なぜ保護、セキュリティ、AIの融合が必要なのか

COHESITY

なぜ保護、セキュリティ、AIの融合が必要なのか

長年にわたり、組織はデータ保護、データセキュリティ、AIイニシアチブをそれぞれ独立した優先事項として扱ってきました。バックアップチームは、復旧に注力してきました。セキュリティチームは、脅威の防止に注力してきました。AIチームは、アナリティクス、自動化、イノベーションに注力してきました。各チームは、独自のツール、目的、アーキテクチャで運用してきました。

今こそ、この分断されたモデルを見直すときです

その理由は極めて実践的です。サイバー攻撃はますます標的型へと進化し、データはオンプレミス、クラウド、SaaSなど、あらゆる場所に存在するようになりました。同時に、企業はAI活用の成果向上に必要なデータへアクセスすることに苦戦しています。さらに、そのデータは異なるシステムに分散していることが多く、複雑性と死角を増大させています。

ツールを追加するだけでは、この問題は解決しません。むしろ状況を悪化させます。

先を行く組織は、レイヤーを追加していません。

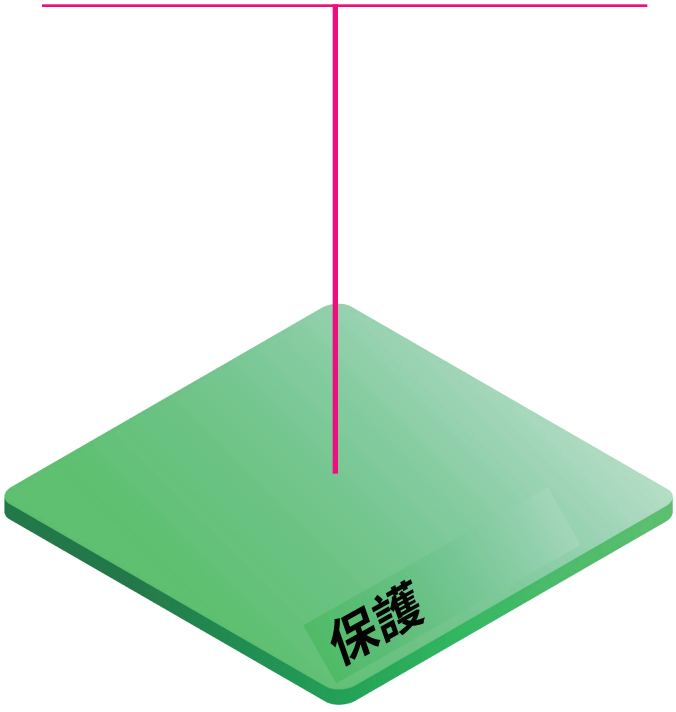
彼らは、基盤そのものを見直しています。

保護は、基盤です

保護はサイバーレジリエンスへの第一歩です。それは、仮想マシン、データベース、ファイルシステム、非構造化ワークロードなど、データ資産全体にわたる包括的なカバレッジから始まります。

保護は、これらすべてのデータを、一貫性をもってギャップなくカバーする必要があります。復旧はこれにかかっています。保護が不完全で、断片化するか、一貫性がない場合、クリーンで迅速な復旧を期待することはできません。保護が包括的で一貫していれば、データの破損、損失、残存リスクを伴わずに復旧を行うことができます。

サイバーレジリエンスは、この基盤となる保護レベルから始まります。



セキュリティはデータレイヤーに統合されなければならない

保護が確立されると、次の課題が明らかになります。

バックアップシステムが侵害され、暗号化されたか、不正にアクセスされた可能性がある場合、復旧データ自体が新たな攻撃対象領域になります。セキュリティは外部に付加したままであってはなりません。データレイヤー上で直接機能する必要があります。

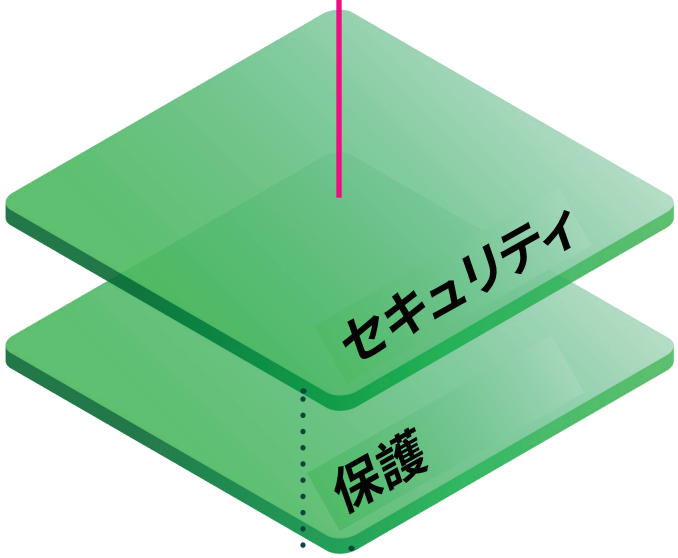
ですから、以下が必要です。

- バックアップ環境内で異常なアクティビティを検知
- ソースでIDとアクセス制御を適用
- データ資産全体で一貫したガバナンスを適用

保護とセキュリティを別々のシステムで運用している場合、チームは、プレッシャーの高い状況でもツール間でシグナルやポリシーを突き合わせる必要性に迫られることがよくあります。ギャップが生じるのは、機能が存在しないからではなく、それが統合されていないためです。

データ保護レイヤーにセキュリティを組み込むことで、これらのギャップを解消し、セキュリティと復旧を相互に強化します。脅威検知はクリーンな復旧をサポートし、ガバナンスは一度適用すれば全体にわたって一貫して実施するようになります。

共に、信頼できるデータ基盤を構築します。



保護
は、レジリエンスを確立します。

セキュリティ
は、それを強化します。

AI をエンタープライズ規模で実用化する

データが確実に保護され、セキュリティが確保されて初めて、新たな機会が生まれます。

AIを効果的に活用するために、組織には次の取り組みが求められます。

- 環境をまたいで分散する非構造化データを統合する
- 過去の変更履歴を取得・保持する
- 一貫したガバナンス、ロールベースアクセス、監査可能性を維持する
- データ重複や意図しない露出のリスクを低減する

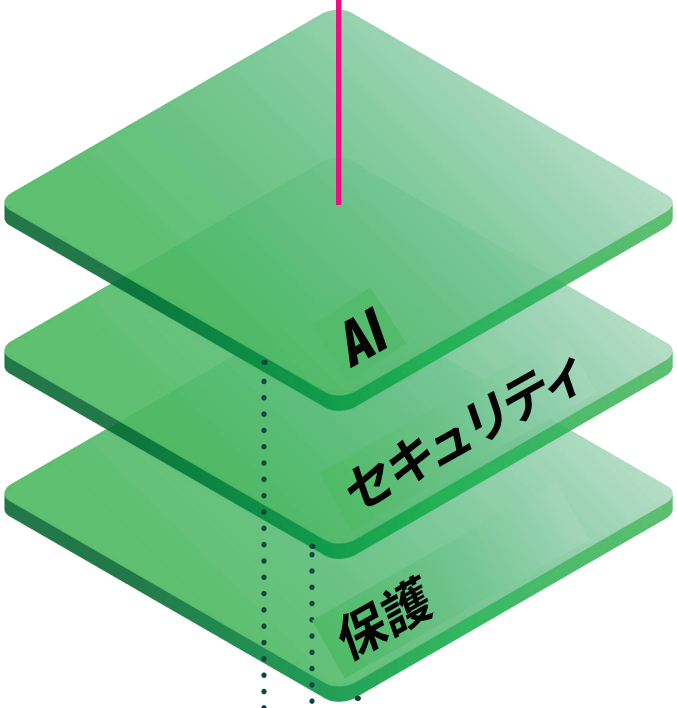
多くのチームは、この課題を解決するためにデータを別個の分析基盤やAIプラットフォームへコピーしようとします。しかし、その結果として生じるのは、コスト増加、複雑化、そして攻撃対象領域の拡大です。

統合された基盤は、この状況を根本から変えます。組織はAI活用に適したデータへ、安全かつ正確に、そして完全な形でアクセスし、利用できるようになります。

保護とセキュリティがすでに統合されていれば、同じ信頼できるデータ基盤を、ガバナンスモデルを崩したり、データやインフラを重複させたりすることなく、検索可能かつ利用可能にできます。継続性を守るためのデータが、そのままインサイトを生み出すAI向けデータになるのです。

このモデルにおいて、AIは二つの役割を果たします。自動化や高度な検知によって基盤プラットフォームそのものを強化すると同時に、生産性向上アシスタントから特化

各レイヤーは、その下のレイヤーの上に構築されます。



保護 は、データを復旧可能にします。

セキュリティ は、データの信頼性を高めます。

AI は、データに価値を与えます。

融合には合理性がある

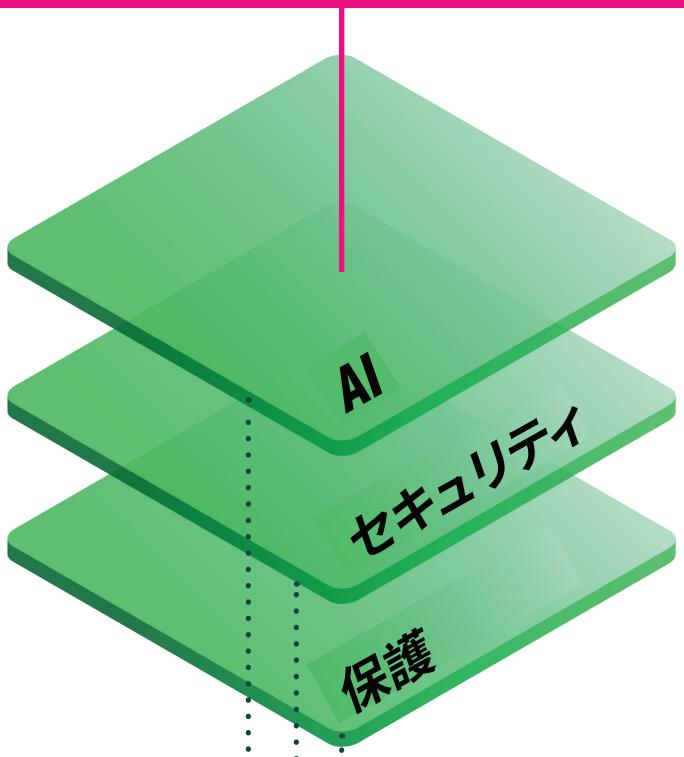
保護、セキュリティ、AI対応が単一の基盤上で統合されると、データは次のようになります。

- 一回管理すれば、さまざまな用途に活用可能
- 保存場所を問わず保護される
- ソースでセキュリティを確保する
- 重複のないAI対応データとなる

不意に、最も安全なデータのコピーが、最もスマートなデータのコピーに変わりました。

サイバーリスクとAI導入の加速によって定義される世界では、アーキテクチャの選択は明確です。単一のデータ基盤を、単一のスケーラブルなシステムとして管理し、混乱に耐えながら、同時にインサイトを生み出すように構築します。

それが、COHESITY DATA CLOUD です。



保護 は、復旧性を確保します。

セキュリティ は、リスクを低減します。

AI は、価値を引き出します。

エンタープライズ規模で実証済

Cohesity Data Cloud は、構築した唯一の統合プラットフォームで、サイバーレジリエンスを強化し、データからより多くの価値を引き出します。

- オンプレミス、クラウド、SaaSにまたがる **1,000超** のワークロードを保護
- バックアップを最大 **18倍** のワークロードを保護
- Instant AIにより、インサイト取得までの時間を **97%** 短縮
- ストレージ使用量を **50%**削減
- 総コストを最大 **40%** 削減

詳細は cohesity.com/DataCloud をご覧ください。

COHESITY
cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

6300010-001-JP 03-2026