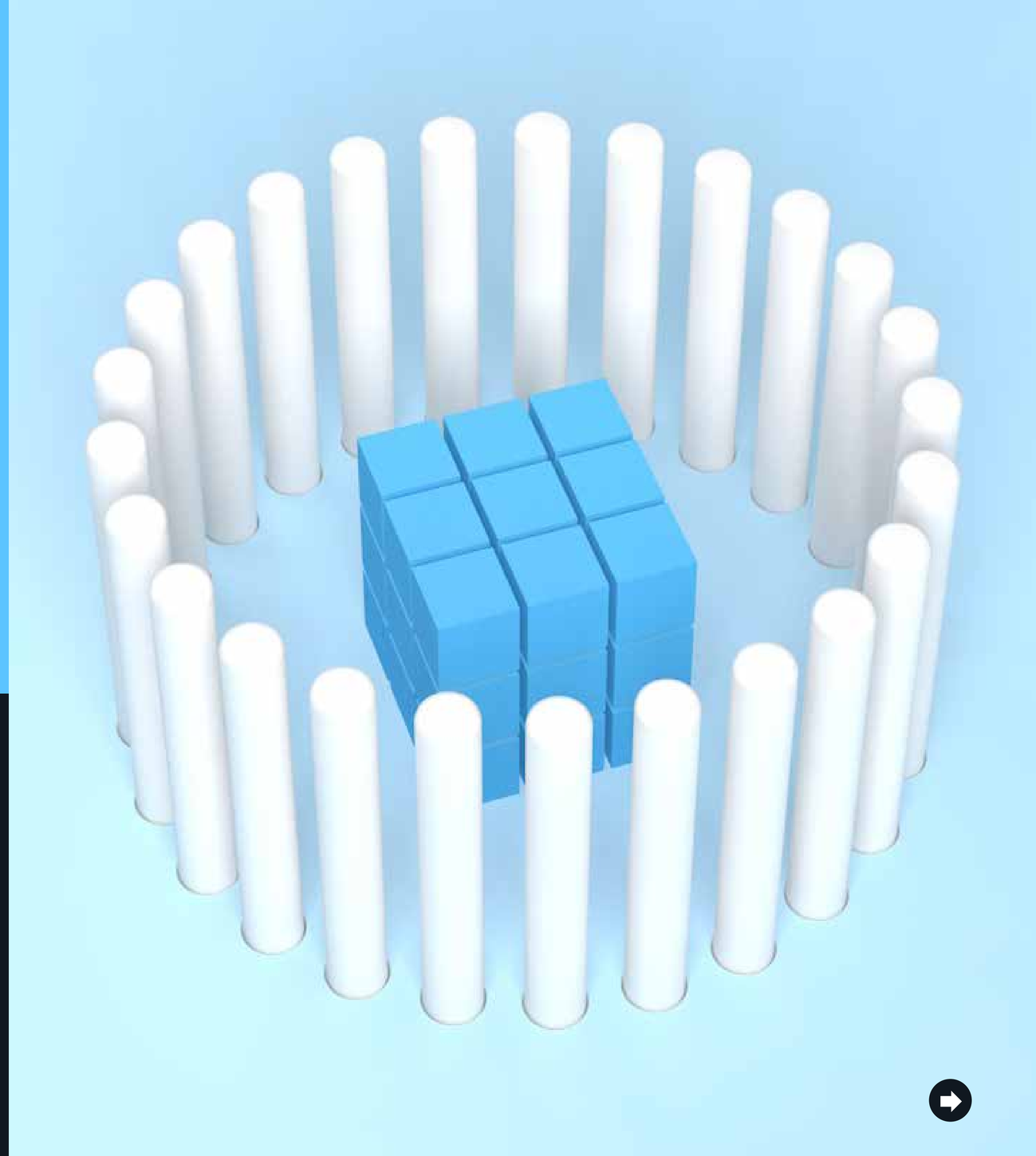
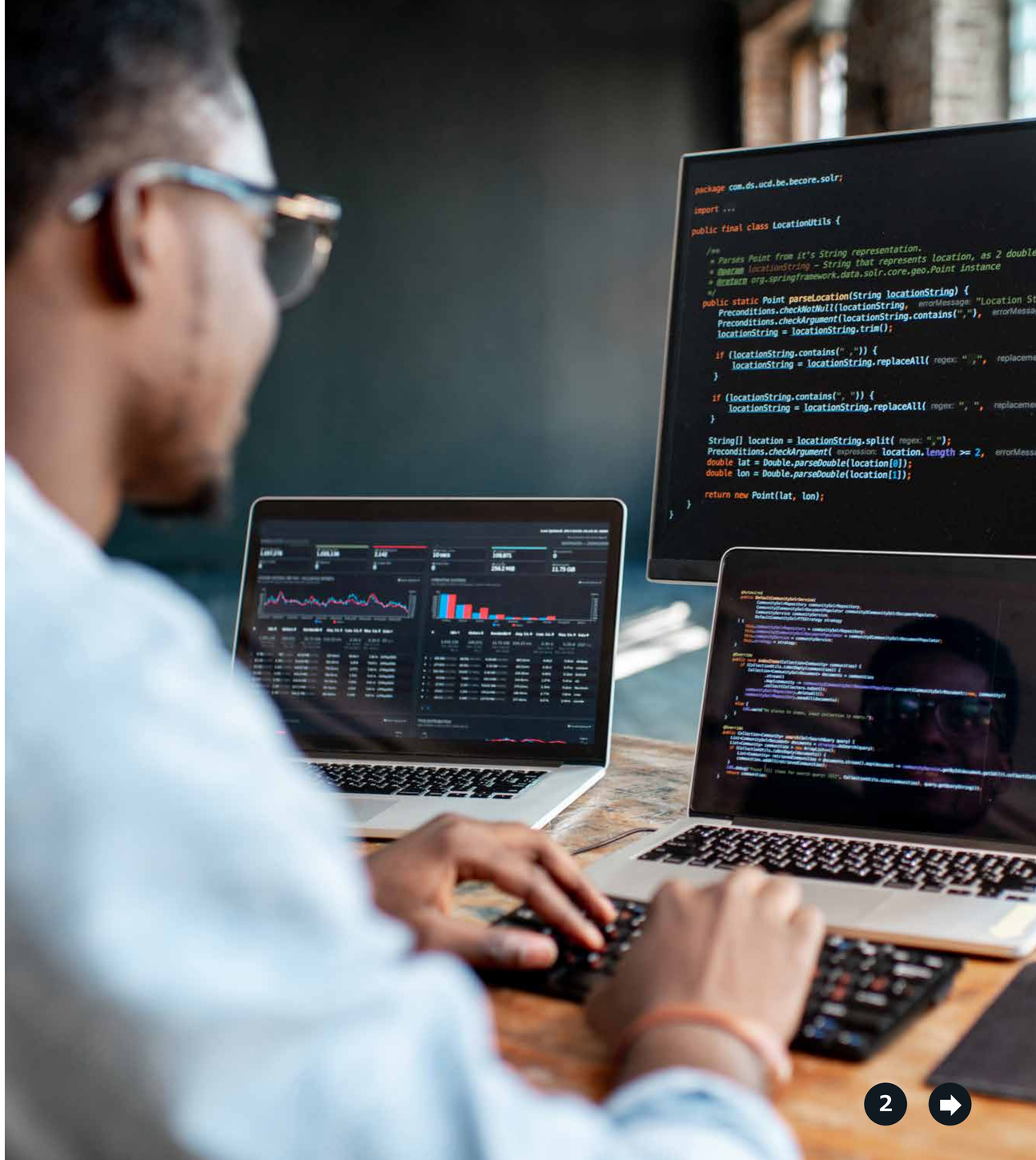
Eブック

サイバー レジリエンス：データを徹底的に保護する方法

NetApp



目次



IT組織の中心に臨むアプローチ

週に一度、食料品を買い出しする日がやってきました。 あなたは買い物用のマイバッグを持ち、車のキーを手にして、「ドライバー レジリエンス ピル」という大きな銀色の錠剤を口に入れてから、玄関を出ます。

これであなたは、 スーパーへ向かう道でどんな衝撃を受けても耐えられる超人的な能力を身につけたことに安心し、 安全に運転することができます。

もし私たちが、 魔法の疲労回復ドリンクを飲んだり、 侵入者を追い出すレンガで家を建てたり、 泥棒の手から宝石を買い戻したりできるなら、 シートベルトや鍵や警報システムなどのことを気に病むことはほとんどないでしょう。

こうした魔法のような防御は現実世界には存在しないかもしれませんが、 仮想世界では姿を現し始め、既存の保護装置と融合しようとしています。 過去数十年間、 ITの世界では、 利用できるからと言う理由で「シートベルトと警報システム」というアプローチでサイバーセキュリティを実現してきました。

今は、 よりスマートな「**サイバー レジリエンス**」というアプローチがあります。

サイバー レジリエンスは、 データ保護と従来のITセキュリティを組み合わせて、 組織がサイバー攻撃から回復できるようにするためのものです。 たとえ侵入者が境界を突破したり、 内部関係者が悪意のある行動を起こしたりしても、 データは保護されます。 後付けではなく組み込みの保護機能を備えているからです。

このアプローチが重要な理由

サイバー レジリエンスが重要なのは、「城と堀」のアプローチを取るサイバーセキュリティ対策では、 進化を続ける犯罪の手口に対応できないからです。 多くのセキュリティ戦略は、 境界の防備を固めることで敵を入り口から通さないことを軸にして展開されています。 しかし今では、 エンドポイントの急速な増加や、 個人所有機器の持ち込み （BYOD） ポリシー、 リモート ワークの普及により、 入り口は1つではなく何百も存在するようになりました。 このような入り口から、 犯罪者は複雑なネットワーク環境を徹底的に監視することが手に負えなくなっている組織に容易に侵入することができます。 そして、 多くの組織は、 目標は侵入防止ではないということを忘れています。 最大の目標は、 最も価値あるもの、 つまりデータを保護することです。

サイバー レジリエンス戦略を データ レイヤから始めているか

あらゆるところに脅威があるなら、 どこから始めれば良いのでしょうか。

まず、 セキュリティと保護をデータ中心にすることから始めましょう。 そして、 それをサイバー レジリエンス計画の中核とします。

ランサムウェア攻撃は全世界で62%増加し[1]、 ランサムウェアの亜種は3.4%増えており[2]、 攻撃者はデータを人質に取ることがますます巧妙になっています。 ランサムウェア攻撃を受けた後で、 約3分の1の組織が暗号化されたデータを取り戻すために結局身代金を支払っています[3]。 具体的には、 2021年のランサムウェア攻撃への対処にかかる平均費用は185万米ドルで、 2020年の76万8,106米ドルから増加しています[4]。

さらに、 二重の恐喝を行うランサムウェア攻撃も増加しており、 組織はデータを失うだけでなく、 そのデータを公開される恐れもあります[5]。 リスクはかつてないほど高く、 現代のコンピューティングにおいて、ランサムウェア攻撃は「起こるかどうか」ではなく「いつ起こるか」という現実の問題です。

では、 次のランサムウェア攻撃に怯えて暮らす必要があるのでしょうか。 いいえ。 データ主体のアプローチでサイバーセキュリティに取り組むことで、 **ランサムウェアを恐れず**、 **サイバー レジリエンスを活性化する**ことができます。

このアプローチは、 境界からではなく、 できるだけデータの近くから始めることになります。

データ レイヤにもう到達したか

データを守るためにIT組織の中心に臨むのであれば、 多少の工夫が必要です。
幸いなことに、 すでに多くの人が挑戦し、 役立つ指標を残しています。

特定

対応

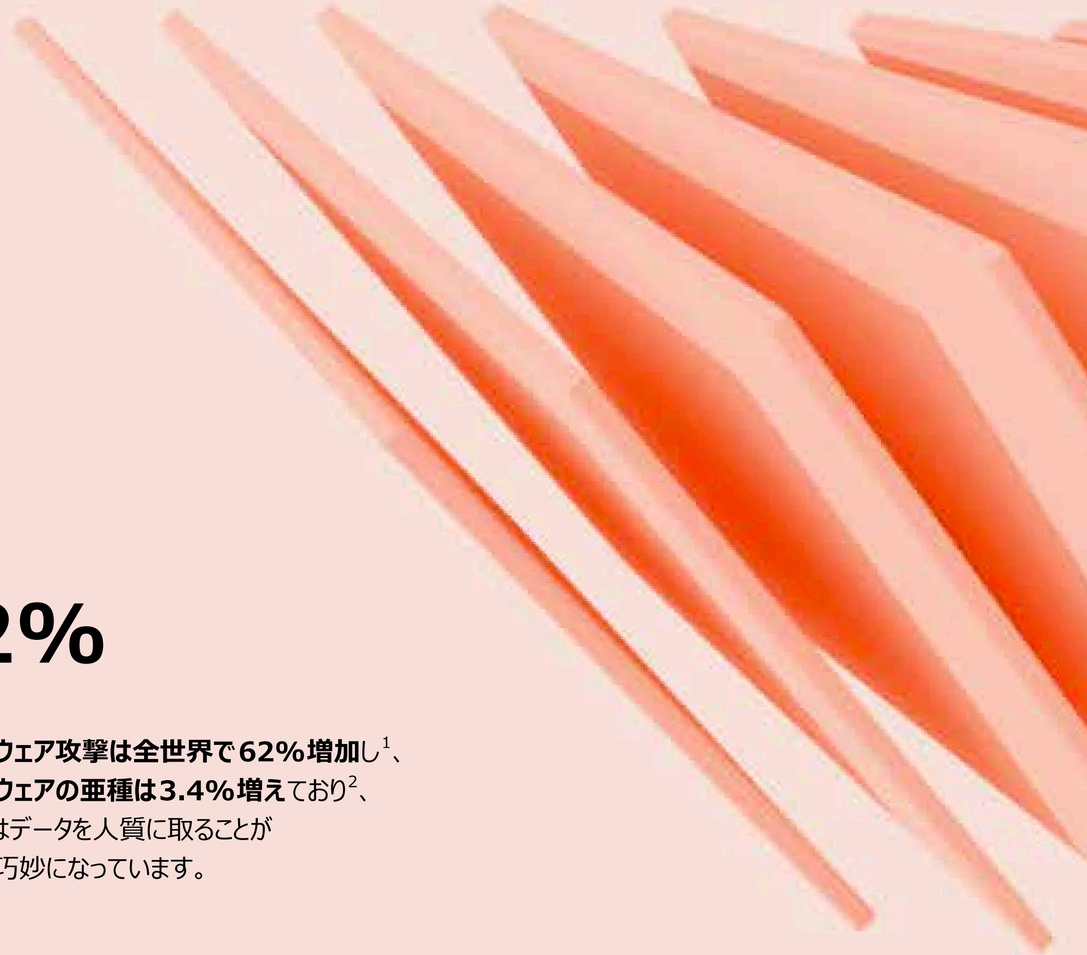
保護

復旧

検出

このような指標があっても、 包括的なサイバー レジリエンス計画を立てることは困難であり、 費用もかかります。 チームは限られたリソースをやり繰りし、 スキルのギャップを埋め、 規制要件を組み入れ、 他の優先事項を駆使して注目を集める必要があります[6]。 サイバー レジリエンスは、 たちまちチームを疲弊させるものとなり、 忘れ去られてしまいます。

では、 各ステップの取り組み方についてご説明します。



62%

ランサムウェア攻撃は全世界で62%増加し[1]、
ランサムウェアの亜種は3.4%増えており[2]、
攻撃者はデータを人質に取ることが
ますます巧妙になっています。

特定 ： 環境を評価する

保護が必要なものを特定し、 各アイテムの重要度をランク付けします。 ビジネスの運用を維持するには、 どのシステムが欠かせないのかを尋ねます。 すべてのハードウェアとソフトウェアのインベントリを作成し、 どこに何があるのか、 ビジネスの運用においてどのような役割を果たしているのか、 悪意のある人物にどのように悪用される可能性があるのかを把握します。 情報の流れを文書化し、 サイバーセキュリティ活動に関連する役割と責任を割り当て、 脅威の特定とリスク管理のための計画を策定します[7]。

言い換えると、 現在のデータ保護とセキュリティを評価する必要があります。 また、 さまざまなタイプのデータを分類し、 そのタイプがどこにあるかを判断し、 その権限を評価することが必要です。

「特定」段階での課題

「特定」の段階は時間がかかります。 ITリーダーは、 日々のインフラ管理やデータ管理に関して、 すでに膨大な数のタスクを抱えています。 ITインフラ全体のインベントリを作成するだけでも、 特に自動化ツールを使用しなければ、 かなりの時間を消費する可能性があります。 また、 このインベントリ作成が特定の計画や標準化された分類プロトコルに基づいて実施されていない場合、 さらに混乱を招くデータが作成され、 チームが解読して運用可能にするのが困難になる可能性があります。

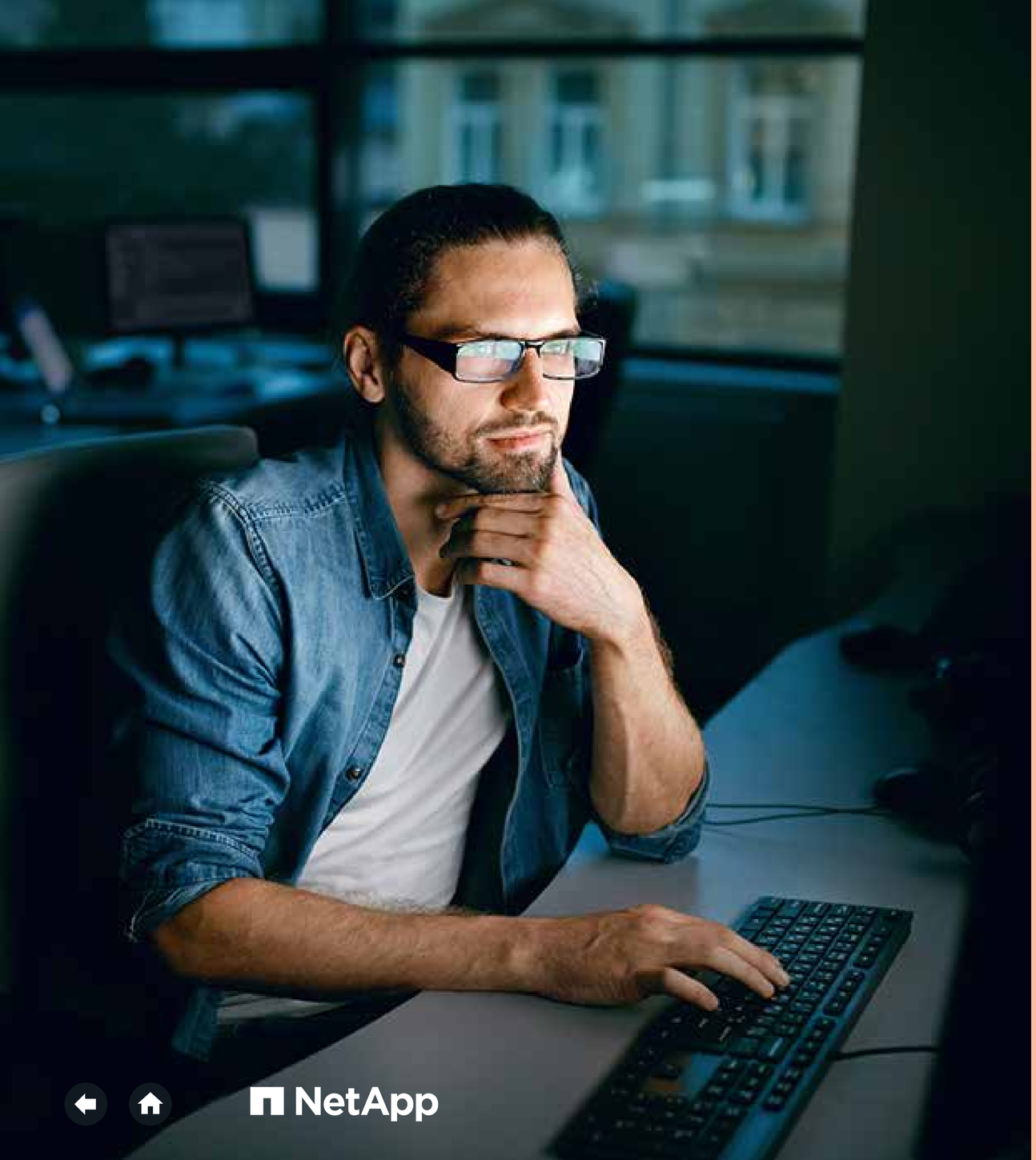
保護 ： 守りを固める

「保護」の段階では壁を作ります。 データの暗号化、 定期的なバックアップの実施、 アクセス制御の徹底、 防御網の導入、 脆弱なオペレーティング システムやアプリケーションの更新、 サイバーセキュリティのベストプラクティスに関するユーザの教育などを行います[8]。

この段階で行われるのは、 悪意のあるユーザのブロック、 潜在的な不良データの隔離、 ディスクへの追加データの書き込み防止、 感染阻止のためのきめ細かな書き換え不能コピーの作成、 消去不能のバックアップによるデータ消去の防止などです。

「保護」段階での課題

「保護」の段階では、 サイバーセキュリティに対するアプローチにおける最新の変化がいくつか明らかになります。 企業は何十年にもわたってファイアウォールやネットワーク侵入防止ツールを使ってIT環境を保護してきましたが、 データ量が膨大であるという新たな現実が、 こうした戦略を複雑なものにしています。 インベントリを作成するよりも速く生成される大量のデータをどのように暗号化すれば良いのでしょうか。 （生産性の低下や安全でない回避策の選択につながる可能性のある） ユーザ エクスペリエンスの著しい毀損を生じさせずにアクセス制御を確実に行うには、 どうしたら良いでしょうか。 また、 発見された死角の数からみて、 すべてに対応したと確信できるようにするには、 どうしたら良いでしょうか。



検出 ： 一歩先を行く

予防は最良の治療です。 実際の脅威となる前に疑わしいアクティビティを特定するには、
以下に対応するシステムを導入します。

- 最新の検出プロセス
- 定期的な監視ログ。 異常なアクティビティを検出して対処できるようにするために必要
- 通常のデータフローの詳細な把握。 データ盗難の兆候となる異常なアクティビティを発見できるようにするため
- 侵入を検出するだけでなく、 その影響 （または「影響が及ぶ範囲」） を測定する能力[9]

つまり、 ユーザの行動を監視して不審なアクティビティがないか確認し、 データ行動の異常を検出する必要があります。

「検出」段階での課題

おそらく「検出」段階で最大の課題は、 企業がふるいに掛けなければならないノイズの多さでしょう。 サイバーセキュリティ チームとセキュリティ オペレーション センター （SOC） は、 脅威のアラートの処理に追われ、手作業で対処しなければならないこともしばしばです。 そのため、誤報や優先度の低いアラートを自動的に調べて取り除き、 より油断のできないアラートに注意を向けられるようにする仕組みが必要です。 また、 サイバーセキュリティ チームには、 これらの脅威をより迅速に検出し、 深刻な被害が発生する前に対処できるようにする仕組みも必要です。 特に、 攻撃者が大量のデータを暗号化できるようになる前に、 漏えいしたクレデンシャルによる不正アクセスを直ちに通知されなければなりません。

対応 ： 危機の際に何をすべきかを知る

セキュリティ対策とともに脅威も進化しています。そのため、常に計画を検証していくことが重要です。チーム メンバー全員が責任を自覚する必要があります。 一般的なサイバーセキュリティに関するベストプラクティスと、 緊急時に取るべき具体的な役割の両方を把握しておくことが必要です。 また、 脅威の進化や攻撃後の教訓をもとに、 計画を更新することも重要です。 最後に、 最新の計画を社内外の関係者とすべて共有し、 攻撃を受けた場合に結束して対応できるようにすることが重要です[10]。

「対応」段階におけるデータの処理では、 攻撃が特定されたときにスナップショットを開始し、 悪意のあるユーザ アカウントをブロックします。

「対応」段階での課題

「対応」段階では、 システムの概要を把握することで、 データの保管場所を評価し、 環境内でどのようなアクティビティが発生しているのかを監視し、 それに応じて計画を更新できるようにする必要があります。 先ほども述べたように、 日々のインフラやデータ管理のニーズに追われている組織にとって、 これは時間のかかる作業です。

しかも、 効果的に対応するためには、 個々の従業員が手作業で計画を実行するよりも速いスピードが必要なのが現実です。これは、どんなに準備を整えていても同じです。サイバーセキュリティ チームには、疑わしいアクティビティをシステムが検出するとすぐに、 事前に決められた手順 （データ スナップショットの取得など） を自動で実行するツールが必要です。

復旧 ： すぐに元の状態に戻す

サイバー攻撃によってビジネスの運用が中断された場合は、 迅速に運用を復旧できるようにする必要があります。 共有が必要となるのはどのような情報か、 その情報にアクセスする必要があるのは誰か、 関係者が必要な情報をタイムリーに入手できるようにするにはどうしたら良いのか、 などの要素を明確にする必要があります。 また、 情報が漏えいしたことを公にし、 個人情報が漏れた可能性のある人々に通知し、 監督官庁と連絡を取るための計画も必要でしょう。

「復旧」段階では、 数分でデータをリストアし、 侵害されていないアプリケーションをオンラインに戻し、インテリジェントなフォレンジックを適用して脅威の発生源を特定することが必要になります。

「復旧」段階での課題

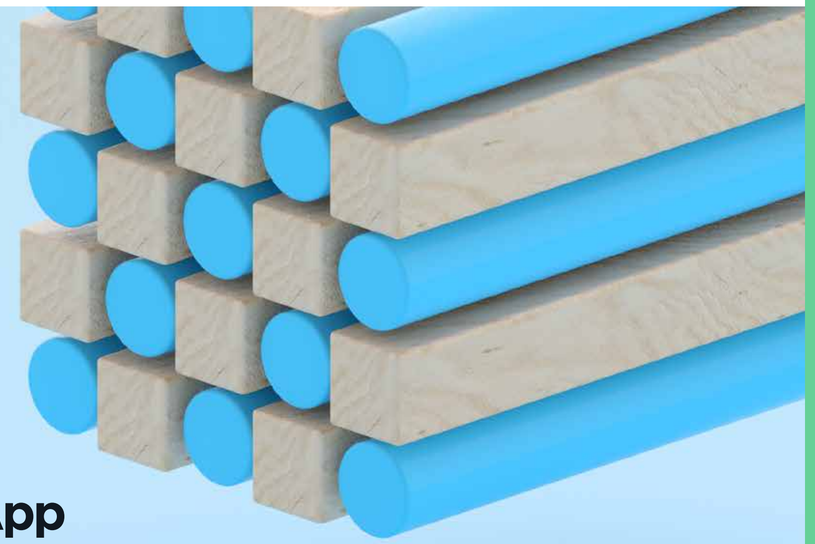
攻撃を受けた直後は、 何がどれだけ流出したかを特定するのに貴重な時間を取られますが、 内部の対応と外部の目をどちらもコントロールするためには、 この情報を迅速に入手する必要があります[11]。

ネットアップのサイバー レジリエンス ソリューションは、 サイバー レジリエンス計画の5つの要素 （特定、保護、検出、対応、復旧） に対応しています。 しかし、 多くの組織では、 断片的なサイバーセキュリティ ツールに資金を投入しているため、 他のプロバイダに移行しようと考えるのは並大抵のことではありません。

ネットアップなら、 この移行にとまどう必要はありません。 完全なソリューションとして、 あるいは既存の投資を補完するものとして、 ランサムウェア対策を導入することができます。

徹底的なサイバー レジリエンスに対する最新アプローチを構築

主にデータ レイヤに注目すれば、
サイバー レジリエンスのニーズにも取り組みやすくなります。
まずは、 以下の質問に答えて、
自社の現状を把握することから始めてください。



予防は最良の治療です。 実際の脅威となる前に疑わしいアクティビティを特定するには、以下に対応するシステムを導入します。

- データの保管場所は、 クラウドか？オンプレミスか？エッジか？複数の地域に分散しているか？
- どのような種類のデータがあるか？
- データにはどのような権限が適用されているか？
- 悪意のあるアクティビティを迅速に特定し、 ブロックするにはどうすれば良いか？
- 脅威を特定し、 それに対処しながら、 迅速に「自己防衛」できるように、 データの内部や周囲に保護を直接構築するにはどうすれば良いか？グローバルなネットワーク全体にわたり、 ユーザの行動を監視し、 疑わしいアクティビティがないかどうかを確認するにはどうすれば良いか？
- 攻撃の影響が及ぶ範囲を見極めながら、 すべてのデータの安全を確保するにはどうすれば良いか？
- 攻撃が発生した場合、 データやアプリケーションを数分でオンラインに戻すにはどうすれば良いか？
- 脅威の発生源を調査し、 今後の同じような試みを防ぐために十分な情報を得るにはどうすれば良いか？

これらの質問にすべて答えることで、 データ主体のサイバー レジリエンス計画の骨格を作って、 組織がランサムウェア攻撃を「恐れない」で済むようにすることができます。

思った以上に「わからない」という答えが多い場合、 ネットアップは、 答えを出すだけでなく、 新しいランサムウェア攻撃からの保護とリカバリのための計画を実行するために必要なツールが装備されたソリューションも提供します。

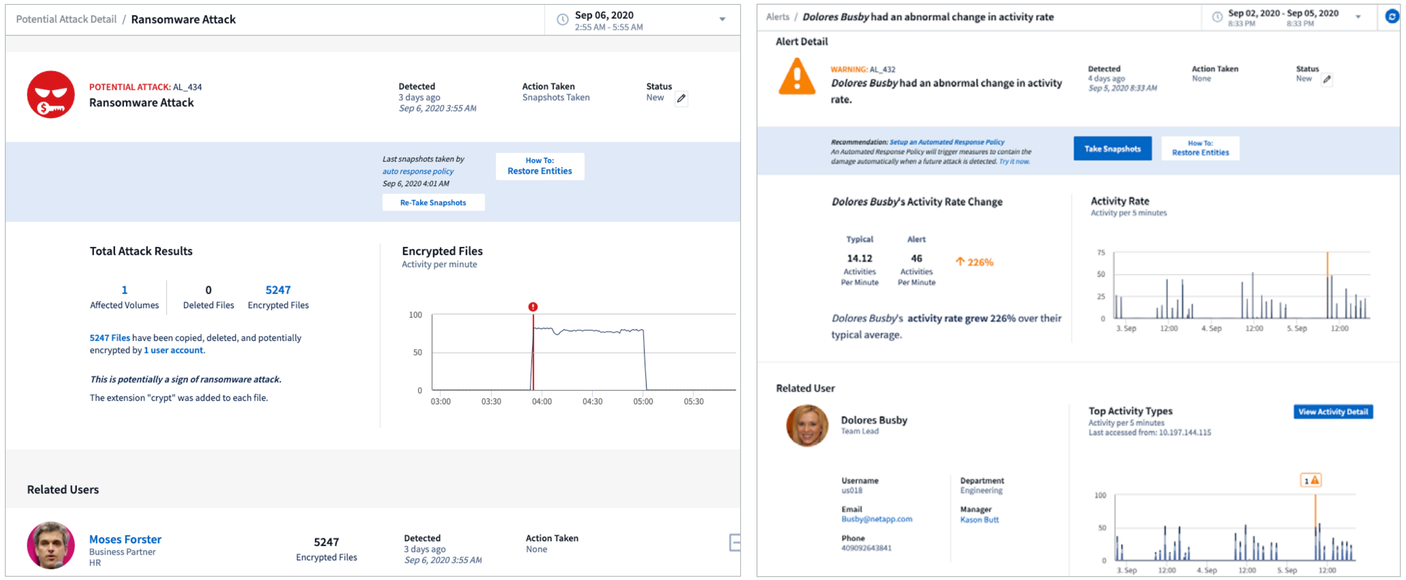
ネットアップが実現するサイバー レジリエンス計画

次のようなシナリオを想定し、 実際のランサムウェア攻撃を受けている間に、 ネットアップと、 先ほどの質問への回答に基づいたサイバー レジリエンス計画が、どのようにチームに役立つのかを考えてみてください。

チームは、 所有しているデータの種類と保管場所を把握する必要があります。 自動化ツールであるNetApp Cloud Data Senseを使用することで、 AIアルゴリズムによってデータの調査、 マッピング、分類を行い、 これらの情報を提供できます。 一方、 NetApp Cloud Insightsは、 ハイブリッド クラウド インフラを可視化し、 環境全体の監視とセキュリティ保護を可能にします。 組織の防御力が試されることになるので、 こちらも優れたツールです。

「当社は最近ランサムウェア攻撃を経験したばかりです。 Cloud Insightsのランサムウェア検知の機能を目にして、 すぐに魅力を感じました」

運輸会社のIT担当ディレクター



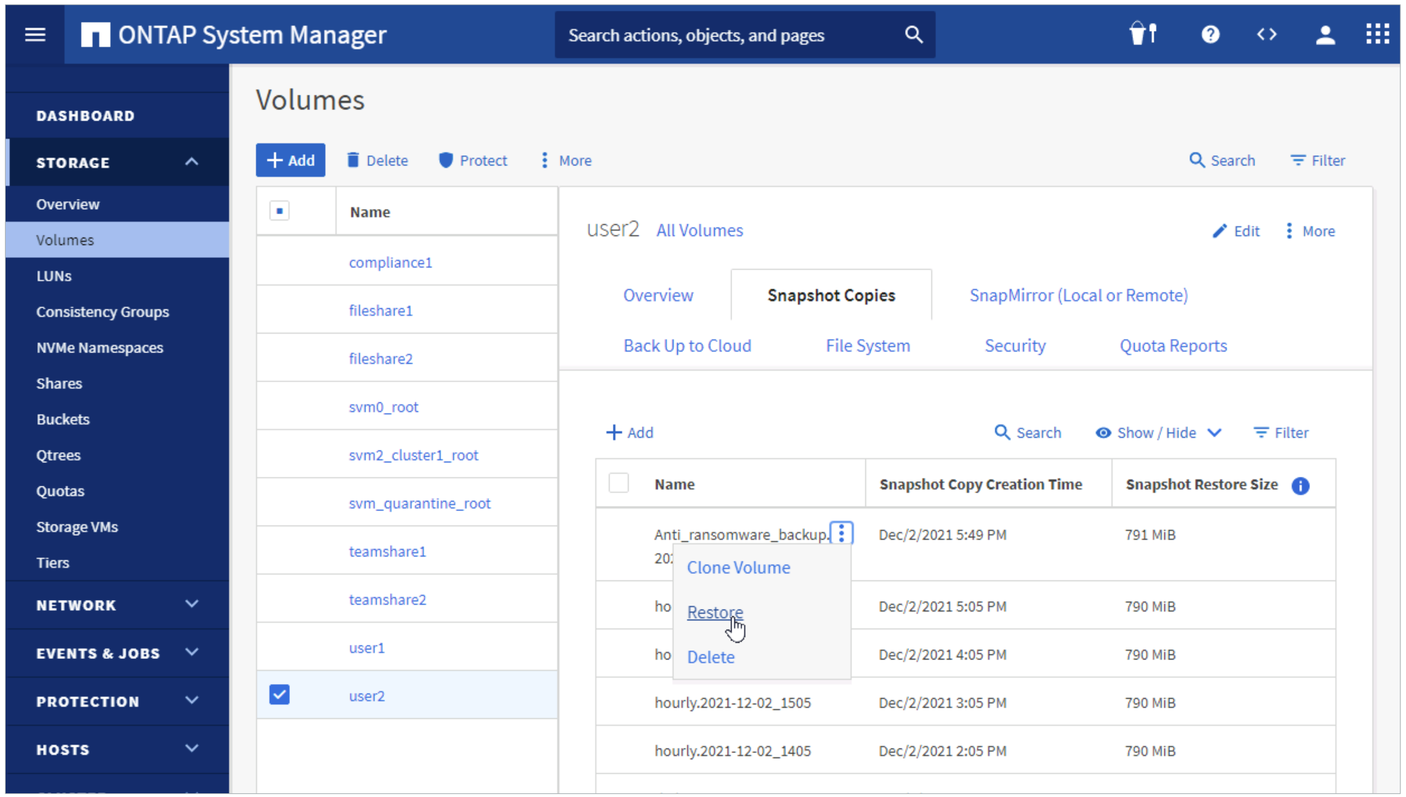
Cloud Insightsは、異常なユーザ アクティビティを検出し、Snapshotコピーを作成します（出典：ネットアップ）。

ある朝、 ニューヨークのITチームが出社し、 ロンドン オフィスの誰かが悪意を持ったEメールのリンクをクリックしたことを知ります。

近くでこの攻撃を物理的に監視していた人はいませんでしたが、NetApp ONTAP®データ管理ソフトウェアの一部であるNetApp FPolicyがゼロトラストのデータ保護ポリシーに基づき、 既知の悪意のあるファイルの拡張子をブロックしました。

それでもハッカーはしつこく食い下がり、 漏えいしたユーザ アカウントを使用して、マルウェアによるゼロデイ攻撃を仕掛けてファイルを感染させます。さらに多くのマルウェアが、 漏えいしたユーザ アカウントをいくつか悪用してデータを暗号化します。 発見されないように、 ゆっくりとした動作で。

このようなアクティビティをすべて察知して対処することは、 わずか数人の担当者では難しいでしょう。 特に、 異なるタイム ゾーンで他の職務もこなしている場合はなおさらです。 しかし、 ITチームにはNetApp Cloud Insightsがあるので、 ネットワーク上のファイル共有を監視し、 ユーザの異常な操作を発見することができます。 チームが攻撃に気づかなくても、Cloud Insightsが察知して瞬時にNetApp Snapshot™コピーを作成し、 データを保護します。 Cloud Insightsを使用して攻撃元を特定した後、 チームは漏えいしたユーザ アカウントを自動的にブロックすることができます。



ネットアップにより、数テラバイトのデータを数分でリストアできます（出典：ネットアップ）。

ファイル ストレージにゆっくりと侵入してくるマルウェアについてはどうでしょうか？問題ありません。 ONTAPに搭載された自律型ランサムウェア対策機能により、 ワークロードのアクティビティとデータのエントロピーを監視し、アラートを送信します。 また、 このアラートによってSnapshotコピーが自動で作成され、 複数のリカバリ ポイントが確保されます。

ITチームは、 ネットアップのツールを使って、 数分で数テラバイトのデータをリストアできます。 復旧の瞬間は劇的なものですが、 NetApp SnapLock®ソフトウェアが論理的なエア ギャップを提供してデータの削除を防いでいるので、 データに関する本当の危険はなかったとチームの誰もが安心していられます。

データ主体のサイバー レジリエンス計画でどんなクラウドも取り残されない

ITチームがオンプレミスのデータを管理している場合でも、 前のシナリオは当てはまるでしょうか？クラウドは？ハイブリッド環境は？エッジはどうでしょうか？答えはイエス、もちろん当てはまります。 サイバー レジリエンスがデータ主体で設計されているため、オンプレミス、遠隔地、クラウドのどこにあっても、 データは常に完全なセキュアな状態で、 耐障害性に優れ、 利用可能です。 ネットアップのサイバー レジリエンス ソリューションは、 ハイブリッド クラウド環境に幅広く対応し、 あらゆる主要なパブリック クラウドと連繋しています。

既存の投資を最大限に活用

データ主体のネットアップ サイバー レジリエンス ソリューションは、 本書で概説した計画の5段階をすべて支援することができます。 ただし、 お客様の組織ではすでにサイバーセキュリティ ツールに投資しているかもしれません。 NetApp ONTAPソフトウェアの機能は、 投資済みのサイバーセキュリティ基盤と統合できるため、 完全にゼロから始めるのではなく、 ギャップを解消するだけで済みます。

データ保護

ONTAP Snapshotとの統合と、
SnapMirrorによる効率的なレプリケーション

NetApp

COMMVAULT　rubrik　veeam

CLEONDRIS　CATALOGIC SOFTWARE　druva

IBM　ProLion　VERITAS

ユーザ行動

FPolicy APIとの統合により、 ファイルや
ユーザの行動をインテリジェントに把握

NetApp
Cloud Insights

Brainwave GRC　CLEONDRIS　ProLion

STEALTHbits TECHNOLOGIES　VARONIS　VERITAS

監査 / ロギング

フォレンジック分析用syslogまたは
SIEMツールとの統合

NetApp
Cloud Insights　splunk>

Brainwave GRC　CLEONDRIS　ProLion

STEALTHbits TECHNOLOGIES　VARONIS　VERITAS

サイバー レジリエンス計画は わずか数回のクリックで完了

犯罪者を排除することはできませんが、 適切なツールで組織のサイバー レジリエンスを有効にすることは可能です。 データ主体のサイバー レジリエンス計画を実行に移すために、 ネットアップが提供できるサポートの詳細をご覧ください。

- ネットアップのデータ保護
- ネットアップのランサムウェア対策ソリューション
- Stay super secure with NetApp

詳細については、 www.netapp.com/ja/をご覧ください。

1.PBS NewsHour「Why ransomware attacks are on the rise—and what can be done to stop them」（2021年7月8日）
2.Business Wire「Ransomware Index Spotlight Report Reveals Steady Increase in Sophistication and Volume of New Ransomware Vulnerabilities and Families in Q3 2021」（2021年11月9日）
3.Statista「Methods of organizations compromised by ransomware to get their encrypted data back as of February 2021」
4.Sophos News「The State of Ransomware 2021」（2021年4月27日）
5.Deloitte「Double-extortion incidents」（2020年10月）
6. Infosec「NIST CSF: Implementing NIST CSF」（2020年2月19日）
7. Infosec「NIST CSF: Implementing NIST CSF」（2020年2月19日）同上
8. Infosec「NIST CSF: Implementing NIST CSF」（2020年2月19日）
9. Infosec「NIST CSF: Implementing NIST CSF」（2020年2月19日）
10. Infosec「NIST CSF: Implementing NIST CSF」（2020年2月19日）
11. Infosec「NIST CSF: Implementing NIST CSF」（2020年2月19日）

ネットアップについて
ジェネラリストが多い世界で、 ネットアップはスペシャリストとしての存在感を示しています。 お客様がデータを最大限に活用できるようにすることを 1 つの目標として、 支援に全力を注いでいます。 ネットアップは、 信頼できるエンタープライズクラスのデータ サービスをクラウドにもたらし、 またクラウドのシンプルな柔軟性をデータセンターにもたらします。 業界をリードするネットアップのソリューションは、 さまざまなお客様の環境や業界最大手のパブリック クラウドに対応します。

クラウド主導の Data-Centric なソフトウェア企業であるネットアップは、 お客様に最適なデータ ファブリックの構築をサポートし、 クラウド対応をシンプルに実現し、 必要なデータ、 サービス、 アプリケーションを適切なユーザにいつでも、 どこからでもセキュアに提供できる唯一のベンダーです。

NetApp

+81-3-6870-7400