

## NeuShield Data Sentinel 2.1

### ランサムウェアは、もう怖くない

#### MIRROR SHIELDING™

受賞歴のある NeuShield の Mirror Shielding™ テクノロジーは、バックアップやロールバックに頼ることなく、サイバー脅威によるあらゆる種類の破壊、消去、暗号化から即座にデータを復元することができます。データが人質に取られることは、二度とありません。

#### ONE-CLICK RESTORE

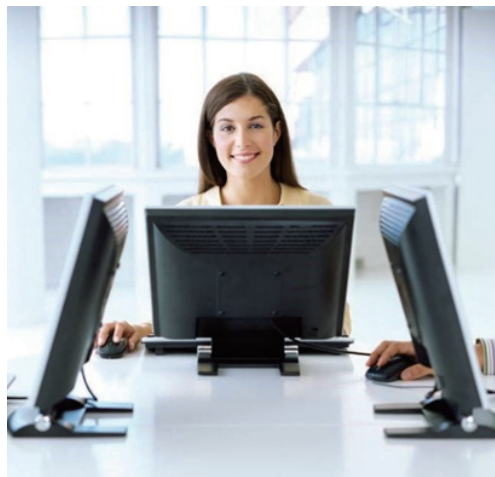
ワンクリックで、数分以内に OS 全体を元の良好な状態に戻すことができます。もう、検出されなかったマルウェア、欠陥のあるパッチ、OS の破損などによる時間の無駄を心配する必要はありません。

#### FILE LOCKDOWN

ランサムウェアの攻撃を受けたとしても、システムを止められない場合があります。それでも問題はなりません。NeuShield Data Sentinel はデータをロックすることができるため、One-Click Restore で OS を復旧させるまでの間、従業員はデータを使って仕事を続けることができます。

#### DATA ENGRAMS™

Mirror Shielding™ を使えば、異なる時点でのデータのコピーを作成することができます。Data Engrams™ はファイルの修正履歴のように機能し、ファイルを以前のバージョンに復元することができます。



- 現在導入しているセキュリティソリューションが、**わずか5分間**でもうまく動作しなかったり、たった1つの脅威でも見逃してしまったら、何が起きますか？
- もしあなたの会社が**標的型攻撃**や**ゼロデイ攻撃**に狙われたとした場合、準備はできていますか？すべての従業員が、そのような状況に適切に対処できるでしょうか？
- 従業員が Web サイトを閲覧して新しい**ファイルレスマルウェア**に感染したとしたら、どうしますか？
- 全く新しい、**完全に検知不能 (FUD: Fully Un Detectable)** なランサムウェアの脅威によって、すべてのデータが暗号化されてしまったらどうしますか？

### NeuShield は何が違うのか？

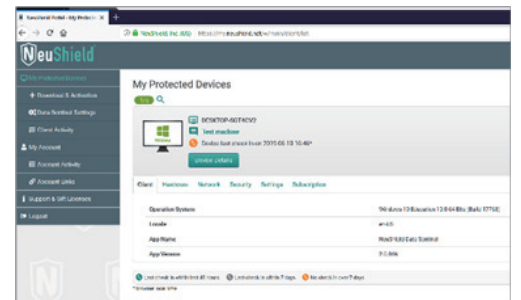
多くの企業が、多階層構造のセキュリティモデルに**莫大な投資**をしています。それにもかかわらず、ランサムウェアの被害は一向に減りません。それは何故でしょうか？

その理由は、ランサムウェアが標的型に進化しているからです。それを防ぐためには、データを保護するための新しいアプローチが必要です。

NeuShield Data Sentinel は、ユーザーのファイルとアプリケーションの間に保護のための防護壁を設けるといって、これまでとは全く異なるアプローチを採用しています。ランサムウェアや他のアプリケーションがファイルを変更した場合でも、**オリジナルのファイル**はそのまま残っており、ユーザーは意図しない変更を元に戻すことができます。ファイルの**バックアップコピー**を作成するタイプのソリューションでは、ディスクの使用量が大幅に増加し、処理速度にも大きな影響を与えます。しかし NeuShield の革新的な Mirror Shielding™ 技術は、バックアップを必要とせずオリジナルのファイルを保持することができるため、Data Sentinel は**ディスク処理 (I/O)** を行わずにファイルを保護することができます。

NeuShield Data Sentinel は、**マルウェアや人的エラー**からデータを保護し、シールドすることができます。その機能には One-Click Restore、File Lockedown、Cloud Protection、Boot Protection、Disk Protection、File/Folder Protection などがあります。

時間に厳しいビジネスで、ダウンタイムが許されない場合であれば、NeuShield はビジネスにとって最も重要な保護層となります。



## 機能とメリット



NeuShield は、マネージドサービスプロバイダー (MSP) とその IT スタッフに、ビジネスに影響を与える可能性のある脅威からすべてのユーザーを**完全に保護**するための完璧なツールを提供します。

デプロイメント、管理、リカバリーのすべてを、マルチテナント型のクラウドベースの管理コンソールから管理することができ、お客様に**ダウンタイムの無い**サービスを提供します。

### Remote One-Click Restore

コンピュータへのローカルアクセスを必要とせずに、**管理インターフェイス**から破損または感染した OS を復元します。

### Remote Revert

コンピュータが感染したり、データが破損したりした場合でも、NeuShield の管理インターフェイスから、破損したファイルや暗号化されたファイルを**即座に復元**することができます。

- Mirror Shielding™
- One-Click Restore
- File Lockdown
- Cloud drive protection
- Boot protection
- Disk wipe protection
- Cloud management
- Data Engrams™ を使ったファイルの履歴管理
- カスタムフォルダ保護
- Kaseya VSA との統合

## お客様の声



“多くの企業では、攻撃を受けると復旧までに半年以上もの時間を費やすこととなります。私たちは、お客様が迅速に業務を再開できるような修復ツールを必要としていました。NeuShield は安心を与えてくれます。”

Darin Harris (Remote Techs COO)

## システム要件

- OS : Windows 7, 8.1, 10, 11
- OS : Windows Server 2008 R2, 2012 (R2 を含む), 2016, 2019, 2022
- プロセッサ : 1 GHz 以上
- メモリ : 1 GB (32 ビット) または 2 GB (64 ビット)
- ディスク容量 : 500 MB の空き容量 (10GB 以上推奨)
- ディスプレイ : 1366x768 以上

提供サービス

- テクニカルサポート
- インストールとセットアップ
- メンテナンス



セキュリティストリングス株式会社

〒102-0082 東京都千代田区一番町6番地 相模屋本社ビル7F  
Email: sales@securitystrings.com  
URL: https://www.securitystrings.com



お問い合わせ