

# Chrome OS |

## データシート



## Deep Instinct D-Client for Chrome OS

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、比類のない精度でリアルタイムに検知・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。

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 テクノロジー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。

#### 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

SSL MitM、HOSTS ファイルの書き換え、証明書インストールなどのネットワーク攻撃の動作を検知します。

#### デバイスレベル

ルート、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 (例: USB デバッグ) など、さまざまな悪意ある活動やデバイス上の問題のある設定を検知します。

### 実行後

#### 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

- 唯一のプロバイダ**  
 Deep Instinct は Chrome OS 向けに唯一の AI ベースのソリューションを提供します。
- 優れたテクノロジー**  
 AI テクノロジー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



## テクノロジーパートナーシップ



## 広範な攻撃ベクトルに対応

### 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、ドロップパー、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。

サイドローディング (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ないように、デバイスを監視します。

### 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にデバイスのコントロールを奪うことができます。デバイスのルートを監視し、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。

### 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。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。

## システム要件

オペレーティングシステム	バージョン 9 以降
ディスク容量	70 MB の空きディスク容量
メモリ使用量	100 MB 以下

## 製品アーキテクチャ

