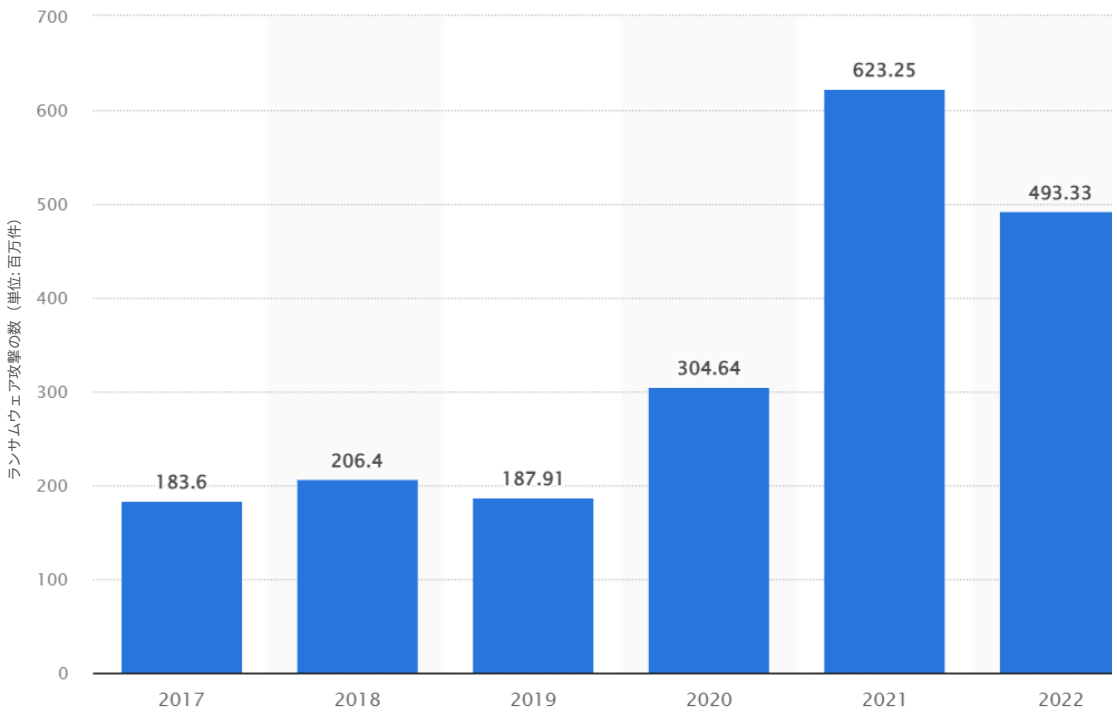
NetVault® Plusを使用したランサムウェア対策とリカバリ

ランサムウェア攻撃は世界中の企業や非営利団体を悩ませ続けており、取り返しのつかない被害と多額の費用を引き起こしています。さらに、ブランドの評判と顧客サービスにも悪影響を与え、最悪の事態を招きます。



ランサムウェア攻撃の数（出典: 2022年Statistaレポート）[1]

ランサムウェア攻撃は2022年にいくらか減少しましたが、それでも全世界で5億件近い攻撃がありました。IBMの「Cost of a Data Breach 2022（2022年データ侵害のコスト）」レポート[2]によれば、身代金の平均支払い額は812,360ドルでした。 しかしながら、身代金の実際の支払いはランサムウェア攻撃の総費用のほんの一部に過ぎず、IBMでは平均で450万ドルにのぼると見ています。IBMはまた、組織がランサムウェア侵害を特定して修復するには、他のタイプの攻撃よりも平均49日長くかかると指摘しました。

組織は、ランサムウェアの影響に対抗する機能が強化されたバックアップソリューションが必要です。Quest® NetVault Plusはまさにそのようなソリューションです。NetVault Plusは、最新のデータ・センター・アプリケーションやインフラストラクチャだけでなく、Microsoft 365のようなクラウドソリュー

1 Statista
2 IBM

ション向けに開発された包括的なデータ保護ソリューションです。広範なランサムウェア対策、リカバリ、および最適化機能を搭載しています。

保護

ランサムウェア攻撃に備えるには多層的なアプローチが必要であり、バックアップ/リカバリの強固なソリューションは、ビジネスリスクを最小限に抑える最後の防衛線です。

まず、NetVault Plusが提供するエンタープライズクラスのバックアップ/リカバリは、世界中の数千の組織で使用されています。オンプレミスとクラウドの両方で、幅広いシステム、アプリケーション、データを保護します。NetVault Plusは、VMware仮想マシンの永久増分保護を実行する継続的データ保護（CDP）を提供し、バックアップの高速化とデータロスと損傷のリスクの低減に役立ちます。

NetVault Plusには、重複除外、圧縮、暗号化、レプリケーション、クラウド接続を提供するソフトウェア定義型のストレージコンポーネントが含まれます。このストレージ技術は、バックアップデータを保護するRapid Data Access（RDA）と呼ばれる未公開のプロトコルに依存しています。Windowsのファイル共有に使用されているServer Message Block（SMB）とは異なり、RDAは非公開プロトコルです。オペレーティングシステムから直接アクセスできず、認証要件がローカルサーバやドメイン管理対象構造の外側に置かれています。また、NetVault Plusはデータ暗号化にも対応しており、オンプレミスとクラウドの両方のデータが確実に保護されます。政府のデータセキュリティ要件に対応するため、NetVault Plusの暗号モジュールはFIPS 140-2レベルに認定されています。

NetVault Plusは、バックアップ保持ポリシーで、NetVault管理者であってもバックアップデータを上書き、変更、削除、暗号化ができないように「変更不可」としてバックアップジョブを割り当てることができるため、ランサムウェア対策を強化します。

NetVault Plus使用時、バックアップデータはソースから宛先に直接送信されます。従来のメディアサーバは不要です。これにより複雑さが軽減され、攻撃の対象となるコアコンポーネントの数が減ることでリスクも軽減できます。

それに加えて、NetVault Plusは、TLS 2.0の安全なレイヤーでデータ転送および管理コマンドをラッピングするSecure Connectテクノロジーを採用しています。これにより、ランサムウェアからバックアップデータへのアクセスが大幅に制限されます。

NetVault Plusを使用すると、バックアップデータを迅速かつ安全に複製して、ディザスタリカバリのための3-2-1バックアップ戦略を可能にします。また、保護をさらに強化するため、NetVault Plusはテープへのエアギャップバックアップも提供しています。

もちろん、NetVault Plusシステム自体がバックアップデータにアクセスできるため、それについても考慮する必要があります。ランサムウェアはWindowsベースのシステムを主な標的としていることが知られていますが、その理由として挙げられるのは、普及率の高さ、そしてランサムウェア犯が悪用できるユーザクライアント/ユーザエンドポイントの多さです。NetVault Plusは、Linuxへのシステムインストールをサポートすることで、その脅威を軽減します。完全に脆弱性がなくなるわけではありませんが、NetVault PlusシステムをLinux上にインストールすることで、潜在的な脅威の数が減少します。

もう1つの考慮事項は、システムアクセス権を付与する方法です。NetVault Plusでアクセス権を付与する方法は2つあり、ディレクトリサービスとの統合を使用するか、独自のロールベースのアクセス方法を使用します。Active Directoryのグループポリシーおよびグループ・ポリシー・オブジェクト（GPO）攻撃のリスクを考慮した場合、アクセス権付与のレベルが侵害されると、バックアップアプリケーションへのアクセスが可能になり、システム全体のデータが削除される恐れがあります。システムアクセスの制御にActive Directoryを利用することはできますが、NetVault Plusも強固なロールベースのアクセスを提供しているため、Active Directoryを使用する必要がありません。これはユーザやグループ管理の面では多少不便かもしれませんが、本番稼働環境の分離と許可されていないサードパーティによるアクセスからの保護がさらに強化されます。

リカバリ

NetVault Plusにより、リカバリが迅速かつ簡単になります。管理者は、必要なものを簡単に見つけて、リカバリを即座に開始できます。NetVault Plus CDP for VMwareを使用すると、NetVault Plusの重複除外されたセカンダリ・ストレージ・リポジトリからVMスナップショットイメージを直接マウントすることで、仮想マシンを即座にリカバリできるインスタントリストアを利用できます。

最適化

NetVault Plusには、データ保護を簡素化し、ITスタッフの生産性を向上させる強力な自動化機能を備えています。グローバルなソース側のデータ重複除外および圧縮を提供し、バックアップ/リカバリを高速化すると同時に、ストレージ要件とコストを90％以上削減します。NetVault Plusの重複除外は、よくある重複除外とはまったく異なります。まず、すべてのバックアップジョブで重複除外を実行し、真にグローバルな重複除外を実現します。これには、可変ブロックの重複除外チャンキング手法と、データストリーム内の追加や削除によって生じる変化に関係なく、データ内のパターンを識別するコンテンツ認識型アルゴリズムを組み合わせています。最終的に、業界で可能な限り最高のストレージ削減が得られるのです。また、このソース側の重複除外により、クライアントマシンからストレージまで、ネットワーク経由で送信されるデータ量が減り、データキャプチャ技術にさらされる機会が更に減ります。

NetVault Plusのクラウド階層化は、より新しいバックアップはオンプレミスに保持し、古いバックアップはクラウドに移動することで、バックアップデータの最適化にも役立ちます。このようにクラウドストレージを使用することで、オンプレミスストレージを使用するよりもコストを節約できます。クラウド階層化は、クラウドから必要なバックアップを取得している間に、より新しいバックアップをローカルディスクから提供するため、データをより迅速にリカバリすることもできます。

主なメリット

結局、準備を万全に整えた組織であっても、ランサムウェア攻撃を完全に防ぐことはできません。ただし、バックアップソリューションがあればリスクを抑えることができます。このソリューションにより、データを迅速かつ完全に復旧できる他、以下のことが可能になります。

- ビジネスに影響を与えるランサムウェアのリスクを軽減する
- 攻撃の可能性がある主要なコンポーネントの数を減少させる
- キャプチャ技術に対するデータの露出度を制限する
- ランサムウェアによるバックアップデータへのアクセスを制限する

NetVault Plusは、今日の困難でリスクの高い環境において、IT管理者や経営幹部が求める保護、リカバリ、および最適化の機能を提供します。

NetVault Plusの詳細については、www.quest.com/jp-ja/products/netvault-plusを参照してください。

Questについて

Questはますます複雑になるIT環境において、新たなテクノロジーのメリットを実現にするソフトウェアソリューションを提供します。データベースとシステムの管理からActive DirectoryとMicrosoft 365の移行および管理、そしてサイバー・セキュリティ・レジリエンスまで、Questは次のIT課題を今すぐ解決できるよう、お客様をサポートします。世界中の13万社を超える企業とFortune 500の95 %が、次のエンタープライズイニシアチブのプロアクティブな管理と監視を実現し、複雑なMicrosoftの課題に対する次のソリューションを見つけ、次の脅威に事前に対処できるQuestを信頼しています。Quest Softwareは今「次」に備えます。詳細については、www.quest.com/jp-ja/をご覧ください。

© 2023 Quest Software Inc. ALL RIGHTS RESERVED.

本書に記載されている専有情報は、著作権によって保護されています。本書に記載されているソフトウェアは、ソフトウェアライセンスまたは機密保持契約のもとに提供されます。本ソフトウェアは、当該契約の条項に従う場合に限り、使用または複製できるものとします。本書のいかなる部分も、Quest Software Inc.の書面による許可なく、複写および録音を含む電子的または機械的ないかなる形式や手段においても、あるいはいかなる目的においても、複製または転載することはできません。

本書に記載されている情報は、Quest Software製品の概要説明を目的としたものです。本書によって、あるいはQuest Software製品の販売に関連して、明示または黙示にかかわらず、禁反言やその他の方法によって生じる、いかなる知的所有権に対するライセンスも許諾されません。当該製品のライセンス契約で指定されている約款に記載されている場合を除き、Quest Softwareはいかなる責任も負うものではなく、商品性、特定目的への適合性、または非侵害性に関する黙示的保証を含め（ただしこれらに限定されない）、その製品に関連する一切の明示的、黙示的、または法令による保証を行いません。Quest Softwareは、いかなる場合においても、本書の使用または使用不可能に起因する直接損害、間接損害、結果的損害、懲罰的損害、特別損害、または付随的損害（営業利益の損失、ビジネスの中断、情報の紛失を含むがこれらに限定されない）について、仮にそれらの発生の可能性を知らされていたとしても、一切の責任を負いません。Quest Softwareは、本書の内容の正確性または完全性に関する保証または表明を行わず、仕様および製品の説明に対する変更をいつでも予告なく行う権利を有します。Quest Softwareは、本書に記載されている情報を更新する確約を一切行いません。

特許

Quest Softwareは、当社の先進的なテクノロジーを誇りにしています。この製品には、特許および出願中の特許が適用される場合があります。この製品に適用される特許の最新情報については、当社のWebサイト（www.quest.com/jp-ja/legal/）をご覧ください。

商標

Quest、Questのロゴ、 Netvault Plus、およびQuest Softwareは、Quest Software Inc.の商標および登録商標です。Questの商標の一覧については、www.quest.com/jp-ja/legal/trademark-information.aspxをご覧ください。その他すべての商標は各所有者に帰属します。

本書の使用に関して不明な点がありましたら、以下までお問い合わせください。
www.quest.com/jp-ja/company/contact-us.aspx