DEEP INSTINCT DATA SECURITY X

ゼロデイデータセキュリティ

0.1% 未満
の誤検知率

99% 以上
の未知のゼロデイおよび
ランサムウェア攻撃を予防

20 ミリ秒以内
でリアルタイム判定

データは組織にとって最も重要な資産です。「Dark AI」が高度なゼロデイ攻撃の急激な増加を引き起こす中、従来のサイバーセキュリティーツールでは攻撃に対応する能力が不十分であり、データは脆弱な状態のままです。Deep Instinct Data Security X (DSX) は、ゼロデイデータセキュリティ (ZDDS) 専用のソリューションであり、他のどのベンダーも検出できない脅威を予防し、ゼロデイ攻撃をリアルタイムで対応・分析することで、この重大なギャップに対処します。

なぜゼロデイデータセキュリティが重要なのか

Deep Instinct DSX は、今日の最も高度なサイバーセキュリティの課題を解決するためにゼロから構築された、最初で唯一のディープラーニングフレームワークを活用しています。DSX は攻撃を受けた瞬間にリアルタイムで防御でき、Web アプリケーション、プライベートやパブリッククラウド、インターネットからのダウンロード、NAS やクラウドストレージ環境、サードパーティのサプライヤからの転送など、様々な場面で悪意のあるファイルからお客様の環境を保護します。

- **法的規制への対応** – 規制や社内ポリシーのコンプライアンス要件に対応
- **リスクの軽減** – ビジネスや評判に深刻なダメージを与える可能性があるコストのかかるゼロデイ攻撃を予防
- **TCO の削減** – 攻撃への対応に関連するインフラのリソースと人件費を最小化

DEEP INSTINCT DSX の利点

- **リアルタイムの予防：** ゼロデイ脅威を 99% 以上の有効性で阻止し、誤検知率はわずか 0.1% 未満
- **リアルタイムの解析：** 生成 AI (DSX Companion) を使用し、ゼロデイ攻撃についての詳細な分析とコンテキストを提供
- **あらゆる場所でデータを保護：** クラウド、NAS、アプリケーション、エンドポイント上でのデータに対する包括的なセキュリティ
- **スケーラブルなソリューション：** 大規模なリポジトリをエンタープライズ規模のスピードとスケールでスキャン
- **プライバシーへの対応：** データのプライバシーとコンプライアンスに対応 – ファイルやデータを環境外へ送ることなく保護
- **自律的動作かつクラウドに依存しない：** 悪性または良性の判定をクラウドへの接続なしにローカルで実施可能、アップデートは年に 1 ～ 2 回のみ

Deep Instinct Data Security X

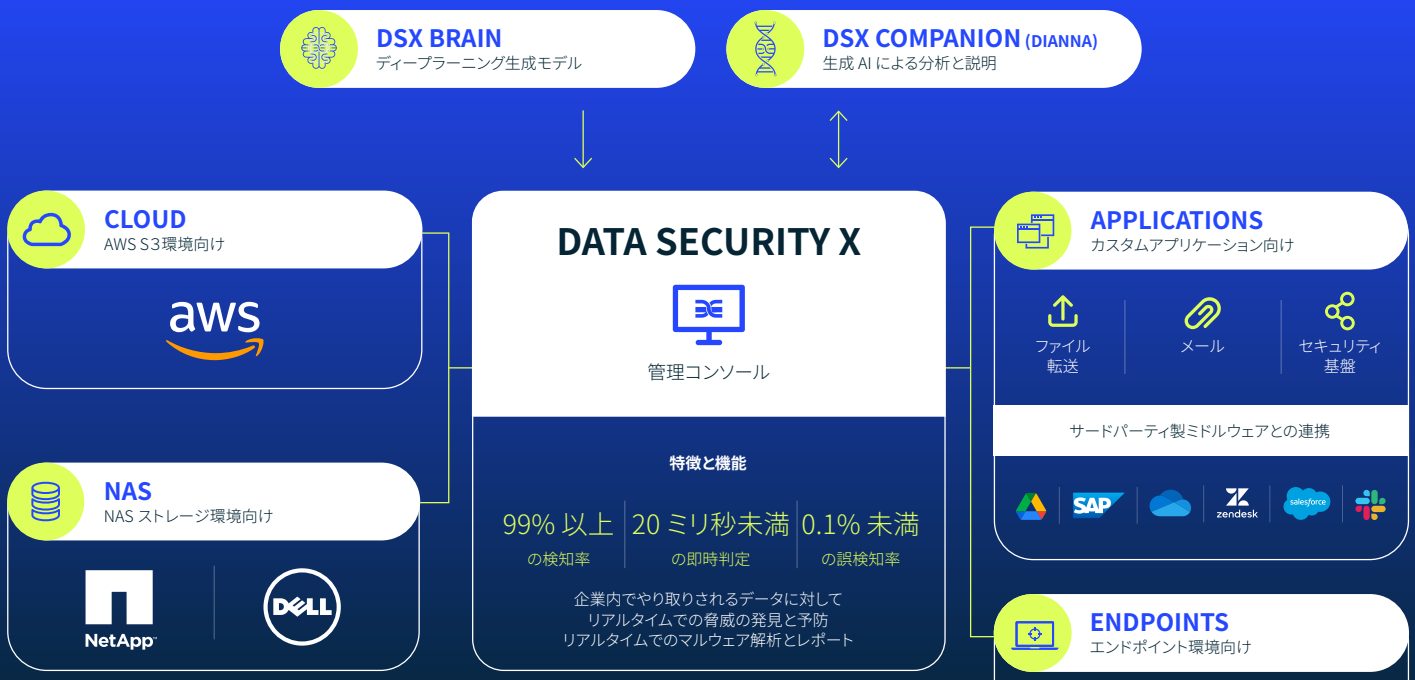
Deep Instinct DSX は、専用のディープラーニングサイバーセキュリティフレームワーク (DSX Brain) と生成 AI (DSX Companion) を活用して、ゼロデイ攻撃をリアルタイムに予防および分析します。

ゼロデイ脅威の予防 (DSX BRAIN)

Deep Instinct DSX は、クラウドや NAS のリポジトリ、アプリケーション、エンドポイント環境のすべてでリアルタイムに脅威を判定し防御できる、市場で最も高速かつ効果的なゼロデイ脅威予防ソリューションを提供します。サイバーセキュリティ専用にゼロから設計された世界で唯一のディープラーニングフレームワークを使って生成された DSX Brain を活用しており、脅威が実行される前に阻止することで、ゼロデイ攻撃のリスクを大幅に低減できます。

ゼロデイ脅威の解析と説明 (DSX COMPANION)

生成 AI の DIANNA を搭載した DSX Companion は、比類ない分析と説明能力を備えた包括的なゼロデイマルウェア解析を提供します。DSX Companion の DIANNA は、DSX Brain と連携して、阻止された脅威の攻撃パターンや振る舞いなど、マルウェアの構造に関する詳細な分析レポートを提供し、他のソリューションでは再現できない包括的な解析をリアルタイムで実現します。これにより、セキュリティおよびインフラチームは、ゼロデイ脅威を迅速に理解して対応することが可能になります。ディープラーニング と生成 AI を活用した独自技術の組み合わせにより、SOC 全体の効率性が向上し、組織の脅威に対する体制が改善されます。



DSX: ゼロデイデータセキュリティの実現

Deep Instinct DSX は、攻撃者に対する圧倒的な優位性を組織にもたらします。クラウドや NAS ストレージ、カスタムアプリケーション、SaaS アプリケーション、エンドポイント環境全体において実行される前に脅威を阻止します。

DSX for NAS

DSX for NAS は、ネットワークアタッチドストレージ (NAS) のスキャンと保護を目的とした予防ファーストのソリューションです。ランサムウェアやマルウェアがストレージに到達して実行されるのを防ぎ、ゼロデイや未知の脅威などを 99% 以上阻止します。ディープラーニングを搭載した DSX for NAS は、超高速 (1 ファイルあたり 20 ミリ秒未満) でストレージ環境全体をスキャンし、データの安全を確保します。

NAS ストレージインフラストラクチャとシンプルに統合

DSX for NAS は、脅威がストレージリポジトリに侵入するのを防ぎ、Dell CAVA や NetApp Vscan などの主要な NAS ソリューションと統合して、迅速な導入や連携を実現します。

プロアクティブにストレージを保護

DSX for NAS は、ストレージ環境に送られるファイルをスキャンし、悪意のあるコンテンツに自動的に対処して、感染したファイルをユーザーが開く前に隔離または削除できます。このプロアクティブなアプローチにより、脅威がストレージリポジトリを通してユーザー環境に広がる前にブロックします。

ボトルネックなし

平均ファイルスキャン速度が 20 ミリ秒未満であるため、チームは待つことなく作業に時間を費やすことができます。また、データリポジトリ全体をフルスキャンをしたとしても、従来製品のように数日や数週間もかかることなく数時間で完了します。

TCO を削減

速さと生産性の向上に加え、必要なインフラを最小限に抑えることで、さらなるコスト削減が可能となり、業界の競合他社よりもはるかに低い TCO を実現できます。

DSX for Cloud

DSX for Cloud は、クラウドストレージの保護に予防ファーストアプローチを適用し、ランサムウェアやマルウェアがデータに到達してクラウドストレージ環境で実行されるのを阻止します。クラウドストレージ環境とシームレスに統合され、比類ない有効性、精度、エンタープライズ規模のスケーラビリティを実現します。

クラウドストレージを数分で保護

DSX for Cloud は、超高速スキャンにより低コストで企業のスケーラビリティを実現し、悪意のあるファイルがストレージバケットに到達するのを防ぎ、ファイルの整合性を確保し、重要な資産へのアクセスを保護します。DSX for Cloud は、ネイティブクラウドサービスを使用して数分でデプロイできます。

プロアクティブにクラウドストレージを保護

DSX for Cloud は、ストレージ内に保存または送信されるファイルをスキャンし、悪意のあるコンテンツに自動的に対処して、感染したファイルをユーザーが開く前に隔離または削除できます。このプロアクティブなアプローチにより、脅威がストレージリポジトリを通してユーザーに広がる前にブロックします。

エンタープライズ規模のスピードとスケールで運用

平均ファイルスキャン速度が 20 ミリ秒未満であるため、リポジトリに保存されている膨大な量のデータのスキャンも短時間で完了でき、クラウドストレージ内のデータの安全性を確保できます。

TCO を削減

スピードと生産性の向上に加え、クラウドインフラの活用によってさらなるコスト削減を可能とし、業界の競合他社よりもはるかに低い TCO を実現します。

DSX for Applications

DSX for Applications は、エージェントレスのオンデマンドマルウェア対策ソリューションで、アプリケーション内を流れるファイルをスキャンして悪意のあるコンテンツを検出します。エンタープライズ規模で機能し、ゼロデイ、未知、既知のマルウェアを検出してブロックできます。

悪意のあるファイルを阻止

99% 以上の有効率を持つ DSX for Applications は、攻撃者に早期に対処し、ランサムウェア、未知、ゼロデイの攻撃など、ファイルに潜む脅威を防ぐことを可能にします。Web アプリケーションを通じたファイルのアップロードをブロックし、インターネットからのダウンロードをスキャンし、サードパーティのサプライヤから環境へのファイルの転送を安全にして、悪意のあるコンテンツがネットワークを通過するのを防ぎます。

ワークフローに合わせた最適化

DSX for Applications は、既存のワークフローに組み込み可能な軽量のエージェントレスソリューションにより、お客様の環境に統合できます。OS やデバイスに依存しない柔軟でプログラマブルな REST API または標準的な ICAP のインタフェースをサポートします。

ペタバイト規模にも対応

毎日数千万ものファイルを迅速にスキャンし、ユーザーエクスペリエンスに影響を与えることなく、あらゆる Web アプリケーションやクラウドストレージ環境を悪意のあるコンテンツから保護します。

DSX for Endpoints

DSX for Endpoints は、多層的な予防ファーストのアプローチで既存の EPP を置き換え、EDR や SIEM ツールと共存できます。攻撃者がエンドポイントに悪意のあるペイロードを仕掛けようとすると、DSX for Endpoints は、それが実行されて感染する前に阻止します。

実行前の防御：静的解析による予測と予防

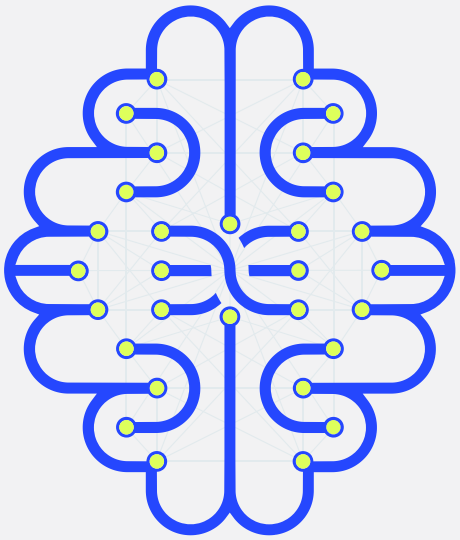
DSX for Endpoints は、ディープラーニングによって生成された静的解析エンジン DSX Brain を使用して、ゼロデイエクスプロイト、ランサムウェア、ファイルベースやスクリプトベースの攻撃など、既知および未知のマルウェアを 99% 以上の精度で阻止します。

実行時の防御：動的解析と振る舞い分析

多層的な予防アプローチを採用し、動的解析と振る舞い分析の機能を追加することで、悪意のあるコードインジェクションや認証情報の盗難などのファイルレス攻撃、未知のシェルコードや多段階攻撃などの高度なスクリプト攻撃、アクティブな敵対的 AI 攻撃など、最も高度な脅威に対する防御と対応の自動化を実現します。

実行後の防御：自動解析

DSX for Endpoints は、脅威ハンティングや MITRE ATT&CK マッピングのための疑わしいイベントなど、セキュリティチームが脅威の重大度や戦術を理解するのに役立つコンテキストと解析を提供します。



なぜディープラーニングが重要なのか

ディープラーニングは、脳が経験から考え学習する能力にヒントを得た、AI の最も洗練された形態です。この能力により、DSX Brain は攻撃者が環境内に侵入する前に攻撃を阻止することができます。

Deep Instinct のディープラーニングベースのソリューションには、以下のような重要な利点があります。

- データセット内の生データを 100% 使ってトレーニングを行い、より大きなコンテキストを用いた非線形の相関分析を行うことができ、より精度が高く、細やかで迅速な分類予測を可能に
- 年に 1~2 回の更新のみでゼロデイの脅威をすべて防御
- 脅威や攻撃者の意図に関する前知識を必要とせず、脅威ファイルの DNA を理解できるため、人手による特徴量エンジニアリングを必要とせず、学習のために必要な時間と労力が少なくて済む
- クラウドへの問い合わせや脅威インテリジェンスフィードに依存せずに自律的に動作し、ローカル判定を行うことで、予防までの時間を短縮
- 他の AI や ML のモデルよりも圧倒的に高い検知精度を誇り、誤検知率も 0.1% 未満に低減

ディープラーニングベースのサイバーセキュリティは、脅威が実行される前に予測して防止することで、組織が予防を実現するのに役立ちます。これにより、エンドポイント、アプリケーション、NAS、クラウドストレージ全体で、攻撃者を環境から可能な限り追い出すことが可能になります。生成 AI を活用したゼロデイ攻撃のリアルタイムの分析と解説を提供する DSX Companion を組み合わせることで、ディープラーニングベースのサイバーセキュリティは、お客様のサイバーセキュリティ能力と、組織を保護するうえで頼りにしている SOC チームの業務効率に変革をもたらします。