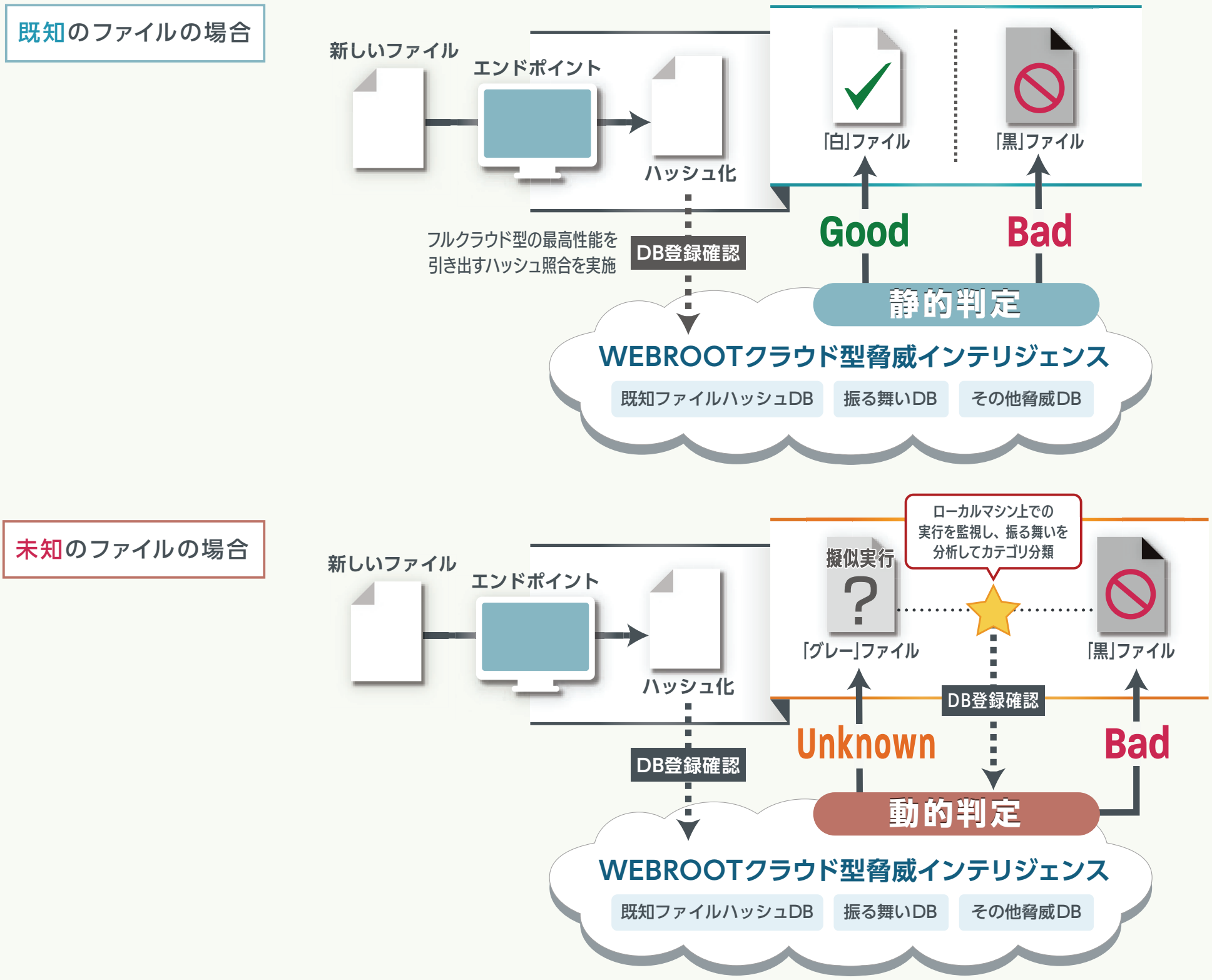
マルチベクトル型の脅威に対応した高度な保護対策を提供

WEBROOT SecureAnywhere®

ビジネスエンドポイントプロテクション

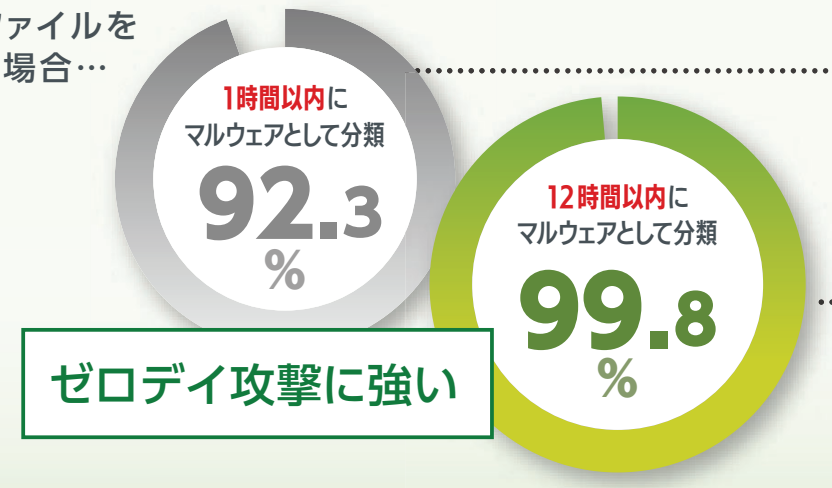
【特徴】
- ハッシュベース・フルクラウドの超高速・軽量セキュリティ
- 定義ファイルのアップデート不要/ 常に最新の保護を提供
- 他のウイルス対策製品と競合なし/ トライアル・展開が容易
- グレー判定による未知の脅威対策/ 標的型攻撃に感染した場合を想定
- サーバー投資のいらないSaaS型管理コンソール

独自アーキテクチャ「リアルタイム脅威モニタリング」



▶未知の脅威でも最短1時間以内、最大12時間以内で対応

未知のファイルを
検出した場合…



「未知のファイル」として判定した「グレー」ファイルの
92.3%を、1時間以内にマルウェアとして分類します。

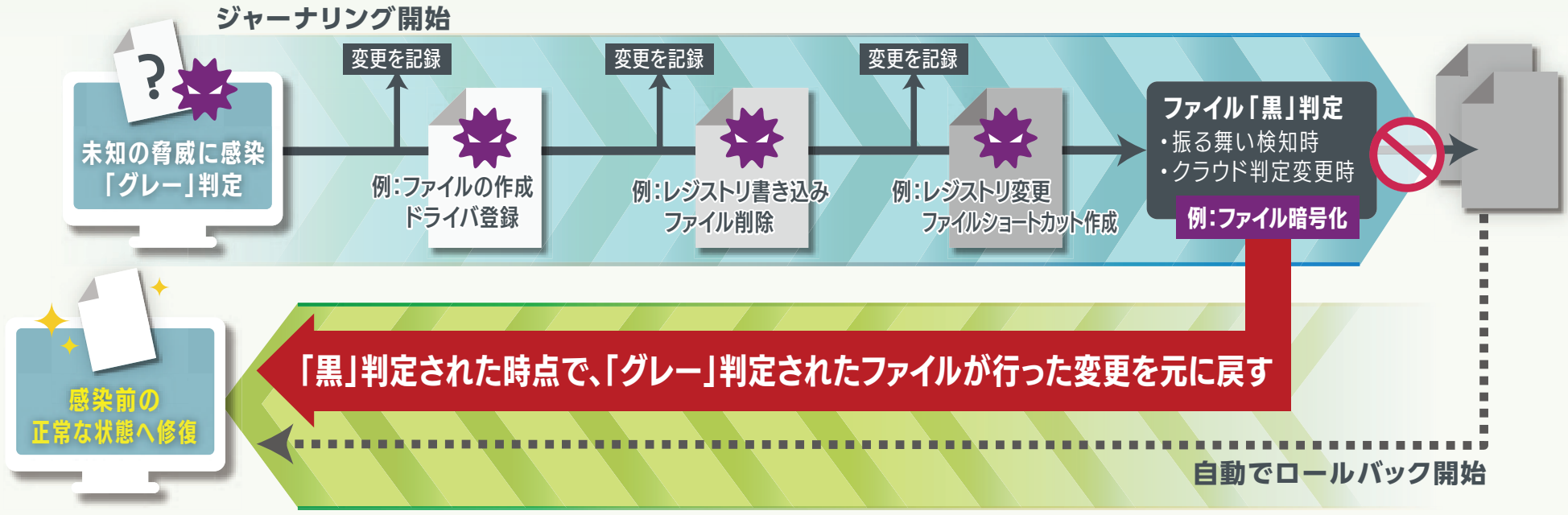
さらに12時間後には 99.8%のファイルを
マルウェアとして分類することが可能です。

ゼロデイ攻撃に強い

WEBROOT
an opentext company

ジャーナリング&ロールバックによる「自動修復機能」

「グレー」→「黒」判定と同時に、ファイルを攻撃前の状態に復元。



追加コストなしでエンドポイントの一元管理が行えます。

直感的な状況把握ができるSaaS型管理コンソール

インターネットの接続さえあれば、どこからでも 管理・制御が行えます。

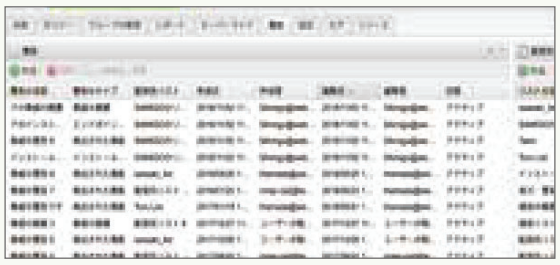
－グループ・PCの一元管理　－ポリシーの設定
－ホワイト・ブラックリスト管理：許可（白）、拒否（黒）、監視（グレー）から選択
－ログ/レポーティング　－遠隔操作：スキャン、シャットダウン、再起動など

パフォーマンスに影響がないエンドポイント

インターネットの接続さえあれば、一元管理下に置かれます。

－定義ファイルの更新を社内の管理サーバーから受信する必要なし

【脅威の検出ログ例】



管理コンソールから登録されている全ての端末から検出された脅威がログに残ります。このログを活用して、具体的にどのマルウェアがどの端末に、どんな影響を与えたかを確認することができます。例えば“Adware”が多いのであれば、該当端末を利用中のユーザーに広告系のサイトへの接続を止めるよう周知するなど、様々な対応が可能であると共に、管理コンソールからの確認、およびCSVファイルとしてデータを抽出し、管理者が活用することも可能です。

【提供要件】

PC
- Windows® 10：32ビットおよび64ビット
- Windows® 8/8.1：32ビットおよび64ビット
- Windows® 7：32ビットおよび64ビット
- Windows Vista®：32ビットおよび64ビット
- Windows® XP** 3：32ビットおよび64ビット
- Windows® XP** Embedded
- macOS® X 10.7 (Lion®)/10.8 (Mountain Lion®)
- macOS® X 10.9 (Mavericks®) / 10.10 (Yosemite®)/10.11 (El Capitan®)
- macOS®10.12 (Sierra®) /10.13(High Sierra®)/ 10.14 (Mojave®)/10.15(Catalina®)

**必須条件：SHA-2への対応

サーバー
- Windows Server® 2012 R2 Standard/Essentials
- Windows Server® 2008 R2 Foundation/Standard/Enterprise
- Windows Server® 2003** Standard/Enterprise、32ビットおよび64ビット
- Windows® Small Business Server 2008/2011/2012
- Windows Server® Core 2003**/2008/2012
- Windows Server® 2003** R2 for Embedded Systems
- Windows® Embedded Standard 2009 SP2
- Windows® XP Embedded SP1/Embedded Standard 2009 P3
- Windows® Embedded for POSバージョン1.0
- Windows Server® 2016 Standard/Enterprise and Datacentre

**必須条件：SHA-2への対応

VMプラットフォーム
- VMware vSphere® 5.5以前（ESX®/ESXi™ 5.5以前/ Workstation 9.0以前/Server 2.0以前
- Citrix® XenDesktop® 5/XenServer® 5.6以前/XenApp® 6.5以前
- Microsoft® Hyper-V® Server 2008/2008 R2
- VirtualBox

ブラウザ
- Google Chrome® 11以降
- Internet Explorer® バージョン7以降
- Microsoft Edge®（サポートは部分的）
- Mozilla® Firefox® バージョン3.6以降
- Safari® 5以降
- Opera 11以降

FAQ

Q.3MBと非常に小さなインストーラと数分のスキャンで、どのように動作し効果があるのでしょうか?

A.従来のアンチウイルスとはまったく違ったアーキテクチャで動作します。ウェブルートのクラウドシステムWebroot BrightCloud Threat Intelligence（BCTI）を利用し、ファイルを「白（安全）」「黒（悪性）」「グレー（不明・未知）」に分類しリアルタイムに判定します。また従来のアンチウイルスのように、定義ファイルを毎日数回ダウンロードし、既知の脅威をベースに作成される定義ファイルによるマッチング方式ではなく、常に更新されるクラウド上のデータベースによりファイルそれぞれのハッシュ値を判定および端末上のファイルの振る舞い判定を行うので、非常に軽快かつ効率的に動作します。

Q.インターネットに接続されていないオフライン時は保護されないのですか?

A.Webroot SecureAnywhere Business - エンドポイントプロテクションは、インターネット接続時に最も堅牢な保護を提供するのはもちろんですが、オフライン時にも十分な保護を提供します。エージェントはオフラインになる前にクラウドで照会したハッシュ値の「白/黒/グレー」判定結果をローカルにキャッシュしています。ローカルキャッシュにないもの、および振る舞い分析により「白/黒」判定されないものは「グレー」判定となり監視下に置かれます。またファイルが行う行動をすべてジャーナリングし、オンラインになった後で該当アプリがクラウドで「黒」であったことが判明すると検出し、すべての変更をロールバックします。

※その他のお問い合わせは右記をご参照ください。**https://www.webroot.com/jp/ja/support/support-business**

ウェブルート株式会社　www.webroot.com