

Independent Tests of Anti-Virus Software



Single Product Test Superna Data Security Edition Commissioned by Superna

TEST PERIOD: JULY - AUGUST 2024

LAST REVISION: 20TH AUGUST 2024

WWW.AV-COMPARATIVES.ORG

Introduction

Superna Data Security Edition works by monitoring user data on storage clusters in real-time and checking for file operations typically conducted by ransomware programs, i.e. encryption of the files. As soon as such activity is detected, access from the infected user's account to the storage cluster is blocked. The product can manage multiple clusters, each with multiple shares, and when ransomware activity is detected on one share on one cluster, the user's access to all managed shares and clusters will be removed. If ransomware activity is detected, an alert is raised immediately and displayed in the web interface of Superna Data Security Edition. The product locks out only the infected user, allowing other users to continue to access the storage. The locked-out user will not be able to use any PC or device since the security lockout is applied at the user level.

The goal of this test is to verify that the protection functions of Superna Data Security Edition work as intended and can be used to detect and respond to ransomware infections and protect the underlying file storage systems. Tests were performed using Qumulo Core as the storage backend.

This report has been commissioned by Superna. The tests were conducted in July/August 2024.

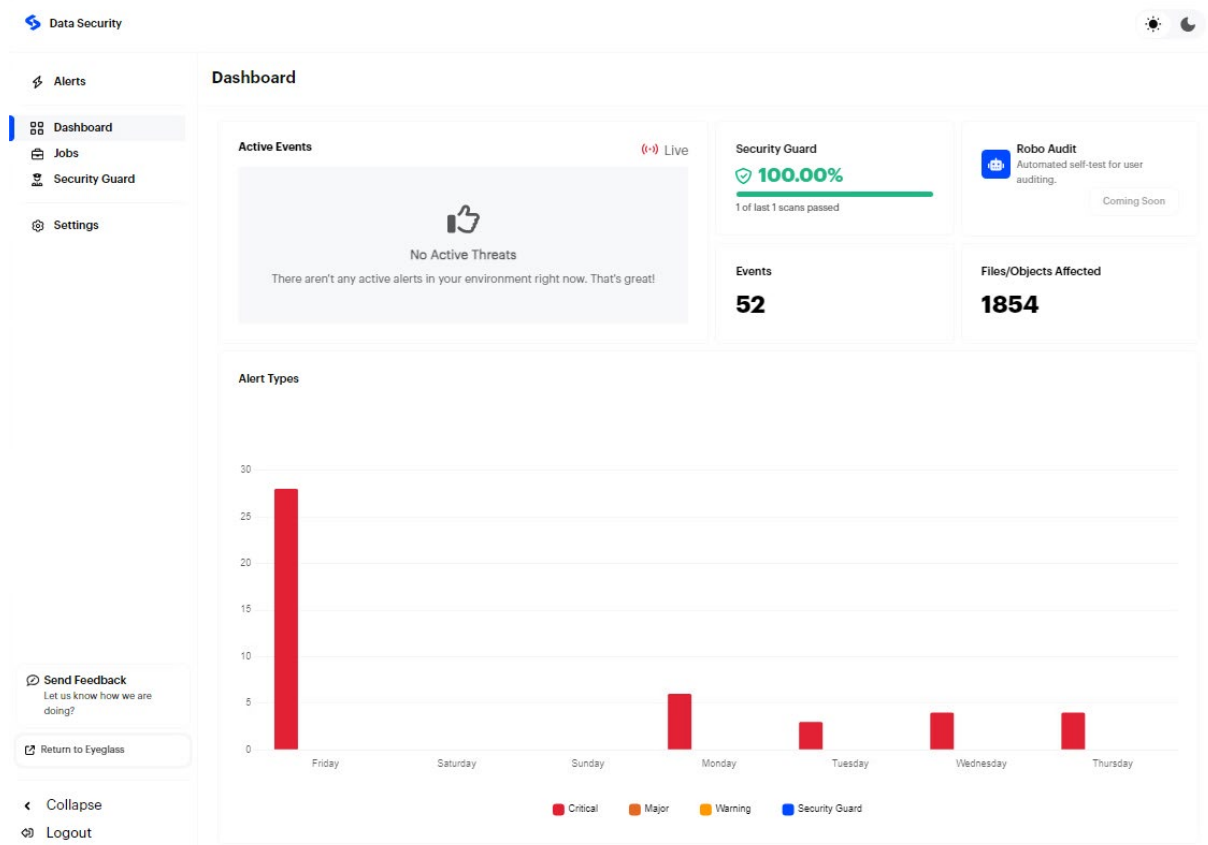


Figure 1: Superna Data Security Edition – Web Interface

Superna Data Security Edition prevents ransomware from encrypting user data on storage clusters. It does not replace endpoint protection software on client or server computers but is designed to be used in conjunction such software.

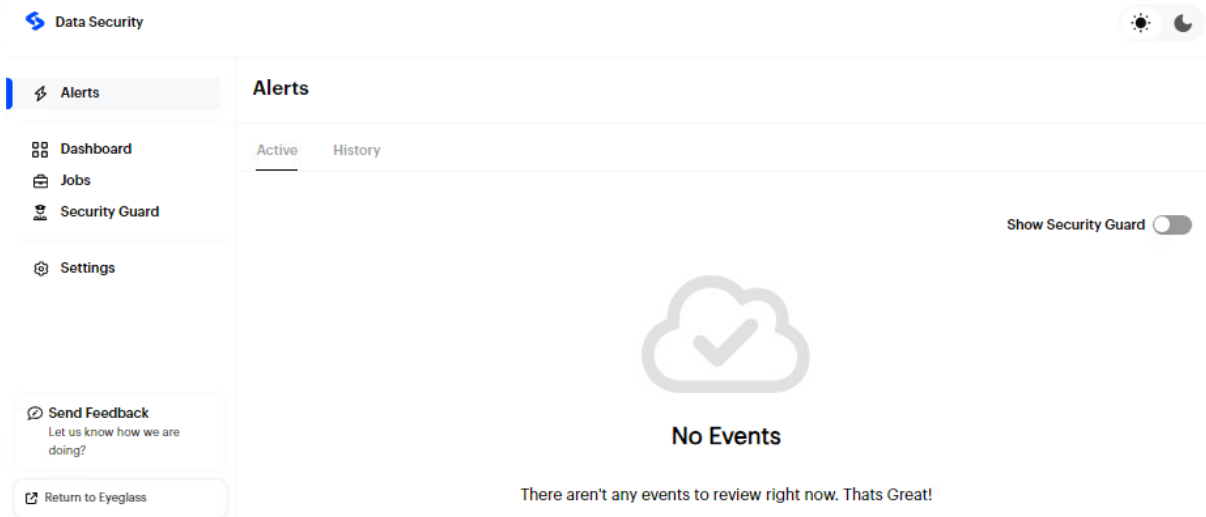


Figure 2: Superna Data Security Edition

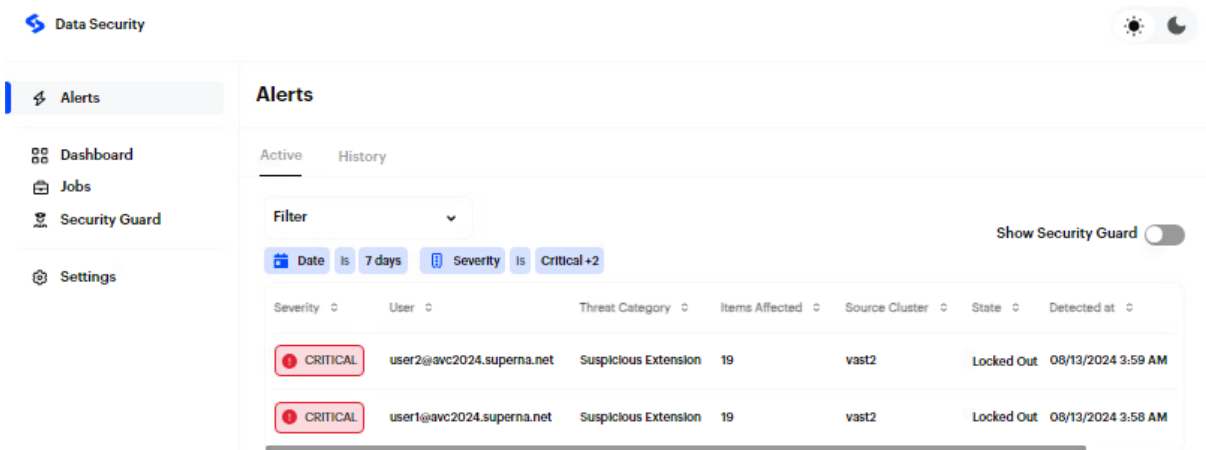


Figure 3: Superna Data Security Edition – Detection

Test Configuration

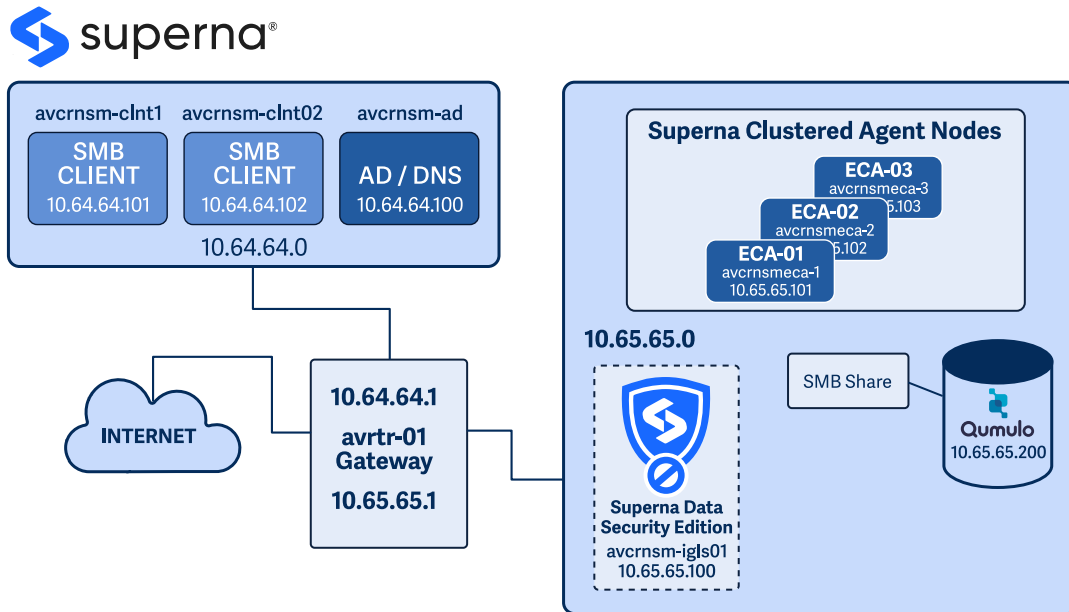


Figure 4: Infrastructure

Product Versions

- Superna Data Security Edition 2.9.0-24085
- Qumulo Core 6.2.2.1 build 276807.1.39

Settings

The settings of Superna Data Security Edition were configured by Superna:

- “Enforcement Mode” activated
- Warning Event Thresholds:
 - Expiry: 30min
 - Signal Strength Threshold: 30
 - Interval: 1h
 - Minimum User Behaviour Duration: 30min
- Major Event Thresholds:
 - Signal Strength Threshold: 5
 - Interval: 10min
 - Upgrade to Major: 2 events
 - Grace Period: 240min
- Critical Event Thresholds:
 - Signal Strength Threshold: 10
 - Interval: 30min
 - Upgrade to Critical: 2 events

Test scenario

Three ransomware samples were executed manually on two clients with connected shares. Before starting the test, a CLI health check was performed to verify that the cluster was operational.

Test Procedure

For each tested ransomware sample, the following test procedure was used:

1. Copy the ransomware sample onto both clients
2. Execute the sample on both clients
3. Monitor the web interface of Superna Data Security Edition for detection events
4. Record screenshots of the event and event details (affected files and shares, username, snapshot list)
5. Verify that the user was locked out of the affected share
6. Recover affected files using the Cyber Recovery Manager
7. Restore user access from the active event
8. Verify that the user can access the share again
9. Verify that all files were recovered correctly
10. Cleanup/prepare for the next test sample execution

Clients

Two Windows 10 64-bit (English) VMware virtual machines were used to access the managed file shares and execute the ransomware samples in this test. Before test execution, for each client, a VM snapshot was created to allow resetting the clients to a clean state after each test iteration. Tests were performed as different Active Directory users on both clients – “User1” and “User2”, respectively.

Shares

On the Qumulo cluster (cf. Figure 4: Infrastructure), a separate SMB share for each test user was configured. The shares were mounted on the respective Windows client/user as network drives before the sample was executed. On each share, 5000 unique text files with a file size of roughly 1kB were created using a PowerShell script. The SHA256 hash of each created file was recorded to be able to verify that all files are restored to their original state in the recovery stage. After creating the test files, two storage snapshots of the respective shares were created in the web console of Qumulo. To allow all internals of Superna Data Security Edition to adapt to the new storage state, tests were started at least one hour after snapshot creation.

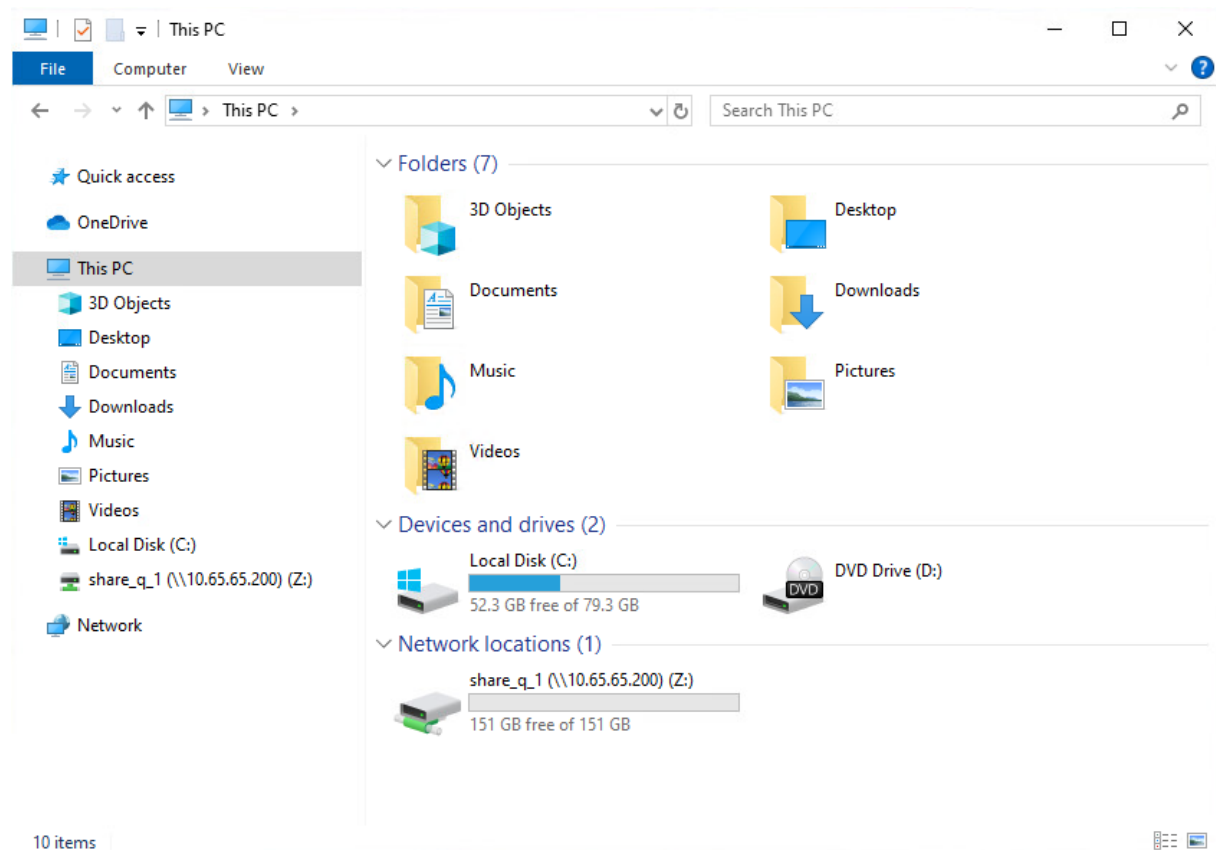


Figure 5: Share on the Windows 10 – User 1 client

Used Ransomware Samples

Two self-compiled ransomware samples, which encrypt files on network shares and can be configured in an attempt to bypass Superna Data Security Edition’s detection, were used for the test:

1. No special modifications – the sample will encrypt all files and add the “.owned” extension to encrypted files
2. Similar to the first version, but will encrypt files without changing their extension

Additionally, one ransomware sample of the CylanCrypt family was used as a representative of ransomware found in-the-wild, since this sample also affects connected network shares.

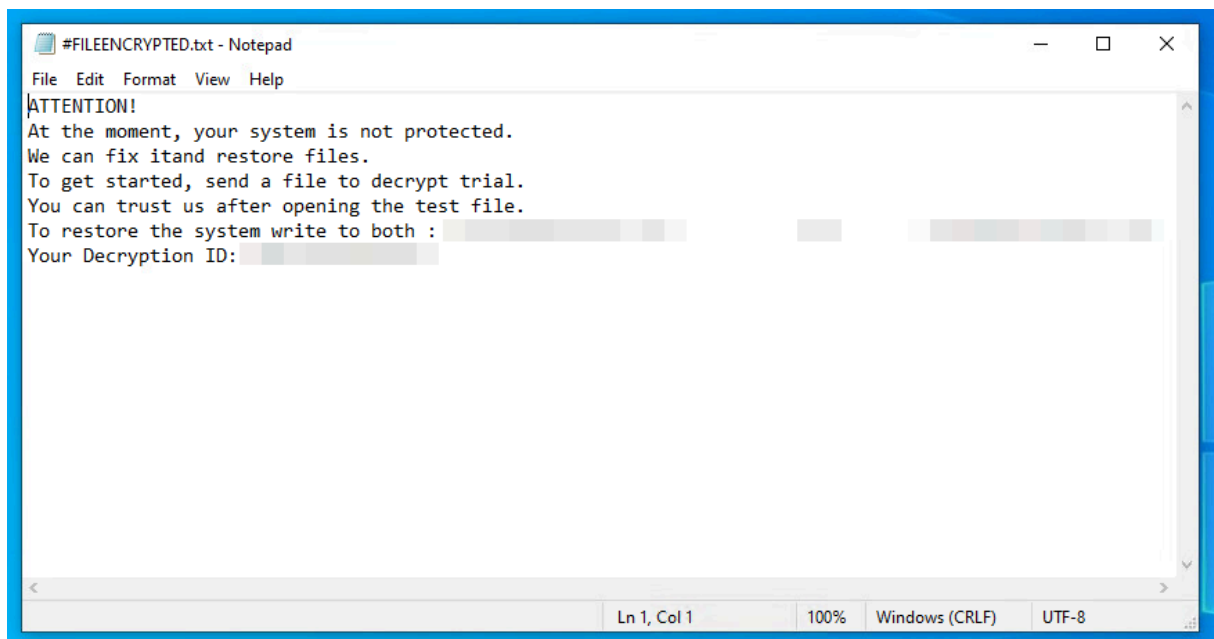


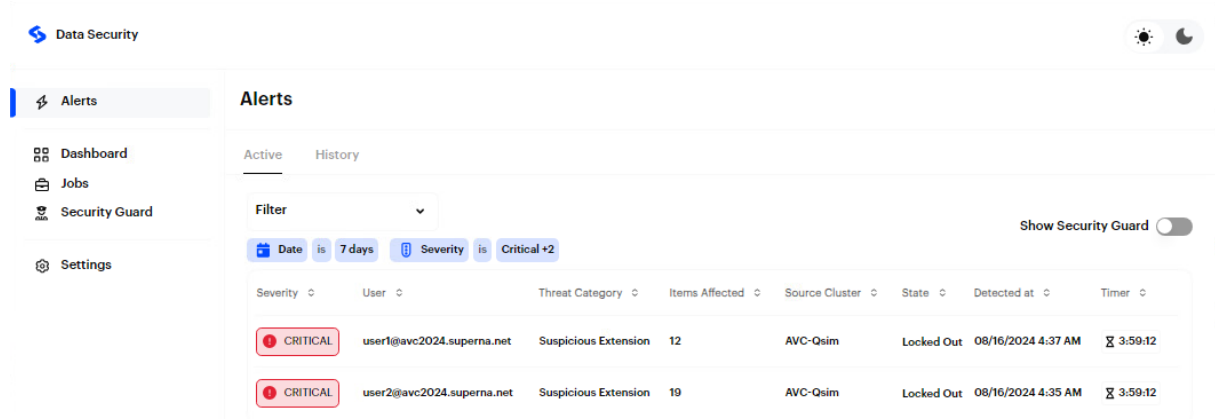
Figure 6: CylanCrypt Encryption Notice

Test Result

The samples encrypted several files on the client and the storage cluster. However, Superna Data Security Edition detected all events, removed write access of the originating user to the affected share and created new storage snapshots for further incident investigation. From the Recovery Manager, all files could be restored back to their state before the infection. In the following sections, screenshots and further details about the reaction of Superna Data Security Edition to the tested samples are provided.

Custom Ransomware, Variant 1:

Shortly after executing the first custom ransomware variant, Superna Data Security Edition raised alarms in the web interface:



The screenshot displays the 'Alerts' section of the Superna Data Security web interface. The interface includes a sidebar with navigation options: Alerts, Dashboard, Jobs, Security Guard, and Settings. The main content area shows a table of active alerts. The table has columns for Severity, User, Threat Category, Items Affected, Source Cluster, State, Detected at, and Timer. Two alerts are visible, both marked as 'CRITICAL'.

Severity	User	Threat Category	Items Affected	Source Cluster	State	Detected at	Timer
CRITICAL	user1@avc2024.superna.net	Suspicious Extension	12	AVC-Qsim	Locked Out	08/16/2024 4:37 AM	⌵ 3:59:12
CRITICAL	user2@avc2024.superna.net	Suspicious Extension	19	AVC-Qsim	Locked Out	08/16/2024 4:35 AM	⌵ 3:59:12

Figure 7: Detection events in the "Alerts" section

After a few files on the connected shares were encrypted, the users were no longer able to access the shares:

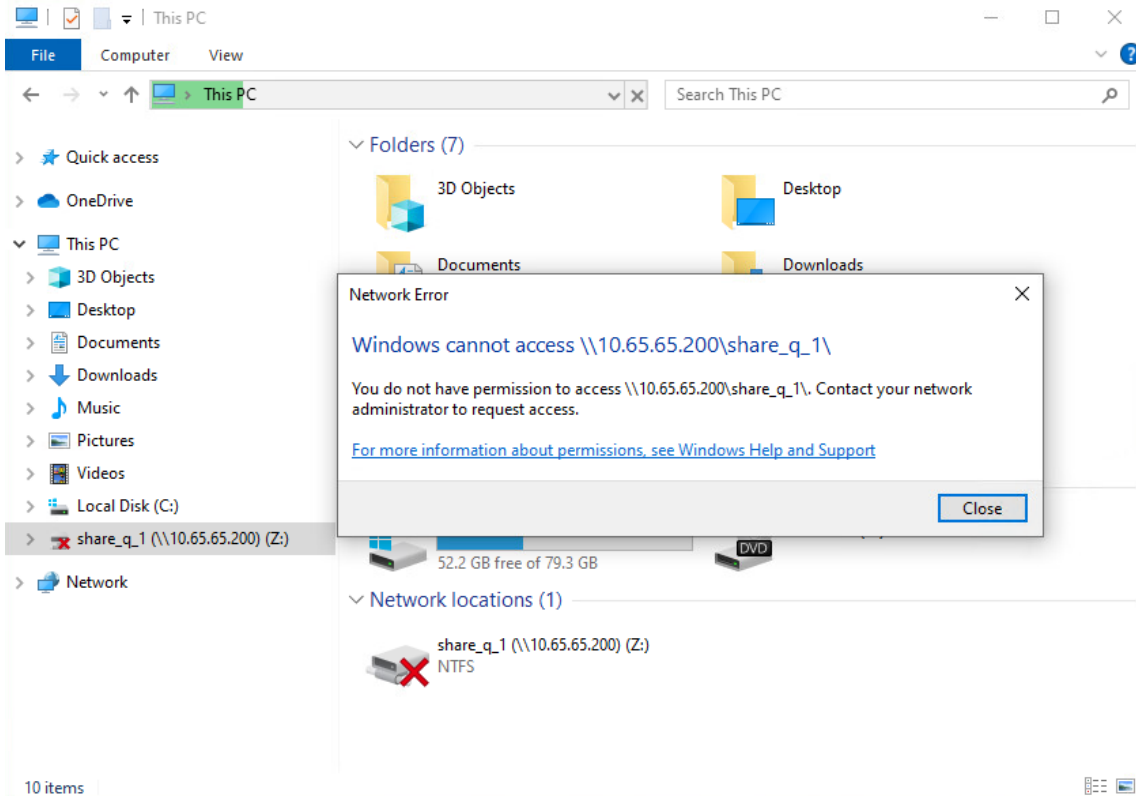


Figure 8: User 1 locked out

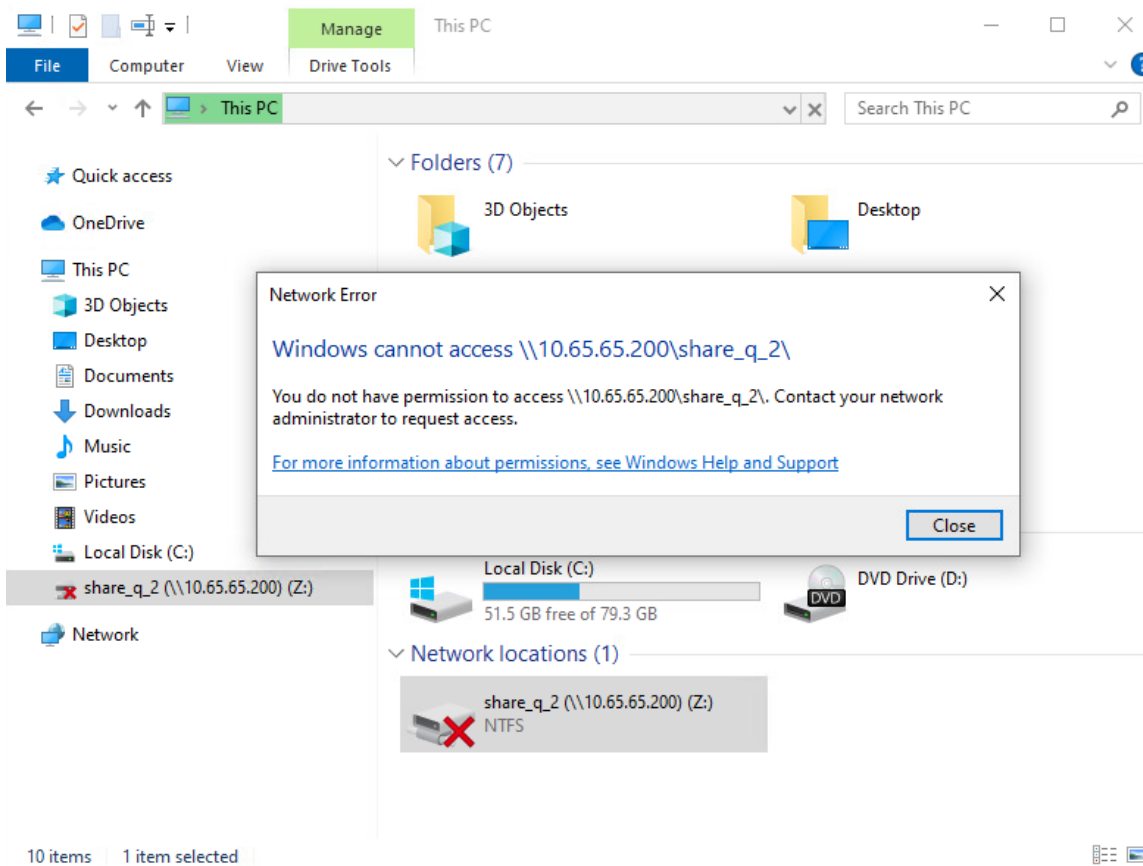


Figure 9: User 2 locked out

As the detection was raised, Superna Data Security Edition created a new storage snapshot to allow an administrator to investigate the incident:

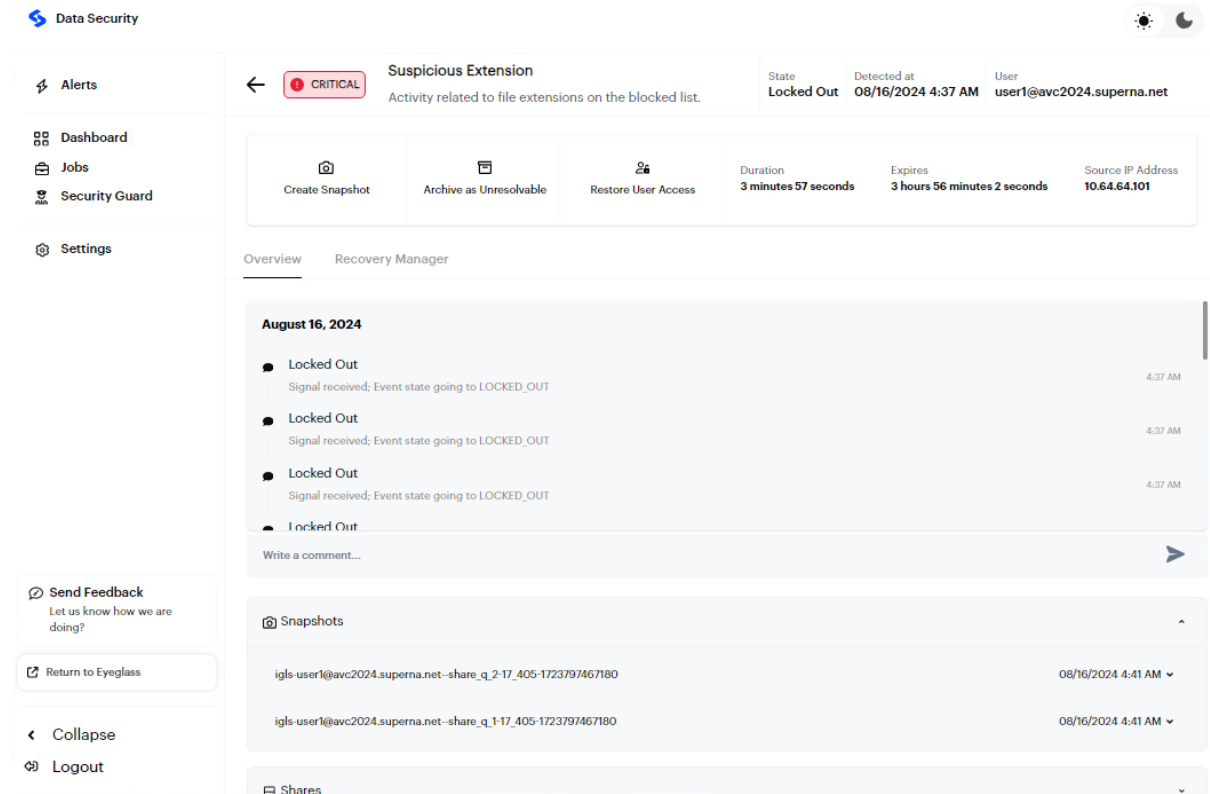


Figure 10: Automatic snapshots created by Superna Data Security Edition – User 1 Event

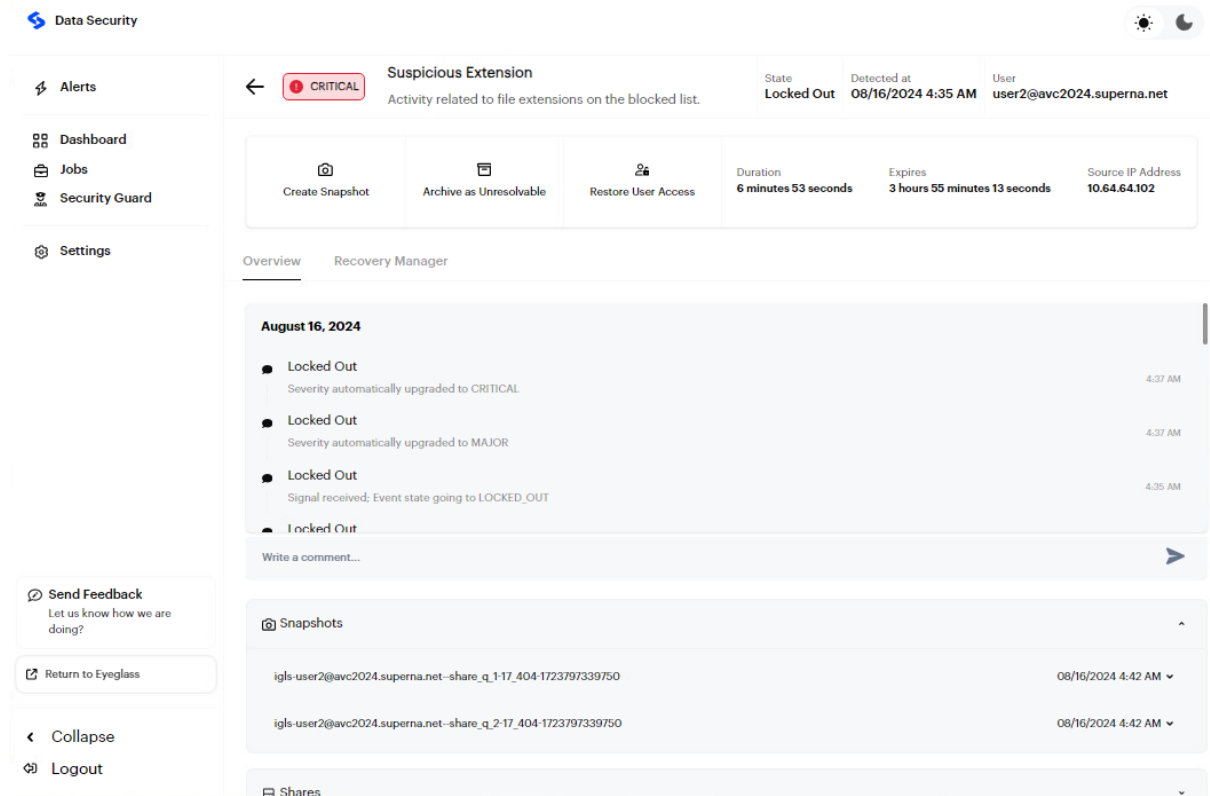


Figure 11: Automatic snapshots created by Superna Data Security Edition - User 2 Event

The „Shares“ view lists all affected shares on the cluster affected by the lock out:

Data Security

Alerts | **Dashboard** | **Jobs** | **Security Guard** | **Settings**

Suspicious Extension (CRITICAL)
Activity related to file extensions on the blocked list.

State: **Locked Out** | Detected at: **08/16/2024 4:37 AM** | User: **user1@avc2024.superna.net**

Create Snapshot	Archive as Unresolvable	Restore User Access	Duration 5 minutes 16 seconds	Expires 3 hours 54 minutes 43 seconds	Source IP Address 10.64.64.101
-----------------	-------------------------	---------------------	---	---	--

Overview | Recovery Manager

August 16, 2024

- Locked Out**
Signal received; Event state going to LOCKED_OUT | 4:37 AM
- Locked Out**
Signal received; Event state going to LOCKED_OUT | 4:37 AM
- Locked Out**
Signal received; Event state going to LOCKED_OUT | 4:37 AM

Snapshots

Shares

share_q_1	AVC-Qsim	/share1
share_q_2	AVC-Qsim	/share2

Figure 12: Affected shares – User 1 Event

Data Security

Alerts | **Dashboard** | **Jobs** | **Security Guard** | **Settings**

Suspicious Extension (CRITICAL)
Activity related to file extensions on the blocked list.

State: **Locked Out** | Detected at: **08/16/2024 4:35 AM** | User: **user2@avc2024.superna.net**

Create Snapshot	Archive as Unresolvable	Restore User Access	Duration 8 minutes 4 seconds	Expires 3 hours 54 minutes 1 second	Source IP Address 10.64.64.102
-----------------	-------------------------	---------------------	--	---	--

Overview | Recovery Manager

August 16, 2024

- Locked Out**
Severity automatically upgraded to CRITICAL | 4:37 AM
- Locked Out**
Severity automatically upgraded to MAJOR | 4:37 AM
- Locked Out**
Signal received; Event state going to LOCKED_OUT | 4:35 AM

Snapshots

Shares

share_q_1	AVC-Qsim	/share1
share_q_2	AVC-Qsim	/share2

Figure 13: Affected shares – User 2 Event

From the “Recovery Manager” Tab in the event details page, administrators can list files affected by the ransomware event and select files to be restored to an earlier state.

The screenshot shows the 'Recovery Manager' interface for a 'Suspicious Extension' event. The event is in a 'Locked Out' state, detected on 08/16/2024 at 4:37 AM by user1@avc2024.superna.net. The interface displays a table of affected files, all of which are selected for recovery. The table columns include Path, Cluster, Event Type, Event Time, File Name, and Recovery Source. The selected files are all located at /share1/user01/testd... and represent FILE_WRITE, FILE_RENAME events. A toolbar at the bottom indicates that 13 items are selected and provides options to recalculate snapshots, export as CSV, or recover the files.

Figure 14: Selecting files to restore

After file recovery was started, the Jobs view of the web interface provided more details about the status of the recovery job:

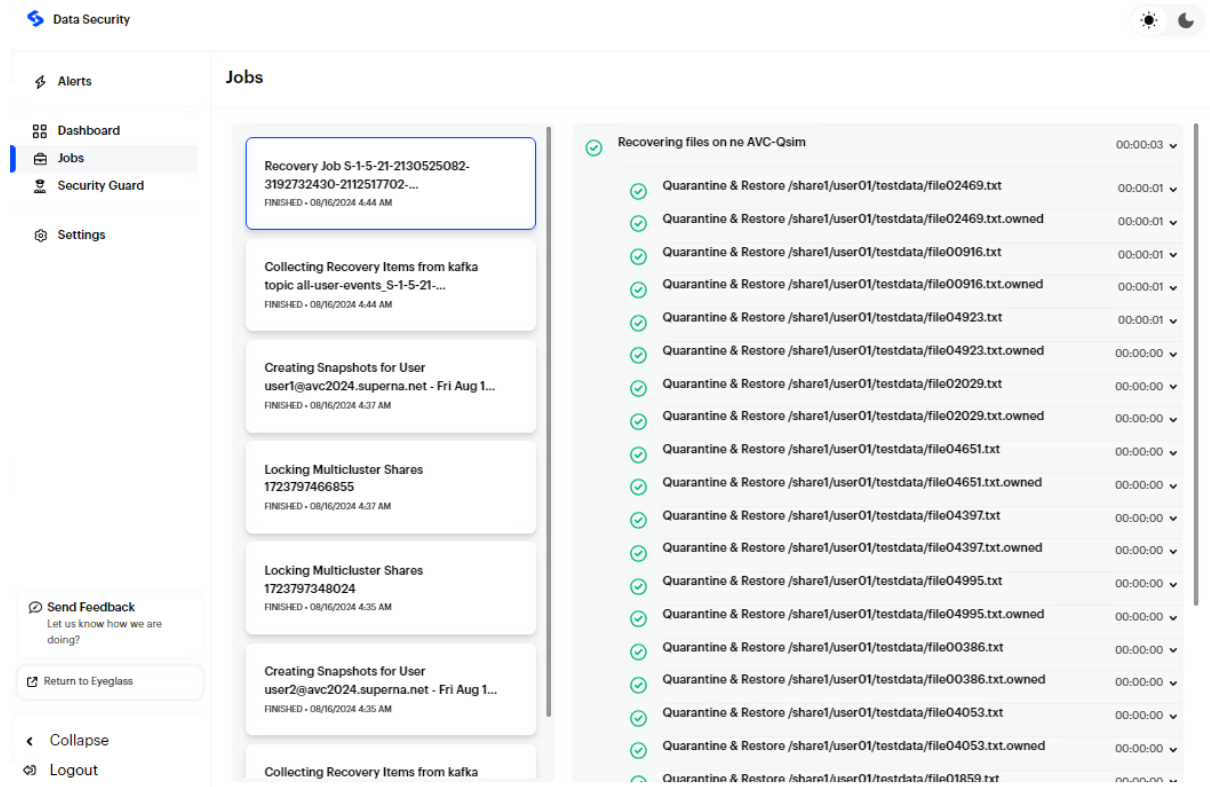


Figure 15: Recovery complete

At this point, both client VMs were reverted to a clean snapshot. After verifying that the recovery of all selected files was complete, User Access was restored using the respective button in the event overview page.

Once User access was restored for both shares, the clients were able to access their shares again:

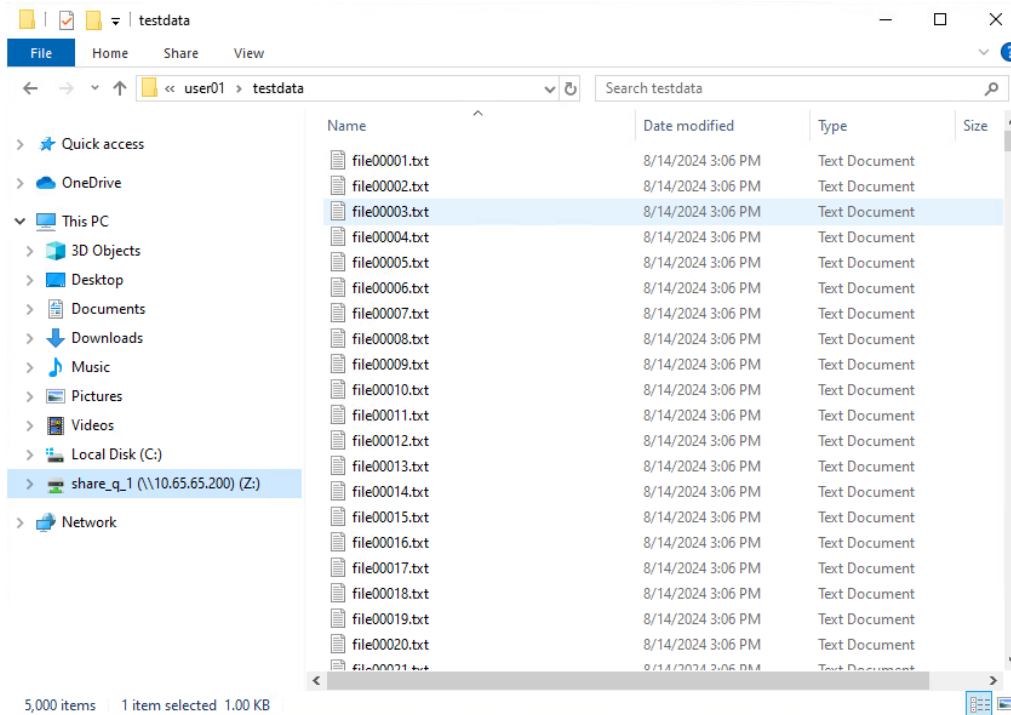


Figure 16: Share access restored for User 1

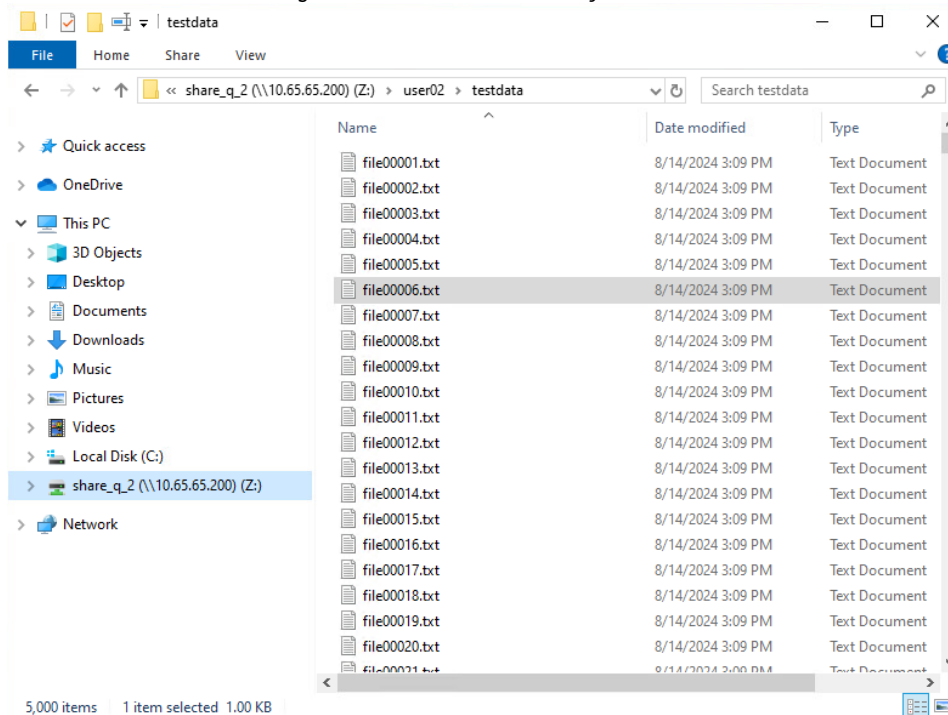


Figure 17: Share access restored for User 2

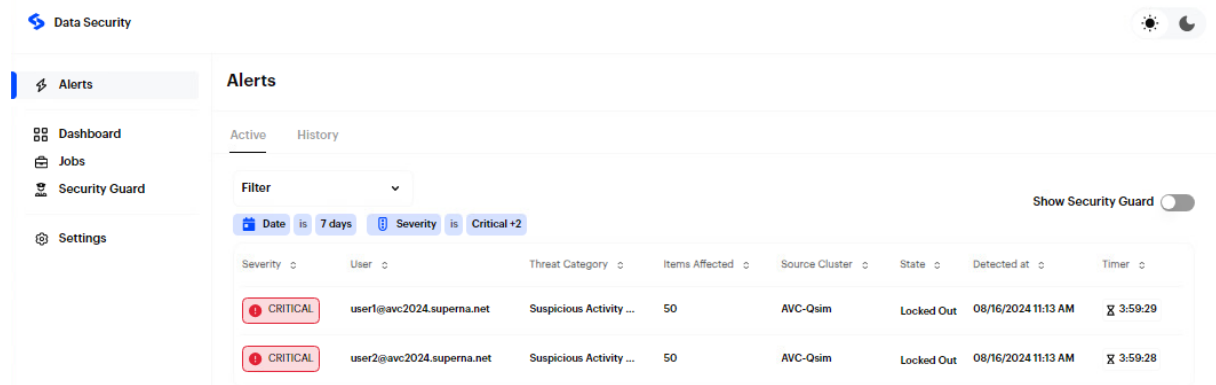
Comparing the SHA256 hashes of the recovered files confirmed that all files were successfully restored to their state before the ransomware infection.

To prepare for testing the next ransomware sample, the automatically generated storage snapshots were deleted using the Qumulo web console. Analog to the initial snapshot creation, Superna Data Security Edition was given more than one hour to adapt to the snapshot deletion.

Custom Ransomware, Variant 2:

The alert messages in Figure 7 indicate that the first custom ransomware variant was detected due to it renaming encrypted files to a suspicious file extension. The second variant was used to test whether Superna Data Security Edition can also detect ransomware, which only encrypts, but does not rename any files.

Indeed, similar to the first test execution, shortly after executing the ransomware, detection events were shown in the web interface, now under the “Suspicious Activity” category:



The screenshot displays the 'Alerts' section of the Superna Data Security web interface. The interface includes a sidebar with navigation options: Alerts, Dashboard, Jobs, Security Guard, and Settings. The main content area shows a table of alerts with the following columns: Severity, User, Threat Category, Items Affected, Source Cluster, State, Detected at, and Timer. Two alerts are visible, both marked as 'CRITICAL' and categorized as 'Suspicious Activity ...'. The alerts are for users 'user1@avc2024.superna.net' and 'user2@avc2024.superna.net', both affected by 50 items from the 'AVC-Qsim' source cluster, and both in a 'Locked Out' state. The detection time for both is '08/16/2024 11:13 AM'.

Severity	User	Threat Category	Items Affected	Source Cluster	State	Detected at	Timer
CRITICAL	user1@avc2024.superna.net	Suspicious Activity ...	50	AVC-Qsim	Locked Out	08/16/2024 11:13 AM	3:59:29
CRITICAL	user2@avc2024.superna.net	Suspicious Activity ...	50	AVC-Qsim	Locked Out	08/16/2024 11:13 AM	3:59:28

Figure 18: Custom Variant 2 detected

As during the first iteration, Superna Data Security Edition quickly locked out both users of their respective shares.

New storage snapshots were created for each event:

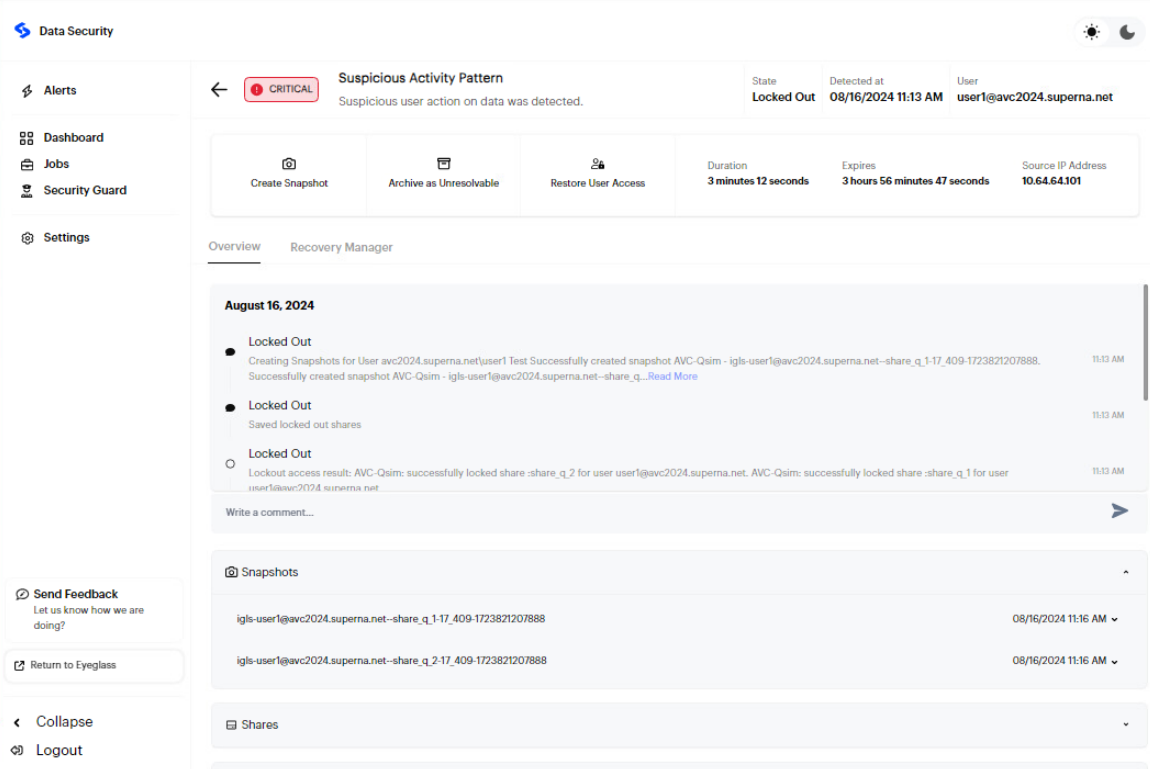


Figure 19: New storage snapshots created by Superna Data Security Edition – User 1

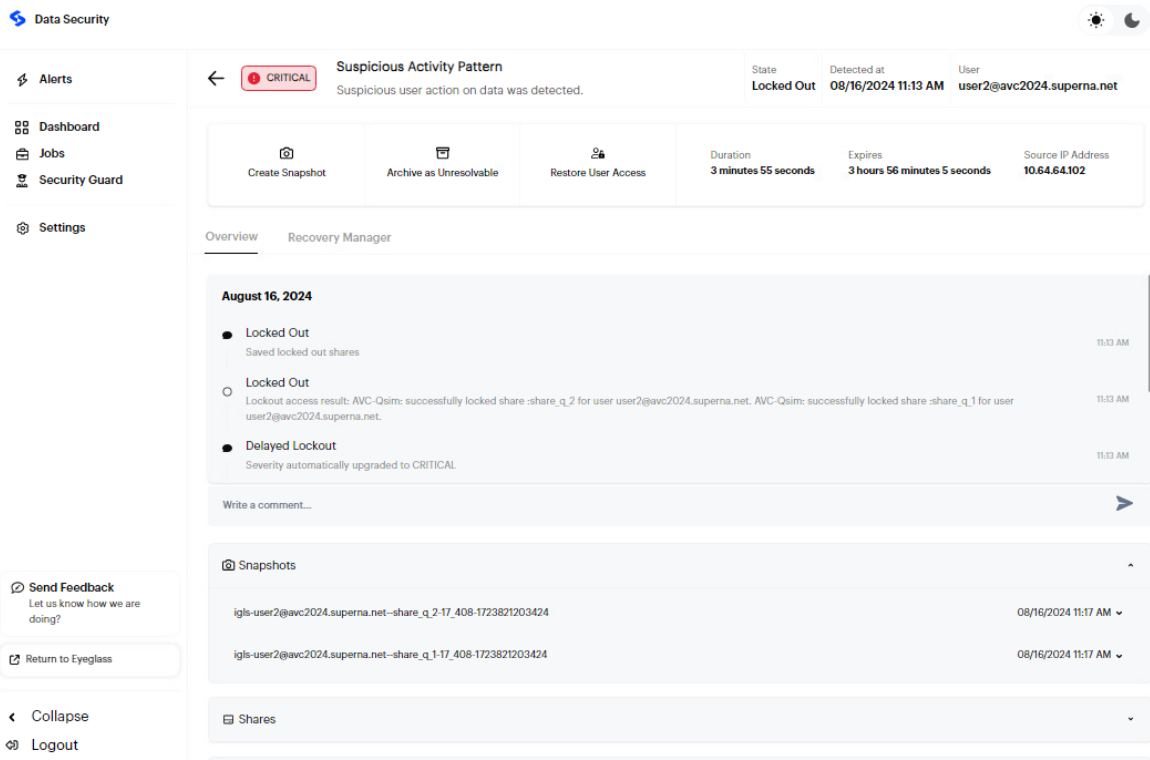


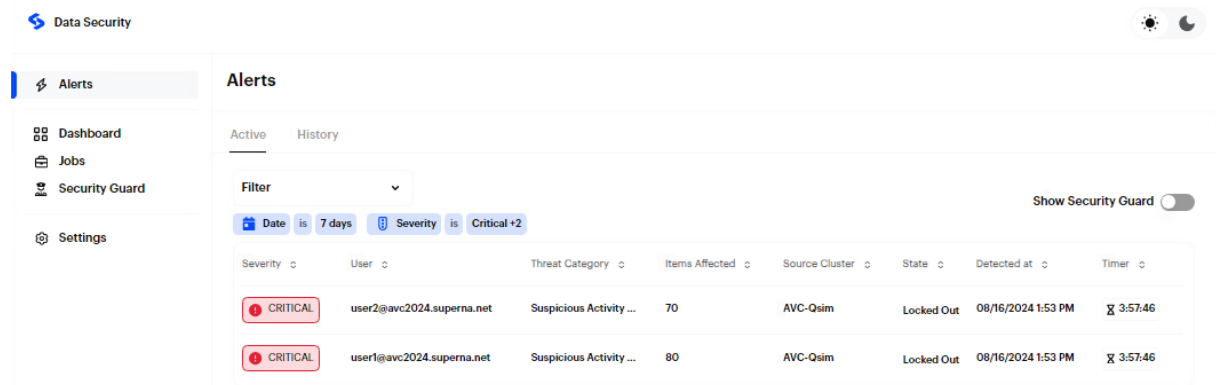
Figure 20: New storage snapshots created by Superna Data Security Edition - User 2

The same procedure as during the previous test iteration was used to recover affected files and restore User access. All files were restored correctly.

CylanCrypt

To test the reaction of Superna Data Security Edition on a ransomware sample found in-the-wild, a sample of the CylanCrypt family was chosen, since it also affects files on network shares.

Similar to the previous test iterations, shortly after executing the malware on the clients, ransomware events were shown in the alerts view of the web interface:



The screenshot displays the 'Data Security' web interface. The left sidebar contains navigation options: Alerts (selected), Dashboard, Jobs, Security Guard, and Settings. The main area is titled 'Alerts' and shows a table of active alerts. The table has columns for Severity, User, Threat Category, Items Affected, Source Cluster, State, Detected at, and Timer. Two alerts are visible, both marked as 'CRITICAL' and 'Locked Out'.

Severity	User	Threat Category	Items Affected	Source Cluster	State	Detected at	Timer
CRITICAL	user2@avc2024.superna.net	Suspicious Activity ...	70	AVC-Qsim	Locked Out	08/16/2024 1:53 PM	3:57:46
CRITICAL	user1@avc2024.superna.net	Suspicious Activity ...	80	AVC-Qsim	Locked Out	08/16/2024 1:53 PM	3:57:46

Figure 21: CylanCrypt detected

As during the previous iterations, both users were quickly locked out of the file shares.

New storage snapshots were created for each event:

Data Security

Alerts | **Suspicious Activity Pattern** | State: **Locked Out** | Detected at: **08/16/2024 1:53 PM** | User: **user1@avc2024.superna.net**

Suspicious user action on data was detected.

Actions: Create Snapshot | Archive as Unresolvable | Restore User Access

Duration: 6 minutes 45 seconds | **Expires:** 3 hours 53 minutes 20 seconds | **Source IP Address:** 10.64.64.101

Timeline (August 16, 2024):

- Locked Out** (1:53 PM): Saved locked out shares
- Locked Out** (1:53 PM): Lockout access result: AVC-Qsim: successfully locked share :share_q_2 for user user1@avc2024.superna.net. AVC-Qsim: successfully locked share :share_q_1 for user user1@avc2024.superna.net.
- To Lockout** (1:53 PM): Signal received; Event state going to TO_LOCKOUT

Snapshots:

- igls-user1@avc2024.superna.net--share_q_2-17_410-1723830804948 (08/16/2024 2:00 PM)
- igls-user1@avc2024.superna.net--share_q_1-17_410-1723830804948 (08/16/2024 2:00 PM)

Figure 22: New storage snapshots created - User 1

Data Security

Alerts | **Suspicious Activity Pattern** | State: **Locked Out** | Detected at: **08/16/2024 1:53 PM** | User: **user2@avc2024.superna.net**

Suspicious user action on data was detected.

Actions: Create Snapshot | Archive as Unresolvable | Restore User Access

Duration: 10 minutes | **Expires:** 3 hours 49 minutes 59 seconds | **Source IP Address:** 10.64.64.102

Timeline (August 16, 2024):

- Locked Out** (1:53 PM): Creating Snapshots for User avc2024.superna.net/user2 test Successfully created snapshot AVC-Qsim - igls-user2@avc2024.superna.net--share_q_1-17_411-1723830817539. Successfully created snapshot AVC-Qsim - igls-user2@avc2024.superna.net--share_q_...[Read More](#)
- Locked Out** (1:53 PM): Saved locked out shares
- Locked Out** (1:53 PM): Lockout access result: AVC-Qsim: successfully locked share :share_q_2 for user user2@avc2024.superna.net. AVC-Qsim: successfully locked share :share_q_1 for user user2@avc2024.superna.net

Snapshots:

- igls-user2@avc2024.superna.net--share_q_1-17_411-1723830817539 (08/16/2024 2:03 PM)
- igls-user2@avc2024.superna.net--share_q_2-17_411-1723830817539 (08/16/2024 2:03 PM)

Figure 23: New storage snapshots created - User 2

The same procedure as during the first test iteration was used to recover affected files and restore User access. All files were restored correctly.

NIST Compliance¹

NIST Framework Attribute	How Superna Data Security Edition Complies	NIST Compliance Status
<i>Identify</i>	Threat identified by username and IP address	Compliant
<i>Protect</i>	Stops the threat with user lockout in real time	Compliant
<i>Detect</i>	Detect malicious ransomware file attack and raise an alert to the user	Compliant
<i>Respond</i>	Create automated Snapshots to protect SMB shares and create new restore points for a multiuser attack	Compliant
<i>Recover</i>	File level recovery from previous snapshots to restore encrypted files and quarantine encrypted data for analysis	Compliant

¹ The table showing NIST compliance is provided solely for informational purposes and does not constitute definitive advice. Serious efforts have been made to ensure the accuracy of the information presented. All trademarks mentioned herein belong to their respective owners and are used for reference purposes only. No endorsement or affiliation is implied.

Copyright and Disclaimer

This publication is Copyright © 2024 by AV-Comparatives®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives
(August 2024)