deep instinct
BEFORE YOU KNOW IT

net one Partners
ネットワンパートナーズ株式会社

Windows
データシート

Deep Instinct™ D-Client for Windows

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。

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。

- 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。

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

PCI HIPAA GDPR
Coalfire
amtso SE Labs

テクノロジパートナシップ

splunk> MICRO FOCUS IBM Radar
CITRIX vmware amazon web services

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。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。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。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。悪意のあるキャンペーンの例には、APT33 などがあります。

既知のペイロードに対する防御

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。

実行後

Deep Instinct では、簡単にイベントを管理し、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

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、人の介入なしに、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。

攻撃解析

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。

高度な脅威解析

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。

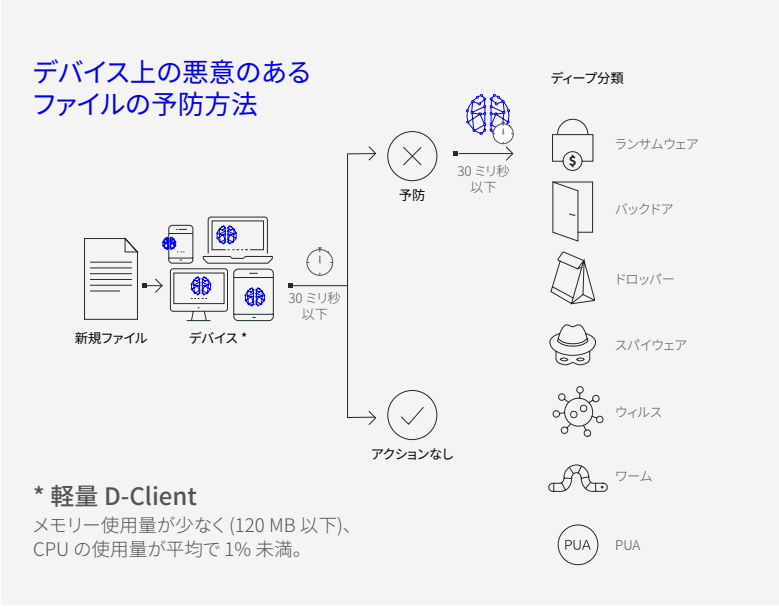
修正

ファイルの隔離

予防時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、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。

対応している攻撃手法

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。

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ベクトルを予防します。

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。

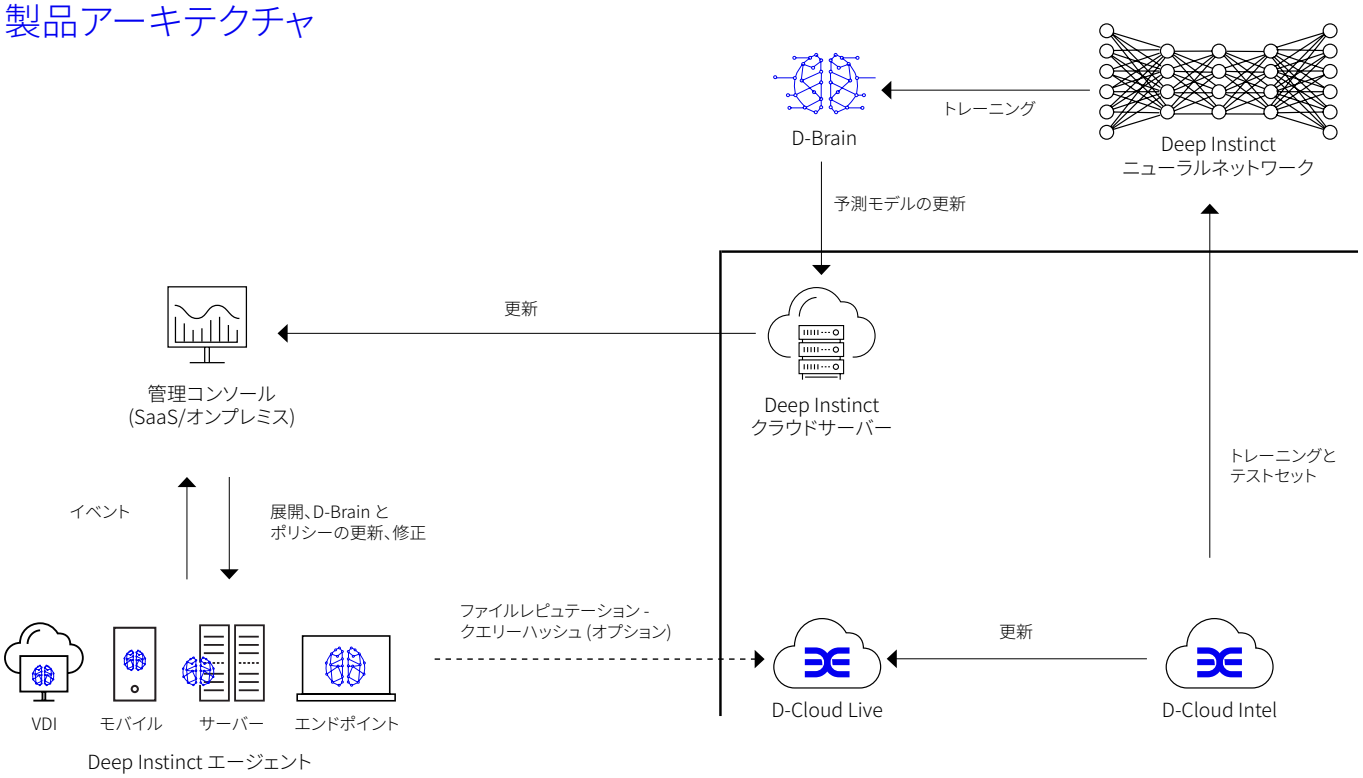
システム要件

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)
ディスク容量	500 MB の空きディスク容量

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

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)

www.deepinstinct.com/ja/