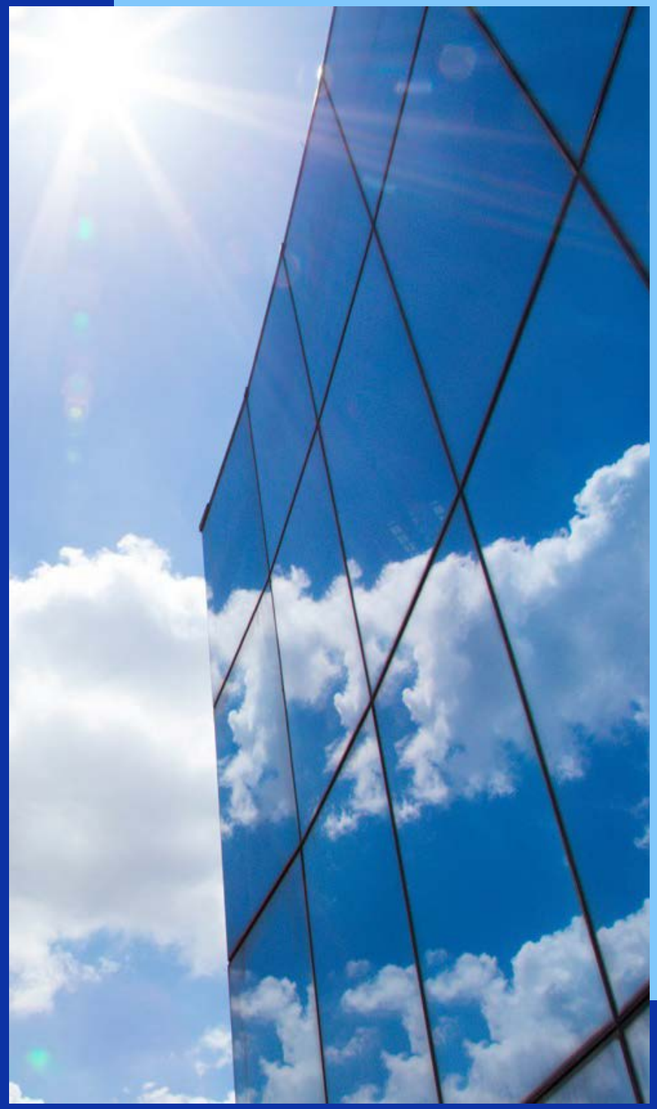
Global Data Protection Index
サイバー レジリエンス マルチクラウド エディション

DELL Technologies

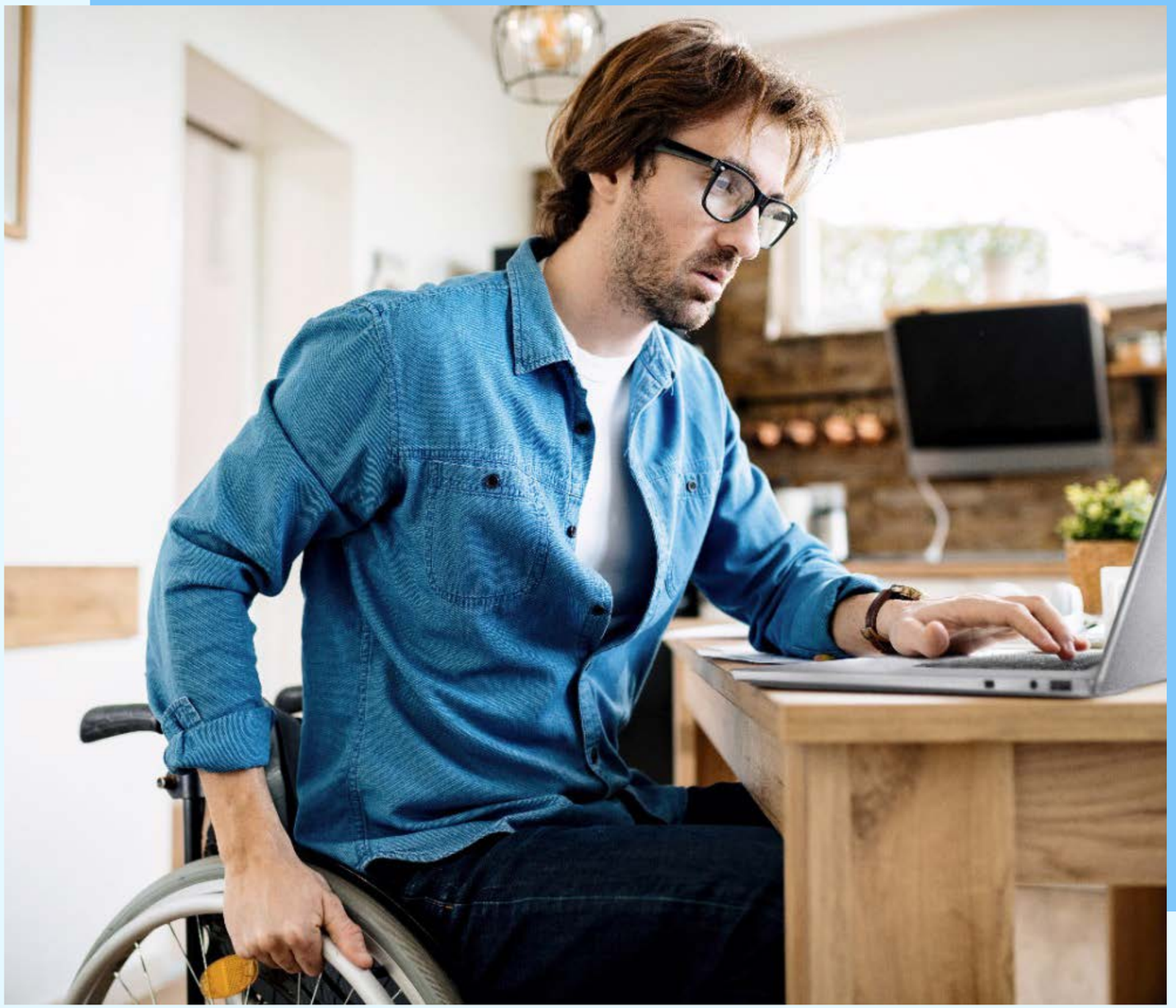
目次



はじめに

今日のデジタル トランスフォーメーションが進んだ世界で、データは、ビジネス戦略における重要な役割を果たしており、エスカレートするサイバー脅威の主要なターゲットになっています。生成AIの台頭と、ハイブリッドなマルチクラウド環境への拡張によってこのようなリスクが高まりました。サイバー攻撃の結果、重大な財務的損害が発生し、その被害額は前年から倍増して平均140万ドルに達しました。このような状況の中、組織はますます複雑化するクラウド資産の保護とセキュリティ確保に関する課題に直面しています。また、この変化し続ける環境において、堅牢でサイバー レジリエントなデータ保護戦略が必要不可欠であるということが浮き彫りになっています。

このe-bookでは、デル・テクノロジーズの委託によりVanson Bourneが実施した2024年版Global Data Protection Index調査で明らかになった結果を紹介します。この調査は、世界中のIT導入決定者1,000人とITセキュリティ導入決定者500人を対象に実施されました。特記のない限り、過去との比較を行う際は、1,000人のIT導入決定者から得られた結果のみを参照しています。



データ保護リスクの現状

データ保護の複雑な状況を切り抜けることは、組織にとって依然として大きな課題であり、デジタル トランスフォーメーションに向けた取り組みに直接的な影響をもたらす障壁でもあります。大多数の組織(90%)が、過去12か月間に何らかの業務中断を経験しています。

このように広まっている業務中断は、ITリーダーやITセキュリティ リーダーにも影響を与えており、79%が今後発生する可能性のある破壊的な出来事に関して懸念を示しています。

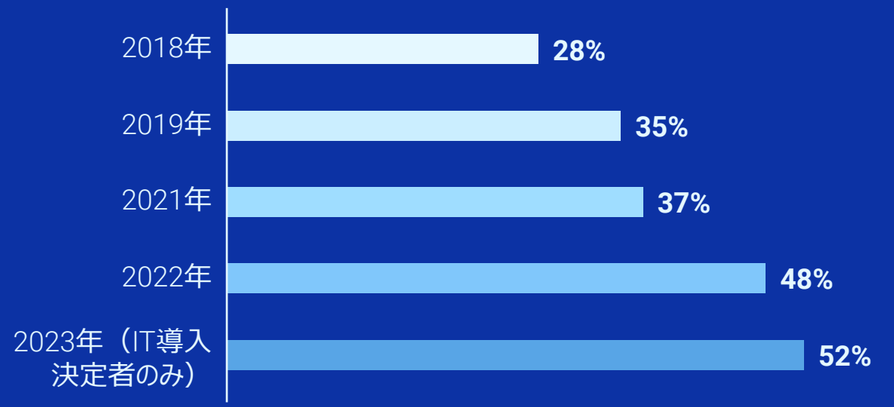
こうした不安が、バックアップ/リカバリーのサービス レベル目標(SLO)の達成に対する自信に影を落としており、60%がこの領域における組織の能力について「あまり自信がない」と感じています。

このような懸念に加えて、データ ロス イベントは組織に重大な財務的影響を与え、そのコストは過去12か月間で平均261万ドル(USD)に上っています。

増大するサイバー攻撃の脅威

サイバー攻撃の脅威は増大し続けており、組織の混乱を引き起こす原因のリストで2年連続第1位になっています。IT導入決定者の半数以上(52%)が、過去12か月以内にデータへのアクセスを妨げるサイバー攻撃やインシデントを経験したことがあると回答しています。

データへのアクセスを妨げるサイバー攻撃やその他のサイバー インシデントを経験した



サイバー犯罪者はさまざまなエントリー ポイントを標的にしますが、攻撃が発生する可能性が高いのは外部ソースです。実際、攻撃者の最初のエントリー ポイントの55%は外部ソースでした。具体的には、ユーザーがスパムやフィッシングEメール、悪意のあるリンクをクリックした、ユーザー認証情報が侵害された、モバイル デバイスがハッキングされた、という事象です。

サイバー攻撃のコスト

サイバー攻撃のコストは、財務面で組織に多大な影響を与えています。サイバー攻撃やその他のサイバー関連インシデントに伴うコストは、過去12か月で2倍以上に増加しています。

2022年
66万ドル

↑

2023年（IT導入決定者のみ）
141万ドル

さらに、組織内でのデータ ロスやシステム ダウンタイムの原因として最も多く挙げられるのは、外部のセキュリティ侵害です。

40%

テレワークのリスク

テレワークやハイブリッド ワークが流行しているにもかかわらず、組織は不安定な立場にあると感じています。現在、10人中8人超(81%)が、テレワーク社員の増加に伴いサイバー脅威によるデータ ロスの可能性が高まっていると考えています。

さらに、既存のデータ保護対策ではマルウェアやランサムウェアの脅威に対抗するのに不十分な可能性があると感じている組織の割合が増えてます。

**テレワーク社員の増加に伴い、
サイバー脅威によるデータ ロスの可能性が高まっている**

2022年 → **2023年**（IT導入決定者のみ）

70% → **81%**

概要：「強くそう思う」と「そう思う」の合計

**自身の組織が行っているデータ保護対策では、マルウェアやランサムウェアの
脅威に対抗するのに不十分な可能性があると懸念している**

2022年 → **2023年**（IT導入決定者のみ）

67% → **75%**

概要：「強くそう思う」と「そう思う」の合計

ランサムウェア保険

サイバー脅威が常に存在する時代において、組織は保険契約によって安心感を得ることができます。しかし、ランサムウェア保険は一般的(93%)ではあるものの、次のような事項に十分注意する必要があります。

57% 組織がサイバー脅威防止活動の「ベストプラクティス」を実施していることを証明する必要がある

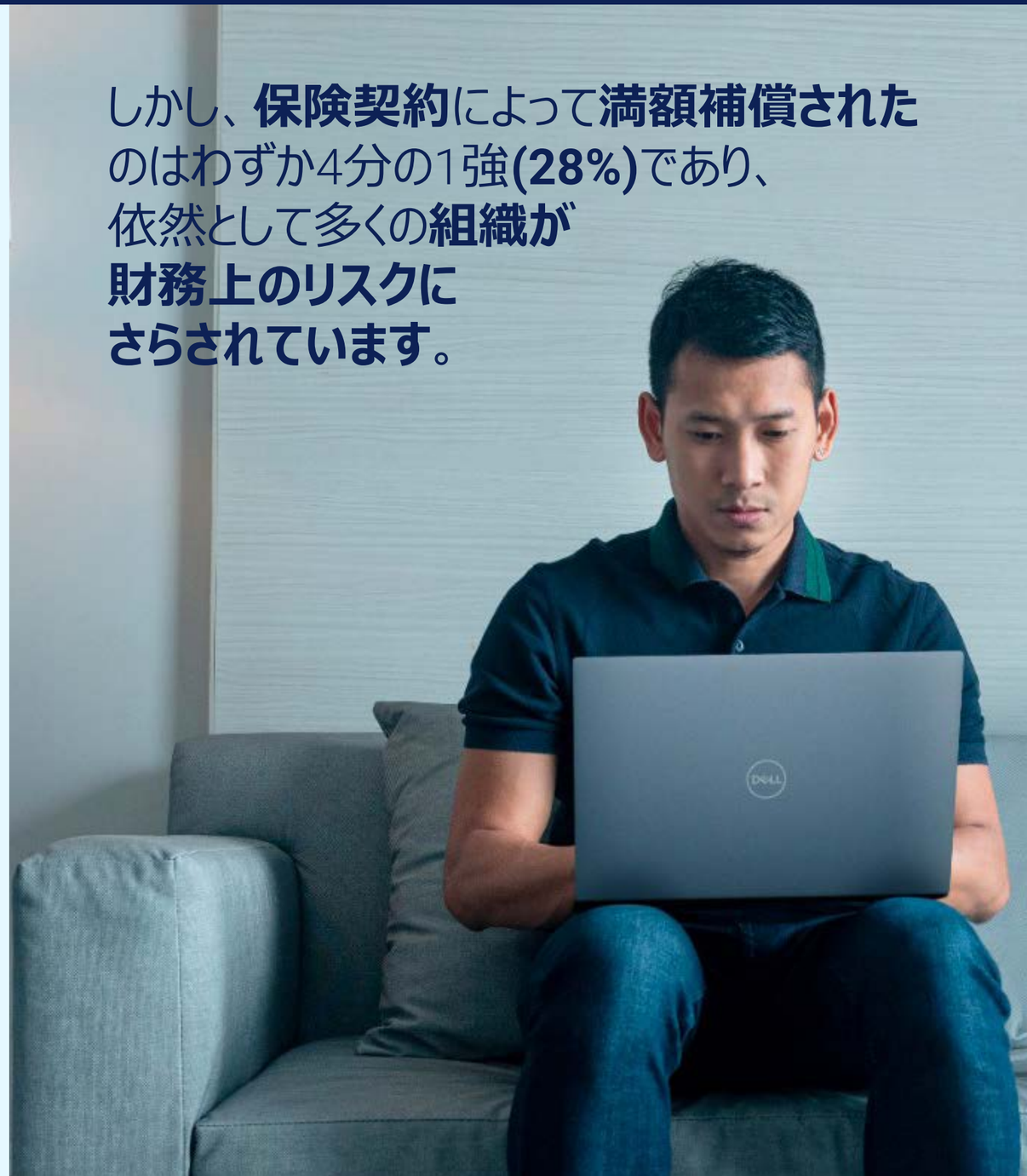
43% 請求に対して支払われる保険金額に上限がある

40% 特定のシナリオでは保険契約が無効になる場合がある

40% 法律で一部の組織への支払いが制限されているために保険金が支払われない場合がある

85% ランサムウェア攻撃を経験した組織の大半が、データにアクセスするために料金を支払いました。

しかし、**保険契約**によって**満額補償された**のはわずか4分の1強**(28%)**であり、依然として多くの**組織が財務上のリスクにさらされています。**



生成AIとサイバーセキュリティ

サイバー脅威のランドスケープが拡大するにつれて、サイバー防御を強化するための戦略的ツールとして生成AIを採用するという重大な転換が生じています。

52%

が、サイバー犯罪者との継続的な戦いにおいて、生成AIを統合することが組織のサイバーセキュリティ体制にメリットをもたらすと考えています。

ただし、個々の課題を認識することで、このような楽観的な考えは減少します。

88%

の専門家が、生成AIを採用すると大量のデータが新たに生成され、保護対策やセキュリティ対策が必要になる、ということに同意しています。

同じように

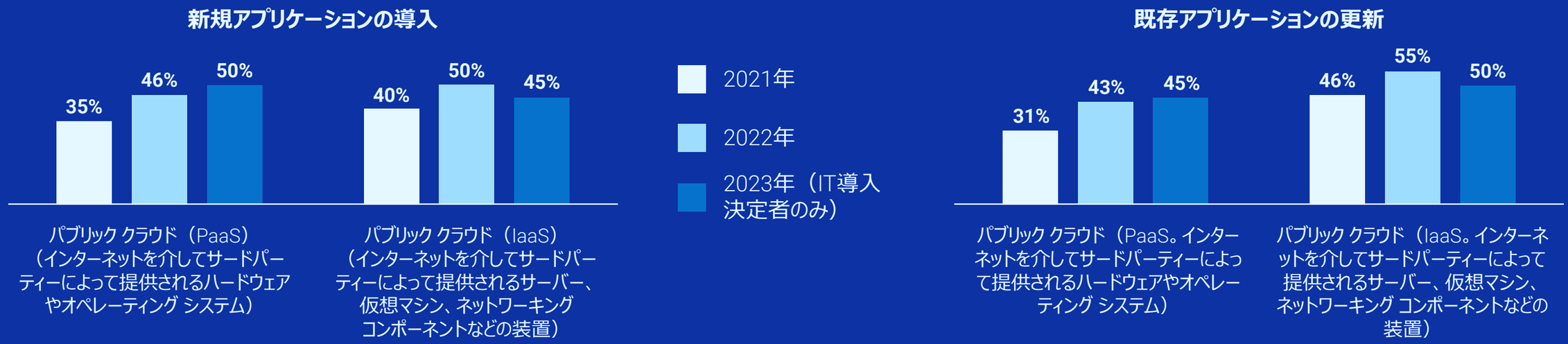
88%

が、生成AIによって特定のデータ タイプの価値が増大し、その結果、より高いレベルのデータ保護サービスが必要になる、ということに同意しています。

以上のインサイトから、生成AIの二面性、つまり強力な防御策であると同時に、サイバーセキュリティの新たな複雑さの原因でもあるという特性が浮き彫りになっています。

マルチクラウドの利用

アプリケーションの導入や更新を検討している組織にとって、パブリッククラウド ソリューションの採用は、引き続き優れた戦略です。しかし、この戦略はデータ保護の複雑さ増大の原因にもなります。



96% の組織が、パブリックなマルチクラウド環境でデータを管理する際に課題に直面しています。

44% の組織が、それぞれ固有の機能と要件を持つ複数のパブリッククラウド プラットフォームを利用する際につきものの複雑さに苦慮しています。

40% の組織が、このような多様な環境全体にわたるデータのセキュリティ確保に懸念を示しています。

マルチクラウド環境のセキュリティ確保

サイバー脅威の増大に伴い、多くの組織が、特に新規アプリケーションの導入や既存アプリケーションの更新の際に、クラウド内でデータの安全性を維持することに対して不安を感じています。実際、組織の自信はかつてないほど低くなっています。

パブリッククラウド環境全体にわたるデータすべてを保護する組織の能力について、「とても自信がある」以外の回答を選んだ組織の割合

当然のことながら、調査対象者の半数以上が、ハイブリッドクラウドやマルチクラウドを効果的に運用するために重要な能力として、次の2つを優先しています。

58%
マルチワークロード環境を保護する能力

56%
堅牢なサイバーセキュリティの確保

50%
以上のような課題に対処するために、組織の半数は既に外部のサポートを取り入れてサイバー レジリエンスを強化しています。

結論

組織がますますパブリッククラウド ソリューションに注目し、ハイブリッド ワーク モデルを実施し、生成AIを試すようになるにつれて、データ保護の重要性がかつてないほど顕著になっています。しかし、デジタル資産の安全確保は、多くの人にとってこれまでより複雑な課題になりつつあります。絶えずサイバー攻撃の脅威にさらされている状況では、企業にとって運用のレジリエンスを高める対策を講じることが必要不可欠です。

Dellのモダンでシンプルかつレジリエンスに優れたマルチクラウド データ保護の詳細について、こちらのページをご覧ください。**www.dell.com/dataprotection**

DELL Technologies

デル・テクノロジーズは、サイバー リカバリー、バックアップ、ディザスター リカバリー、長期保存などを提供することで、お客様がすべてのデータとアプリケーションを保護できるよう支援します。

VansonBourne

Vanson Bourneは、テクノロジー セクターの市場調査を専門とする独立した調査会社です。同社の堅牢で信頼できるリサーチ ベースの分析に対する高い評価は、厳格なリサーチの原則およびあらゆるビジネス分野と主要市場における技術部門およびビジネス部門の上級意思決定者の見解を明らかにする能力が基盤となっています。www.vansonbourne.com