Enterprise Strategy Group

SHOWCASE

APRIL 2025

サイバーレジリエンスがミッションクリティカルなストレージには不可欠

Scott Sinclair（プラクティス ディレクター） 、Monya Keane（シニア リサーチ アナリスト）共著

要約：IT を取り巻く環境は一変しました。今やデータは非常に価値の高い資産であるため、サイバー脅威も蔓延しています。そのため、ミッションクリティカルなストレージを選択する際には、サイバーレジリエンスを中心に据える必要があります。デル・テクノロジーズは、PowerMax によって、必要不可欠なサイバーレジリエンス機能をこれらのシステムに直接構築して統合することにより、ミッションクリティカルなストレージのリーダーとしての地位をさらに確立しています。

概要

データは、重要で非常に価値の高いビジネス資産です。新たに Omdia の傘下に入った Enterprise Strategy Group の調査によると、調査対象組織の 55%が、データが事業の要であると答えました。[1]ミッションクリティカルなストレージ インフラストラクチャの役割は、停止を許されないワークロードやアプリケーションを支えるデータを保存、保護、提供することにあります。

何十年もの間、「ミッションクリティカルなストレージ」を導入することは、必要なパフォーマンスと拡張性を提供すると同時に、コンポーネント障害、サイト障害、ユーザー エラー、自然災害から保護するために常時稼働できるようにすることと同義でした。それが今では、悪意のある攻撃がますます増えています。したがって、ミッションクリティカルなストレージの基本的な考え方では、従来の機能だけでなく、組織のサイバー レジリエンス体制の改善も含めて進化させる必要があります。

エンタープライズ ストレージのリーダーであるデル・テクノロジーズは、最も要求の厳しい IT 環境のミッションクリティカルなニーズを満たすために、主力のストレージ プラットフォームである PowerMax を進化させ続けています。Dell は最近、データと重要なアプリケーションの保護、ブランドの評判の維持、長期的な成功を目指すあらゆる組織のサイバーレジリエンス体制を向上させるために、PowerMax 製品ラインに一連の堅牢な機能を搭載することを中心にイノベーションに取り組んでいます。

データに対するサイバー脅威が絶え間なく存在する時代

サイバー脅威の増加に伴い、IT の複雑さも増しています。Enterprise Strategy Group の調査回答者の半数以上(60%)が、現在の IT は 2 年前よりも複雑であると回答しています。サイバーセキュリティに関する状況の急速な進化（42%が回答）と、データ

[1]出典：Enterprise Strategy Group 調査レポート、『*Navigating the Cloud and AI Revolution: The State of Enterprise Storage and HCI*』（2024 年 3 月）。

セキュリティとプライバシーに関する新しい規制に準拠するための取り組み(32%)、この 2 つが IT の複雑さを助長する最大の要因として挙げられました。[2]

残念ながら、組織は現在、その複雑さを克服するのに十分なスキルを持つサイバーセキュリティ人材の採用に苦戦しています。調査対象組織の 37%が、サイバーセキュリティの専門性に長けたスタッフが不足していると報告しています。これは現在、人工知能(47%)に次いで、企業の IT 部門で 2 番目に頻繁に指摘されるスキル不足の分野です。[3]

ランサムウェアとマルウェアの蔓延

ビジネスが直面しているさまざまな脅威の中で、ランサムウェアやマルウェアによる外部からの攻撃は事実上避けられなくなっています。ランサムウェアから企業を保護するためのテクノロジーとプロセスを監督する IT およびサイバーセキュリティのプロフェッショナルを対象に最近実施された Enterprise Strategy Group 調査アンケートでは、75%が過去 12 か月以内にランサムウェア攻撃を経験したと報告しています。また、そのうちの 27%は、こうした攻撃が毎週またはそれ以上の頻度で発生していると回答しています。[4]

攻撃を経験した組織のうち、75%が少なくとも 1 回は実際の被害を受けています。しかし、このような状況では、身代金の支払いは最適な戦略ではなく、賢明な戦略とも言えません。攻撃によって被害を受けた組織の 56%が支払いに応じています。しかし、要求された身代金を支払った組織は、次のような被害に遭っています。

- **85%**が、さらに金銭を要求する別の恐喝未遂を経験している。実際に、最初に支払いに応じた組織のうちの 57%が、最終的にさらに多額の金銭を支払っています。
- 身代金を支払った後、データの 100%を取り戻した企業はわずか **16%**であった。
- また、**42%**は、支払い後にデータを 75%以下しか取り戻せなかった。

明確に言うと、ランサムウェアの本格的な対策には、検出、防止、リカバリーに重点を置いた複数のテクノロジーとツールを組み込んだ、より多面的な戦略が必要です。

現在、多くの組織は、NIST サイバーセキュリティ フレームワークのガイダンスに基づいてサイバーレジリエンス戦略をモデル化しています。このフレームワークでは、組織が重要なリソースを特定して、そのリソースを保護し、障害と違反を検出して、サイバーインシデントに対する対応とリカバリーを計画することを推奨しています。組織が広く採用している NIST フレームワークのもう 1 つのコンポーネントは、ゼロ トラスト アーキテクチャです。これは、保護ネットワーク エッジの概念を無視して、「決して信頼せず、常に検証する」という理念を支持するものです。このモデルでは、ユーザー（組織内で働く人も含む）のセキュリティ設定を、そのユーザーがアプリケーションとデータにアクセスする前に定期的に繰り返し検証する必要があります。

---

[2]出典：Enterprise Strategy Group 調査レポート『*2025 Technology Spending Intentions Survey*』（2024 年 12 月）。

[3]同上。

[4]出典：Enterprise Strategy Group 調査結果、『*2023 Ransomware Preparedness: Lighting the Way to Readiness and Mitigation*』（2023 年 11 月）。特に明記されていない限り、本概要のすべてのデータはこの調査から引用しています。

このサイバーセキュリティ アプローチには、ストレージ システムが含まれている必要があります。Enterprise Strategy Group の調査によると、最も一般的にランサムウェア攻撃の標的となるインフラストラクチャ コンポーネントは、主要な IT インフラストラクチャ(38%)とストレージ システム(36%)です。

ミッションクリティカルなストレージによるランサムウェアへのレジリエンスの向上

ランサムウェア攻撃は、重要なビジネス データにアクセスし、それを暗号化することに重点を置きます。多くのサイバーレジリエンス戦略は、脅威を排除し、受けた攻撃を早期に**検出**して脅威を**防止**することに重点を置いたツールとテクノロジーに基づいて構築されています。しかし、ランサムウェアの場合は、**リカバリーの迅速化**にも焦点を当てることが重要です。

ミッションクリティカルなストレージ システムは、攻撃発生後にデータを迅速にリカバリーできるようにする上で重要なデータ パス内のスポットに存在します。たとえば、ランサムウェア攻撃の成功回数が増加するにつれて、一部のストレージ システムでは、安全かつ不変のデータ ボリューム コピーを保管してから提供することで、迅速にリカバリーできるよう設計された機能を活用できるようになりました。

このようなサポートは、リカバリーを加速させる上で非常に重要です。スナップショットは「既知の正常な」ボリュームとして迅速に識別され、IT 部門によって迅速にリカバリーされて、データ セットを元の状態にリストアできます。ただし、ミッションクリティカルなアプリケーション環境では、ストレージ テクノロジーはさらに多くの役割を果たす必要があります。

Dell PowerMax は組織のサイバーレジリエンス体制を改善できる

数十年の間に製品名が変わり、機能も向上してきましたが、1980 年代後半に EMC によってエンタープライズ ストレージが IT の独立したカテゴリーとして確立されて以来、デル・テクノロジーズのミッションクリティカルなインフラストラクチャ ストレージ システムはこの分野をリードしてきました。現在、Dell PowerMax は、ミッションクリティカルなワークロードにおける負荷の高い要件を満たすように設計された、次のような複数の機能を提供しています。

- 大規模な環境でも極めて安定したパフォーマンスを発揮する、オール NVMe のマルチモード スケールアウト アーキテクチャ。
- メインフレーム ワークロード、ベアメタル システム、VM、コンテナなどを含む多様なブロックおよびファイル アプリケーション環境をサポートする大規模なワークロード統合。
- 最高レベルのセキュリティ、可用性、レジリエンス。PowerMax は、ホストから PowerMax へのエンドツーエンドのデータ暗号化、静止データ暗号化、セキュア スナップショットにより、99.9999%の可用性を実現します。Dell によると、具体的には、アレイあたり最大 *6,400* 万個のスナップショットをサポートしています。さらに、Dell の Symmetrix Remote Data Facility (SRDF)ディザスター リカバリー ソフトウェアは、高度なトポロジーとオートメーション機能を使用して、レジリエンスの強力な基盤を提供します。SRDF を使用すると、組織はエアギャップ ヴォールトを作成することもできます。そのヴォールト内では、データは分離され、ヴォールトへの接続は断続的かつ厳しく制限されています。

Dell がレジリエンス向けの PowerMax を設計

最近、Dell は、PowerMax にさらに多くのセキュリティ機能を構築して組み込むことに力を注いでいます。例えば、PowerMax は、Dell のゼロ トラストの 7 本の柱に基づき、ゼロ トラスト セキュリティ環境向けに設計されており、次のような方法でシステム自体を攻撃から本質的に保護しています。

- **変更不可能なハードウェア ルート オブ トラスト機能**：ノード、メディア エンクロージャ、Control Station 全体のハードウェアとソフトウェアの変更を認証します。メモリーに物理的に統合された変更不可能なコンポーネント レベルの暗号形式キーが組み込まれています（Dell 製）。
- **セキュア ブート チェーン オブ トラスト機能**：悪意のあるブート、カーネル、ドライバーのルートキットに対してファームウェアの「トラスト チェーン」を確立して拡張します。セキュア ブート チェーン オブ トラストは、Dell の署名に基づいて後続のファームウェア ロード/ブート ローダーに対して暗号形式認証を使用します。
- **デジタル署名されたファームウェア アップデート**：PowerMax では、Dell のデジタル署名認証も活用して、不正なファームウェア アップデートから保護します。暗号形式認証キーを使用したノード、メディア、Control Station コンポーネントのスキャンを実行します。

PowerMax は、この信頼性の高い設計に加え、ランサムウェア攻撃や他のサイバーセキュリティ脅威に対する予防、検出、リカバリーを向上させる追加機能を備えています。

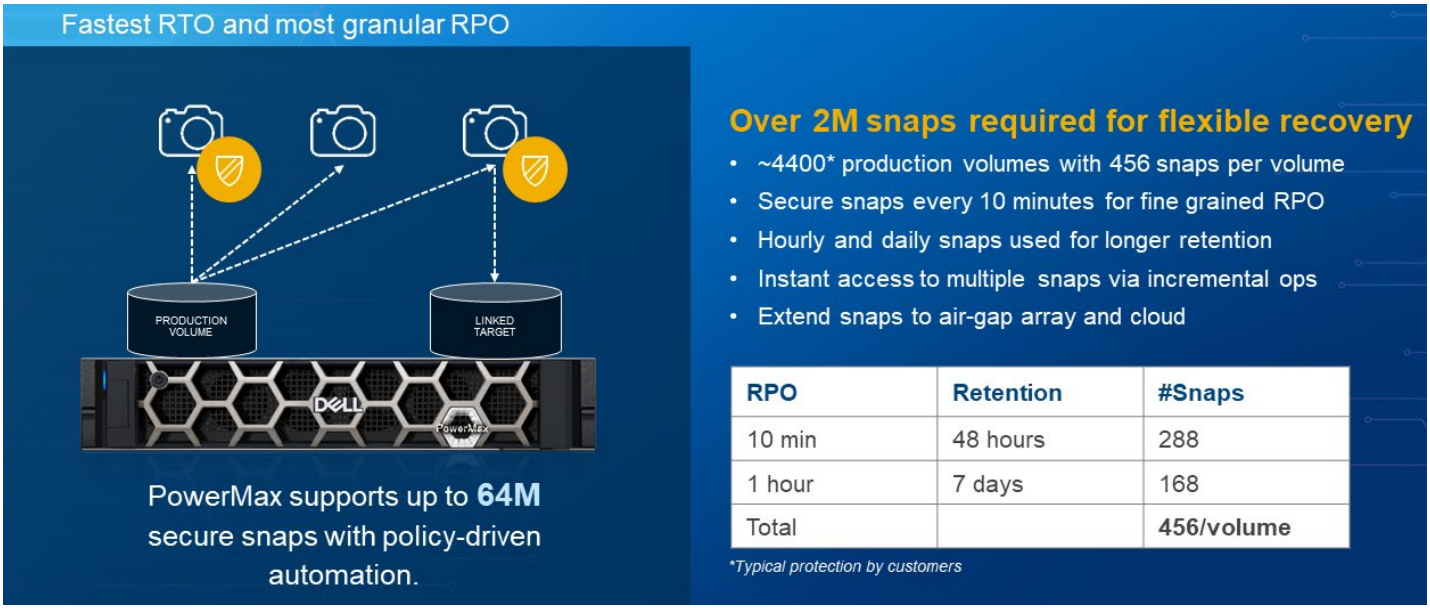
予防について、PowerMax は、組み込みのハードウェア セキュリティに加え、不正なユーザー アクセスを防止するための高度なセキュリティで攻撃を防ぐのに役立ちます。Common Criteria、STIG Hardening/APL、FIPS 140 認定のセキュリティ認証、次のような信頼できる管理者アクセス制御メカニズムのサポートが備わっています。

- SecurID と Yubikey 多要素認証で、管理者の身元を確認します。
- 米国連邦政府内のオンライン リソースにアクセスするための証明書/秘密キーを含む CAC/PIV スマートカードをサポートします。
- ロール ベースのアクセス制御(RBAC)、LDAP サポート、zDP 2 Actor（特定の zDP コマンドを実行するには 2 人のユーザーが必要）により、許可されたユーザーのみがストレージのプロビジョニングなどの指定された操作を実行できます。

検出については、PowerMax ハードウェアと Dell AIOps AI ソフトウェアの両方がマルウェアの異常検出を提供します。これは、サイバーセキュリティ アラート プロトコルに基づくコンプライアンス アラートであり、セキュリティで保護された Syslog アラートとエクスポートとともに提供されます。具体的には、AIOps は、PowerMax ストレージの異常な使用率と疑わしいアクティビティ メトリックを監視することで、サイバー攻撃を迅速に検出します。次に、暗号化の可能性による大幅な変更を管理者に警告します。また、ストレージ インフラストラクチャを継続的に監視して、システム設定の設定ミスによるサイバーセキュリティ リスクを自動で特定し、その問題を修正するための詳細な推奨事項を提供することもできます。

リカバリーについては、PowerMax のセキュア スナップショット テクノロジーがデータ セキュリティと保護を次のレベルに引き上げます。ビジネスのサービス レベル目標に応じて、IT 部門は各 PowerMax で最大 6,400 万個のスナップショット コピーを構成できます（図 1 を参照）。

図 1：PowerMax が高速 Cyber Recovery をサポートする方法



出典：*Dell Technologies*

この機能により、PowerMax では、攻撃が成功するまでのわずか数分間の目標リカバリー ポイント(RPO)に対応できます。また、多くのスナップショットをサポートすることで、IT 部門は、大規模かつ統合されたミッションクリティカルなストレージ環境を実質的に分単位で保護できる十分なコピー数を確保できるため、ほぼ即時のミッションクリティカルなアプリケーションのリカバリーを実現できます。このような保護レベルの柔軟性は、大規模な本番環境にとって革新的なものです。Dell によると、PowerMax は RPO を最適化するために大規模で最も細分性の高い Cyber Recovery を提供します。

Dell は、リモートヴォールト エアギャップ リカバリー オプション(SRDF)を必要とする組織向けに、PowerMax Cyber Recovery ヴォールト オプションを追加することもできます。これにより、オープン システムとメインフレーム ストレージなどのヴォールト化/リカバリーのオーケストレーションが可能になります。PowerMax サイバー リカバリー ヴォールト製品は、SRDF リモート レプリケーションを使用してエア ギャップを作成します。このソリューションは、高速リカバリー(RTO)で本番ネットワーク外部にデータをコピーする必要があるお客様向けに設計されています。しばらくの間、PowerMax のお客様はこの構成を手動で導入してきましたが、Dell の最近の発表では、導入オーケストレーションの自動化と Dell Professional Services を取り入れて、導入の効率化を図っています。

まとめ

通常、Dell はセキュリティ ベンダーとして真っ先に思い浮かぶ企業ではありません。その認識を変える必要があります。悪意のある攻撃者はさらに組織化され、その脅威はより巧妙になっています。Dell は、これらの脅威に対抗し、データを保護し、セキュリティとレジリエンスの管理全体をよりシンプルにすることを目的として行ってきた多大な投資を、今後も継続していきます。

データは、組織の最も重要な資産です。保護する必要があり、常に利用可能でなければなりません。その可用性に対する最新の脅威が、ランサムウェア、マルウェアなどのサイバー攻撃です。そして、PowerMax には、ハイエンドのミッションクリティカルなワークロードをサポートする強力な製品があります。Dell は長年にわたりこれらに対応してきましたが、PowerMax の新機能は特に、今日のほぼすべてのストレージ購入者に適しています。誰もがランサムウェアやマルウェアに懸念を抱き、マスコミに取り上げられることを心配しています。

問題は、一攫千金を狙う窃盗者と戦うことではありません。このようなハッカーは、外国政府のために働き、自国の国家安全保障や軍事力を強化するために知的財産を盗んでいるかもしれないのです。データを暗号化して、アクセス権を奪うことができてしまえば、ほかにデータを使ってどんなことができるかはわかりません。

不正なユーザーに絶対に渡してはならないビジネス情報がある場合は、ストレージ インフラストラクチャの適切な保護方法について Dell にご相談ください。

Enterprise Strategy Group について
新たに Omdia の傘下に入った Enterprise Strategy Group は、焦点を絞った実践的なマーケット インテリジェンス、デマンドサイド調査、アナリスト アドバイザリー サービス、GTM 戦略ガイダンス、ソリューション検証、エンタープライズ テクノロジーの売買をサポートするカスタム コンテンツを提供しています。

contact@esg-global.com
www.esg-global.com