ESG SHOWCASE

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

日付：2022年10月 **作成者：**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）

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。ESGの調査によると、調査対象の組織の59%が、データをビジネスに不可欠なものであると認識しており、その割合は2年後には81%に増加すると予想されています。[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、決して止めることのできないワークロードとアプリケーションを支えるデータを保存、保護、提供することです。

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

[1]出典：ESG 調査レポート『Data Infrastructure Trends』（2021 年 11 月）。

サイバー脅威の増加に伴い、ITの複雑さも増しています。ESGの調査回答者のほぼ半数(46%)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（37%が回答）と、データ 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48%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おり、これは現在、企業のIT部門で最も頻繁に指摘されるスキル不足の分野になります。[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ESG調査アンケートでは、79%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30%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、73%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。

- この組織のうちの**87%**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、最初に支払に応じた組織のうちの61%が、最終的にさらに多額の金銭を支払っています。[5]
- 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**14%**であった。
- また、**61%**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

[2]出典：ESG 全数調査結果『2022 Technology Spending Intentions Survey』（2021 年 11 月）。
[3]同上。
[4]出典：ESG 調査レポート『The Long Road Ahead to Ransomware Preparedness』（2022 年 6 月）。本 Showcase における ESG 調査の参考資料は、別段の記載のない限り、すべて本調査報告書から引用しています。
[5]出典：ESG 調査結果詳細『The Long Road Ahead to Ransomware Preparedness』（2022 年 6 月）。

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や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。

ストレージ システムは、このサイバーセキュリティ アプローチに含まれていなければなりません。結局のところ、ESGの調査によると、ランサムウェア攻撃の標的として最もよく挙げられるインフラストラクチャ コンポーネントは、ストレージ ハードウェアです。これは、回答者の40%が挙げた最も多い回答でした。

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 セットを以前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のマルチコントローラー 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がレジリエンスむけの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は、Dellのデジタル署名認証を利用して、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。

- 管理者の身元を確認するためのSecurID多要素認証。
- 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スマートカードのサポート。
- 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 CloudIQ 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、CloudIQ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 Cyber Recoveryヴォールト製品は今月後半に一般提供される予定で、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、今月の発表では、導入オーケストレーションのオートメーションとDellのプロフェッショナル サービスを取り入れて、導入の効率化を図っています。

さらに重要な事実

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、多大な投資を行ってきました。

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、常に利用できる状態にし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。確かに、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は何年もそうしてきましたが、PowerMaxの新機能は現在のほぼすべてのストレージ購入者に特に適用できます。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 (ESG)は、テクノロジー分析、リサーチ、戦略立案を行う統合企業で、マーケット インテリジェンス、実用的なインサイト、ゴートゥマーケット コンテンツ サービスを、世界のITコミュニティーに提供しています。

www.esg-global.com contact@esg-global.com 508-482-0188