deep instinct
BEFORE YOU KNOW IT

nop
net one Partners
ネットワンパートナーズ株式会社

モバイルデータシート

ANDROID iOS

Deep Instinct™ D-Client for Mobile

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。D-Client は悪意のあるアプリケーションを予測して予防します。また、初期インストール時またはオンデマンドで完全なアプリケーションスキャンを実行することができます。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

振る舞い解析

ネットワーク攻撃や証明書の不正使用など、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。

ネットワーク攻撃

MitM (ARP ポイズニング)、SSL MitM、HOSTS ファイルの書き換えなど、ネットワーク攻撃の動作を検知します。

証明書の不正使用

悪意のある活動を実行するために使用可能な新規証明書のインストールを検知します。

コンプライアンス

- root 化またはジェイルブレイクされたデバイスの検出
- OS バージョンの監視
- パスコード、ストレージの暗号化、ロック画面のタイムアウト (物理アクセス攻撃)
- 不明なソース、USB デバッグ (アプリケーションの望ましくないインストール方法)

実行後

対処

ホワイトリスト

ハッシュに基づいてアプリケーションをホワイトリストに登録する機能を提供します。

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 Coalfire GDPR 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

広範な攻撃ベクトルに対応

悪意のあるアプリケーション

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、Android アプリケーション (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、望ましくない方法 (不明なソースや USB デバッグなど) でのアプリケーションのインストールが許可されないよう、デバイスを監視します。

エクスプロイト

悪用されていないことを確認するために、root 化またはジェイルブレイクされた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にデバイスのコントロールを奪うことができます。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。

物理アクセス

デバイスに物理的にアクセスできる攻撃者は、個人データや機密データを見つけてアップロードしたり、エンドユーザーになりすましたりする可能性があります。さまざまな設定 (パスコード、ストレージの暗号化、ロック画面のタイムアウトなど) を実施することにより、攻撃者が悪用できる攻撃可能面を減らすことができます。

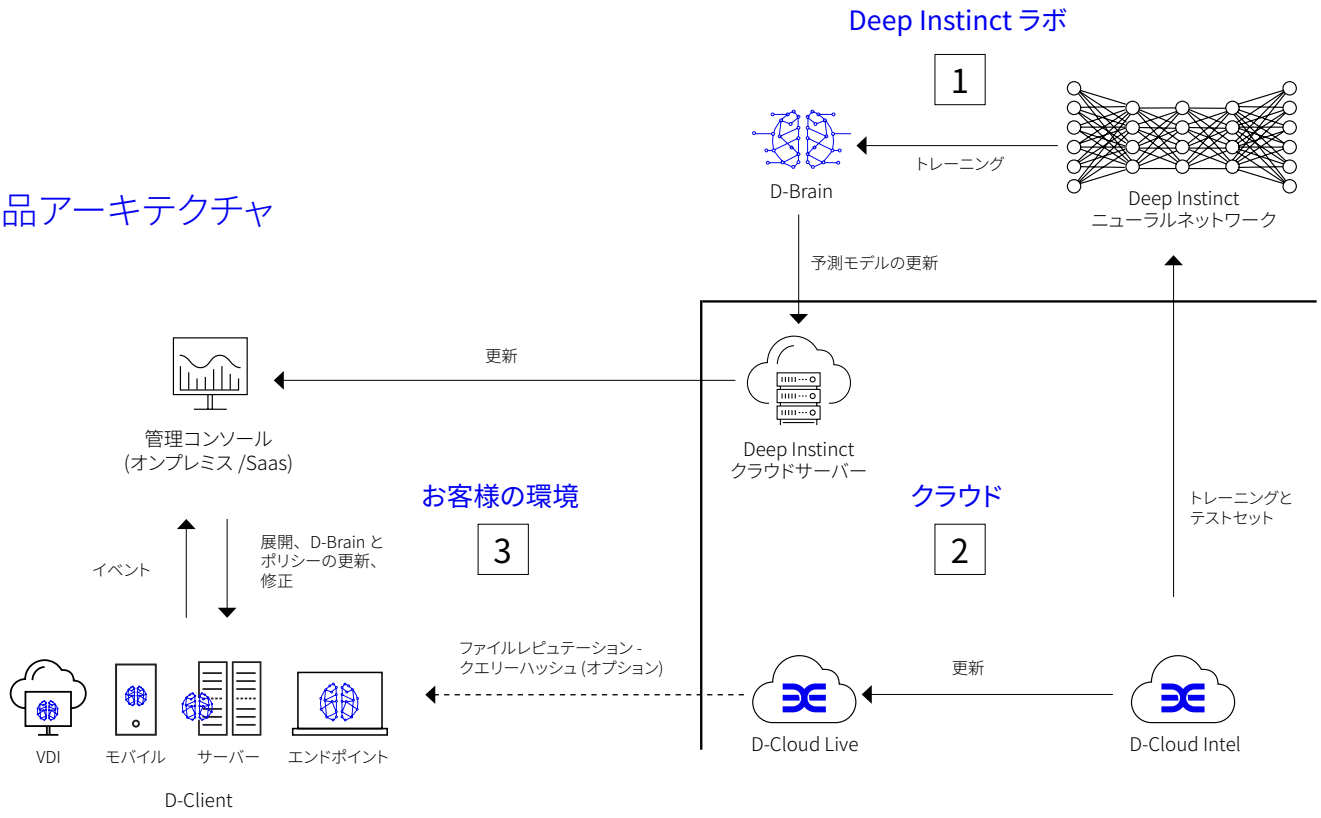
ネットワーク攻撃

通常、デバイスは常時ネットワークに接続されています。MitM (ARP ポイズニング)、SSL MitM、HOSTS ファイルの書き換え、証明書の不正使用など、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。

システム要件

	Android	iOS と iPadOS
オペレーティングシステム	バージョン 5 以降	バージョン 11 以降
ディスク容量	70 MB の空きディスク容量	80 MB の空きディスク容量
メモリ使用量	100 MB 以下	30 MB 以下

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/