DELL Technologies

サイバーセキュリティとゼロトラストの成熟度を高める。

リソースと知識の不足を補い、サイバー攻撃に対する防御体制を強化しましょう。

今日、脅威は急速に変化しています。特に生成AIへの注目が高まりを見せ、ベテランのサイバーセキュリティ スペシャリストでさえ予期できない新たな課題が生まれています。経験豊富なセキュリティ プロフェッショナルと連携すれば、サイバー攻撃を回避し、強固なセキュリティ プラクティスを維持できます。その詳細をご紹介します。

サイバー脅威はもぐら叩きのようなもの

1つ対処しても、すぐに別の脅威が現れます。

ますます相互につながり合うこの世界で、組織はデジタル インフラストラクチャに大きく依存しており、データは生活に欠かせないものでありながら広範囲に広がっています。そのため、自社のIT環境がすでに巧妙な攻撃者の侵害を受けていると想定しておくのがベストです。

幸いなことに、テクノロジーとサイバーセキュリティの両方に精通した経験豊富なパートナーがいます。

デル・テクノロジーズは、社内では用意できない可能性のある革新的なソリューションと価値ある専門知識をもたらし、変化し続ける脅威の状況を切り抜けるお手伝いをします。

- ハードウェアとソフトウェアのセキュリティ
- 新たなリスクに関するインサイト
- 高度な攻撃手法の把握
- 急速に変化する脅威に対応するためのAIOps
- 新しいセキュリティ戦略とベスト プラクティス

多層防御を構築することで、セキュリティ プラクティスを継続的に進化させ、ゼロトラスト アプローチを取り入れます。

デル・テクノロジーズは、サイバーセキュリティ パートナーとして包括的なプロフェッショナル サービス、ハードウェア ソリューションとソフトウェア ソリューション、堅牢なパートナー エコシステムを提供します。

このような対策を通じて、攻撃の機会を制限し、脆弱性を特定して最少化し、事業運営の迅速な回復を支援します。

攻撃対象領域の縮小 →

サイバー脅威の検出と対処 →

攻撃からの迅速な復旧 →

エッジ　**コア**　**マルチクラウド**

プロフェッショナル サービス

ビジネス/テクノロジー パートナー エコシステム　**セキュアなサプライ チェーン**

DELL Technologies

攻撃対象領域の縮小

防御力を上げ、標的になりにくくなるよう、サイバー犯罪者が悪用したくなるような経路を減らしましょう。

セキュリティ体制を強化するには、エッジ、コア、クラウドなどのさまざまな領域でアプリケーション、システム、ネットワークの侵害につながる可能性のある脆弱性とエントリー ポイントを特定し、最少化する必要があります。

脆弱性ポイントを特定

- ソフトウェアの脆弱性
- 構成エラー
- 脆弱な認証メカニズム
- パッチ未適用のシステム
- 過度なユーザー権限付与
- 開かれているネットワーク ポート
- 不十分な物理的セキュリティ

予防措置を実装

- セキュアなサプライヤーとの協力
- 包括的なネットワーク セグメンテーションの適用
- 重要なデータの分離
- 厳格なアクセス制御の実施
- システムやアプリケーションのアップデートとパッチ適用
- AIや定期的な評価とテストを使用した脆弱性の特定と対処

ゼロトラスト アプローチを取り入れる

ゼロトラスト アーキテクチャとは、組織がその境界内外のあらゆるものを無条件には信頼しないことを意味します。システムに接続しようとするすべてのものを無条件に信頼するのではなく、アクセス権を付与する前に検証を行います。このモデルは、米国国防総省が確立、規定しました。体系的に成熟度を高めるための相互関係にある7つの柱を掲げています。

1. ユーザーの信頼性
2. デバイスの信頼性
3. データの信頼性
4. アプリケーションとワークロード
5. ネットワークと環境
6. 可視性と分析
7. 自動化とオーケストレーション

DELL Technologies

攻撃対象領域の縮小

トラブルが発生する前に、システムの能力を低下させる弱点を特定しましょう。

サイバーセキュリティは、一度限りのタスクではなく、継続的な取り組みです。経験豊富なセキュリティ サービス パートナーの力を借りて、監査、侵入テスト、脆弱性評価を定期的に実施すれば、不足している領域を特定して補い、結果としてリスクを軽減できるのです。

セキュアなサプライチェーン プラクティス

セキュリティ対策は、皆様が思っているよりも早い段階から始まります。セキュアなサプライチェーン、セキュアな開発ライフサイクル、厳格な脅威モデリングで設計、製造、納品されたデバイスとインフラストラクチャを使用し、信頼できる基盤を確立します。

組み込み型セキュリティ

組み込み型かつハードウェアベースのセキュリティを備えたデバイスとインフラストラクチャを業務に使用することで、攻撃を検知して損害を未然に防げます。

定期的なパッチ適用とアップデート

既知の脆弱性に対処して悪用のリスクを最小限に抑えるため、アプリケーション、ファームウェア、OSに最新のセキュリティ パッチを適用して最新の状態に保ちます。

最小限の権限付与

ユーザー アカウントとシステム アカウントを絞り、タスクの実行に最小限必要なアクセス権を付与します。このようなアプローチにより、不正なアクセス権を取得した攻撃者が及ぼす可能性のある影響を抑制できます。

ネットワークセグメンテーション

重要なデータ、ビジネス グループ、ビジネス アプリケーションに最新のネットワーク セグメンテーションを適用し、重要な資産を分離してネットワーク アクセスを制限します。ラテラル ムーブメントなどの攻撃を封じ込めることができます。

アプリケーションセキュリティ

セキュアなコーディング プラクティスを実装し、セキュリティ テストとコード レビューを定期的に実施し、Webアプリケーション ファイアウォール(WAF)を使用すると、一般的なアプリケーション レベルの攻撃を防ぎ、Webアプリケーションの攻撃対象領域を減らすことができます。

プロフェッショナルサービスとパートナーシップ

サイバーセキュリティ サービス プロバイダーと協力し、ビジネス パートナーやテクノロジー パートナーと提携すると、社内では用意できない可能性のある専門知識とソリューションを手に入れることができます。

ユーザーの教育と意識向上

従業員とユーザーに対して、潜在的なセキュリティの脅威、フィッシングの試み、ソーシャル エンジニアリング戦術を識別して報告するための研修を実施し、人間の脆弱性が悪用されるリスクを最小限に抑えます。

DELL Technologies

サイバー脅威の検出と対処

従来型のセキュリティ プラクティスは、ダイヤルアップのインターネットのようなもので、今日の要求の厳しい環境では遅すぎて効果がありません。

巧妙化するサイバー脅威に対抗するには、AIやMLが組み込まれたアプリケーションや手法で既知の脅威も未知の脅威も特定して対応するなど、優れたセキュリティ対策を用意しておく必要があります。

侵入検出と侵入防止のための強力なシステムを実装

異常検知のためにAIとMLを活用

ネットワーク トラフィックとユーザーの行動に対するリアルタイムなモニタリングを確立

経験豊富なプロフェッショナル サービスと連携して特殊な専門知識を手に入れ、レジリエンスを高めましょう。

デル・テクノロジーズは、経験豊富なテクノロジー パートナーとして、インシデント対応と復旧のためのプロアクティブなプロトコルの確立を支援できます。このようなプロトコルは、役割と責任の概要を示し、関係者間のシームレスなコミュニケーションと調整を確保するために役立ちます。

以下のような高度な対策を利用して、サイバー脅威をプロアクティブに検出して対応する能力を強化しましょう。

- 脅威インテリジェンス
- インシデント対応
- セキュリティ情報イベント管理
- エンドポイント保護
- 行動分析

以下のような対策を利用して、効率的で迅速な復旧を促進し、データ ロスを最小限に抑えましょう。

- 適切に定義されたインシデント対応計画と協力
- 重要なデータとシステムの定期的なバックアップ
- セキュアなオフサイト ストレージ ソリューションとデータ暗号化

DELL Technologies

サイバー脅威の検出と対処

常に警戒し、迅速に行動を起こしましょう。

サイバー脅威を検出して対処するには、常に警戒し、最悪のシナリオに備えておくこと必要があります。組織全体が攻撃の影響を軽減する方法を把握できるよう、対応と復旧の計画を確立し、継続的に更新し、定期的に演習を実施しましょう。これは継続的で反復的な取り組みであり、テクノロジー、熟練した担当者、適切に定義されたプロセス、チームの協力を組み合わせる必要があります。

継続的モニタリング

侵入検出システム(IDS)、侵入防止システム(IPS)、ログ分析、脅威インテリジェンスなどのセキュリティ ツールは、不正アクセス、侵入、マルウェア感染、データ侵害の兆候を特定するために役立ちます。

脅威の検出

AIとMLを活用してデータを分析し、脅威につながる可能性のあるパターン、異常、侵害指標(IoC)を特定します。例えば、既知の攻撃シグネチャを認識したり、逸脱行動を識別したりできます。

警告と通知

早期に警告を出し、調査と対応を促します。アラートと通知が明確に表示されるため、統合セキュリティで迅速に措置を講じることができます。OSの上層にデバイスレベルのテレメトリーをフィードすると、脅威の検出を迅速化できます。また、潜在的な脅威やインシデントが検出された際にセキュリティ担当者やセキュリティ オペレーション センター(SOC)にアクセスできます。

インシデント対応

対応計画を開始し、確認されたセキュリティ インシデントを調査してその影響を軽減します。例えば、影響の封じ込め、根本原因の特定、システムの回復や損害の拡大防止に必要な措置の実施などが必要です。

フォレンジック分析

インシデントの詳細な分析を実施して、攻撃手法を把握し、侵害の範囲を判断し、影響を受けるシステムやデータを特定し、証拠を収集します。その結果、セキュリティ上の弱点を見つけて対処することができます。

修復と復旧

脆弱性の修復、システムへのパッチ適用、マルウェアの削除、セキュリティ対策を強化するための措置を講じ、同様のインシデントを防止します。影響を受けたシステムとデータを通常の状態に回復して、復旧プロセスを完了します。

サイバー攻撃からの復旧

できる限り迅速に業務を通常の状態に戻せるよう、全力で取り組みましょう。

サイバー レジリエンスは今日のデータ主導型の世界において必要なものであり、お客様やパートナー様にも期待されています。成功を収めるには、重要なデータを確実に保護して分離するための多層防御が必要です。このような対策をとれば、攻撃を受けたとしても、重要なデータを確実かつ迅速に復旧できます。
こちらからサイバー レジリエンス評価（英語）を受けられます ›

- サイバー攻撃が原因で発生する損害を軽減するための措置を講じる
- 侵害を受けた、または破壊されたサービスとデバイスを再構築
- インシデントを分析して今後の攻撃を防ぐ
- ビジネスのSLAを満たし、事業活動を通常の状態に戻す

組織が効果的かつ効率的に復旧できるよう、包括的なサイバーセキュリティ戦略を策定しましょう。

サイバー攻撃から復旧するには、ITチーム、サイバーセキュリティの専門家、経営陣が協力して取り組む必要があります。場合によっては外部の専門家が関与することもあります。復旧の鍵は、システムと事業活動を迅速に通常の状態に戻すと同時に、発生したインシデントから学ぶことです。中断やダウンタイムを削減し、サービスとデータの完全性を回復し、財務状況や評判への影響を最小限に抑え、今後の同様の攻撃を防ぐためにサイバーセキュリティを強化することを目指します。

- 攻撃が事業活動に与える影響を評価
- 重要なサービスを優先
- データ保護システムを導入
- インシデントと復旧の進行状況について伝達
- 継続性を確保するため、計画を作成し、演習を繰り返し実施

DELL Technologies

サイバー攻撃からの復旧

インシデント後にシステム、ネットワーク、データを回復して、通常の運用状態に戻しましょう。

サイバー レジリエンス戦略を達成すると、人材、プロセス、テクノロジーが、組織全体を保護する総合的な枠組みに組み込まれます。

インシデントの封じ込め

まず、サイバー攻撃により影響を受けた部分を分離して封じ込めます。具体的には、影響を受けたシステムをネットワークから切断し、侵害されたアカウントを無効化し、損害の範囲や程度の拡大を防ぐための対策を実施する必要があります。

システムまたはデバイスの回復

インシデントの封じ込めが完了したら、影響を受けたシステムとネットワークを清浄で安全な状態に回復します。侵害を受けたシステムの再構築、ソフトウェアの再インストール、セキュリティ パッチとアップデートの適用が必要となる場合があります。事業を通常の状態に戻すために、自動化と自己修復が重要な役割を果たす可能性があります。

データの復旧

攻撃を受けた際に侵害、暗号化、削除された可能性のあるデータは、復旧する必要があります。バックアップからデータを回復する、または専用のデータ復旧手法を使用して失ったファイルや暗号化されたファイルを取り戻すことが必要となる場合があります。

フォレンジック分析

攻撃を受けた後に、侵害の発生状況、悪用された脆弱性、同様の攻撃を防ぐための手順を把握することが重要です。セキュリティ情報イベント管理(SIEM)のようなシステムや、オフホストBIOS比較などの機能を利用すると、有用なインサイトが得られます。

インシデント対応評価

復旧後、インシデント対応プロセスを評価し、改善の余地がある領域を特定することが重要です。攻撃から得た教訓を、セキュリティ プラクティスの強化、インシデント対応計画のアップデート、今後発生するインシデントに対する保護の改善に活かすことができます。

プロフェッショナル サービスとパートナーシップ

サイバーセキュリティのサービス プロバイダーとテクノロジー パートナーは、価値ある専門知識とリソースをもたらし、組織の復旧を支援します。また、フォレンジック分析などのタスクの手助けもできます。侵害の発生を特定し、今後のインシデント防止に向けた対策を推奨してくれるのです。

DELL Technologies

サイバーセキュリティを エッジ環境やクラウド環境に拡張

ネットワークがコアからエッジ、クラウドへと広がるにともない、環境は重大な脆弱性ポイントとなっています。

サイバーセキュリティ戦略を推進する際に、組織はゼロトラスト原則の適用範囲をエッジとクラウドに拡大し、厳格なアクセス制御と継続的な認証を実行し、ネットワーク トラフィックの包括的な可視化と制御を確保する必要があります。脅威の状況が変化するに従い、AI 機能を防衛の最前線として導入することが重要です。さらに、戦略を完全なものにするには、コア ネットワークとクラウド環境に、ネットワーク セグメンテーション、暗号化、継続的モニタリングなどのセキュリティ対策を配備する必要があります。

サイバーセキュリティ プロフェッショナル サービスが総合的なアプローチの採用に役立ちます。

さまざまなセキュリティ ソリューションを繋ぎ合わせる作業は、困難な場合があります。エッジ、コア、クラウドのセキュリティに特化したプロフェッショナル サービスと連携すれば、効果的な対策を講じ、組織をあらゆる角度から保護するための専門知識を得ることができます。

エッジ

エッジやネットワークで、またハードウェアやソフトウェア内で、多層のセキュリティを確立しましょう。

コア

AI、ML、自動化を利用して、インフラストラクチャをゼロトラスト アプローチに合わせて調整しましょう。

マルチクラウド

パブリッククラウド、コンテナ、クラウド ネイティブ ワークロードなど、あらゆる環境ですべてのワークロードを保護しましょう。

DELL Technologies

生成AI：サイバーセキュリティにとって両刃の剣

次世代のAIにより変化のスピードが上がる中、新たなリスクが発生していますが、セキュリティも向上しています。

新たな段階に進んだAIである生成AIは、さまざまなタスクにおける知識を理解、学習、適応、実装できる各種システムを包含しています。

一方では、脅威の検出と対処、予測的機能、運用効率の向上が期待できます。他方では、新たな課題が生まれているため、サイバーセキュリティ戦略を発展させる必要があります。リスクに対処するために、堅牢なセキュリティ対策、継続的モニタリング、定期的なアップデートとパッチ適用、データ プライバシーと倫理に対する絶えず進化するアプローチが求められます。

生成AIで組織のセキュリティを確保

生成AIは、サイバーセキュリティに欠かせない要素となっており、組織を保護するための新たな手段をもたらしています。

- 脅威の検出と対処の有効性を改善します。
- 今後の脅威を予測し、潜在的な脆弱性を特定します。
- 脅威の検出を自動化し、効率を高めます。
- フォレンジック分析を通じて、パターン、異常、侵害指標を迅速に特定します。
- パーソナライズされたセキュリティ意識向上研修を作成します。
- セキュリティ運用の規模を調整し、豊富なインサイトにすばやくアクセスできます。

生成AIシステムのセキュリティを確保

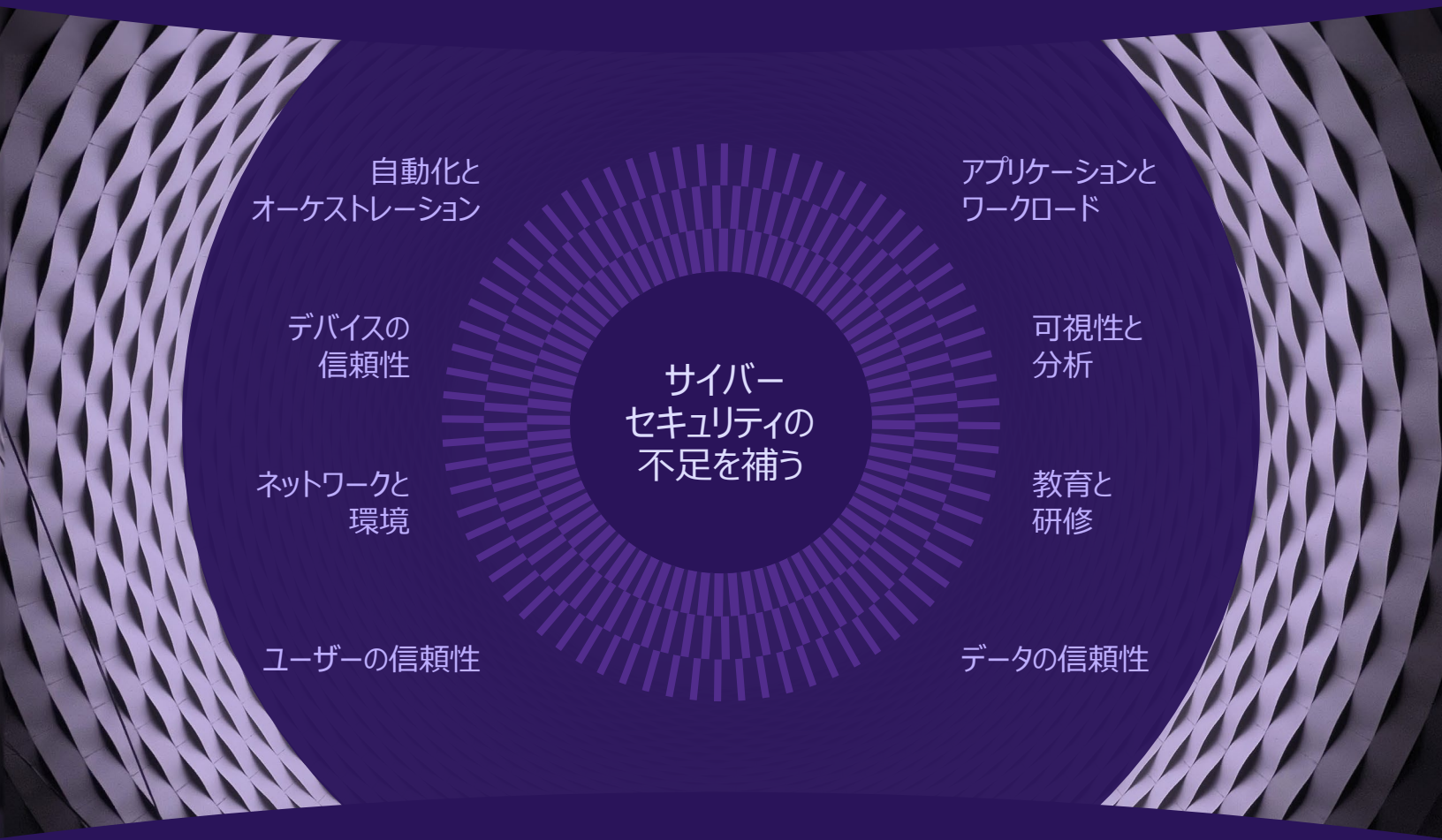
生成AIは、セキュリティ面で大きなメリットをもたらします。しかし適切に保護しなければ、その機能が悪用される可能性があります。

- データ プライバシーとデータの完全性を確保します。
- AIシステムを欺いて不具合を引き起こそうとする敵対的な攻撃を緩和します。
- 悪意のあるAIによるシステムの誤用を検出して対処します。
- 倫理的な問題や偏見を監査し、低減します。
- AIシステムに対する強力なアクセス制御を実装します。
- 大規模言語モデル(LLM)を安全に保護、復旧します。

DELL Technologies

最新のサイバーセキュリティには インテリジェンス、拡張性、自動化が必要

デル・テクノロジーズは、お客様が包括的なセキュリティを確立し、変化するサイバー脅威から身を守れるよう支援します。テクノロジーの進歩に合わせて、当社のサイバーセキュリティに対するアプローチは一歩先を行き、AIとMLの力を活用してデジタル インフラストラクチャの安全を確保し、デジタル領域における信頼を維持します。当社は、お客様がサイバーセキュリティの取り組みにおけるどの段階にあるとしても、俊敏性とレジリエンスを維持するための手順で組織を保護するだけなく、それ以上の支援を行います。



DELL Technologies

Dell.com/SecuritySolutions