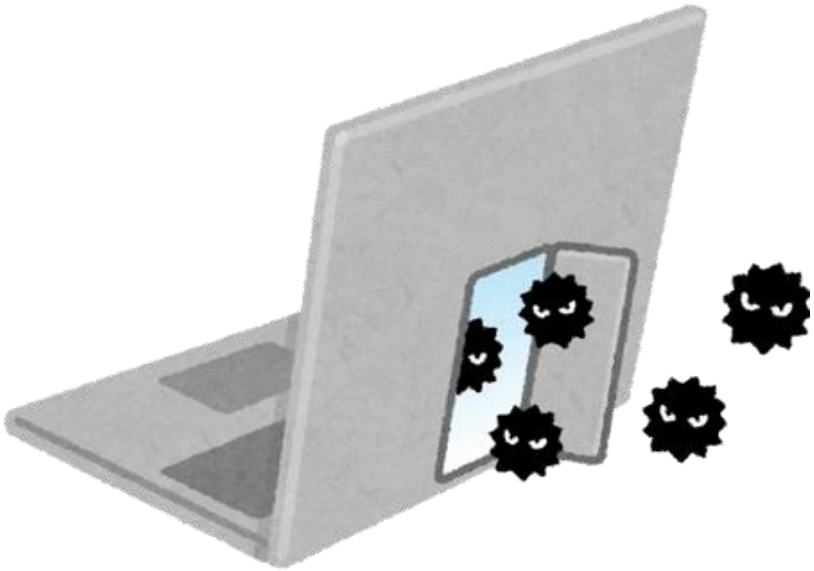
- 悪質性の有無
- 種類(スパイウェア,ボットネット,トロイの木馬等)
- ウイルス名称
- 推定製造国
- 推定される目的

詳細は、https://pcmatic.jp/pro/analysis/

Copyright © 2023 Bluestar Corporation.

脆弱性診断サービス

PC Matic 法人版のお客様へは、定期的な脆弱性診断サービスを実施させていただくことが可能です。



脆弱性スキャナで社内の脅威を診断

6万件を超える既知の脆弱性情報を基にHIPAA法、PCI DSS基準など必要に応じた水準での脆弱性診断を検査ツールを用いて調査します。

Wi-Fiの脆弱性診断にも対応し、ビルに侵入しなくても近隣ビルからの社内ネットワーク侵入が可能かの診断も可能です。

診断料金は、対象となるネットワーク機器数と事業所数、ネットワークセグメントなどの組み合わせによりお見積りさせて頂きます。

定期的な実施によりパソコンはもとより、様々なネットワーク機器の脆弱性を洗い出すことが可能です。

詳細は、https://pcmatic.jp/pro/analysis/

Copyright © 2023 Bluestar Corporation.

MDRセキュリティ状況監視サービス

PC Matic 法人版のお客様へは、標準で米国本社による365日24時間の感染監視サービスを標準サービスにてご利用頂けます。

また日本国内(京都烏丸SoC)から日本人による、セキュリティ上の問題点の指摘や専門家による監視サービスを個別契約によりご利用頂けます。

京都三条セキュリティ・オペレーションセンター:
販社様へ卸売（1拠点10台より契約可）

セキュリティ専門家による監視(常駐/京都三条SoC)

お客様のパソコン稼働状況において問題が発生していないか、PC Matic SuperShield利用状況ログ(EDR)や稼働プロセスを用いて監視を行います。

監視・実施内容一例

- 監査状況の常時監視
- ブラック・ホワイト判定とローカルリストへの迅速追加
- スナップショットによる問題点の有無確認
- スナップショット内容(稼働サービスとプロセス)
- スナップショット内容(不審なアプリケーションの有無)
- スナップショット内容(不審なサービスやドライバの有無)
- 月次運用状況報告書

など

詳細は、https://pcmatic.jp/pro/analysis/

Copyright © 2023 Bluestar Corporation.

感染時の現地分析と対応策提案

PC Matic 法人版のお客様へは、悪質と思われるファイルの個別分析を個別対応させて頂きます。

感染時の現地分析と駆除

国内外問わず、現地へ駆けつけて感染経路や方法の分析を行います。PC Matic稼働クライアントのみならず、NC工作機やネットワーク機器などが感染した場合においても、感染経路や種類の特定などを解決までお客様と共同作業として日本人セキュリティエンジニアが迅速に行います。

対応策の提案

前項目にて分析された結果、今後の感染を防止するための防止策をベンダーニュートラルな立場で複数提案致します。

詳細は、https://pcmatic.jp/pro/analysis/

Copyright © 2023 Bluestar Corporation.

パソコン快適化機能も搭載（Windowsのみ）

PC Maticは世界中の利用者の稼働状況をもとにしたビッグデータを基にした安定性を目的に作られたパソコン快適化機能を有しています。

使い続けていると遅くなってくるWindowsパソコン。
性能低下によって引き起こされる労働生産性を低下を抑制するべく、パソコン快適化機能を実装しています。

快適化は、決め打ちではなくビッグデータによる機種毎や利用環境にあわせた最適化が行われ、不具合が発生する確率を極端に下げています。

- 不必要なファイル削除
- 不要スタートアップ削除
- ネットアクセス最適化
- デフラグ機能
- ドライバ自動更新
- 著名アプリ自動更新

Copyright © 2023 Bluestar Corporation.

PC Matic 法人版ラインナップ

	PC Matic PRO 法人版	PC Matic PRO Embedded 組込版	PC Matic MSP マルチテナント版	PC Matic federal 政府機関版
想定利用対象	法人、NPO、 社会基盤企業	製造業	大企業、MSP事業者、 個人事業主	政府機関、軍、 地方自治体
最低台数	10	10	5	100
複数企業管理	×	×	○	○
クラウド型	○	○	○	○
オンプレミス型	×	×	×	○
初期費用	不要	不要	不要	個別見積
月間基本料金	不要	不要	不要	基本運用費
契約期間	年次契約 (1～5年)	想定機器寿命契約 (1～15年)	毎月自動更新	年次契約 (1年のみ)
同一アカウントで 利用年次の異なる運用	×	×	○	×
価格決定要素	契約年次、台数	寿命、台数、Offlineか	実稼働台数	台数
最低台数での 利用価格感	数万円/年	Online: 数万円/年 Offline, Intra: Onlineの半額	数百円/月	PC Maticクラウド: 数十万円/年 プライベートクラウド:数億円/年 オンプレ: 数億円/年
販売体系	販社/直接	販社/直販	直販	federal版 指定販社
支払方法	請求書	請求書	クレジットカード	請求書
エンドユーザ 問い合わせ先	PC Matic サポート窓口	PC Matic サポート窓口	MSP事業者様	PC Matic 専任チーム

Copyright © 2023 Bluestar Corporatic

4つの法人製品

PC Matic PRO

販社経由一般製品

本製品は、自動運用で安全・迅速かつ簡単な方法で最高水準のセキュリティとIT資産管理を提供します。ライセンス認証キーを利用した一般的な法人向けのセキュリティ対策と同一です。

想定対象企業:企業全般、学校法人、医療機関、政府とその関連機関、団体など

PC Matic MSP

MSP事業者向け

PROのマルチテナント版。次世代エンドポイントセキュリティと強力な運用管理ツールが統合したパソコン運用サポートツールです。グローバル企業の情報システム部門子会社がグループ企業に対して包括的な提供を行う際にもご利用頂けます。

想定対象企業:マネージドサービス事業者、事務機器販社、グローバル企業の情報システム子会社、プロバイダなど

PC Matic FEDERAL

政府機関向け

オンプレミス・クラウド両対応製品。グローバル・ホワイトリスト利用可否を選択可能。

想定対象企業:国際的な企業、政府機関など

Copyright © 2023 Bluestar Corporation.

産業機器組込用途 PC Matic PRO Embedded

【調達容易】

- ライセンス料は製造時の一括支払いでOK

【導入簡単】

- インストール時は、オンラインが必要。1分程度で完了

【稼働時のメンテナンスも容易】

- プログラム差し替え時に、ホワイトリスト更新の必要なし
- 「デジタル署名」や「ファイルパス」で起動指定可能

他社

バイナリー形式

プログラム　　ホワイトリスト

プログラムとホワイトリストの
両方を差し替える必要がある

ファイルレス暗号化ウイルスにより影響を受ける

PC Matic Embedded PRO

バイナリー形式/スクリプト形式

プログラム

プログラムのみを差し替えればいい

ファイルレス暗号化ウイルスを完全阻止

【オンライン保守】（緊急時にオンライン接続で対応）

- 管理者リモートデスクトップで即座に画面共有
- ファイルマネージャでファイル送受信
- 遠隔コマンドプロンプトを利用可能
- EDRスナップショットで稼働中プロセス一覧を取得可能
- EDR稼働ログで不審なプロセスの稼働履歴を把握可能

Copyright © 2023 Bluestar Corporation.

結論

Conclusion

- PC Maticは、使いやすさを維持しながら、優れた最新のアプリケーション・ホワイトリスティング方式のセキュリティを実現します。
- PC Maticの全顧客で共有される1億件以上が登録済のグローバルリストでブラックリスト方式と変わらない運用の容易性を持ち、顧客企業が独自に利用可能なローカル・ホワイトリストで即時性を発揮します。
- これら２つのホワイトリストは、進化するサイバー脅威に対して、最高のパフォーマンスを発揮するために相互補完しています。
- ローカル・ホワイトリストへの追加は簡単で、即座に反映されます。
- PC Maticのアプリケーション・ホワイトリスティングにより、組織を柔軟かつ効率的に管理することが可能です。

Copyright © 2023 Bluestar Corporation.

開発・発売元:PC Matic, Inc.

PC Matic, inc.

本　　社:	アメリカ合衆国	アイオア州
マーケティング拠点:	アメリカ合衆国	サウスダコタ州
研究開発拠点:	アメリカ合衆国	サウスキャロライナ州

Founder & Owner: Rob Cheng
元ゲートウェイPC 最高マーケティング責任者(CMO)

PC Matic, Inc社設立の理由

PC Matic, Inc社設立者であるRob Cheng(ロブ・チェン)は、パソコンベンダー「ゲートウェイ」社の上級副社長であり、マーケティングと顧客サポートの責任者でした。

高性能なパソコンを安価に提供していた同社は、数年後に顧客から「使っているうちにパソコンが遅くなってきた」「ウイルスに影響されたので駆除して欲しい」といったパソコンの故障でない問題が顧客サポートに寄せられ、そのサポートコスト負担に悩んでいました。

顧客が抱える問題や利用環境は様々。またパソコンもモデルにより利用されているドライバも異なる。この解決方法にインターネットを活用できないかと考え、PC Maticを開発しました。

パソコンの修正箇所の特定やセキュリティ対策をビッグデータを用いた診断を通じて、その解決策を提供し続けることを社是に、パソコン本来の性能を引き出すセキュリティソリューションを提供し続けています。誕生秘話:https://pcmatic.jp/about/info/

Copyright © 2023 Bluestar Corporation.

政府・軍基準を搭載した新方式の
統合型セキュリティスィート

PC Matic PRO

EPP:エンドポイント保護

EDR:エンドポイント検出応答

RMM:端末運用管理

Performance:パソコン快適化

Application Whitelisting (NIST SP 800-167)