Deep Instinct™ 技術概要

2020 年 6 月

目次

はじめに

Deep Instinct は、サイバーセキュリティにエンドツーエンドのディープラーニングを適用した初めての企業であり、唯一の企業です。ディープラーニングは脳の学習能力から発想を得ています。脳はある物体を識別することを学習すると、それを元に予測ができるようになります。同様に、Deep Instinct の人工知能はあらゆるタイプのサイバー脅威の検知を学習することによって、これらを予測する機能を備えていきます。この結果、ゼロデイ攻撃や APT 攻撃を、比類のない精度で、ゼロタイムで検知し、予防することができます。

Deep Instinct ではディープラーニングを活用して、あらゆるファイル攻撃またはファイルレス攻撃からの既知および未知の脅威に対して、多層防御を備えた予測型脅威予防プラットフォームを提供します。Deep Instinct による防御は、どのようなオペレーティングシステムを搭載した、どのようなデバイス (エンドポイント、モバイルデバイス、およびサーバー) にも適用できます。

Deep Instinct™ は新たなマルウェアを認識してその予測モデル (D-Brain) を最適化するように継続的にトレーニングされ、最適化された D-Brain が D-Client 上で更新されます。デバイス上でファイルが最初にアクセスされる際、まずオンデバイスのクライアントによりファイルが静的に解析され、ファイルが悪意のあるものか無害であるかが判断されます。これにより、マルウェアのゼロタイム予防が可能になります。

Deep Instinct には、プロセスが悪意のある動作を実行しているかどうかを動的に判断するための振る舞い解析も実装されています。これには、ランサムウェア、コードインジェクション、および既知のシェルコードに対するソリューションが含まれます。このような検知が発生すると、プロセスの終了、元のファイルの削除、ネットワークからのデバイスの隔離などの自動対処アクションが実行されます。

スクリプトなどの攻撃面の縮小や、Deep Instinct のクラウドデータベース (D-Cloud) によるファイルレピュテーション (評価) を使用したファイルのスキャンなど、その他のセキュリティ機能も利用可能です。

ディープラーニング

ディープラーニング革命の到来

ディープラーニングは人工知能 (AI) テクノロジの最も先進的な技術の 1 つです。「ディープニューラルネットワーク」とも呼ばれ、人間の脳が意思決定を行う際に使用するデータ処理およびパターン作成のしくみから発想を得ています。マシンに入力されるデータが多いほど、新しいデータの意味を直観的に理解する能力が高まります。

ディープニューラルネットワークは、人工的に構築された何十万ものニューロンとシナプスの組み合わせから構成されます。人間の脳と同様に、このニューラルネットワークは線形でなく、各層のすべてのニューロンがそれに続く層内のすべてのニューロンに直接接続されていることにより、同時並列処理が可能です。

機械学習の他の形態と比べたディープラーニングの利点は、データのエンドツーエンド処理にあります。ここでエンドツーエンドとは、次の 3 つの要素を意味します。それは、特徴量エンジニアリングフェーズ (専門家による解析用の特徴点の特定と選択という機械学習の本質部分) の撤廃、サンプル内の利用可能なすべてのデータ (専門家により選択されたデータだけを使用するのではありません) の解析、および表現学習 (より高いレベルの特徴点ではなく、まったく加工されていないレベルの特徴点を解析する、たとえるなら画像の各構成要素ではなく、画像の各ピクセルを観察することにより、データの階層抽象化を実現する能力) を含んでいます。これらの要素を組み合わせることにより、ディープラーニングは精度を飛躍的に向上させています。

機械学習 vs. ディープラーニング

サイバーセキュリティ製品を検討する際、検討している製品がディープラーニングテクノロジに基づいているのか、それとも人工知能と機械学習に基づいているのかを、はっきり理解できないこともあります。以下のチェックリストを使用すると、この 2 つのテクノロジを識別する上で役立ちます。

従来型機械学習アルゴリズムは多数の問題を抱えている :

機械学習には特徴量エンジニアリングと抽出が必要

学習を行うための特徴点の定義と操作に、特定分野の専門家が必要です。

ディープラーニングでは生データを元に学習

完全に自律的な方法でデータを処理して、学習します。

従来型機械学習の解析には制限がある

従来型機械学習では、データは統計的相関などの、細かな特徴ベクトルに変換されます。この方法では、必然的にデータの大部分が無視されることになります。

ディープラーニングでは生データを 100% 活用

たとえば、ピクセル、波形、バイトなどを処理します。ディープラーニングの主要な強みの 1 つが、生データから自動的に抽出される膨大な数の特徴点と、それを元に行われる学習です。

機械学習では表現学習は行わない 複雑なデータパターンの解析は可能ですが、粒度の細かい詳細ではなく、大まかな特徴点の解析に依存しているため、解析の厳密性はより低く、誤判定 (誤検知) の可能性が高くなります。	ディープラーニングでは表現学習を行う 大まかな特徴点ではなく、まったく加工されていないレベルの特徴点を解析することによって、データを階層抽象化することができ、新しいサンプルに対しても正しいラベル付け (推論判定) を行うことができます。
機械学習のスケーラビリティには制限がある 機械学習は多様なデータセットに応じて拡大縮小可能ですが、情報の限界値があり、これに達すると、さらにデータトレーニングを実行してもそれ以上の精度は得られません。	ディープラーニングはサンプル数が増えるほど精度が向上 ディープニューラルネットワークはトレーニングデータセットが拡大するに伴って継続的に改善されるため、数億個のトレーニングサンプルへと拡大することで利点が得られる唯一の手法です。

これらの違いはサイバーセキュリティの分野にも当てはまる :

機械学習では脅威を識別するために人に依存 この選別プロセスは研究者の知識と経験により制限されるため、サンプルが誤認されやすくなります。	ディープラーニングは人に依存しない 完全に自動化されたソリューションであるため、脅威の検知に特徴量エンジニアリングやデータ操作を使用しません。
機械学習は限定的なファイルタイプ (PE) のみ 現在、従来型機械学習ベースのソリューションでは、一般的に PE ファイルのみがサポートされています。特徴抽出はファイル形式ごとで異なります。 つまり、ファイルタイプが異なれば完全に別の特徴抽出プロセスが必要になるため、労力も知識も一から必要になります。	ディープラーニングはあらゆるファイルタイプに適用可能 ディープラーニングは入力に依存しないため、ファイルタイプにも依存しません。このため、ディープラーニングは大幅な変更なしに簡単に新しいファイルタイプに適用でき、ソリューションの精度を向上させます。

機械学習では誤検知が多い

特徴量エンジニアリングでは、特徴点を定義するために特定分野の専門家が必要です。 特徴点を選択する方法が原因となって、これらのモデルでは無害なファイルが悪意があるとして頻繁に誤認され (誤検知)、その結果、多くのリソースが不要に消耗されることになります。

ディープラーニングの誤検知はきわめて少ない

ディープラーニングアルゴリズムは完全に自律型であり、データの 100% を解析します。したがって、人的エラーの可能性はなく、誤検知率が劇的に低下します。

Deep Instinct のトレーニングサイクル

アルゴリズムとハードウェアの両方の向上により、近年、ディープラーニングは大きく前進しています。ディープニューラルネットワークの理解とトレーニングにおける近年の多くの進歩により、 多数の隠れ層を持つディープネットワークをトレーニングすることが可能になっています。また、高速な GPU により、このようなネットワークのトレーニング時間は何十倍もスピードアップしています。これら2つの要因によって、数十億個ものシナプスから構成される大規模なニューラルネットワークのトレーニングが可能になっています。

トレーニングフェーズは、Deep Instinct のラボで実施されます。サイバーセキュリティ業界のニーズに合わせて入念に調整された当社独自のディープラーニングインフラストラクチャとアルゴリズムを使用して実行されます。

マルウェアの検知と予防モデルのトレーニングは管理下で行われ、数億個の悪意のあるファイルと無害なファイルの両方に適用されます。 ファイルは、公開リポジトリ、非公開リポジトリ、ダークネット、独自で作成された亜種、Deep Instinct 研究チームにより内部で開発されたマルウェアなど、多数のソースから日々集められます。

トレーニングでは、ディープニューラルネットワークのシナプスを繰り返し調整して分類精度を向上させるために、すべてのファイルが何度も処理されます。

何百ものマルウェアタイプやクラス、攻撃ベクトル、自社開発マルウェア、APT、および誤検知テストといったさまざまなテストが完了すると、 予測モデル (D-Brain) の生産準備が整い、 お客様に届けられます。

Deep Instinct でトレーニングを行うもう一つの予測モデルが、ディープ分類モデルです。ファイルが悪意のあるものか無害であるかを識別することを目的とする D-Brain に加え、このモデルはマルウェアを分類します。 分類には、ランサムウェア、ワーム、ウイルス、ドロッパー、スパイウェア、バックドア、および PUA が含まれます。

セキュリティ機能

予防ファーストアプローチによる完全防御

Deep Instinct のソリューションは、既知および未知のサイバー脅威に対する予測と予防ファーストアプローチ、それに続く検知と対応など、複数のレイヤーに基づく完全防御を提供します。

1. Windows エンドポイント

実行前

静的解析

最も先進的な AI テクノロジであるディープラーニングを利用します。モデルによる静的解析はシグネチャおよびヒューリスティックソリューションよりもはるかに高い精度を提供し、検知率が低く誤検知率が高い従来の機械学習アルゴリズムよりも正確です。ファイルタイプに依存しないこのディープラーニングの実装は、あらゆるファイルタイプに適用でき、以下のファイルタイプをサポートしています。

- Windows 移植可能な実行ファイル: PE (.exe、.dll、.sys、.scr、.ocx など)
- オブジェクトのリンクと埋め込み: OLE (.doc、.xls、.ppt、.jdt、.hwp など)
- Office Open XML: OOXML (.docx、.docm、.xlsx、.xlsm、.pptx、.pptm など)
- 埋め込みマクロ (OLE および OOXML ファイル内)
- PDF (Portable Document Format) ファイル : .pdf
- RTF (Rich Text Format) ファイル : .rtf
- Adobe Flash ファイル : .swf
- JAR (Java ARchive) ファイル : .jar
- 画像ファイル : .tiff
- フォントファイル : .ttf、.otf
- アーカイブファイル : .zip、.rar

D-Client は、ファイルがデバイスに初めて到達した際に、悪意のあるファイルであるかどうかを予測し、予防します。また、初回インストール時またはオンデマンドで完全なファイルスキャンを実行できます。さらに、組織のニーズに合わせたさまざまなしきい値を使用して悪意のあるファイルを予防または検知するように設定することが可能です。

D-Cloud ファイルレピュテーション (クラウドベース)

既知の悪意のあるファイルおよび無害なファイルの両方に対する、ファイルレピュテーション (評価) に基づく追加の防御機能です。

スクリプト制御

PowerShell、JavaScript、VBScript、マクロ、HTML アプリケーション、rundll32 など、スクリプトベースの攻撃可能面を排除するためのコンプライアンスとポリシー。

ブラックリスト

ファイルはハッシュに基づいてブラックリストに登録できます。ハッシュに基づく IoC のリストをインポートする機能も提供されています。

予測と予防にかかる時間

20

ミリ秒

D-Brain を使用

調査にかかる時間

50

ミリ秒

ディープ分類を使用

修正と阻止

1

分以下

実行時

振る舞い解析

脅威による悪性の高い振る舞い動作を検知して阻止することが可能な動的解析機能です。

- ランサムウェアに対する防御:

  このモジュールは、ランサムウェアの実行中にその動作を検知します。暗号化手法およびファイルを暗号化するための読み取り / 書き込み処理の手法もすべて把握しています。このモジュールは、100% の検知率と 0% の誤検知率で、すべての手法に対処できます。これは、Deep Instinct の研究チームにより実行された数万回を超えるテストにより裏付けられています。このモジュールは、最近のランサムウェア対策で検知されることが多い、ハニートークン / おとり / カナリアファイルに依存せずに実装されています。

- コードインジェクションに対する防御:

  このモジュールは、プロセス間を横方向に移動するために使用されるリモートコードインジェクション手法を検知します。コードインジェクションは一般的に以下のいずれかの目的を達成するために実装されます。

  - 正規プロセス (explorer.exe など) の上で悪意のあるコードを実行することにより、検知を回避する。
  - ファイルレス手法を使用して検知を回避する。
  - 高い特権のプロセスに注入することにより、特権を昇格させる。
  - 対応しているコードインジェクション手法:
    - プロセスハロウィング: 正規プロセスが一時停止状態で実行され、その元のコードが悪意のあるコードで置き換えられます。この手法は、エントリポイントを書き換えるか、一時停止されたプロセスの内容を書き換えることによっても実行できます。この悪意のあるキャンペーンの例には、Duqu、Cobalt Strike などがあります。
    - リモートスレッドの作成: リモートプロセス内に作成されたスレッドとして悪意のあるコードが実行されます。
    - ライブラリのロード: DLL がリモートプロセスにロードされ、その悪意のある関数の 1 つが呼び出されます。
    - SetWindowsLong: ウィンドウハンドラが悪意のあるコードを実行するように書き換えられます。
    - 非同期プロシージャコール: これは、APC を使用してリモートプロセス内に作成されたスレッドとして悪意のあるコードを実行する、リモートスレッド作成手法に似ています。
    - スレッドコンテキストの設定: スレッドのコンテキストが変更され、その結果、悪意のあるコードが実行されます。
    - IAT フッキング: 悪意のあるコードを実行するために、インポートアドレステーブル (IAT) からの関数がフックされます。
    - AtomBombing: Windows のアトムテーブルを悪用して、悪意のあるコードがリモートプロセスに書き込まれ、その後実行されます。この悪意のあるキャンペーンの例には、Dridex バンキング型トロイの木馬などがあります。

- PROPagate: 悪意のあるコードを実行するためにウィンドウコールバックハンドラが書き換えられるSetWindowsLong 手法に似ています。この悪意のあるキャンペーンの例には、RIG EK などがあります。
- Early Bird: セキュリティソリューションによる検知を迂回するための機能が追加された、APC 手法の変化形。この悪意のあるキャンペーンの例には、APT33 などがあります。

既知のシェルコードに対する防御:

このモジュールは、既知のペイロードの実行中にその動作を検知します。MSFvenom、Shellter、Veil などの多くのツールにより生成されたシェルコードから防御します。

コンテキストスクリプトの実行:

このモジュールは、疑わしいスクリプトや、悪意があるか疑わしい PowerShell コマンドの実行を検知します。

2. macOS エンドポイント

実行前

静的解析

最も先進的な AI テクノロジであるディープラーニングを利用します。静的解析はシグネチャおよびヒューリスティックソリューションよりもはるかに高い精度を提供し、検知率が低く誤検知率が高い従来の機械学習アルゴリズムよりも正確です。ファイルタイプに依存しないこのディープラーニングの実装は、あらゆるファイルタイプに適用でき、現在、以下のファイルタイプをサポートしています。

- macOS 実行ファイル : Mach-O (.macho など)
- オブジェクトのリンクと埋め込み: OLE (.doc、.xls、.ppt、.jdt、.hwp など)
- Office Open XML: OOXML (.docx、.docm、.xlsx、.xlsm、.pptx、.pptm など)
- 埋め込みマクロ (OLE および OOXML ファイル内)
- PDF (Portable Document Format) ファイル : .pdf
- RTF (Rich Text Format) ファイル : .rtf
- Adobe Flash ファイル : .swf
- JAR (Java ARchive) ファイル : .jar
- 画像ファイル : .tiff
- フォントファイル : .ttf、.otf
- ディスクイメージファイル: .dmg
- アーカイブファイル: .zip、.xar、.7z、.tar、.tar.z、.tar .gz、.tar.bz2

D-Client は、ファイルがデバイスに初めてアクセスする際に、悪意のあるファイルであることを予測し、予防します。 また、初回インストール時またはオンデマンドで完全なファイルスキャンを実行できます。さらに、組織のニーズに合わせたさまざまなしきい値を使用して悪意のあるファイルを予防または検知するように設定することが可能です。

D-Cloud ファイルレピュテーション (クラウドベース)

既知の悪意のあるファイルおよび無害なファイルの両方に対する、ファイルレピュテーション (評価) に基づく追加の防御機能です。

ブラックリスト

ファイルはハッシュに基づいてブラックリストに登録できます。ハッシュに基づく IoC のリストをインポートする機能も提供されています。

98%
検知率

0.001%
特定された誤検知

3. モバイルと Chrome OS

実行前

静的解析

最も先進的な AI テクノロジであるディープラーニングを利用します。モデルによる静的解析は、シグネチャおよびヒューリスティックソリューションよりもはるかに高い精度を提供し、検知率が低く誤検知率が高い従来の機械学習アルゴリズムよりも正確です。

D-Client は初期インストール時またはオンデマンドで完全なスキャンを実行することにより、悪意のあるアプリケーションを予測し、予防します。組織のニーズに合わせたさまざまなしきい値を使用して悪意のあるアプリケーションを予防または検知するように設定することが可能です。

D-Cloud ファイルレピュテーション (クラウドベース)

既知の悪意のあるアプリケーションおよび無害なアプリケーションの両方に対する、ファイルレピュテーション (評価) に基づく追加の防御機能です。

実行時

動的振る舞い解析

悪意のある振る舞いロジックを検知して阻止することが可能な動的解析機能です。

ネットワークレベル : MitM (ARP ポイズニング)*、SSL MitM、HOSTS ファイルの書き換え、証明書のインストールなど、ネットワーク攻撃の動作を検知します。

デバイスレベル : root 化 / ジェイルブレイク、OS バージョン、アプリケーションの望ましくないインストール方法 (不明なソース * や USB デバッグを含む) など、さまざまな悪意のある活動やデバイス上の問題のある設定を検知します。

* Android のみ

Deep Instinct の特徴

- **あらゆるオペレーティングシステムに対応**

  D-Client は次のようなさまざまな種類のエンドポイントオペレーティングシステムにインストールできます : Windows、macOS、Android、Chrome OS、iOS、および iPadOS。

- **軽量なエージェント**

  軽量であり、初期インストール中またはそれ以降も、エンドポイントを大きく低下させるような影響を与えません。D-Client はメモリー消費が小さく (150 MB 以下)、CPU の使用量も 1% 未満です。

- **毎日のシグネチャ更新は不要**

  このソリューションは、1 年に 2 回だけ、モデルが更新されます。これは、1 日に数回の更新を必要とする他のウイルス対策ソリューションや、脅威情報フィードを受信するために常時接続を必要とする EDR ソリューションと異なります。

- **使いやすく、柔軟性が高い管理**

  Deep Instinct の管理コンソールは、管理者が使いやすく、管理サーバはクラウドまたはオンプレミスのいずれでも実装可能です。

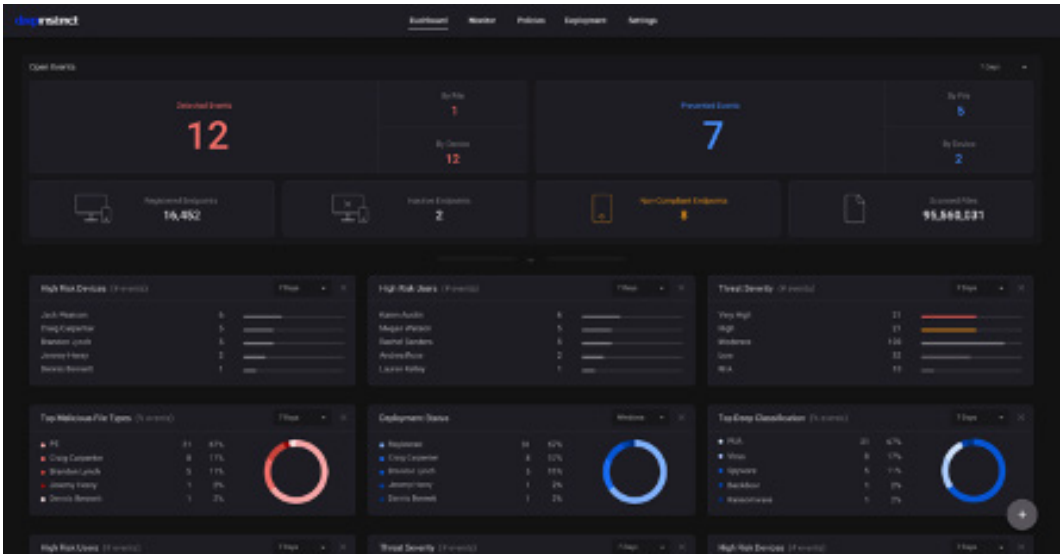
- **インターネット接続に依存しない**

  完全自立型で、デバイス上で動作をするため、デバイスがオフラインでインターネットに接続されていないときでも防御します。

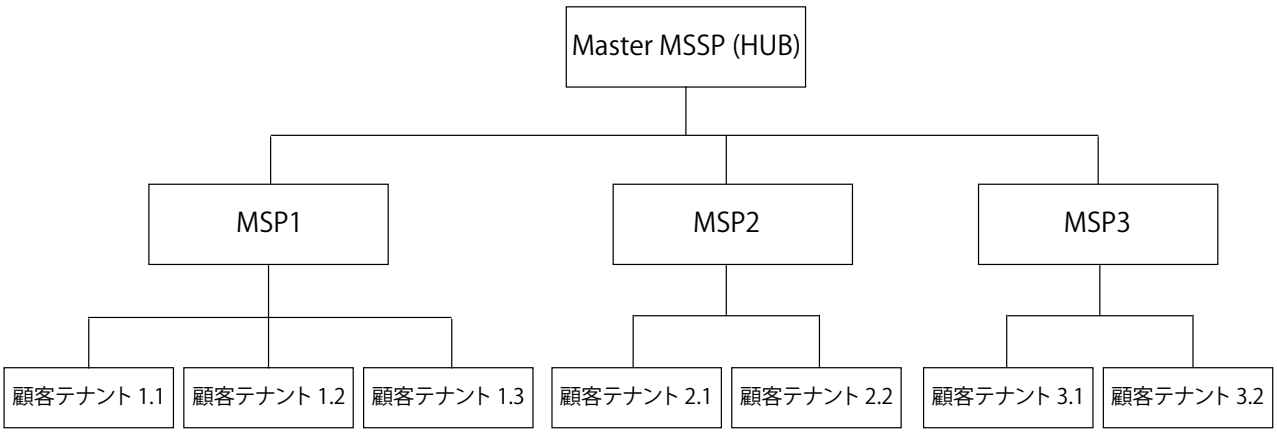
先進的な脅威解析と管理機能

管理コンソールは以下の機能から構成されています。

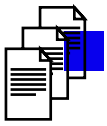
- イベント解析: 以下のような複数の機能から構成されています。
  - Deep Classification (分類): 独自のディープラーニングマルウェア分類モジュールを使用して、人の関与なしに、マルウェア (既知および未知の) をリアルタイムで 7 つのマルウェアタイプと 7 つの PUA タイプにすばやく分類します。
  - イベント解析: 攻撃チェーンとともに、調査中に環境内で何が起きているのかを簡単に理解できます。
  - 先進的な脅威解析: 静的解析とサンドボックス解析の両方により、組織内で検知されたマルウェアに対して、追加設定なしで、マルウェアの解析と洞察を実行できます。
- 管理者による対処機能 :
  - リモートから隔離されたファイルの復元
  - ホワイトリスト : ハッシュ、証明書、パスに基づいて、悪意があると誤って検知されたファイルをホワイトリストに登録することができます。ハッシュに基づく IoC のリストをインポートする機能も提供されています。追加されたハッシュは元に戻されます。
  - リモートからのファイル削除: 予防および隔離されなかった検知されたファイルは、エンドポイントからリモートで削除できます。
  - 実行中のプロセスの終了: 悪意があるとして検知されたファイルおよび悪意のある動作を実行していると検知されたプロセスは、リモートから終了できます。
  - ネットワークからのデバイスの隔離: 組織にリスクを招く可能性があるデバイスは、リモートから隔離することができます。
- ポリシー: 組織のセキュリティポリシーを設定することができます。次の要素に基づいてデバイスグループごとに異なるポリシーを定義できます : デバイス名、AD ツリー、OS バージョン、Deep Instinct エージェントバージョン、IP 範囲、タグなど。
- レポートと外部連携 :
  - 新規イベントについて、電子メール、syslog、および RESTful API を使用して通知
  - RESTful API を使用して、イベント、デバイス、および全般設定に対処
  - 主要 SIEM 製品 (Splunk、Micro Focus ArcSight、IBM QRadar) の認定アプリケーション
  - サポートされている syslog 形式: RFC 5424、CEF、LEEF
  - SOAR ソリューションとの統合
  - UEM/MDM ソリューションとの統合により、感染したデバイスについてレポートし、自動的に追加の修正措置を実行
- レポート: 特定期間中の正確な詳細を含むエグゼクティブサマリーを、オンデマンドおよびスケジュールに従って生成します。
- ロールベースの管理 (RBAC): 管理コンソールのユーザーに対して、さまざまなユーザーロールを設定できます。
- 二要素認証 (2FA): 電子メールまたは Google Authenticator を使用して、2FA を設定できます。
- スケーラビリティ: 1 台の管理サーバーで、20 万台までのデバイスを管理できます。



管理コンソールには、複数の MSP 顧客、個々の MSP、および大企業にサービスを提供する組織をサポートするマルチテナント機能も含まれます。同じ管理コンソールから、すべてのエンティティを管理することが可能です。

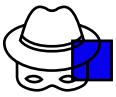


対応している攻撃手法 | エンドポイント



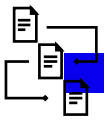
ファイルベースのマルウェア

ウイルス、ワーム、バックドア、ドロッパー、ワイパー、コインマイナー、既知のシェルコード、PUA などを予測して予防するために、実行ファイルおよび非実行ファイルをスキャンします。



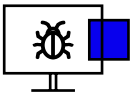
スパイウェア

バンキング型トロイの木馬、キーロガー、クレデンシャルダンパーなど、あらゆるタイプのスパイウェアから保護します。



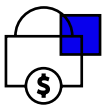
ファイルレスマルウェア

スクリプトベースの攻撃、デュアルユースツール、コードインジェクション手法などのファイルレス攻撃を予防します。



エクスプロイト

あらゆるクライアント側攻撃から保護します。



ランサムウェア

静的解析および動作解析の両方による総合的な防御を使用して、ランサムウェアのリスクを軽減します。

対応している攻撃手法 | モバイルと Chrome OS

アプリケーションレベル

ランサムウェア、インフォスティーラ、ルーター、プレミアム SMS/ 通話、RAT、ワーム、ネットワークリダイレクタ、ボットネット、バンキング型トロイの木馬、ドロッパー、バックドア、コインマイナー、PUA などを予測および予防するために、APK をスキャンします。これらの攻撃タイプはほとんどの場合、情報の盗み出しや金銭の取得のために使用されます。

また、サイドローディング (不明なソースや USB デバッグを含む) などの望ましくない方法でのアプリケーションのインストールが許可されていないことを確認するために、デバイスを監視します。

ネットワークレベル

デバイスは常時ワイヤレスネットワークに接続される傾向にあります。MitM (ARP ポイズニング)、SSL MitM、HOSTS ファイルの書き換え、証明書のインストールなど、ネットワークに対して悪意のある攻撃を行うために実行可能なさまざまな手法を監視します。

デバイスレベル

悪用されていないことを確認するために、デバイスを監視します。攻撃者はこのタイプのエクスプロイトを利用して、攻撃を隠し、機密情報を取得するための制御を得ることができます。デバイスの root 化/ジェイルブレイクの有無を監視し、またデバイスが最新の状態であり、パッチが適用された既知の脆弱性が後から悪用されないことを確認するために、OS のバージョンを監視します。

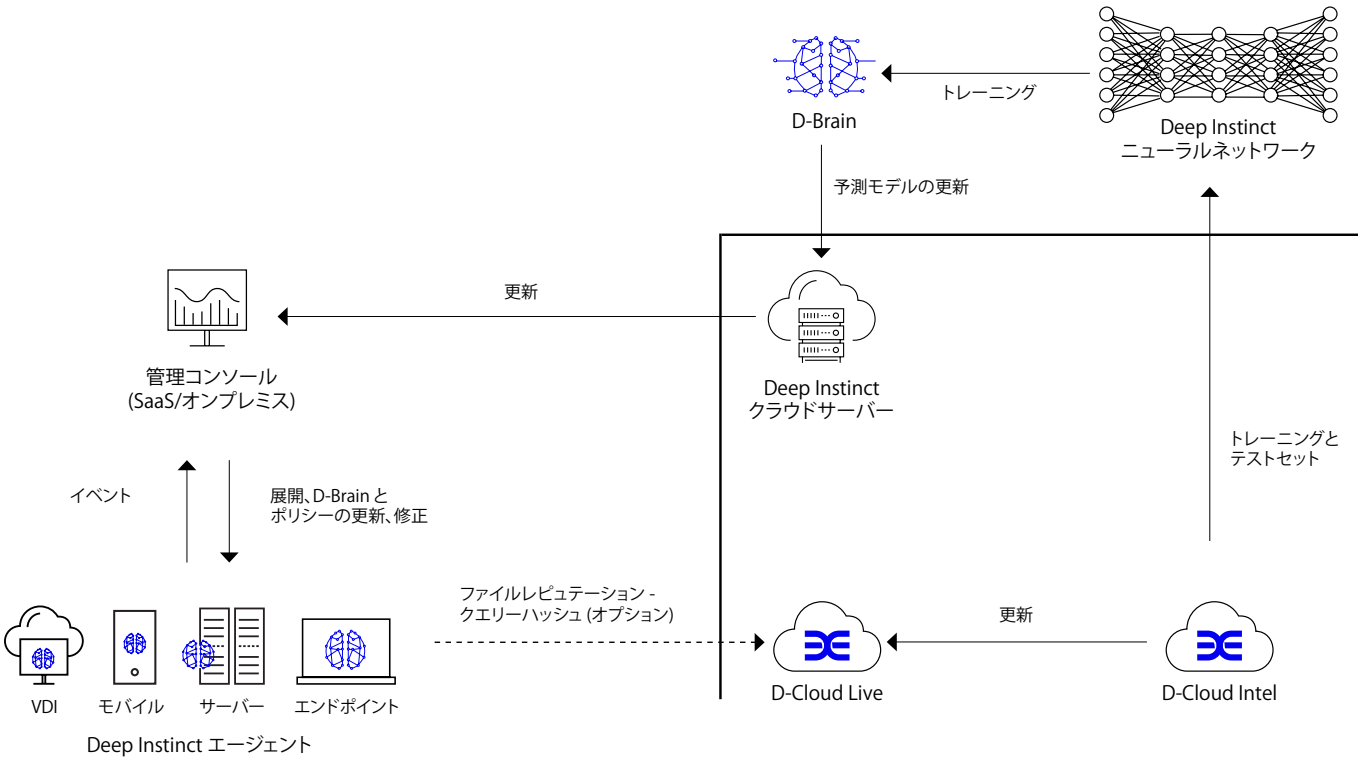
アーキテクチャ

概要

Deep Instinct™ では、クライアント用の総合的なソリューションを提供しています。企業のニーズに合わせた広範なソリューションを展開しています。

このクライアントベースのソリューションでは、エンドポイント、サーバー、およびモバイルデバイス上で実行される軽量クライアントを使用します。これは、オンプレミスまたはクラウド上に設置可能な D-Appliance を使用して管理します。

Deep Instinct
システムアーキテクチャ



Deep Instinct™ の主要な構成要素 :

Deep Instinct™ ニューラルネットワーク

ディープラーニングニューラルネットワークは、Deep Instinct™ のラボに設置されています。これは、Deep Instinct™ が開発したディープラーニングサイバー防御ソリューションのコアコンポーネントです。ディープラーニングニューラルネットワークは、絶え間なく進化するサイバー脅威環境を反映して、継続的に学習します。この継続的なディープラーニングプロセスの出力が、軽量予測モデル (D-Brain) です。この D-Brain は、管理対象のすべての D-Client に展開され、デバイス上で動作します。

D-Brain: 予測モデル

D-Brain は、学習の結果として生成される予測モデルで、サイバー脅威を検知します。クライアントソフトウェア (D-Client) にインストールされます。デバイスにインストールされた予測モデルは、デバイス上のサイバー脅威を自律的に検知して予防するために使用され、オンデバイスでのゼロデイ攻撃および APT 攻撃からの防御を可能にします。

Deep Instinct™ サーバー

Deep Instinct™ ニューラルネットワークとすべての D-Appliance 間の連携を行うコンポーネントです。最新の予測モデル (D-Brain) を D-Appliance に送信し、D-Appliance により D-Client が更新されます。

D-Cloud

D-Cloud Intel は、さまざまなデータソースから収集され、各判定およびクラスにラベル付けされた、数十億個のファイルから構成されるデータベースです。D-Brain のトレーニングとテストのためのデータセットの役割を果たします。

D-Cloud Live は、追加の防御機能を提供します。D-Cloud サービスにより、既知のファイルについての知的情報を含む D-Cloud データベースを使用してファイルを再分類でき、正しい判定がリアルタイムで更新されます。

管理サーバー

組織のデータセンターにてオンプレミスで、またはクラウド上でホスティングされる、管理および監視サーバーです。

D-Client

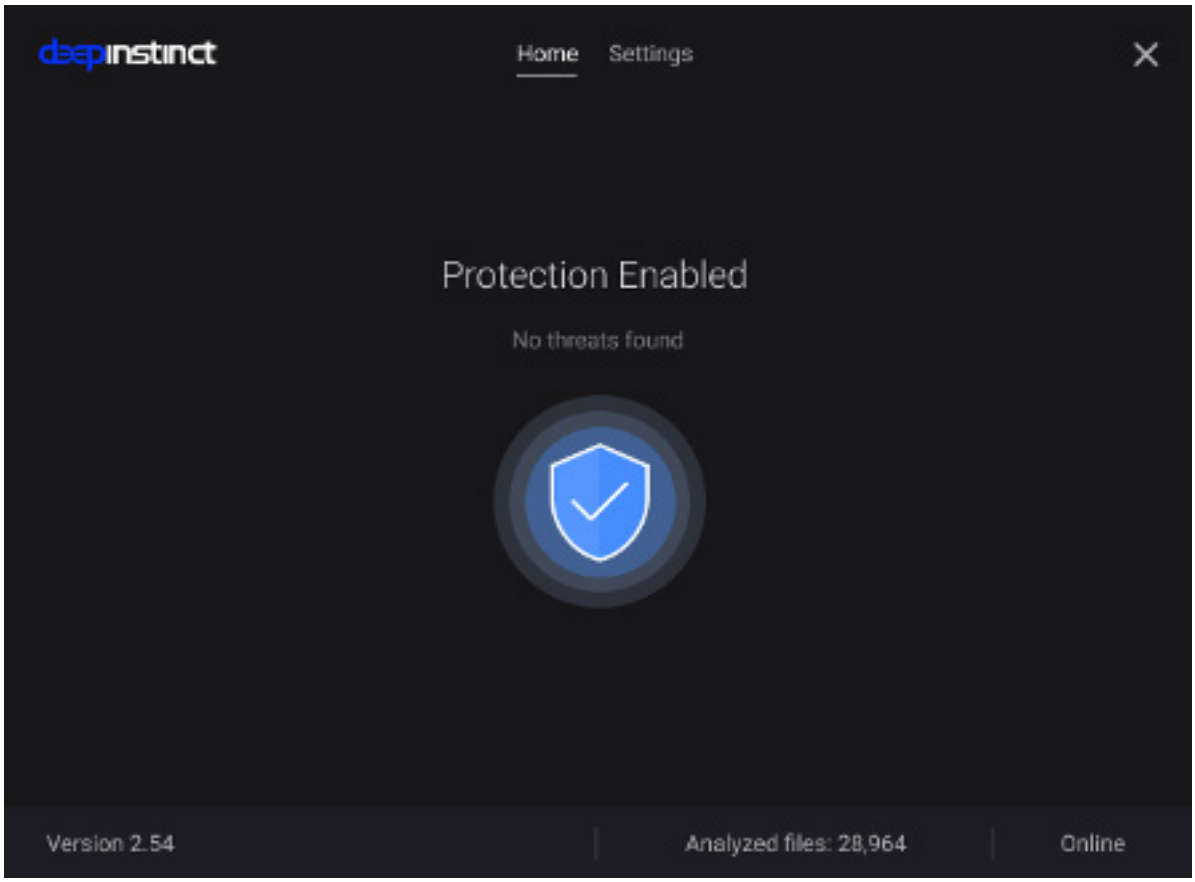
プラットフォーム (Windows、macOS、Android、Chrome OS、iOS、および iPadOS) に応じてデバイス上にインストールされる軽量クライアントソフトウェアです。Deep Instinct™ 予測モデル (D-Brain) の核心となる部分を取り込み、オンデバイスでの静的解析、振る舞い解析、およびその他の主要防御エンジンの、軽量で自律した方法でのリアルタイムの実行を可能にします。管理サーバーと通信してポリシーとソフトウェアの更新を受信し、イベントを送信します。

D-Client は、サードパーティ製のソフトウェア配布ツールを使用したり、または管理コンソールから直接ダウンロードしたりすることで、ローカルまたはリモートで展開およびアップグレードすることができます。

インストール後の再起動は不要であり、インストール後は一度システム全体に対してスキャンを実行して、すでに存在する脅威を特定できます。

D-Client のユーザーインタフェースは 14 の言語で表示可能です。また、エージェントの無効化やアンインストールを防ぐための改ざん防止機能を備えています。

D-Client はさらに、Amazon Workspaces、Citrix Hypervisor と XenDesktop、VMware ESX と Horizon、Microsoft Hyper-V、Oracle VirtualBox などの VDI プラットフォームもサポートしています。VDI インスタンスが作成されると、新しいデバイスとして管理コンソールに自動的に登録されます。



システム要件

クライアントのシステム要件

Windows	
オペレーティングシステム	Windows 7 SP1、8、8.1、10 Windows Server 2008 R2 SP1、2012、2012 R2、2016、2019
.NET Framework	バージョン 3.5 以降
CPU	デュアルコア CPU 以上
RAM	2 GB 以上 (4 GB 推奨)
ディスク	500 MB の空きディスク容量
macOS	
オペレーティングシステム	macOS Sierra (バージョン 10.12) macOS High Sierra (バージョン 10.13) macOS Mojave (バージョン 10.14) macOS Catalina (バージョン 10.15)
CPU	デュアルコア CPU 以上
RAM	2 GB 以上 (4 GB 推奨)
ディスク	500 MB の空きディスク容量
Android	
オペレーティングシステム	バージョン 5 以降
ディスク	70 MB の空きディスク容量
Chrome OS	
オペレーティングシステム	バージョン 9 以降
ディスク	70 MB の空きディスク容量
iOS と iPadOS	
オペレーティングシステム	バージョン 11 以降
ディスク	80 MB の空きディスク容量

管理コンソールの要件

対応ブラウザ	
Google Chrome	最新バージョン
Internet Explorer	11.0 以降
Firefox	最新バージョン
ディスプレイ	
対応 解像度	1366 x 768 1920 x 1080

サポートしている仮想環境

Amazon Workspaces
Citrix Hypervisor および XenDesktop
VMware ESX および Horizon
Microsoft Hyper-V
Oracle VirtualBox

CPU 消費量

一般的に、Deep Instinct™ による CPU 消費は、D-Client がインストールされているデバイスのパフォーマンスにほとんど影響を与えません。

D-Client (Windows、macOS、Android、Chrome OS、iOS、および iPadOS) の CPU 消費量は通常 1% 未満です。

メモリ消費量

Windows	< 150 MB
macOS	< 100 MB
Android	< 100 MB
Chrome OS	< 100 MB
iOS と iPadOS	< 30 MB

必要ディスク容量

Windows	500 MB
macOS	500 MB
Android	70 MB
Chrome OS	70 MB
iOS と iPadOS	80 MB

コンプライアンス

Deep Instinct は PCI、HIPPA、ISO/IEC 27001、および GDPR に適合しています。

Deep Instinct について

Deep Instinct は、サイバーセキュリティにエンドツーエンドのディープラーニングを適用した初めての企業であり、唯一の企業です。ディープラーニングは脳の学習能力から発想を得ています。脳はある物体を識別することを学習すると、それを元に予測ができるようになります。同様に、Deep Instinct の人工知能はあらゆるタイプのサイバー脅威の検知を学習することによって、これらを予測する機能を備えていきます。この結果、ゼロデイ攻撃や APT 攻撃を、比類のない精度で、ゼロタイムで検知し、予防することができます。

Deep Instinct はサイバーセキュリティに対して、プロアクティブで予防的な、まったく新しいアプローチを採用しています。その総合的な防御は、組織のエンドポイント、サーバー、およびモバイルデバイスを、最も捉えづらい未知のマルウェアからもリアルタイムで保護するように設計されています。

詳細については、www.deepinstinct.com をご覧ください。

デモを依頼

ネットワンパートナーズ株式会社
https://www.netone-pa.co.jp/
本 社 〒100-7026 東京都千代田区丸の内 2-7-2 JP タワー TEL 03-6256-0700（代表）
西日本営業部 〒532-0003 大阪府大阪市淀川区宮原 3-5-36 新大阪トラストタワー TEL 06-6105-0356（代表）

www.deepinstinct.com/ja/

DeepInstinct.v.1.2020.1