

2021年11月18日
日本クアンタムストレージ株式会社

クアンタム社、データ・テープとロボット・テープ・システム間に物理的なブロックを構築する 業界初のソリューション Scalar Ransom Block を発表

リモートで即座に起動が可能、テープに保存されたデータを確実に完全なオフラインにすることでセキュリティを確保し、サイバー・レジリエントなアーカイブのための究極のデータ・セキュリティを提供する新機能

日本クアンタムストレージ株式会社（東京都港区、カントリーマネージャ：瀧口昭彦、以下クアンタム社）は、ランサムウェアやその他の形態のサイバー攻撃からの保護を目的とした最新のイノベーションを発表しました。Quantum Scalar® Ransom Block は、業界初、ネットワークを介したデータのアクセスや漏洩を防ぐ、Quantum Scalar テープ・システムの機能です。この特許出願中の機能は、こちらの[ショート・ビデオ](https://www.quantum.com/qdxapi/brightcove/?contentLink=45637) (<https://www.quantum.com/qdxapi/brightcove/?contentLink=45637>)に示すように、テープに保存されたデータと、ロボット・テープ・システムを含むすべてのネットワーク接続デバイスとの間に、ハードウェアの「ブロック」を構築します。

Ransom Block はリモートで起動でき、人手でテープを操作する必要がなく、テープ・ライブラリがハッキングされてもネットワークを介してデータにアクセスできないようにします。また、データの安全性とセキュリティを確認できるよう、テープ・ライブラリを監査できる状態を維持します。

クアンタム会長兼 CEO の Jamie Lerner は次のように述べています。「ランサムウェアやその他の形態のサイバー攻撃は弊社のお客様にとって最大の懸念のひとつです。テープ・ストレージ・システムは、大規模アーカイブにとっても、包括的なデータ保護戦略の一環としても、サイバー・レジリエントなインフラストラクチャを構築する上で重要な役割を果たします。しかし、テープ・ライブラリ自体がハッキングされてしまえば、テープに保存されているデータでさえ危険にさらされる可能性があります。そのため、大手クラウド・プロバイダーと提携してこれらの新機能を設計しました。Quantum Scalar Ransom Block は、ボタンをクリックするだけでデータを保護してセキュリティを確保し、テープに保存されたデータに究極の保護層を提供する業界初のソリューションです。」

<テープ上のデータを確実に攻撃から保護する Quantum Scalar Ransom Block>

サイバー脅威はとどまるところを知りません。データは暗号化され、盗まれ、ダーク・ウェブに漏洩しています。アナリスト企業の Enterprise Strategy Group (ESG) が 300 人を超える IT 部門と基幹業務部門の幹部を対象に実施した最近の調査によると、回答者の 5 人に 2 人がランサムウェア攻撃の成功を許してしまい、80%以上がデータを取り戻すために身代金を支払ったと報告しています¹。ランサムウェアがネットワークの侵入に成功すると、金銭的な損害が大きいだけでなく、重要なシステムのダウンタイム、収益機会の損失、世評の低下といったリスクにもなりかねません。

テープ・システムは、ランサムウェア攻撃が発生した場合にデータを保護し、迅速に回復できるようにするための、包括的な戦略の重要な一部です。テープに保存されたデータはネットワークに接続されないため、テープ・システムはハード・ドライブ (HDD) やフラッシュ (SSD) ストレージ・システムよりも本質的にセキュアです。しかし、テープ・ライブラリ自体はネットワーク接続デバイスであるため、テープ・ライブラリ自体がハッキングされるという万が一の事態が発生すれば、リモート・ハッキングのリスクがあります。クアンタムでは、このリスクにシンプルで自動化された方法で対処するため、Scalar Ransom Block 機能を設計しました。

<Ransom Block の仕組み>

ライブラリに保管されているテープはマガジンに置かれています。クアンタムの特許出願中の設計では、マガジンを部分的に取り外し、オペレーターがマガジンを物理的に再挿入するまで、ロボットがテープを選択できないようにします。マガジンは部分的に取り外されるだけなので、ロボットのバーコード・スキャナーはテープ・バーコードをスキャンできます。これにより、システム管理者はテープ・システムの監査を定期的に行ってテープがそこに存在することを確認できます。

テープ・ライブラリに物理的にアクセスできるオペレーターがマガジンを再挿入するまで、テープにアクセスすることはできません。テープ・システムは、入室許可を必要とするセキュアなデータセンターに保管することができます。

さらに、管理者がソフトウェア・コマンドを使用して、マガジンがテープで満杯になったときに、テープが取り出される前に、ドライブにテープがロードされないようにする「Logical Tape Blocking」機能を導入しました。ソフトウェアベースの機能であり、物理的なブロック・メカニズムではありませんが、この新機能は Ransom Block が開始されるまでのリスク・ウィンドウをさらに削減します。

<包括的セキュリティ・フレームワークの一部となる最新のイノベーション>

Ransom Block と Logical Tape Blocking は、Scalar テープ・システムを市場で最もセキュアなテープ・ストレージ・システムの 1 つにする包括的セキュリティ・フレームワークの一部となる、最新のイノベーションです。

以下をはじめとする多くの機能は Quantum Scalar テープ・システム独自の機能です²。

- リモート・ハッキングが発生した場合でも、テープに保存されたデータのセキュリティを確保する、Scalar Ransom Block と Logical Tape Blocking

- ネットワーク接続がなく、アプリケーションやネットワークからは見えない、分離されたセキュアなライブラリ内のボルト・パーティションにテープを移動できる、Scalar Active Vault
- 予定どおりまたは予想外にメディアがライブラリから取り出されたときに管理者に通知を行う、Scalar Media Security Alerts
- アクセス制御のセキュリティを強化する、管理者とユーザーのログインに対する多要素認証

これらの独自機能は、システム・アクセスの制御、システムの監視とイベント検出、データ・セキュリティと暗号化、サイバー保護とデータ整合性のための独自機能など、包括的な Quantum Scalar セキュリティ・フレームワークを形成する 25 を超える機能の一部です。

<出荷時期と価格>

Ransom Block と Logical Tape Blocking は、2021 年 12 月に新しい Scalar i6 および Scalar i3 テープ・ライブラリで利用可能になる予定です。Quantum Scalar セキュリティ・フレームワークの一部としてリストされているその他の機能は、現在、一般利用が可能です。一部の機能は別売りとなっており、一部の機能に対応していないモデルがあります。Quantum Scalar Ransom Block、Logical Tape Blocking、および Quantum Scalar セキュリティ・フレームワーク全体の詳細については、

<https://www.quantum.com/security-framework> を参照してください。

¹ Validating Data Challenges (データ課題の検証)、Enterprise Strategy Group、2021 年 9 月

² 一部の機能に対応していないモデルがあります。詳細については <https://www.quantum.com/jp> を参照してください。

クアンタム社について

クアンタム社の技術とサービスは、お客様のデジタル・コンテンツのキャプチャ、作成、共有を支援し、且つ長期に渡って保存および保護します。データ・ライフサイクルのあらゆる段階に最適なソリューションを搭載したクアンタム社のプラットフォームは、高解像度ビデオ、画像、産業用 IoT に、最速のパフォーマンスをご提供いたします。これが、世界中の大手エンターテインメント企業、プロスポーツチーム、研究機関、政府機関、大企業、クラウド・プロバイダーがクアンタム社のソリューションで世界を幸福に、安全に、スマートにしている理由です。詳細は www.quantum.com/jp を是非ご覧ください。

お問い合わせ

日本クアンタムストレージ株式会社 (<https://www.quantum.com/jp/>)

email: japan_info@quantum.com

Tel: 03-6890-3038 (代表)