Data Guards

ランサムウェアによって暗号化された 6TB ものデータを瞬時に復元 ～加 Data Guards の NeuShield 活用事例～

Data Guards はカナダのオンタリオ州に拠点を置くマネージドサービスプロバイダー（MSP）で、地域の企業や非営利団体に IT 管理およびサイバーセキュリティサービスを提供しています。同社は、技術者が毎晩クライアントマシンにログインしてアップデートおよびメンテナンス、そしてプロアクティブな脅威チェックを行うなど、ハンズオンの実践的なシステム管理アプローチを提供しています。

信頼性およびパフォーマンス、そして迅速な復元に重点を置く Data Guards は、教育機関から文化遺産関連施設まで、幅広い業界のクライアントをサポートしています。最近、クライアントの 1 つである地域の博物館が大規模なランサムウェア攻撃に遭った際には、数日かかると思われた復元作業を、NeuShield を使うことで迅速に完了させることができました。

Data Guards のマネージドセキュリティへのアプローチ

Data Guards は、従来型のウイルス対策やファイアウォール、ネットワーク監視、継続的なパッチ管理を組み合わせた多層防御モデルをクライアントに提供しています。同社は自動化されたスケジューリングに頼らず、すべてのソフトウェアとシステムのアップデートを毎晩実施することで脅威に先手を打つことに、特に重点をおいています。

こうした努力にもかかわらず、サイバー攻撃は常に進化しているため、万全なセキュリティ対策を講じた組織であっても、ランサムウェアやマルウェアによるインシデントに遭遇することがあります。そのため Data Guards は保護スタックに NeuShield Data Sentinel を追加しており、他の防御策が失敗した場合でも、クライアントがシステムを即座に復元できるように備えています。

ポイント 1：ランサムウェアが地域の博物館を攻撃した際に、NeuShield が 15 分でサーバーを復元

ある日の午後、Data Guards はクライアントである博物館の Windows サーバーから、定期バックアッププロセス中にトロイの木馬が検知されたことを示す自動アラートを受信しました。数分のうちに、ランサムウェアはサーバーの D ドライブ上のファイルを暗号化し始めました。このファイルには、**6.2 テラバイトを超える貴重なデータ**が含まれていました。

Data Guards の CEO である Andy David 氏は、直ちに博物館に連絡し、スタッフにサーバーをネットワークから切断するよう指示しました。その後マシンを回収して検査したところ、ランサムウェアはスケジュールされたバックアップタスクによって起動し、プロセスが実行されるたびに実行されていることがわかりました。

システムドライブに問題がないことを確認した後、Data Guards は NeuShield Data Sentinel を使用して暗号化されたデータを復元しました。

Andy David 氏は「私はただ、D: ドライブを右クリックして『Restore』を選択しただけです。」と言います。「たったそれだけでした。」

NeuShield は**わずか 15 分**で 6.2TB のデータすべてを攻撃前の状態に復元し、クラウドバックアップからのダウンロードやスクラッチからの再構築を行うことなく、博物館のサーバー全体を復元したのです。

これとは対照的に、今年初めに起きたランサムウェア攻撃では、博物館が NeuShield の保護を導入する前であったため、従来型のバックアップツールを使用した復元プロセスには**5 日間以上**の時間を要しました。

「15 分で復元できたのは驚きでした。」と David 氏は言います。「前回の攻撃の時と比べ、数日間のダウンタイムを回避できましたし、多大なストレスが緩和されました。博物館も非常に感謝しています。」

ポイント 2：バックアップソリューションだけでは不十分

前回のランサムウェア攻撃では、Data Guards は博物館のシステムを復元するために、Datto を使用したクラウドバックアップソリューションに頼らざるを得ませんでした。この復元プロセスでは、サーバーの再イメージ化、ドメインへの再参加、アカウントの復元、そして数テラバイトのデータのダウンロードが必要でした。

このクライアントの環境は 100Mbps の対称型接続でしたが、バックアップイメージのダウンロードには **5 日半**かかり、サーバー自体の再構築よりも時間がかかりました。

「サーバーの再構築よりも、データのダウンロードに時間がかかりました。」と David 氏は言います。「システムの準備が整ってからファイルがダウンロードされるまで、さらに 4 日間待たなければなりませんでした。」

ポイント 3：MSP 向けの実用的なセキュリティと信頼性

Data Guards は、迅速な復元と最小限のダウンタイムを望むクライアント向けに NeuShield を提供しています。このソフトウェアは既存の環境に簡単に統合でき、MSP にリモートからのワンクリック復元機能を提供します。

「クライアントによく言うのですが、NeuShield は本当に最高です。」と David 氏は言います。「シンプルで効果的で、最も必要なときに役立ってくれます。」

この高速なロールバック機能により、Data Guards は、攻撃やアップデート失敗の際に必要となる技術者の作業時間を大幅に削減しながら、プレミアムサービス並の短い復元時間を実現できるのです。

NeuShield Data Sentinel 独自の復元技術

NeuShield のミラーシールド技術（特許取得済）は、ストレージ層でファイルとオペレーティングシステムを保護することで迅速な復元を可能にします。通常、バックアップイメージからシステムを再構築する復元プロセスには時間がかかりますが、NeuShield はファイル削除や更新履歴を使ったアプローチにより攻撃前の状態にデータを復元するため、迅速な復元が可能になります。

この設計により、MSP は、テラバイト単位のデータを含むデバイスであっても、ランサムウェアやアップデートの失敗、または誤った削除から、システムを数分以内に復元することができます。完全に検知不可能（FUD：Fully Undetectable）な脅威やゼロデイ脅威も、システムの再インストールやクラウドへの依存なしに無効化できます。

従来型のバックアップシステムは長期的なデータ保持という観点では依然として有用ですが、NeuShield はローカルでの迅速な復元という重要なギャップを埋め、数日間におよぶダウンタイムを排除し、MSP とクライアントのコストと複雑な作業を緩和します。

NeuShield について

NeuShield は、データ保護における革新的なアプローチを提供します。同社の特許取得済み製品である「NeuShield Data Sentinel」は、脅威を個々に検知して阻止するのではなく、重要なデータそのものを守ることで、脅威による改ざんを防止します。企業ユーザーやエンドユーザーは、ウイルス対策やランサムウェア対策などの他のマルウェア対策が失敗した場合にデジタルファイルやデバイスを攻撃前の状態に戻すための、シンプルで信頼性が高く、費用対効果の高い方法として NeuShield Data Sentinel を利用しています。

SECURITY STRINGS AUTHORIZED VALUE ADDED DISTRIBUTOR
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