



Alerts

Cloud Insights

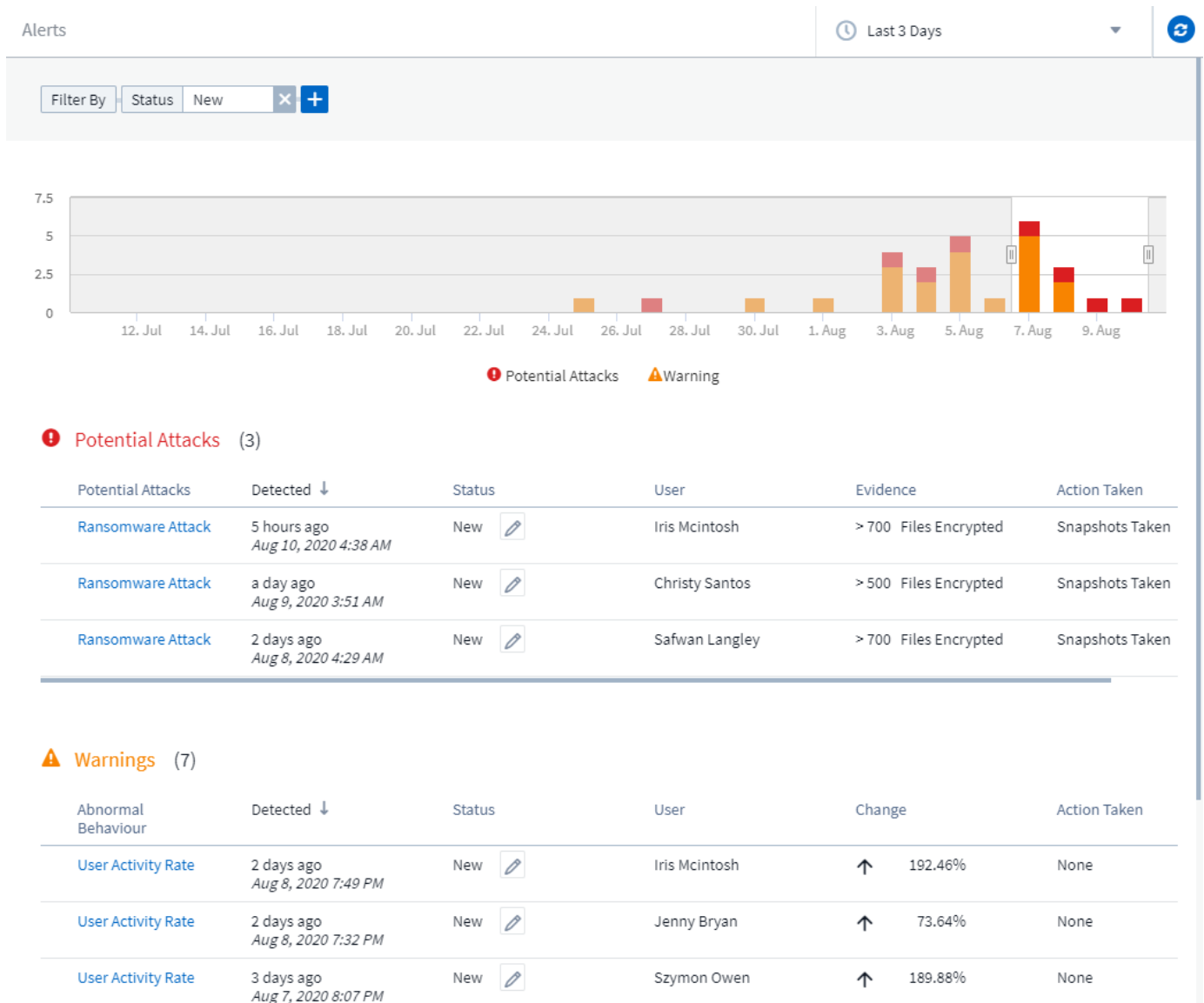
Tony Lavoie
December 02, 2020

Table of Contents

- Alerts 1
 - Alert 1
 - Filter Options 3
 - The Alert Details page 3
 - Take a Snapshot Action* 5
 - Alert Notifications 6
 - Retention Policy 6
 - Troubleshooting 7

Alerts

The Cloud Secure Alerts page shows a timeline of recent attacks and/or warnings and allows you to view details for each issue.



Alert

The Alert list displays a graph showing the total number of Potential Attacks and/or Warnings that have been raised in the selected time range, followed by a list of the attacks and/or warnings that occurred in that time range. You can change the time range by adjusting the start time and end time sliders in the graph.

The following is displayed for each alert:

Potential Attacks:

- The *Potential Attack* type (for example, Ransomware)
- The date and time the potential attack was *Detected*

- The *Status* of the alert:
 - New (this is the default for new alerts)
 - In Progress
 - Resolved
 - Dismissed

An administrator can change the status of the alert and add a note to assist with investigation.

The image shows a modal dialog box titled "Change Status To". At the top, there is a dropdown menu with "In Progress" selected. Below the dropdown is a text input field with the placeholder text "Enter notes or updates here". At the bottom of the dialog, there are two buttons: "Cancel" and "Save".

- The *User* whose behavior triggered the alert
- *Evidence* of the attack (for example, a large number of files was encrypted)
- The *Action Taken* (for example, a snapshot was taken)

Warnings:

- The *Abnormal Behavior* that triggered the warning
- The date and time the behavior was *Detected*
- The *Status* of the alert:
 - New (this is the default for new alerts)
 - In Progress
 - Resolved
 - Dismissed

An administrator can change the status of the alert and add a note to assist with investigation.

- The *User* whose behavior triggered the alert
- A description of the *Change* (for example, an abnormal increase in file access)
- The *Action Taken*

Filter Options

You can filter Alerts by the following:

- The *Status* of the alert
- Specific text in the *Note*
- The type of *Attacks/Warnings*
- The *User* whose actions triggered the alert/warning

The Alert Details page

You can click an alert link on the Alerts list page to open a detail page for the alert. Alert details may vary according to the type of attack or alert. For example, a Ransomware Attack detail page may show the following information:

Summary section:

- Attack type (in this example, Ransomware) and Alert ID (assigned by Cloud Secure)
- Date and Time the attack was detected
- Action Taken (for example, an automatic snapshot was taken. Time of snapshot is shown immediately below the summary section))
- Status (New, In Progress, etc.)

Attack Results section:

- Counts of Affected Volumes and Files
- An accompanying summary of the detection
- A graph showing file activity during the attack

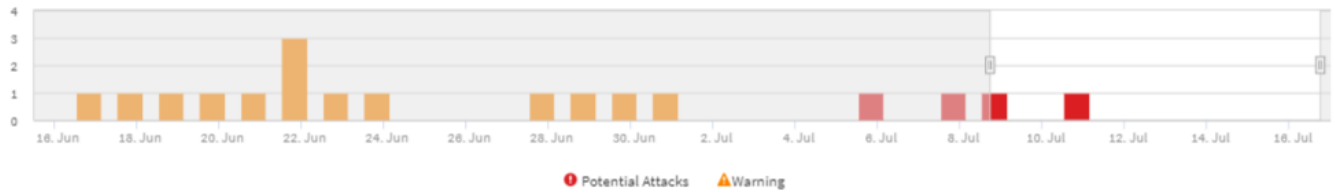
Related Users section:

This section shows details about the user involved in the potential attack, including a graph of Top Activity for the user.

Alerts page showing potential ransomware attack:



Filter By +



Potential Attacks (1)

Potential Attacks	Detected ↓	Status	User	Evidence	Action Taken
Ransomware Attack	5 days ago Jul 11, 2020 4:02 AM	New	Kristjan Egilsson	> 700 Files Encrypted	None

Warnings (0)

Abnormal Behaviour	Detected ↓	Status	User	Change	Action Taken
No Data Available					

Detail page for potential ransomware attack:



POTENTIAL ATTACK: AL_305
Ransomware Attack

Detected
5 days ago
Jul 11, 2020 4:02 AM

Action Taken
None

Status
New

Total Attack Results

1 Affected Volumes | 0 Deleted Files | 4173 Encrypted Files

4173 Files have been copied, deleted, and potentially encrypted by 1 user account.

This is potentially a sign of ransomware attack.
The extension "crypt" was added to each file.

Encrypted Files

Activity per minute



Related Users



Kristjan Egilsson
Accountant
Finance

4173
Encrypted Files

Detected
5 days ago
Jul 11, 2020 4:02 AM

Action Taken
None



Username
us035

Email
Egilsson@netapp.com

Phone
387224312607

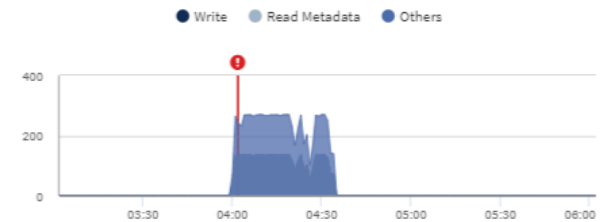
Department
Finance

Manager
Lyndsey Maddox

Top Activity Types

Activity per minute
Last access location: 10.197.144.115

[View Activity Detail](#)



Take a Snapshot Action

Cloud Secure protects your data by automatically taking a snapshot when malicious activity is detected, ensuring that your data is safely backed up.

You can define [automated response policies](#) that take a snapshot when ransomware attack or other abnormal user activity is detected.

You can also take a snapshot manually from the alert page.

Automatic Snapshot taken:



POTENTIAL ATTACK: AL_307
Ransomware Attack

Detected
4 days ago
Jul 26, 2020 3:38 AM

Action Taken
Snapshots Taken

Status
In Progress

Last snapshots taken by
Amit Schwartz
Jul 30, 2020 2:54 PM

How To:
[Restore Entities](#)

[Re-Take Snapshots](#)

Total Attack Results

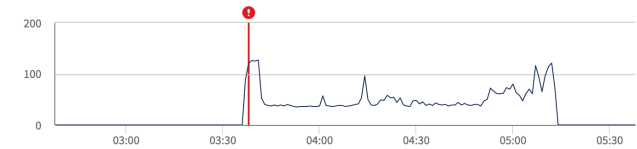
1 Affected Volumes | **0** Deleted Files | **5148** Encrypted Files

5148 Files have been copied, deleted, and potentially encrypted by 1 user account.

This is potentially a sign of ransomware attack. The extension "crypt" was added to each file.

Encrypted Files

Activity per minute



Related Users



Ewen Hall
Developer
Engineering

5148
Encrypted Files

Detected
4 days ago
Jul 26, 2020 3:38 AM

Action Taken
Snapshots Taken

Manual Snapshot:

MONITOR & OPTIMIZE

Alerts / **Nabilah Howell had an abnormal change in activity rate**

Jul 23, 2020 - Jul 26, 2020
1:44 AM - 1:44 AM

CLOUD SECURE

- ALERTS
- FORENSICS
- ADMIN
- HELP

Alert Detail



WARNING: AL_306
Nabilah Howell had an abnormal change in activity rate.

Detected
5 days ago
Jul 25, 2020 1:44 PM

Action Taken
None

Status
New

Recommendation: Setup an Automated Response Policy. An Automated Response Policy will trigger measures to contain the damage automatically when a future attack is detected. Try it now.

[Take Snapshots](#)

How To:
[Restore Entities](#)

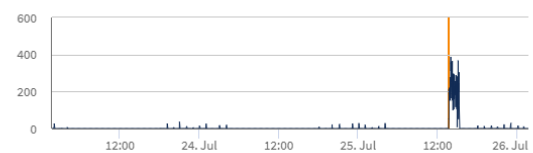
Nabilah Howell's Activity Rate Change

Typical	Alert	
122.8	210	↑ 71%
Activities Per Minute	Activities Per Minute	

Nabilah Howell's activity rate grew 71% over their typical average.

Activity Rate

Activity per 5 minutes



Alert Notifications

Email notifications of alerts are sent to an alert recipient list for every action on the alert. To configure alert recipients, click on **Admin > Notifications** and enter an email addresses for each recipient.

Retention Policy

Alerts and Warnings are retained for 13 months. Alerts and Warnings older than 13 months will be deleted. If the Cloud Secure environment is deleted, all data associated with the environment is also deleted.

Troubleshooting

Problem:	Try This:
For snapshots taken by Cloud Secure (CS), is there a purging/archiving period for CS snapshots?	No. There is no purging/archiving period set for CS snapshots. The user needs to define purging policy for CS snapshots. Please refer to the ONTAP documentation on how to setup the policies.
There is a situation where, ONTAP takes hourly snapshots per day. Will Cloud Secure (CS) snapshots affect it? Will CS snapshot take the hourly snapshot place? Will the default hourly snapshot get stopped?	Cloud Secure snapshots will not affect the hourly snapshots. CS snapshots will not take the hourly snapshot space and that should continue as before. The default hourly snapshot will not get stopped.
What will happen if the maximum snapshot count is reached in ONTAP?	<p>If the maximum Snapshot count is reached, subsequent Snapshot taking will fail and Cloud Secure will show an error message noting that Snapshot is full.</p> <p>User needs to define Snapshot policies to delete the oldest snapshots, otherwise snapshots will not be taken.</p> <p>In ONTAP 9.3 and earlier, a volume can contain up to 255 Snapshot copies. In ONTAP 9.4 and later, a volume can contain up to 1023 Snapshot copies.</p> <p>See the ONTAP Documentation for information on setting Snapshot deletion policy.</p>
Cloud Secure is unable to take snapshots at all.	<p>Make sure that the role being used to create snapshots has xref: proper rights assigned.</p> <p>Make sure <i>csrole</i> is created with proper access rights for taking snapshots:</p> <pre>security login role create -vserver <vservname> -role csrole -cmddirname "volume snapshot" -access all</pre>
Snapshots are failing for older alerts on SVMs which were removed from Cloud Secure and subsequently added back again. For new alerts which occur after SVM is added again, snapshots are taken.	This is a rare scenario. In the event you experience this, log in to ONTAP and take the snapshots manually for the older alerts.
In the <i>Alert Details</i> page, the message “Last attempt failed” error is seen below the <i>Take Snapshot</i> button. Hovering over the error displays “Invoke API command has timed out for the data collector with id”.	<p>This can happen when a data collector is added to Cloud Secure via SVM Management IP, if the LIF of the SVM is in <i>disabled</i> state in ONTAP.</p> <p>Enable the particular LIF in ONTAP and trigger <i>Take Snapshot manually</i> from Cloud Secure. The Snapshot action will then succeed.</p>

Copyright Information

Copyright © 2021 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.