個人情報の格納場所を把握したり、ランサムウェア検出とデータ復旧をしたい

課題・悩み

- クラウド上に個人情報(メールアドレスやクレジットカード番号、社会保障番号等)が格納されているかどうかを自動で検出したい。
- ハッキング等による漏洩があった際に、どこ(どのクラウドのどのNASサービス)にどのような個人情報が保管されていたか、漏洩した可能性のあるデータの対象者は誰か、などをすぐに特定・報告できるようにしたい。
- 仮にランサムウェアに感染しても、素早く検知して対処をしたい。
- 人質となったデータの復旧のため、データの論理バックアップ(=Snapshot)の世代数を90(1日3回、1か月)以上保持したい。

解決策： 格納されているデータを参照し、個人データの有無を判断するツールを導入する。
通常時と異なるアクセスパターンを検知する仕組みを導入し、かつ復旧のためのスナップショット世代数も増やす。

a. Cloud Compliance機能の有効化
   - クラウドストレージのみ監視可能 (2020年8月時点)
   - Cloud Volumes ONTAP (AWS/Azure版)を使っている場合、Cloud Managerより有効化する (無償。GCPは今後対応)
   - Azure NetApp FilesやAmazon S3にも対応。(ANFは無償、S3は有償。2020年8月時点)

b. ONTAPのFPolicy機能

c. Cloud Secure (Cloud Insightsの機能の一つ)
   - オンプレとクラウドのストレージを監視可能 (CVSは未対応)
   - Cloud Insightsのプレミアムエディションで利用可能

d. 多くの世代を保持できるONTAP Snapshot

キーワード

- Cloud Compliance (SaaSサービス)
- ONTAP - FPolicy機能 (無償)
- Cloud Insights / Cloud Secure (SaaSサービス)
- ONTAP - Snapshot機能 (無償)

関連動画・資料

- New Normal時代のデータ セキュリティ (「新たな日常」時代における データ セキュリティの考え方)
- NetApp Cloud Compliance (英語)
- Deploy NetApp Cloud Compliance (無音動画)
- Cloud Secure Demo (英語)
- NetApp Cloud Insights Deep Dive (英語)
- NetApp Overview of Cloud Insights (英語, 50分)

© 2020 NetApp, Inc. All rights reserved.

NetApp