



Ransomware Protection のドキュメント

Ransomware Protection

NetApp
April 01, 2022

目次

Ransomware Protection のドキュメント	1
ランサムウェア対策の新機能	2
2021 年 4 月 5 日	2
2022 年 3 月 15 日	2
2022 年 2 月 9 日	2
はじめに	3
ランサムウェア防御についてご確認ください	3
ランサムウェア対策を活用	5
データソースに対するサイバーセキュリティの推奨事項を管理します	5
知識とサポート	14
サポートに登録します	14
ヘルプを表示します	14
法的通知	15

Ransomware Protection のドキュメント

ランサムウェア対策の新機能

ランサムウェア対策ソリューションの最新情報をご確認ください。

2021 年 4 月 5 日

ONTAP 環境のセキュリティ強化を追跡する新しいパネル。

新しいパネル「ONTAP 環境の強化」には、ONTAP システムの特定の設定のステータスが表示され、に従って導入する際のセキュリティを追跡できます。"『[NetApp Security Hardening Guide for ONTAP Systems](#)』を参照してください" およびを参照してください "[ONTAP ランサムウェア対策機能](#)" これにより、異常なアクティビティをプロアクティブに検出して警告します。

推奨事項を確認し、潜在的な問題への対処方法を決定できます。次の手順に従って、クラスタの設定を変更したり、変更を別の時間に延期したり、推奨された設定を無視したりできます。"[詳細については、こちらをご覧ください](#)"。

Cloud Backup を使用してさまざまなカテゴリのデータを保護する方法については、新しいパネルを参照してください。

この新しい「バックアップステータス」パネルでは、ランサムウェア攻撃によってリカバリが必要になった場合に、最も重要なカテゴリのデータを包括的にバックアップする方法を紹介します。このデータは、Cloud Backup によってバックアップされる、環境内の特定のカテゴリの項目数を視覚的に表したものです。

2022 年 3 月 15 日

ビジネスクリティカルなデータの権限ステータスを追跡する新しいパネル

新しいパネル「ビジネスクリティカルなデータアクセス権分析」には、ビジネスに不可欠なデータのアクセス権ステータスが表示されます。これにより、ビジネスクリティカルなデータの保護状況を迅速に評価できます。"[詳細については、こちらをご覧ください](#)"。

[アクセス許可] 領域に OneDrive アカウントと SharePoint アカウントが含まれるようになりました

ランサムウェア対策保護ダッシュボードの [開くアクセス許可] 領域に、OneDrive アカウントと SharePoint アカウントでスキャンされるファイルに存在するアクセス許可が表示されるようになりました。

2022 年 2 月 9 日

新たなランサムウェア対策サービス

新しいランサムウェア防御サービスでは、サイバーセキュリティに関する関連情報を表示し、データがサイバー攻撃に対する復元力を評価することができます。また、データのセキュリティを強化するためのアラートと修正措置のリストも記載されています。

"この新しいサービスの詳細については、[こちらをご覧ください](#)"。

はじめに

ランサムウェア防御についてご確認ください

ランサムウェア攻撃は、ビジネス時間、リソース、評判を低下させる可能性があります。ランサムウェア防御サービスを使用すると、サイバーセキュリティに関する関連情報を表示し、データがサイバー攻撃に対する復元力を評価できます。また、データのセキュリティを強化するためのアラートと修正措置のリストも記載されています。

"ランサムウェア対策ソリューションのユースケースをご紹介します"。



ランサムウェア対策サービスは現在ベータ版です。

の機能

現在、ランサムウェア攻撃からの保護に役立ついくつかの機能が提供されています。今後追加される予定です。現在の機能では、次のような状況

- 作業環境内のボリュームは、定期的な Snapshot コピーを作成して保護されていません。
- を使用してクラウドへのバックアップを作成することで、作業環境内のボリュームを保護することができません ["クラウドバックアップ"](#)。
- 作業環境のデータやデータソースは、ではスキャンされません ["クラウドデータの意味"](#) コンプライアンスやプライバシーに関する懸念を特定し、最適化の機会を見つける。
- 作業環境またはデータソースで暗号化ファイルの割合が異常に増加しています。

これは、ランサムウェア攻撃がネットワークで開始されたことを示すインジケータになります。

- 機密データがファイルで検出され、作業環境やデータソースでアクセス権限レベルが高すぎます。
- ユーザーが Active Directory ドメイン管理者グループに追加されました。
- クラスタ上の ONTAP ソフトウェアのバージョンは古く、最高の保護機能とセキュリティ機能を提供するために更新する必要があります。
- ONTAP システムで NAS ファイルシステムの監査が有効になっていません。

CIFS 監査を有効にすると、システム管理者に対して、フォルダの権限の変更、ファイルの読み取りや書き込みの失敗、ファイルの作成、変更、削除などの情報を追跡する監査イベントが生成されます。

- 組み込みのランサムウェア対策機能が ONTAP システムで有効になっていない。

ONTAP ランサムウェア対策機能は、ランサムウェア攻撃を示す可能性のある異常なアクティビティをプロアクティブに検出して警告します。

["潜在的な問題をランサムウェア対策ダッシュボードで確認する方法をご確認ください。"](#)

Cloud Volumes ONTAP システムを使用している場合、作業環境から直接導入できるランサムウェアの保護機能がいくつか追加されています。 ["ランサムウェアに対する保護を強化する方法をご確認ください"](#)。

サポートされている作業環境とデータソース

"クラウドデータの意味" ランサムウェア対策サービスを使用するための前提条件です。データセンスをインストールして有効化すると、ランサムウェア防御を使用して、次のような作業環境やデータソースに対するサイバー攻撃に対するデータの復元力を確認できます。

- 作業環境： *
- Cloud Volumes ONTAP （AWS、Azure、GCP に導入）
- オンプレミスの ONTAP クラスタ
- Azure NetApp Files の特長
- ONTAP 対応の Amazon FSX
- Amazon S3
- データソース： *
- ネットアップ以外のファイル共有
- オブジェクトストレージ（S3 プロトコルを使用）
- データベース
- OneDrive アカウント
- SharePoint アカウント

ランサムウェア攻撃からの保護では、グローバルな Active Directory 構成も監視されます "これはクラウドデータセンサで設定されています"。

ランサムウェア防御の仕組み

ランサムウェア対策による防御の概要は次のようになります。

1. ランサムウェア防御は、データセンサ、Cloud Backup、およびその他の Cloud Manager リソースから情報を収集し、ランサムウェア対策保護ダッシュボードにデータを表示します。
2. Ransomware Protection ダッシュボードを使用して、システムの保護状況の概要を収集します。
3. 提供されているレポート作成ツールを使用して、サイバーストレージの保護を強化できます。

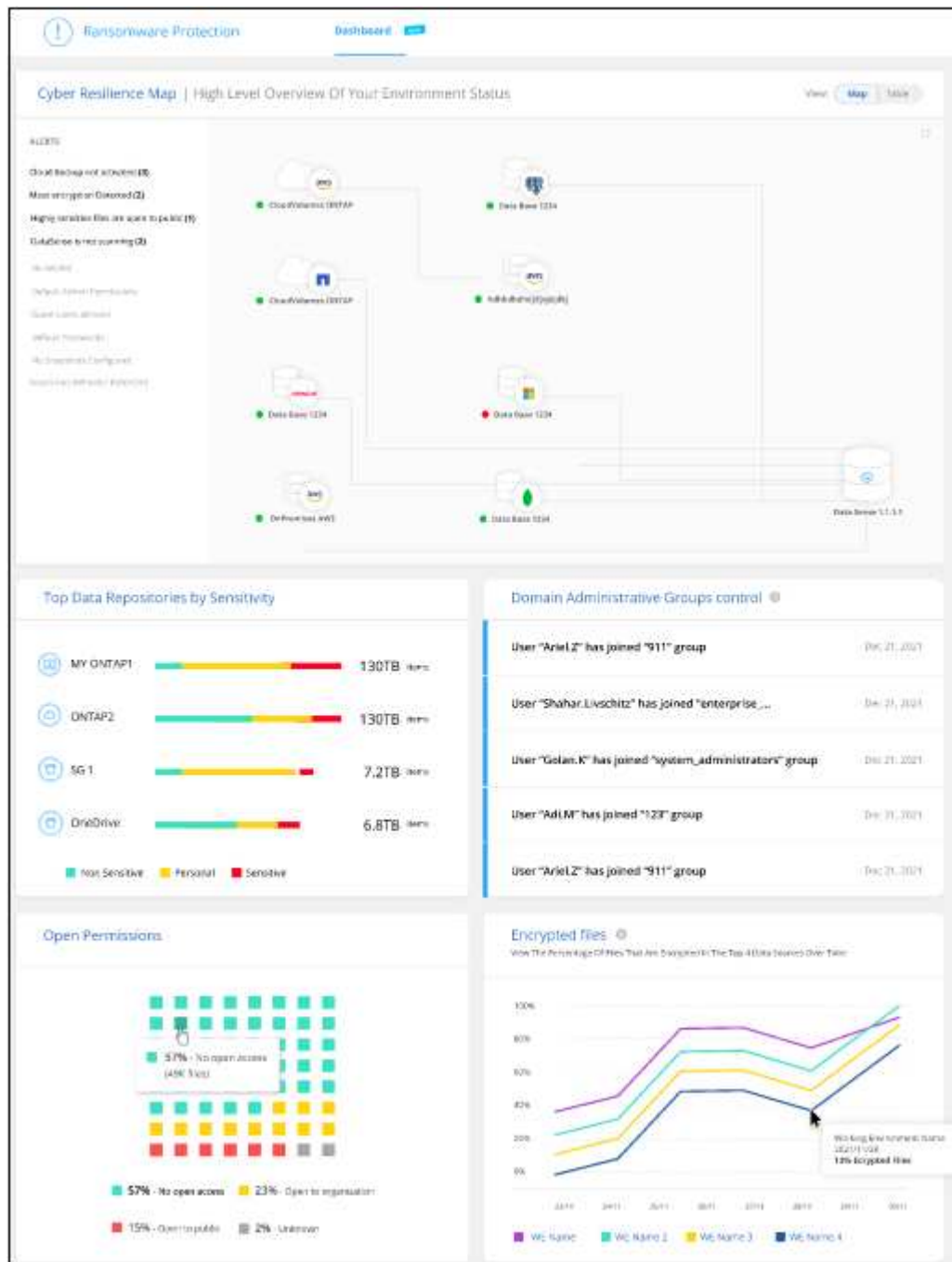
コスト

ベータ版では、ランサムウェア対策サービスに個別のコストはかかりません。

ランサムウェア対策を活用

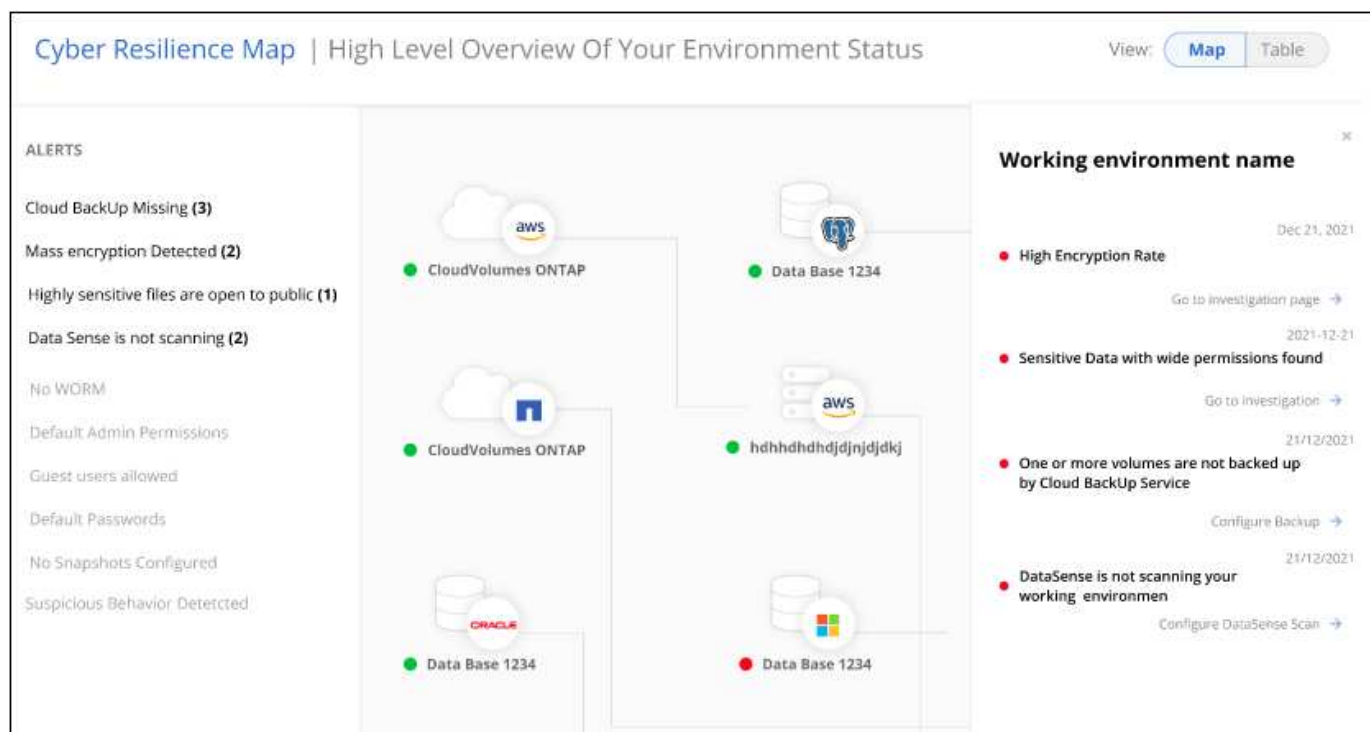
データソースに対するサイバーセキュリティの推奨事項を管理します

Ransomware Protection ダッシュボードでは、すべての作業環境とデータソースのサイバー復元力の概要を確認できます。各領域にドリルダウンすると、詳細および考えられる対処方法を確認できます。



サイバーレジリエンスマップ

レジリエンス・マップは、ダッシュボードのメイン領域です。これにより、すべての作業環境とデータソースを視覚的に表示し、関連するサイバー復元情報を表示できます。



マップは3つの部分で構成されています。

左パネル

すべてのデータソースについてサービスが監視しているアラートのリストが表示されます。また、環境内でアクティブになっている個々のアラートの数も示します。アラートの種類を1つ多く設定することは、そのアラートを先に解決しようとするよい理由になります。

センターパネル

すべてのデータソース、サービス、および Active Directory がグラフ形式で表示されます。正常な環境では、緑のインジケータが表示され、アラートがある環境では赤色のインジケータが表示されます。

右パネル

赤のインジケータが表示されているデータソースをクリックすると、そのデータソースのアラートが表示され、アラートを解決するための推奨事項が提示されます。アラートはソートされて、最新のアラートが最初に表示されます。さまざまな推奨事項があるため、別の Cloud Manager サービスを利用して問題を解決できます。

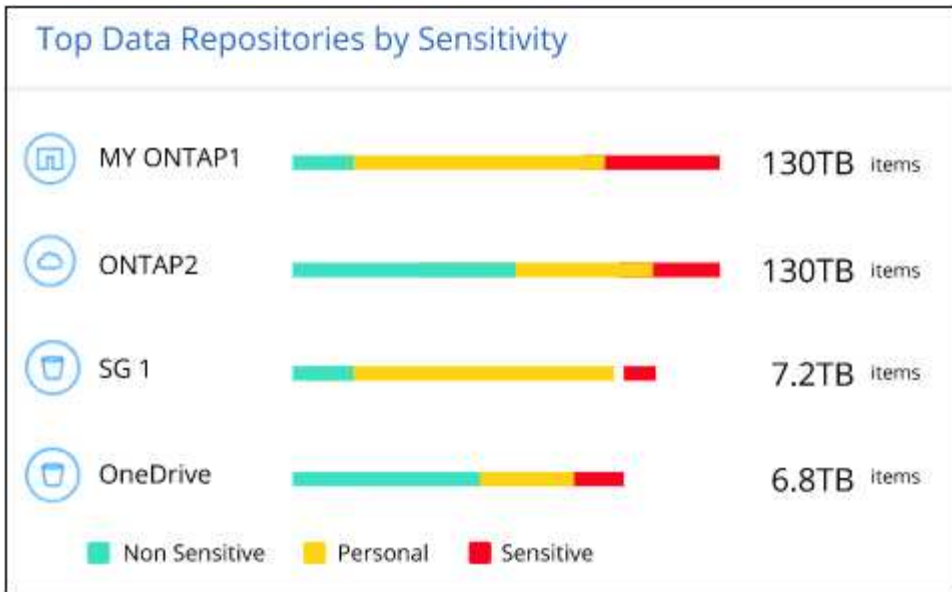
これらは、現在追跡されているアラートおよび推奨される対処方法です。

アラート	説明	修正
高いデータ暗号化レートが検出されました	データソースで暗号化ファイルまたは破損ファイルの割合が異常に増加しています。つまり、過去 7 日間の暗号化ファイルの割合が 20% を超えました。たとえば、ファイルの 50% が暗号化されている場合は、この値が 1 日後に 60% に増えてしまうと、このアラートが表示されます。	リンクをクリックしてを起動します "Data Sense Investigation ページ" 。ここでは、特定の _ 作業環境 _ および _ カテゴリ（暗号化および破損） _ のフィルタを選択して、すべての暗号化および破損したファイルのリストを表示できます。
広範囲の権限を持つ機密データが見つかりました	機密データがファイルに見つかりました。データソースのアクセス権限レベルが高すぎます。	リンクをクリックしてを起動します "Data Sense Investigation ページ" 。ここでは、特定の _ 作業環境 _、_ 感度レベル（機密性の高い個人） _、_ 許可 _ のフィルタを選択して、この問題を持つファイルのリストを表示できます。
Cloud Backup を使用してバックアップされていないボリュームがあります	を使用して、作業環境内の一部のボリュームが保護されていません "クラウドバックアップ" 。	リンクをクリックして Cloud Backup を起動し、作業環境にバックアップされていないボリュームを特定してから、それらのボリュームでバックアップを有効にするかどうかを決定します。
データソース内の 1 つ以上のリポジトリ（ボリューム、バケットなど）がデータセンスでスキャンされていません	データソースの一部のデータがを使用してスキャンされていません "クラウドデータの意味" コンプライアンスやプライバシーに関する懸念を特定し、最適化の機会を見つける。	リンクをクリックして Data Sense を起動し、スキャンされていない項目のスキャンとマッピングを有効にします。
ONTAP システムは強化されていません	ONTAP システムの一部の設定がからの推奨事項に従って設定されていません "『NetApp Security Hardening Guide for ONTAP Systems』を参照してください" 。	リンクをクリックすると、にリダイレクトされます ONTAP 環境パネルを強化します 下の図は、アラートの原因となっている問題、および問題の修正方法を調査するためのものです。

データの感度が高い上位のデータリポジトリ

Top Data Repositories by Sensitivity Level パネルには、最も機密性の高い項目を含む上位 4 つのデータリポジトリ（作業環境およびデータソース）が表示されます。各作業環境の棒グラフは、次のように分割されています。

- 機密性のないデータ
- 個人データ
- 機密性の高い個人データ



各セクションにカーソルを合わせると、各カテゴリの項目の総数を確認できます。

各領域をクリックすると、フィルタリングされた結果が [データセンシ調査] ページに表示され、さらに調査できます。

ドメイン管理者グループ制御

ドメイン管理者グループのコントロールパネルには、ドメイン管理者グループに追加された最新の 5 人のユーザーが表示されます。これにより、これらのグループですべてのユーザーを許可するかどうかを確認できます。が必要です ["グローバル Active Directory を統合"](#) クラウドデータセンシに移行して、このパネルをアクティブにします。

Domain Administrative Groups control ⓘ	
User "Ariel.Z" has joined "911" group	Dec 21, 2021
User "Shahar.Livschitz" has joined "enterprise_..."	Dec 21, 2021
User "Golan.K" has joined "system_administrators" group	Dec 21, 2021
User "Adi.M" has joined "123" group	Dec 21, 2021

デフォルトの管理者グループには、「Administrators」、「Domain Admins」、「Enterprise Admins」、「Enterprise Key Admins」、および「Key Admins」があります。

オープンアクセス権のタイプ別に一覧表示されるデータ

[アクセス権を開く] パネルには ' スキャンするすべてのファイルに存在するアクセス権の種類ごとの割合が

表示されますこのグラフは Data Sense で提供されており、次の種類の権限が表示されています。

- オープンアクセスがありません
- 組織に開く（Open to Organization）
- [パブリック]に移動します
- 不明なアクセスです

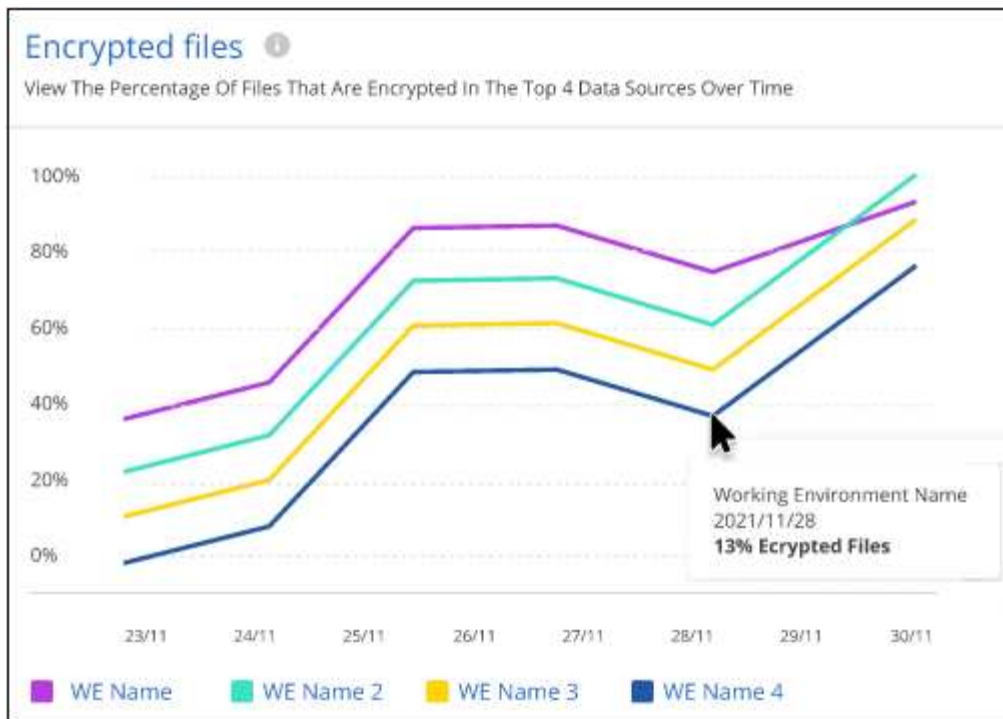


各セクションにカーソルを合わせると、各カテゴリのファイルの割合と合計数を確認できます。

各領域をクリックすると、フィルタリングされた結果が [データセンス調査] ページに表示され、さらに調査できます。

暗号化されたファイル別にリストされたデータ

_encrypted Files_panel には ' 暗号化されたファイルの割合が時間の経過に伴う上位 4 つのデータ・ソースが表示されます通常、これらはパスワードで保護されている項目です。過去 7 日間の暗号化率を比較して、20% を超える増加のデータソースを特定することで、この比較が行われます。この量が増えると、ランサムウェアがすでにシステムに攻撃されている可能性があります。















いずれかのデータソースの行をクリックすると、フィルタリングされた結果が [データ検出の調査] ページに表示され、さらに調査できます。

ONTAP システムのセキュリティ設定のステータス

hardening your ONTAP environment panel では、ONTAP システムの特定の設定のステータスが提供され、に応じた導入の安全性を追跡します "『[NetApp Security Hardening Guide for ONTAP Systems](#)』を参照してください" およびを参照してください "[ONTAP ランサムウェア対策機能](#)" これにより、異常なアクティビティをプロアクティブに検出して警告します。

推奨事項を確認し、潜在的な問題への対処方法を決定できます。次の手順に従って、クラスタの設定を変更したり、変更を別の時間に延期したり、推奨された設定を無視したりできます。このパネルは、現在オンプレミスの ONTAP および Cloud Volumes ONTAP システムをサポートしています。

Harden your ONTAP environments

Working Environment	ONTAP Anti Ransomware ⓘ	ONTAP Version ⓘ	Snapshots ⓘ
MY ONTAP1	 100%	 9.10.XX	 90%
ONTAP2	 50%	 9.10.XX	 50%
AccOI_ONTAP	 25%	 9.10.XX	 50%
CVO828	 -	 9.8.XX	 50%

追跡される設定は次のとおりです。

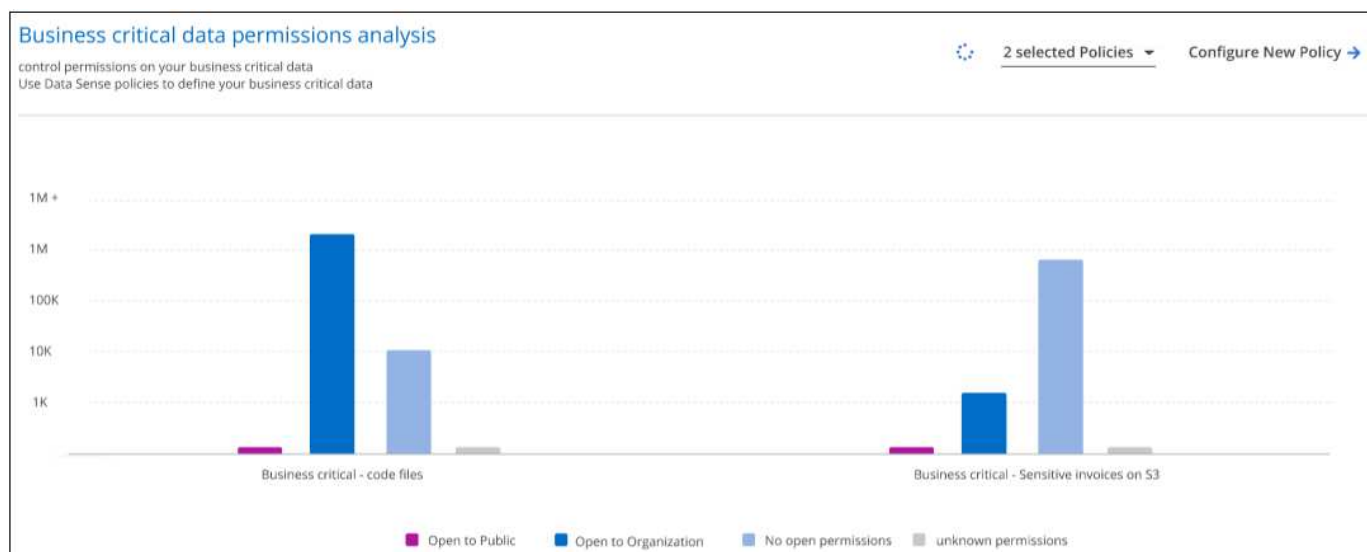
硬化目標 (Hardening Objective)	説明	修正
組み込みのアンチランサムウェア	組み込みのアンチランサムウェアがアクティブ化されているボリュームの割合。オンプレミスの ONTAP システムにのみ有効です。緑のステータスアイコンは、ボリュームの 85% 以上が有効であることを示しています。黄色は、40 ~ 85% が有効であることを示します。赤は 40% 未満が有効であることを示します。	"ボリュームでアンチランサムウェアを有効にする方法をご確認ください" System Manager を使用
ONTAP バージョン	クラスタにインストールされている ONTAP ソフトウェアのバージョン。緑のステータスアイコンは、バージョンが最新であることを示します。黄色のアイコンは、オンプレミスシステムの場合は 1 つまたは 2 つのパッチバージョン、または 1 つのマイナーバージョンがクラスタに対応していることを示し、それ以外の場合は 1 つのメジャーバージョンが背後にあることを示しています。赤のアイコンは、クラスタのパッチのバージョンが 3 つ、マイナーバージョンが 2 つ、オンプレミスシステムの場合は 1 つ、それ以外の場合は 2 つのメジャーバージョンの背後にあることを示します。	"オンプレミスクラスタをアップグレードする最善の方法をご確認ください" または "Cloud Volumes ONTAP システム"。

硬化目標 (Hardening Objective)	説明	修正
Snapshot	データボリュームでアクティブ化されている Snapshot 機能であり、ボリュームの何パーセントに Snapshot コピーがあるか。緑のステータスアイコンは、ボリュームの 85% 以上で Snapshot が有効であることを示しています。黄色は、40 ~ 85% が有効であることを示します。赤は 40% 未満が有効であることを示します。	"オンプレミスクラスターで Snapshot を有効にする方法をご覧ください" または "Cloud Volumes ONTAP システムで実行します"。

Cloud Backup ボタンをクリックしてボリュームのバックアップをアクティブ化するか、Data Sense ボタンをクリックしてクラスター上のボリュームをスキャンし、コンプライアンスとガバナンスの準拠状況を調査できます。

重要なビジネスデータに対する権限のステータス

ビジネスクリティカルなデータアクセス権分析パネルには、ビジネスに不可欠なデータのアクセス権ステータスが表示されます。これにより、ビジネスクリティカルなデータの保護状況を迅速に評価できます。



データは、作成したデータセンスポリシーを選択して最も重要なビジネスデータを表示した後のみ読み込まれるため、このパネルには最初はデータがありません。方法を参照してください ["データセンスを使用してポリシーを作成します"](#)。

このパネルに最大 2 つのポリシーを追加すると、ポリシーの条件を満たすすべてのデータの権限分析がグラフに表示されます。次の項目の数が表示されます。

- 公開アクセス権-データが公開されているとみなす項目
- 組織のアクセス許可を開く - データが組織に対してオープンであるとみなす項目
- オープンアクセス権なし-データがオープンアクセス権を持たないと判断する項目
- 不明な権限-データが不明な権限とみなす項目

グラフの各バーにカーソルを合わせると、各カテゴリの結果の数が表示されます。バーをクリックすると、[データセンスの調査] ページが表示されます。このページでは、どのアイテムにオープンなアクセス許可があるか、およびファイルのアクセス許可を調整する必要があるかどうかを詳細に調べることができます。

知識とサポート

サポートに登録します

...

ヘルプを表示します

...

法的通知

""

""

- "Cloud Manager 3.9 に関する注意事項"

Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.