macOS

データシート

Deep Instinct™ D-Client for macOS

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ゼロタイムで保護するように設計されています。

人工知能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訓練されており、最適化された D-Brain はデバイス上の Deep Instinct クライアント (D-Client) 上に展開され、動作します。

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、多層に基づく包括的な防御を提供します。

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。

- 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。

実行後

Deep Instinct では、簡単にイベントを管理して環境を運用するための一連の運用ツールを提供しています。

自動解析

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把握できます。

Deep Instinct™ の特徴

- **優れたテクノロジ**
  AI テクノロジの最も先進的なサブセットであるディープラーニングに基づいた、比類のないセキュリティソリューションです。
- **リアルタイムを超えたゼロタイム**
  サイバー脅威を確実にゼロタイムで予防するために、実行前に静的ファイル解析を行います。
- **トレードオフなし**
  最高の検知率と最低の誤検知数を誇ります。
- **すべての環境で一貫したセキュリティ**
  Windows、macOS、Chrome OS、Android、iOS などのエンドポイント、サーバーそしてモバイルデバイスを幅広くサポートします。また広く使われているファイル種別をサポートしており、すべて実行前にスキャンします。さらに、ファイルベースの攻撃とファイルレス攻撃の両方に対して効力を発揮し、ネットワークへの接続の有無に関わらず運用可能です。

認証とコンプライアンス

Coalfire

SE Labs

テクノロジパートナシップ

修正

ファイルの隔離

予防のために悪意のあるファイルを隔離します。

ホワイトリスト

ハッシュ、証明書、パスなどに基づいて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。追加されたファイルは元に戻されます。

リモートからのファイル削除

予防と隔離がされずに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。

システム要件

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)
ディスク容量	500 MB の空きディスク容量
メモリ使用量	100 MB 以下

広範な攻撃ベクトルに対応

ファイルベースのマルウェア

ウィルス、ワーム、バックドア、ドロッパー、ワイパー、コインマイナー、既知のペイロード、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。

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。

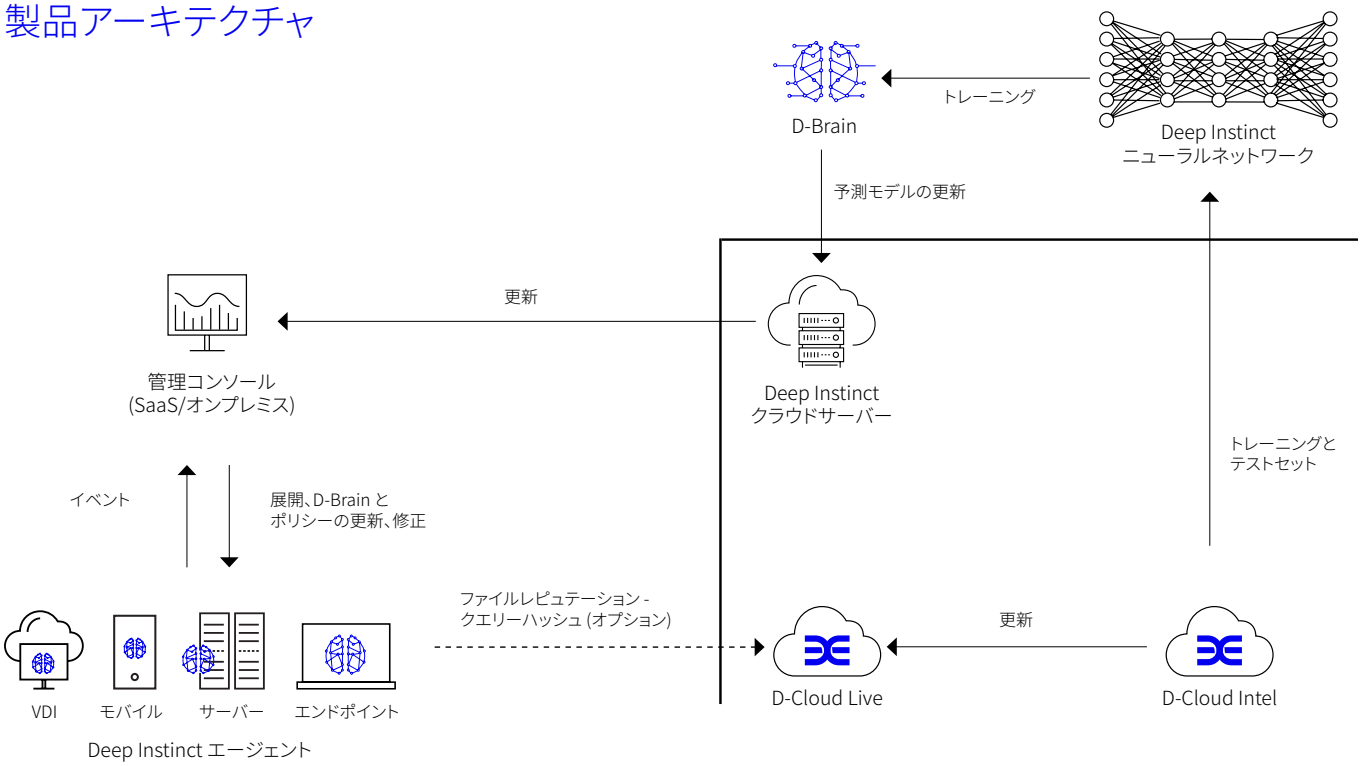
スパイウェア

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。

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。

製品アーキテクチャ



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)

BEFORE YOU KNOW IT
www.deepinstinct.com/ja/