

UTXのシグネチャー更新の仕組みと ゼロデイ対策

THE CHECK POINT ADVANTAGE

THREATCLOUD

世界中で動作する15万のセキュリティー・ゲートウェイを通過するトラフィックから日々脅威情報を収集

脅威情報を防御可能な情報に活用

リアルタイムに防御情報をアップデート



500,000,000以上
疑わしいファイルの
ハッシュやWebサイト

700,000 以上
日々のマルウェア
検知数

250,000,000
C&Cアドレス
(攻撃者のサイト)

17,000,000
サイバー攻撃の
検知数(週単位)

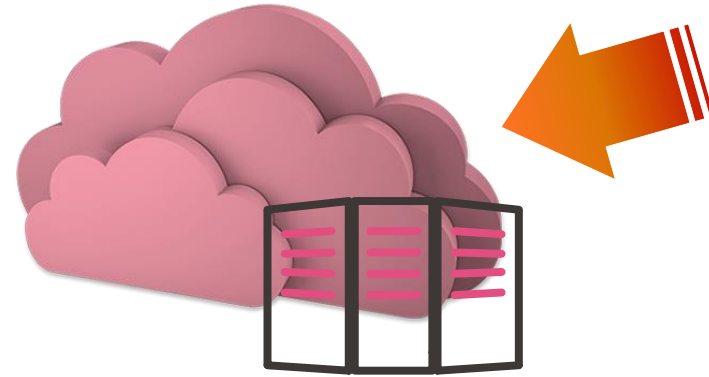
11,000,000
マルウェアの
シグネチャ

Agenda

- ・UTXのシグネチャー更新の仕組み
 - シグネチャデータベース配信
 - ゼロデイ攻撃への対策：Threat Cloud

シグネチャデータベース配信

- IPS
- アンチウイルス
- アンチボット
- アプリケーションコントロール



① シグネチャファイルは1日に複数回更新され配信サーバへアップロードされる

② UTXがシグネチャ配信サーバへ設定されたタイミングで定期的にお問い合わせを行い



③ 最新のシグネチャデータベースをダウンロード



昨今の脅威状況

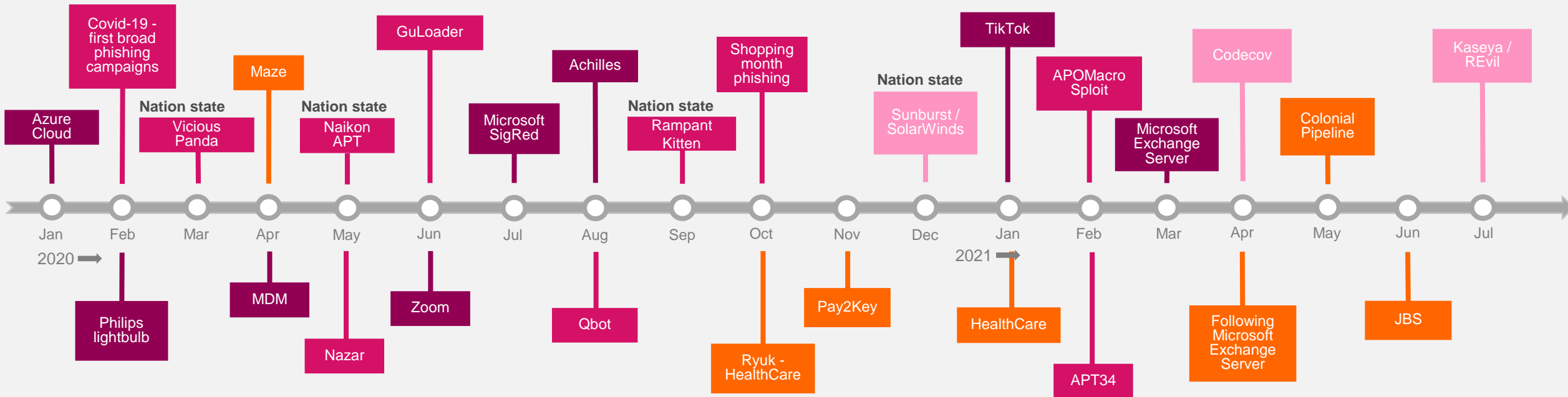


毎月...

400,000 を超えるゼロデイ攻撃*



- APT攻撃（高度標的型攻撃）
- サプライチェーン攻撃
- ラムサムウェア
- ソフトウェアの脆弱性



*According to ThreatCloud



THREATCLOUD

THE BRAIN BEHIND
CHECK POINT'S POWER



AI テクノロジー
30以上のAI・機械学習技術により
新たな脅威を特定・遮断する



ビッグデータ脅威のインテリジェンス
常に最新のIoC（侵害の痕跡）を取得し
最新の攻撃を正確に防御する

正確な PREVENTION
(MALICIOUS/SAFE)

テレメトリー

テレメトリー



ThreatCloud APIs



QUANTUM
Network Security



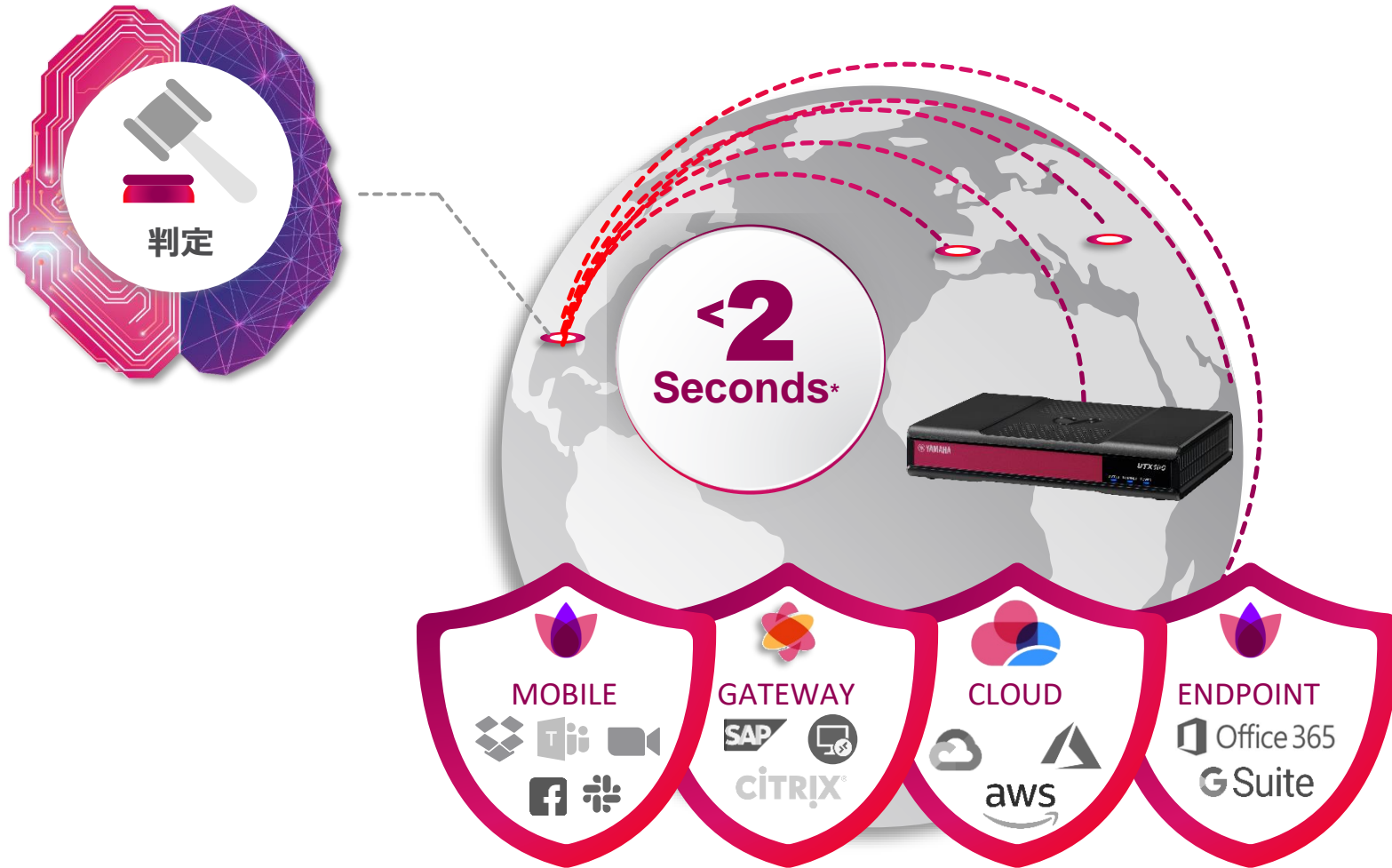
CLOUDGUARD
Cloud-Native Security

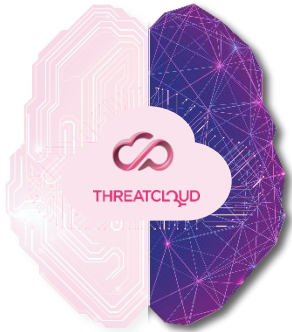


HARMONY
User & Access Security



脅威データベースはクラウド上でリアルタイムにアップデートされます





テレメトリによりリアルタイムで収集される脅威情報のビッグデータ
1日に数百万のIOC（侵害の痕跡）を解析



チェックポイントの
顧客及びプロダクト



150,000 のセキュリティー・ゲートウェイ

数百万のエンドポイントデバイス

2,000,000,000 の日々検査されるウェブサイトとファイル

WEBをクローलする外部フィードから脅威情報を取得

日々650,000の疑わしいドメインを検出する
独自の機械学習アルゴリズム

Patented

200人を超えるセキュリティ研究者、アナリスト、データサイエンスの専門家を擁するセキュリティ専門チーム

CPRによる研究、調査、解析によって発見される独占的なインテリジェンス



WindowsDNSサーバー上の
ワーム攻撃可能な重大な脆弱性

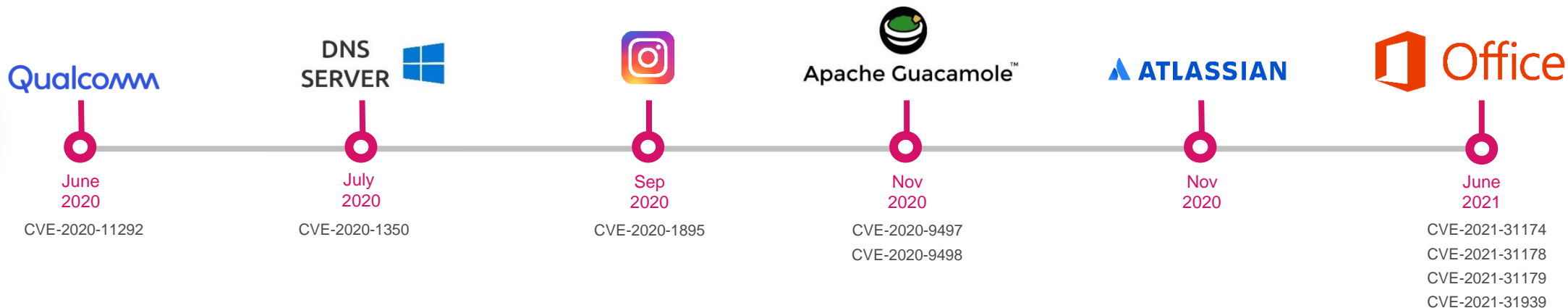


Qualcomm のチップセット
「Snapdragon」に含まれる
400を超える脆弱性



標的型攻撃で使用される
未知のランサムウェアPay2Key

重大な未知のソフトウェアの脆弱性からの即時保護



CPR によって発見された脆弱性に対するプロテクションはThreatCloudを通じて即時伝搬



ThreatCloud APIs



QUANTUM



CLOUDGUARD



HARMONY

No patch needed

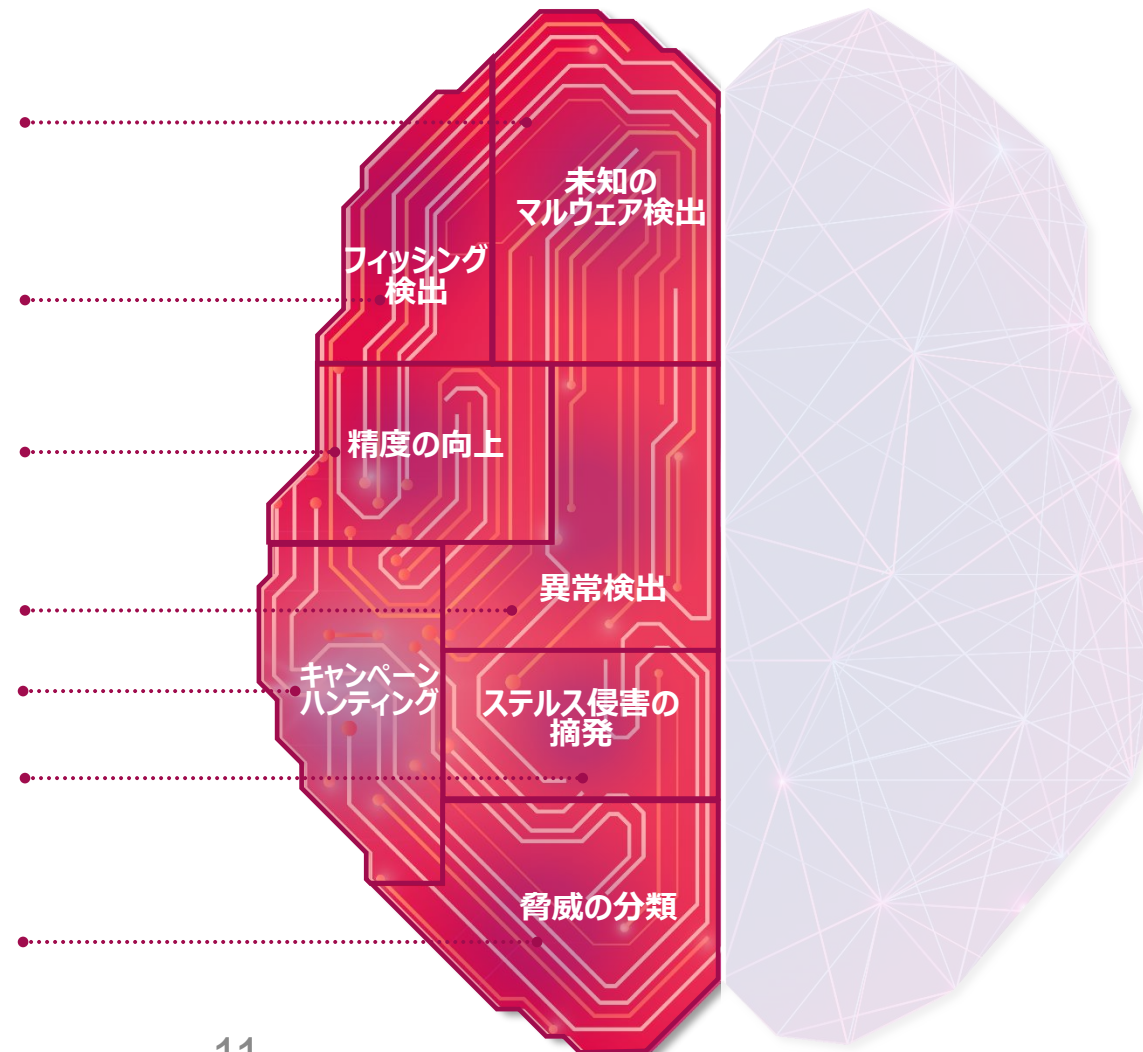


INFINITY VISION

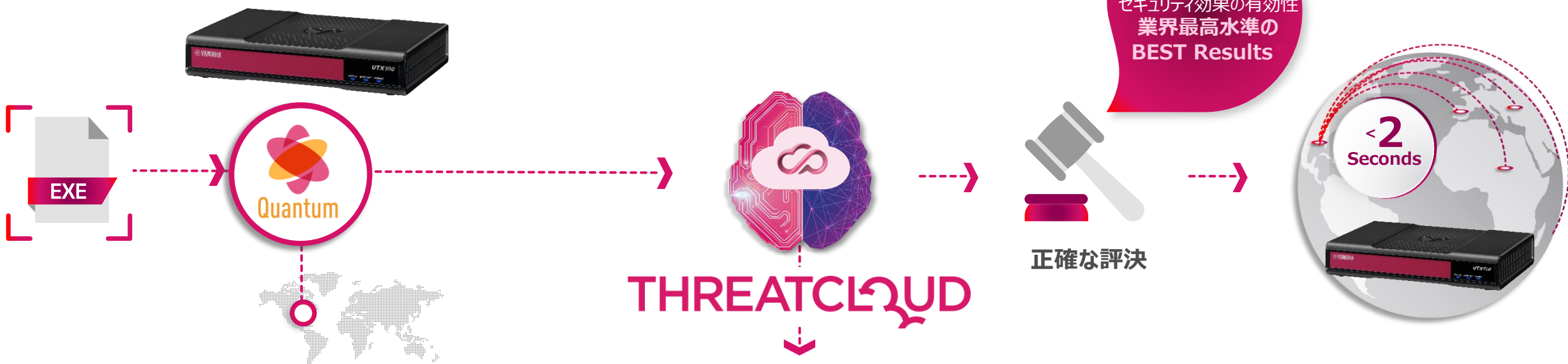


様々なセキュリティ機能に関する30以上のAI技術

- 感染ホスト検出
- サンドボックス静的解析
- サンドボックス動的解析
- メール静的解析
- モバイル・ゼロフィッシング検知
- フィッシング対策AIエンジン
- ネットワークAIエンジンアグリゲータ
- モバイルAIエンジンアグリゲータ
- 検証済み署名の機械学習
- クラウドネットワークの異常検知
- ThreatCloud キャンペーンハンティング
- アナリストマインド
- 悪意あるアクティビティの検出
- ドキュメントメタ分類器／ベクトル化ファミリー分類器
- ML類似性モデル
- MRAT分類器



Use case :ゼロデイマルウェアのブロック



98.4%
セキュリティ効果の有効性
業界最高水準の
BEST Results



60+ の検出エンジン

ディープラーニング ファイルレピュテーション

機械学習 エミュレーション ランタイム

評決 エンジン

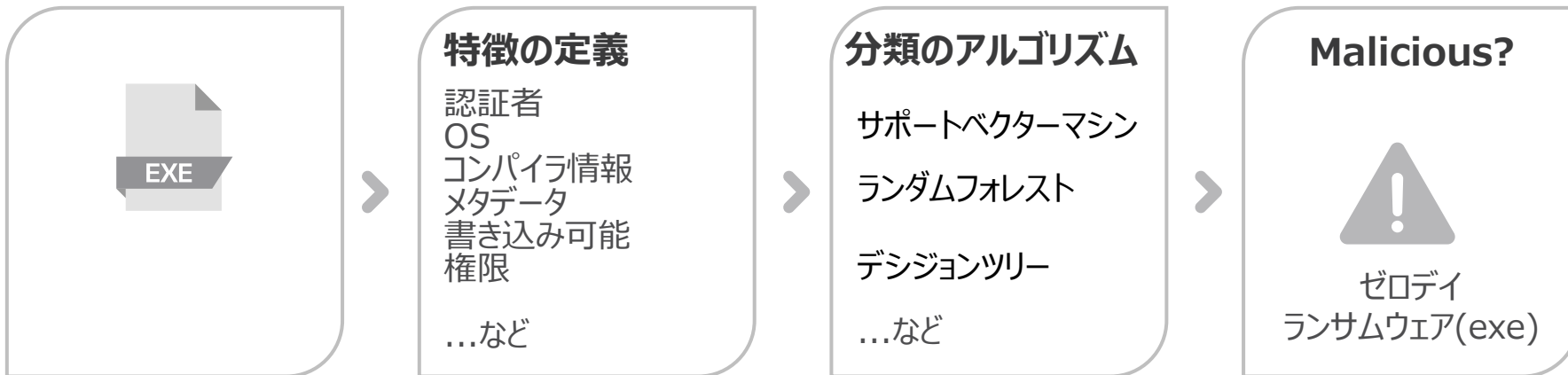
Machine Learning

ディープラーニングで誤検知を90%以上削減

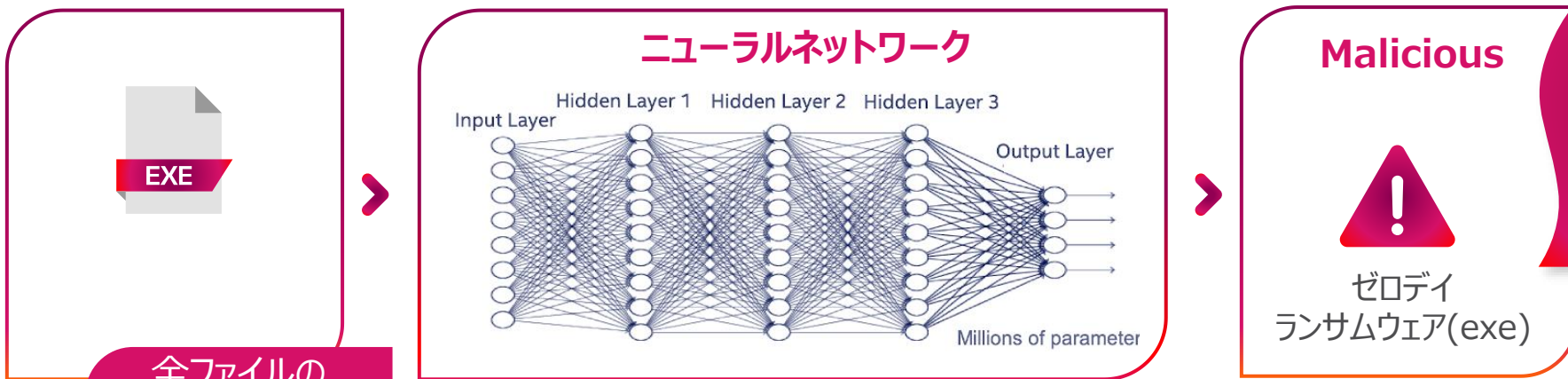
ThreatCloudの ディープラーニング vs クラシックな機械学習との比較



古典的な
機械学習



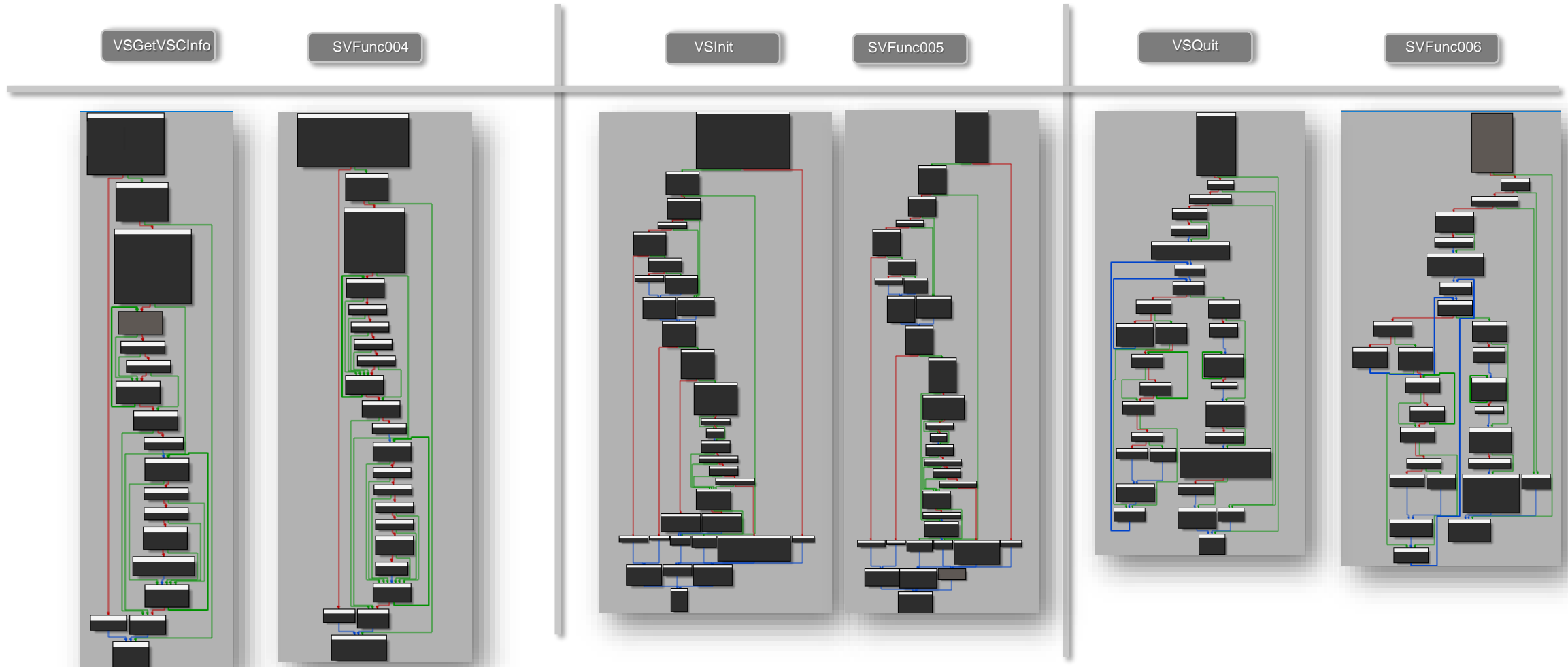
ディープ
ラーニング



全ファイルの
バイトを処理

ブロック
30%
以上の
検出率向上

Decode >> コード分解し類似性を検出



Malware DNA エンジン

Neshta

Neshta is a trojan which was first seen in the wild on 2010. Neshta makes modifications in the system registries and in the browser settings in order to install malicious toolbars or extensions. Neshta distributes itself by injections its code to other executable files.

Read more on Check Point Threatcloud Intelligence

Similarity Analysis

Similar code blocks

Similar behavioral IOCs

```
Code block 1 of 3
1 push ebp
2 mov ebp, esp
3 add esp, -0x20
4 xor eax, eax
5 mov dword ptr [ebp - 0x20], eax
6 mov dword ptr [ebp - 0x18], eax
7 mov dword ptr [ebp - 0x1c], eax
```

Threat Details Report

flash_update

SIZE: 3.44 MB | TYPE: EXE | HASH: ...

Verdict: Malicious | Action: Prevent | Confidence: High | Secure / Risk: Critical | Classification: Trojan

ATTACK VECTOR | 18/12/2018 13:35

127.0.0.1 → flash_update → 127.0.0.1

Similarity Analysis

Similar code blocks

Similar behavioral IOCs

```
Code block 1 of 3
1 push ebp
2 mov ebp, esp
3 add esp, -0x20
4 xor eax, eax
5 mov dword ptr [ebp - 0x20], eax
6 mov dword ptr [ebp - 0x18], eax
7 mov dword ptr [ebp - 0x1c], eax
```

FILE LIST

NAME	TYPE	VERDICT	SIZE	CONTEXT
1002-01cb4004b1ee971a690bae2011574cfae98d057a1svigent.exe	EXE	Malicious	85.98 KB	dropped
1002-01cb4004b1ee971a690bae2011574cfae98d057ajusched.exe	EXE	Malicious	287.42 KB	dropped
1002-01cb4004b1ee971a690bae2011574cfae98d057ajps.exe	EXE	Malicious	198.48 KB	dropped
1002-01cb4004b1ee971a690bae2011574cfae98d057ajvaw.exe	EXE	Malicious	281.48 KB	dropped
1002-01cb4004b1ee971a690bae2011574cfae98d057ajvaw.exe	EXE	Malicious	210.48 KB	dropped
1002-01cb4004b1ee971a690bae2011574cfae98d057ajvaw.exe	EXE	Malicious	103.98 KB	dropped
1002-01cb4004b1ee971a690bae2011574cfae98d057ajvaw.exe	EXE	Malicious	210.48 KB	dropped
1002-01cb4004b1ee971a690bae2011574cfae98d057ajvaw.exe	EXE	Malicious	267.42 KB	dropped

SUSPICIOUS ACTIVITIES

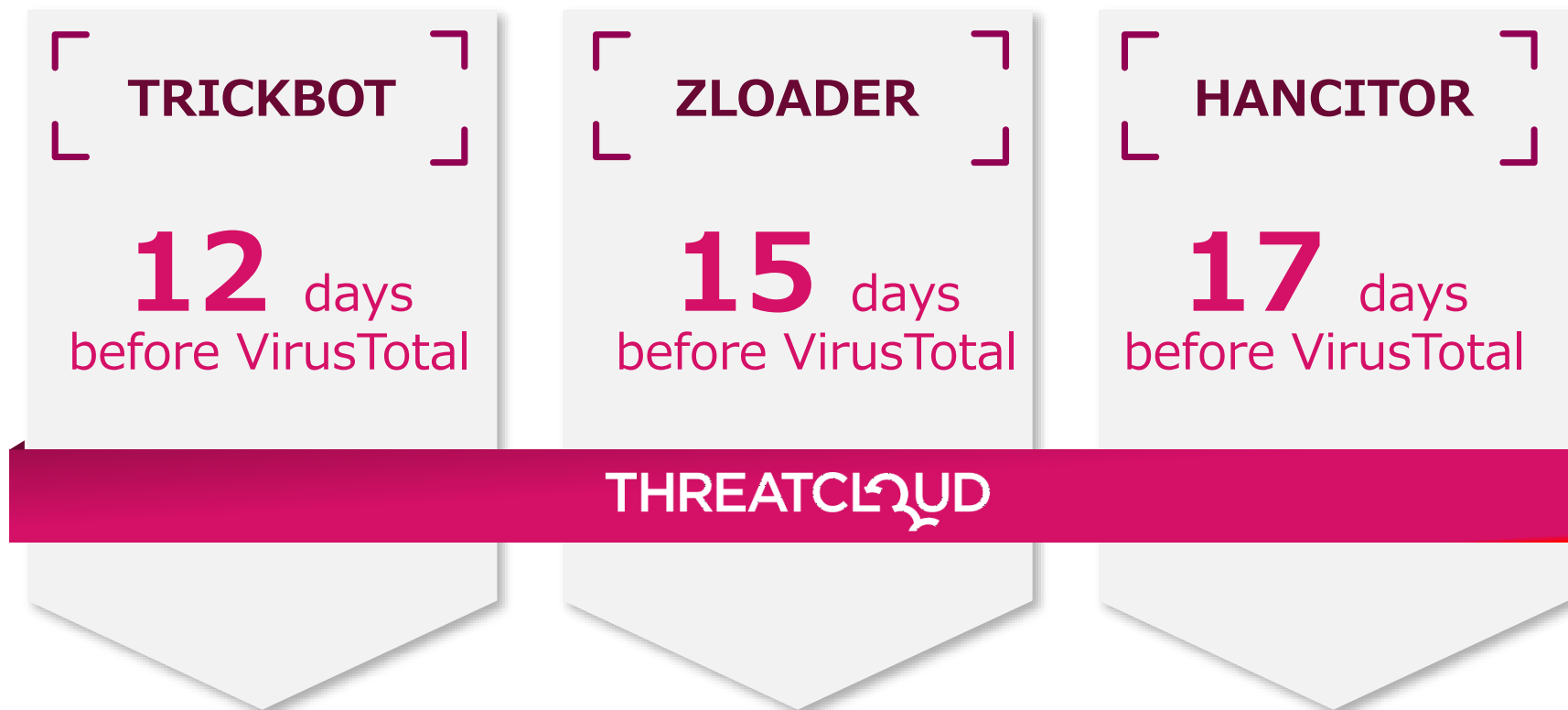
CATEGORY	COUNT	DESCRIPTION
Evasion	1	Observe a program that creates a new process
Evasion	1	The program dynamically calls imported functions
Evasion	1	The program queries a process cookie
Evasion	1	The program queries information on its own process
Evasion	1	The program queries its own PEB
Evasion	1	The program uses a native API call to load a DLL
Evasion / Persistence	1	The program executes other programs or commands
File system event	13	Suspicious file was accessed during emulation
Generic	1	Appends a known multi-family ransomware file extension to files that have been encrypted
Generic	1	Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory available
Generic	1	Creates executable files on the filesystem

未知のマルウェア遺伝子をA.I.で分類





VirusTotalより前にThreatCloudで検出された
マルウェアの亜種の例





リアルタイムアップデート
誰よりも早く攻撃をブロック



ベストキャッチレート
既知および未知の脅威に対応



最高の脅威インテリジェンスデータベース
誤検知の少ない正確な防御





YAMAHA

Make Waves
