YAMAHA
Make Waves

# UTXのシグネチャー更新の仕組みとゼロデイ対策

# 脅威情報データベースとの連携

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

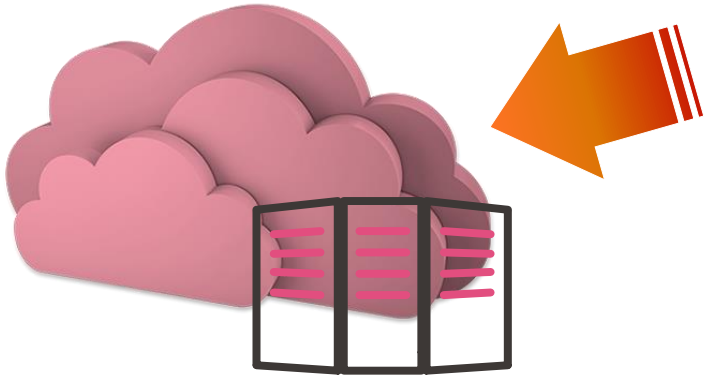
# Agenda

・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
- アンチウィルス
- 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

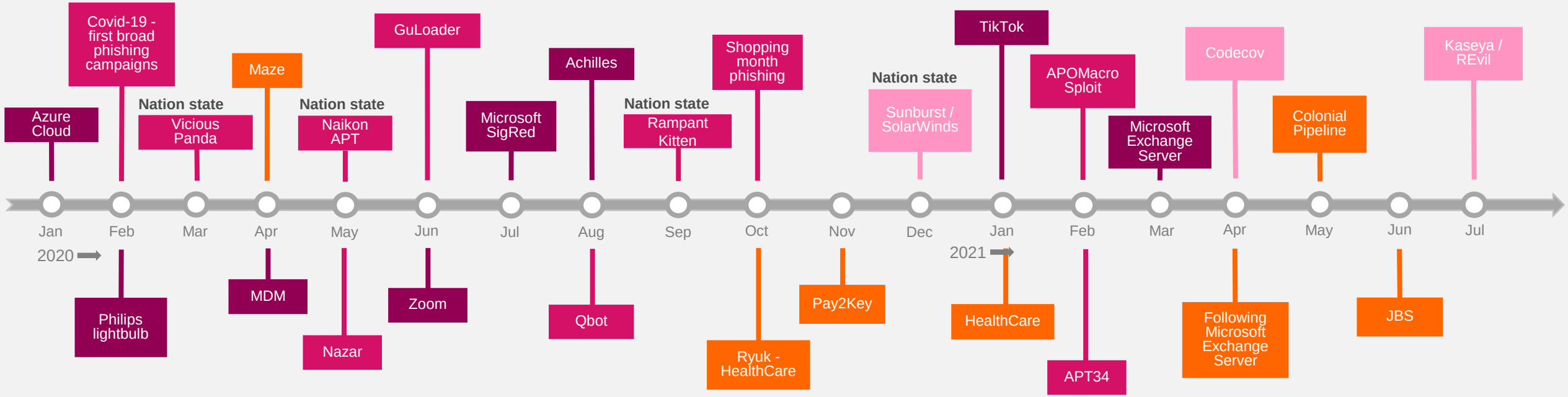

③ 最新のシグネチャデータベースを
ダウンロード

# 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

CHECK POINT™

# THREATCLOUD

## THE BRAIN BEHIND

CHECK POINT'S POWER


# ThreatCloud: 最新の脅威に対応する脅威インテリジェンス

YAMAHA

**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

テレメトリー

**正確な PREVENTION**
(MALICIOUS/SAFE)

テレメトリー

API

**ThreatCloud APIs**

**QUANTUM**
Network Security

**CLOUDGUARD**
Cloud-Native Security

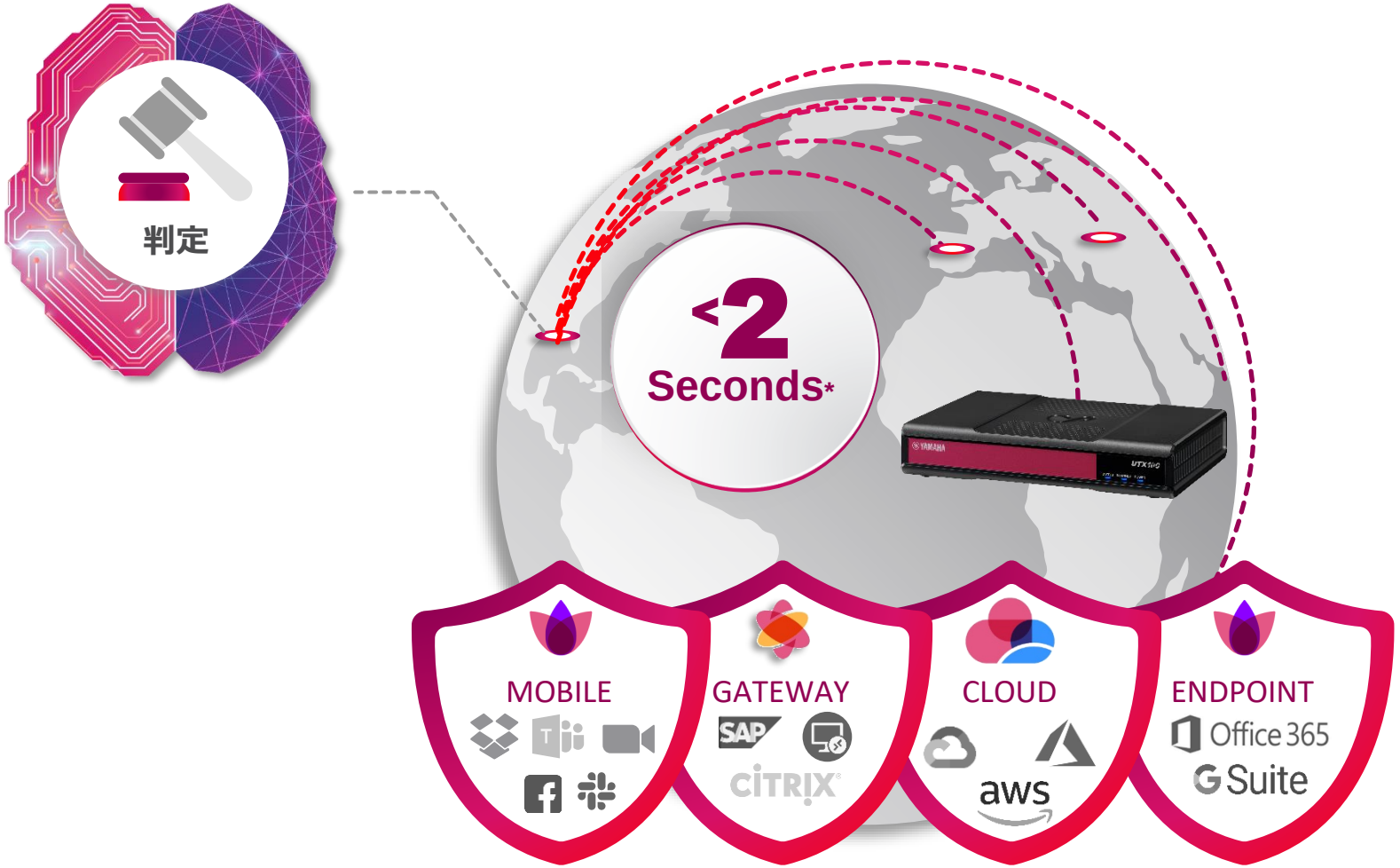
**HARMONY**
User & Access Security

CHECK POINT

# 脅威判定情報は2秒未満で世界中のすべてのプロダクト･ユーザ様へ提供

YAMAHA

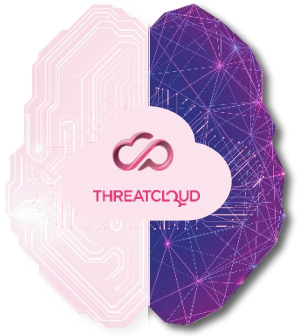
## 脅威データベースはクラウド上で**リアルタイム**にアップデートされます




CHECK POINT™

# ビッグデータ脅威インテリジェンス

YAMAHA




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をクロールする外部フィードから脅威情報を取得

cp<r>
CHECK POINT RESEARCH

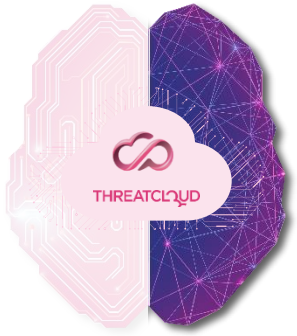
日々**650,000**の疑わしいドメインを検出する
独自の機械学習アルゴリズム

Patented

CHECK POINT™

# Check Point Research (CPR)

YAMAHA




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

CHECK POINT™

# 重大な未知のソフトウェアの脆弱性からの即時保護

YAMAHA

cp<r> CHECK POINT RESEARCH

| Qualcomm | DNS SERVER | | Apache Guacamole™ | ATLASSIAN | Office |
|---|---|---|---|---|---|
| June 2020 | July 2020 | Sep 2020 | Nov 2020 | Nov 2020 | June 2021 |
| CVE-2020-11292 | CVE-2020-1350 | CVE-2020-1895 | CVE-2020-9497<br>CVE-2020-9498 | | CVE-2021-31174<br>CVE-2021-31178<br>CVE-2021-31179<br>CVE-2021-31939 |

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


No patch needed


ThreatCloud APIs

QUANTUM

CLOUDGUARD

HARMONY

INFINITY VISION

CHECK POINT™

# ThreatCloud で使用されるAIベースのテクノロジー

YAMAHA


## 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

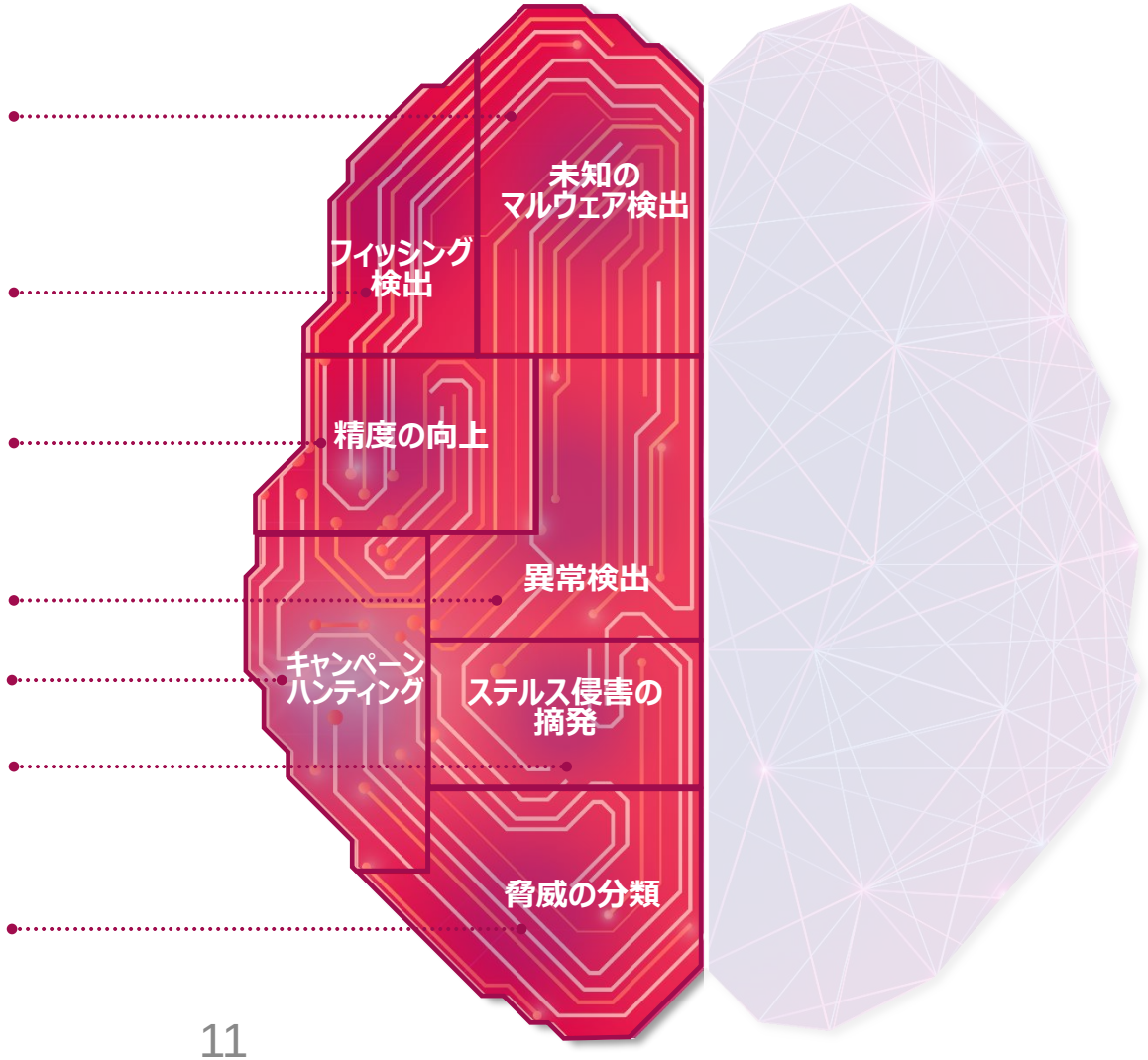
ネットワークAIエンジンアグリゲータ
モバイルAIエンジンアグリゲータ
検証済み署名の機械学習

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




CHECK POINT

# Use case :ゼロディマルウェアのブロック

YAMAHA

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

EXE

Quantum

THREATCLOUD

正確な評決


**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

CHECK POINT™

# ディープラーニングで誤検知を90%以上削減

YAMAHA

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

Deep Learning

**古典的な機械学習**

EXE

**特徴の定義**

認証者
OS
コンパイラ情報
メタデータ
書き込み可能
権限

…など

**分類のアルゴリズム**

サポートベクターマシン

ランダムフォレスト

デシジョンツリー

…など

**Malicious?**

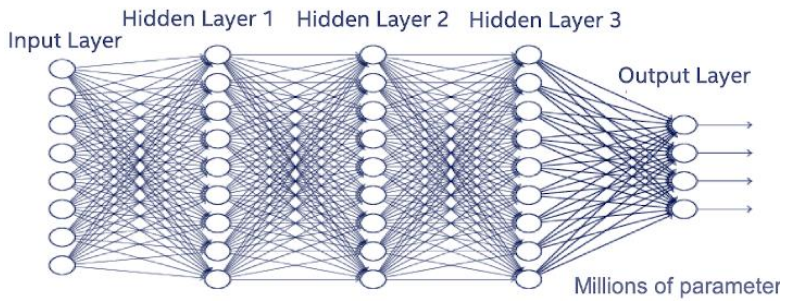
ゼロデイ
ランサムウェア(exe)

**ディープラーニング**

EXE

全ファイルのバイトを処理

**ニューラルネットワーク**

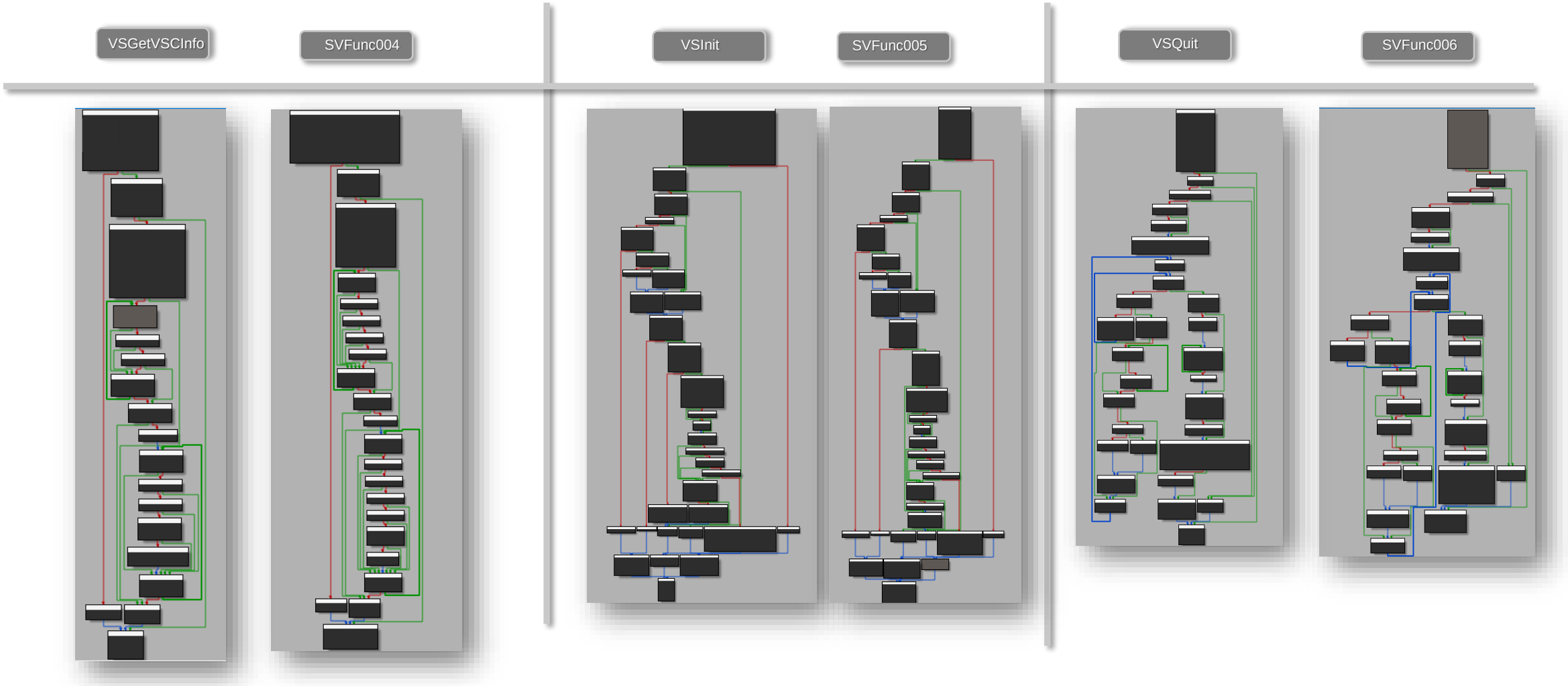



**Malicious**

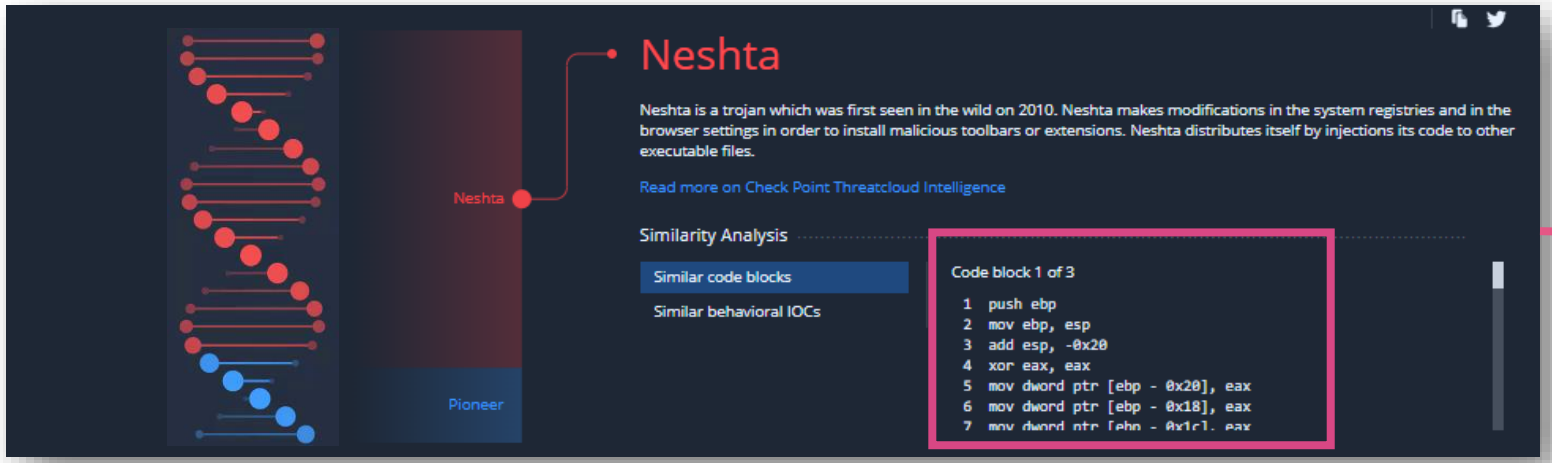
ゼロデイ
ランサムウェア(exe)

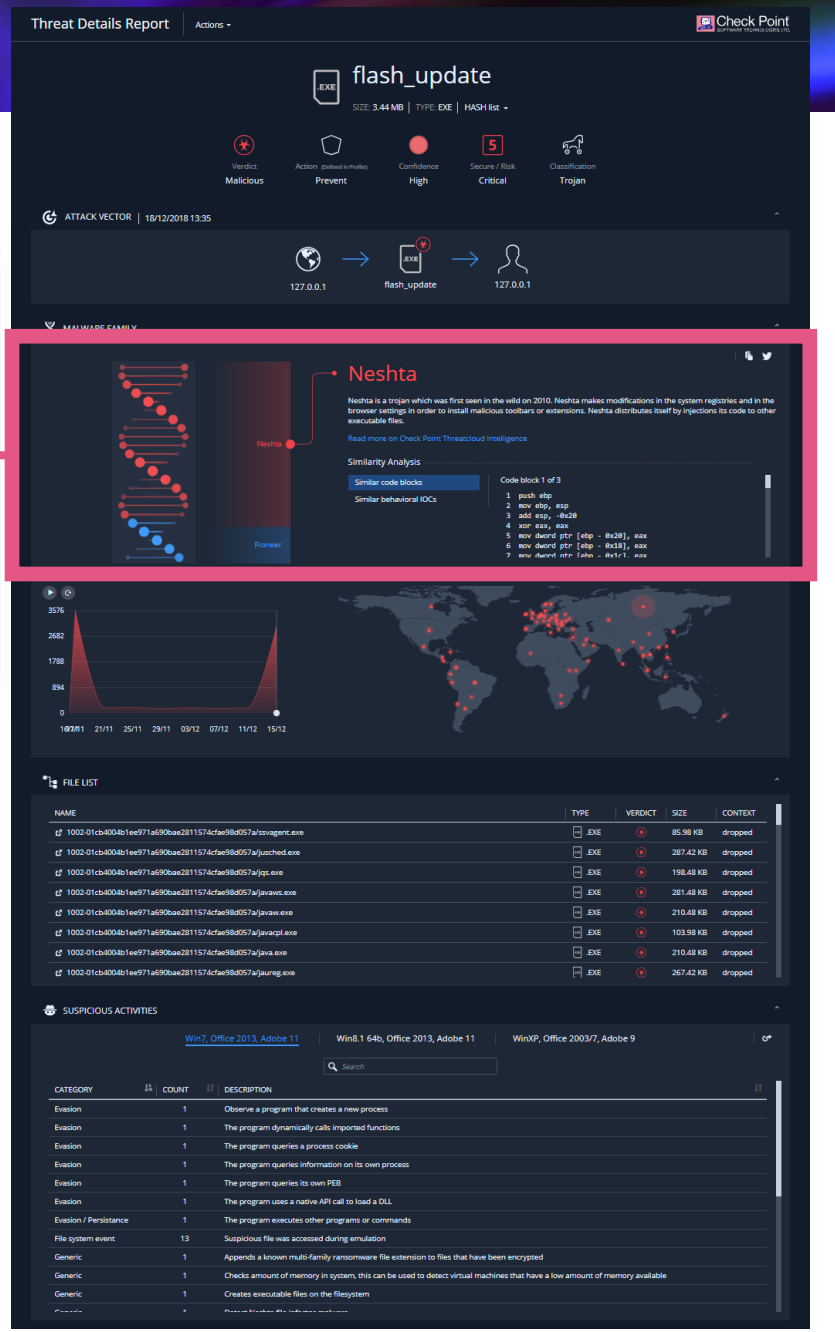
ブロック
**30%**
**以上の検出率向上**

# Decode >> コード分解し類似性を検出



# Malware DNA エンジン




未知のマルウェア遺伝子をA.I.で分類

# 事例紹介：ゼロデイマルウェアの検出

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

| TRICKBOT | ZLOADER | HANCITOR |
| --- | --- | --- |
| 12 days before VirusTotal | 15 days before VirusTotal | 17 days before VirusTotal |

THREATCLOUD

# 最高のゼロデイ対策を全てのUTXユーザ様へ！

YAMAHA

**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


CHECK POINT™


YAMAHA
Make Waves