Independent Tests of Anti-Virus Software



Single Product Test Superna Data Security Edition Commissioned by Superna

TEST PERIOD: JULY - AUGUST 2024

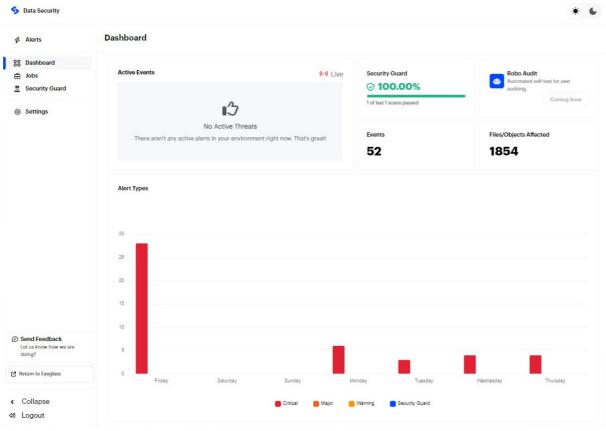
LAST REVISION: 20TH AUGUST 2024

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.

6

6

🌖 Data Security . Alerts 🖇 Alerts BB Dashboard History Active 🖨 Jobs Security Guard Show Security Guard Settings Ø Send Feedback Let us know how we are No Events doing? There aren't any events to review right now. Thats Great! 🖸 Return to Eyeglass Figure 2: Superna Data Security Edition

& Alerts	Alerts			
음 Dashboard 한 Jobs Security Guard	Active History			
 Settings 	Date is 7 days Jerror Caller Severity 0 User 0 Threat Caller	tegory ≎ litems Affected ≎	Show Source Cluster © State ©	Security Guard
	CRITICAL user2@avc2024.superna.net Suspiciou	is Extension 19	vast2 Locked Out	08/13/2024 3:59 AM
	CRITICAL user1@avc2024.superna.net Suspiciou	is Extension 19	vast2 Locked Out	08/13/2024 3:58 AM

Figure 3: Superna Data Security Edition – Detection

🌖 Data Security

Test Configuration

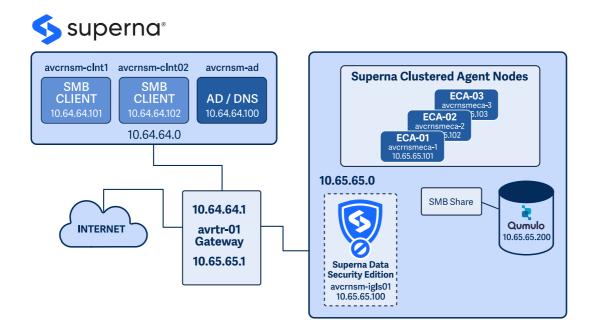


Figure 4: Infrastructure

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.

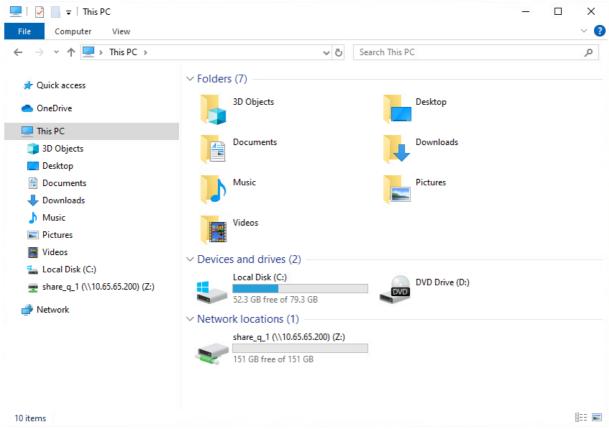


Figure 5: Share on the Windows 10 - User 1 client

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.

#FILEENCRYPTED.txt - Notepad				_ C	x L
File Edit Format View Help					
ATTENTION!					~
At the moment, your system is not protected.					
We can fix itand restore files.					
To get started, send a file to decrypt trial.					
You can trust us after opening the test file. To restore the system write to both :					
Your Decryption ID:					
					Y
<	1.1.0.11	1000/	145 L (CDLD)		
	Ln 1, Col 1	100%	Windows (CRLF)	UTF-8	2ð

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.

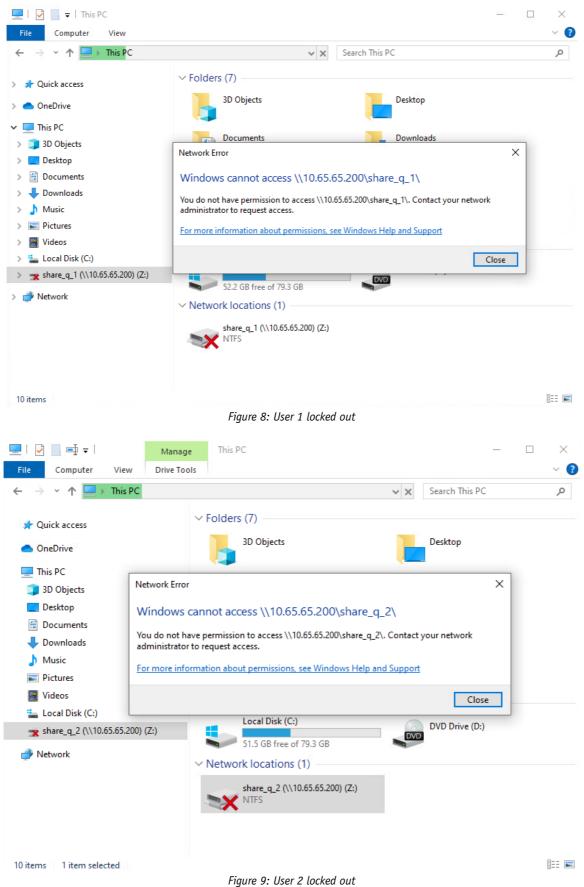
Custom Ransomware, Variant 1:

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

Data Security		6
🖇 Alerts	Alerts	
문 Dashboard 은 Jobs 옷 Security Guard	Active History Filter Show Security Guard	
Settings	Image: Severity Image: Severity	
	CRITICAL user1@avc2024.superna.net Suspicious Extension 12 AVC-Qsim Locked Out 08/16/2024 4:37 AM g 3:59:12	2
	O CRITICAL user2@avc2024.superna.net Suspicious Extension 19 AVC-Qsim Locked Out 08/16/2024 4:35 AM ∑ 3:59:12	2

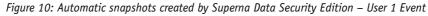
Figure 7: Detection events in the "Alerts" section

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

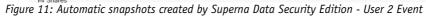


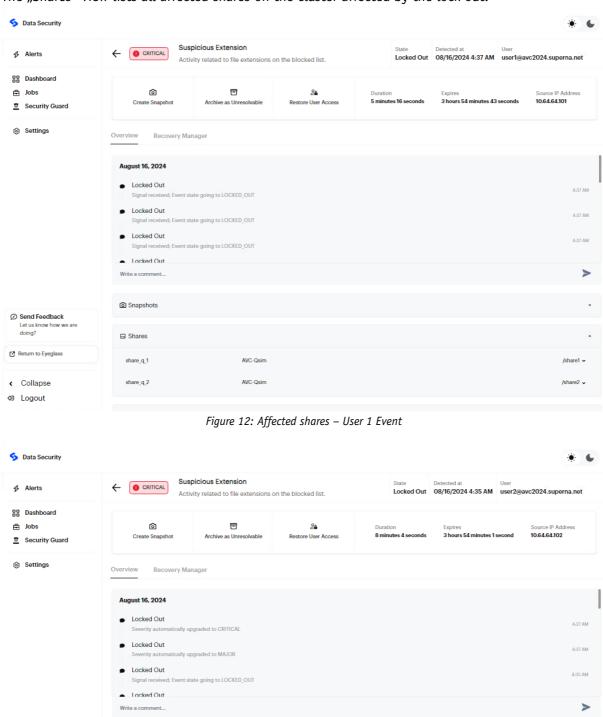
As the detection was raised, Superna Data Security Edition created a new storage snapshot to allow an administrator to investigate the incident:

Alerts	CRITICAL	uspicious Extension ctivity related to file extension	ions on the blocked list.		Detected at 08/16/2024 4:37 AM	User user1@avc2	024.superna.net
BB Dashboard 금 Jobs 흜 Security Guard	D Create Snapshot	T Archive as Unresolvable	2 6 Restore User Access	Duration 3 minutes 57 seconds	Expires 3 hours 56 minute	es 2 seconds	Source IP Address 10.64.64.101
③ Settings	Overview Recovery M	Nanager					
	August 16, 2024 Locked Out Signal received; Event	t state going to LOCKED_OUT					4:37 A
		t state going to LOCKED_OUT					4:37 A
	-	state going to LOCKED OUT					4:37 A
	-	state going to LOCKED_OUT					
) Send Feedback Let us know how we are doing?	Signal received; Event	t state going to LOCKED_OUT					
Let us know how we are	Signal received; Event I ocked Out Write a comment	: state going to LOCKED_OUT erna.net-share_q_2-17_405-1723	3797467180			0	4.37 M



5 Data Security							۰
& Alerts	CRITICAL	uspicious Extension ctivity related to file extensi	ions on the blocked list.	State Locked Out	Detected at 08/16/2024 4:35 AM	User user2@avc20	024.superna.net
B Dashboard Jobs Security Guard	ි Create Snapshot	T Archive as Unresolvable	2 6 Restore User Access	Duration 6 minutes 53 second	Expires Is 3 hours 55 minute	es 13 seconds	Source IP Address 10.64.64.102
③ Settings	Overview Recovery	Manager					
	August 16, 2024						4:37 AM
	 Locked Out 	y upgraded to CRITICAL y upgraded to MAJOR					4:37 AN
	 Locked Out Signal received; Even Locked Out 	at state going to LOCKED_OUT					4:35 AN
	Write a comment						>
) Send Feedback Let us know how we are doing?	🗑 Snapshots						
Return to Eyeglass	igls-user2@avc2024.su	perna.netshare_q_1-17_404-1723	3797339750			08)	/16/2024 4:42 AM 🗸
Collapse	igls-user2@avc2024.su	perna.netshare_q_2-17_404-172	3797339750			08,	/16/2024 4:42 AM 🗸
Logout							





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



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.

Data Security						
好 Alerts	CRITICAL	bicious Extension	on the blocked list.	State Locked Out		User user1@avc2024.superna.net
 Dashboard Jobs Security Guard 	(2) Create Snapshot	T Archive as Unresolvable	<u>ੁੰਛੇ</u> Restore User Access	Duration 6 minutes 28 seconds	Expires 3 hours 53 minutes 31 s	Source IP Address econds 10.64.64.101
මු Settings	Overview Recovery Mai	ager				
	13 100% Total Recoverable	0% 0% Unrecoverable Recovered	1		Filter	· v
	AVC-Qsim	♥ Path ♥	Cluster 🗸 Ever	nt Type 🗸 Event Tir	ne 🗸 File Name 🗸	Recovery Source 🗸 Reco
		✓ /share1/	/user01/testd AVC-Qsim FILE	WRITE, FILE_RENAME 08/16/20	024 4:37 AM /share1/user01/t	estd user01_base
		✓ /share1/	/user01/testd AVC-Qsim FILE	WRITE, FILE_RENAME 08/16/20	024 4:37 AM /share1/user01/t	estd user01_base
		/share1,	/user01/testd AVC-Qsim FILE	WRITE, FILE_RENAME 08/16/20	024 4:37 AM /share1/user01/t	estd user01_base
		✓ /share1/	/user01/testd AVC-Qsim FILE	WRITE, FILE_RENAME 08/16/20	024 4:37 AM /share1/user01/t	estd user01_base
Send Feedback Let us know how we are doing?		/share1,	/user01/testd AVC-Qsim FILE	WRITE, FILE_RENAME 08/16/20	024 4:37 AM /share1/user01/t	estd user01_base
Return to Eyeglass		-		WRITE, FILE_RENAME 08/16/20		
Collapse		 /share1, 13 Items Selected 		WRITE, FILE_RENAME 08/16/20		estd user01_base std user01 base
		10 items delected	2 Neu	alculate onapon0ts M EAL		

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:

🏂 Data Security			۲
8 Alerts	Jobs		
BB Dashboard		Recovering files on ne AVC-Qsim	00:00:03 🗸
🖨 Jobs	Recovery Job S-1-5-21-2130525082-	Recovering files on ne AVC-Qsim	00.00.03 🗸
👮 Security Guard	3192732430-2112517702 FINISHED - 08/16/2024 4-44 AM	Quarantine & Restore /share1/user01/testdata/file02469.txt	00:00:01 🗸
③ Settings		Quarantine & Restore /share1/user01/testdata/file02469.txt.owned	00:00:01 🗸
	Collecting Recovery Items from kafka	Quarantine & Restore /share1/user01/testdata/file00916.txt	00:00:01 🗸
	topic all-user-events_S-1-5-21 FINISHED • 08/16/2024 4:44 AM	Quarantine & Restore /share1/user01/testdata/file00916.txt.owned	00:00:01 🗸
	FINISHED - UB/16/2024 4544 AM	 Quarantine & Restore /share1/user01/testdata/file04923.txt 	00:00:01
	Creating Snapshots for User	Quarantine & Restore /share1/user01/testdata/file04923.txt.owned	00:00:00
	user1@avc2024.superna.net - Fri Aug 1	Quarantine & Restore /share1/user01/testdata/file02029.txt	00:00:00
	FINISHED - 08/16/2024 4:37 AM	Quarantine & Restore /share1/user01/testdata/file02029.txt.owned	00:00:00
		Quarantine & Restore /share1/user01/testdata/file04651.txt	00:00:00
	Locking Multicluster Shares 1723797466855	Quarantine & Restore /share1/user01/testdata/file04651.txt.owned	00:00:00
	FINISHED - 08/16/2024 4:37 AM	Quarantine & Restore /share1/user01/testdata/file04397.txt	00:00:00
		Quarantine & Restore /share1/user01/testdata/file04397.txt.owned	00:00:00
	Locking Multicluster Shares 1723797348024	Quarantine & Restore /share1/user01/testdata/file04995.txt	00:00:00
Send Feedback Let us know how we are	FINISHED • 08/16/2024 4:35 AM	Quarantine & Restore /share1/user01/testdata/file04995.txt.owned	00:00:00
doing?		Quarantine & Restore /share1/user01/testdata/file00386.txt	00:00:00
Return to Eyeglass	Creating Snapshots for User user2@avc2024.superna.net - Fri Aug 1	Quarantine & Restore /share1/user01/testdata/file00386.txt.owned	00:00:00 🗸
	FINISHED - 08/16/2024 4:35 AM	Quarantine & Restore /share1/user01/testdata/file04053.txt	00:00:00 🗸
Collapse		Quarantine & Restore /share1/user01/testdata/file04053.txt.owned	00:00:00 🗸
Logout	Collecting Recovery Items from kafka	Quarantine & Restore /share1/user01/testdata/file01859.txt	00.00.00

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.

					~ (
← → × ↑ 📙 « user01 > testda	ta	~ Ū	Search testdata		م ر
	Name		Date modified	Туре	Size
🖌 📌 Quick access	file00001.txt		8/14/2024 3:06 PM	Text Document	1
OneDrive	file00002.txt		8/14/2024 3:06 PM	Text Document	
	file00003.txt		8/14/2024 3:06 PM	Text Document	
This PC	file00004.txt		8/14/2024 3:06 PM	Text Document	
> 🧊 3D Objects	file00005.txt		8/14/2024 3:06 PM	Text Document	
> 📃 Desktop	file00006.txt		8/14/2024 3:06 PM	Text Document	
> 🔮 Documents	file00007.txt		8/14/2024 3:06 PM	Text Document	
> 🕂 Downloads	file00008.txt		8/14/2024 3:06 PM	Text Document	
Music	file00009.txt		8/14/2024 3:06 PM	Text Document	
> 📰 Pictures	file00010.txt		8/14/2024 3:06 PM	Text Document	
_	file00011.txt		8/14/2024 3:06 PM	Text Document	
> 😽 Videos	file00012.txt		8/14/2024 3:06 PM	Text Document	
> 🏪 Local Disk (C:)	file00013.txt		8/14/2024 3:06 PM	Text Document	
> 🛫 share_q_1 (\\10.65.65.200) (Z:)	file00014.txt		8/14/2024 3:06 PM	Text Document	
🔿 Network	file00015.txt		8/14/2024 3:06 PM	Text Document	
	file00016.txt		8/14/2024 3:06 PM	Text Document	
	file00017.txt		8/14/2024 3:06 PM	Text Document	
	file00018.txt		8/14/2024 3:06 PM	Text Document	
	file00019.txt		8/14/2024 3:06 PM	Text Document	
	file00020.txt		8/14/2024 3:06 PM	Text Document	
	 ≕ €1,00001 ++ 		0/14/2024 2:06 DM	Text Document	>
5,000 items 1 item selected 1.00 KB	•				

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

🛃 📑 🖛 🕇 I testdata			– 🗆 X
File Home Share View			~
- → → ↑ <mark> </mark> ≪ share_q_2 (\\10.6	5.65.200) (Z:) > user02 > testdata	✓ [™] Search testdat	a p
	Name	Date modified	Туре
📌 Quick access	file00001.txt	8/14/2024 3:09 PM	Text Document
len OneDrive	file00002.txt	8/14/2024 3:09 PM	Text Document
💻 This PC	file00003.txt	8/14/2024 3:09 PM	Text Document
_	file00004.txt	8/14/2024 3:09 PM	Text Document
3D Objects	file00005.txt	8/14/2024 3:09 PM	Text Document
Desktop	file00006.txt	8/14/2024 3:09 PM	Text Document
Documents	file00007.txt	8/14/2024 3:09 PM	Text Document
🕂 Downloads	file00008.txt	8/14/2024 3:09 PM	Text Document
h Music	file00009.txt	8/14/2024 3:09 PM	Text Document
Pictures	file00010.txt	8/14/2024 3:09 PM	Text Document
Videos	file00011.txt	8/14/2024 3:09 PM	Text Document
	file00012.txt	8/14/2024 3:09 PM	Text Document
🏪 Local Disk (C:)	file00013.txt	8/14/2024 3:09 PM	Text Document
🚍 share_q_2 (\\10.65.65.200) (Z:)	file00014.txt	8/14/2024 3:09 PM	Text Document
Active Retwork	file00015.txt	8/14/2024 3:09 PM	Text Document
	file00016.txt	8/14/2024 3:09 PM	Text Document
	file00017.txt	8/14/2024 3:09 PM	Text Document
	file00018.txt	8/14/2024 3:09 PM	Text Document
	file00019.txt	8/14/2024 3:09 PM	Text Document
	file00020.txt	8/14/2024 3:09 PM	Text Document
	☐ file00021 bet	0/14/2024 2:00 DM	Taxt Document

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:

Data Security								۲
3 Alerts	Alerts							
음 Dashboard 글 Jobs	Active Histor	У						
	Filter	~					Show Sec	urity Guard
Security Guard	Filter		1+2 Threat Category c	ltems Affected ≎	Source Cluster c	State c	Show Sec Detected at o	curity Guard
	📸 Date is 7 c	days [Severity is Critical		Items Affected c	Source Cluster c AVC-Qsim	State c	Detected at \circ	Timer c

Figure 18: Custom Variant 2 detected

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

🖇 Alerts	CRITICAL	picious Activity Pattern picious user action on data wa	as detected.		State Locked Out	Detected at 08/16/2024 11:13 AM	User user1@av	vc2024.superna.net
CB Dashboard ⊕ Jobs Security Guard	ර Create Snapshot	ਰ Archive as Unresolvable	은 6 Restore User Access	Duration 3 minutes	12 seconds	Expires 3 hours 56 minutes 47	seconds	Source IP Address 10.64.64.101
ම Settings		Jser avc2024.superna.net\user1 Te	st Successfully created snapshot	t AVC-Osim - igls-u	serl@avc2024	curama nati chana n 117	400 1222021	207888 11-13 Al
	Locked Out Saved locked out shares Locked Out	VC-Qsim: successfully locked shar	0024.superna.net_share_qRead	1 More				11:13 AN
Send Feedback Let us know how we are doing?	Locked Out Saved locked out shares Locked Out Locked Out Lockout access result: A userLisev27024 surema Write a comment Snapshots	VC-Qsim: successfully locked shar	e share, q.2 for user user1@avc2	1 More				11-13 AM
	Locked Out Saved locked out shares Locked Out Locked Out Locked Out Locked access result: A ursert@wwr?0704 surnerna Write a comment Snapshots igls-usert@wvc2024.supern	VC-Qsim: successfully locked shar net	e :share_q2 for user userl@avc2 07888	1 More				11.23 AM

New storage snapshots were created for each event:

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

Alerts	CRITICAL	picious Activity Pattern picious user action on data wa	is detected.	State Locked Out	Detected at 08/16/2024 11:13 AM	User user2@avc2024.superna.net
B Dashboard 국 Jobs 중 Security Guard	1 Create Snapshot	급 Archive as Unresolvable	දි ස් Restore User Access	Duration 3 minutes 55 seconds	Expires 3 hours 56 minutes 5	Source IP Address seconds 10.64.64.102
3 Settings	Overview Recovery Ma	nager				
	August 16, 2024 Locked Out Saved locked out shares					11:13 AJ
	Locked Out Lockout access result: A user2@evc2024.superna Delayed Lockout Severity automatically up		e :share_q.2 for user user2@avc2	2024.superna.net. AVC-Qsim: s	uccessfully locked share :shar	
	 Lockout access result: A user2@avc2024.superna Delayed Lockout 	i.net.	e :share_q 2 for user user2@avc2	2024.superna.net. AVC-Qsim: s	uccessfully locked share share	11.13 A
Send Feedback	 Lockout access result: A user2@ewc2024.superna Delayed Lockout Severity automatically up 	i.net.	e :share_q,2 for user user2@avc2	2024.superna.net. AVC-Qsim: s	uccessfully locked share share	1625, 101 daar 1613 AA
Let us know how we are	Lockout access result: A user2@wv2024.superna Delayed Lockout Severity automatically up Write a comment Snapshots	i.net.		2024.superna.net. AVC-Qaim: s	uccessfully locked share shar	1625, 101 daar 1613 AA
Let us know how we are doing?	Lockout access result: A user2@wv2024.superna Delayed Lockout Severity automatically up Write a comment G Snapshots igls-user2@wv2024.supern	unet.	03424	2024.superna.net. AVC-Qsim: s	uccessfully locked share share	11-23 A
Send Feedback Let us know how we are doing? Return to Eyeglass Collapse	Lockout access result: A user2@wv2024.superna Delayed Lockout Severity automatically up Write a comment G Snapshots igls-user2@wv2024.supern	na.net-share_q.2-17,408-17238212	03424	2024.superna.net. AVC-Qeim: s	uccessfully locked share :shar	11-12 AA > 08/16/2024 11-17 AM ↓

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:

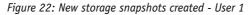
Data Security								۲
3 Alerts	Alerts							
B Dashboard B Jobs 중 Security Guard	Active Histor	~					Show Sec	curity Guard 🔵
) Settings	Severity 0	days i Severity is Critical	Threat Category 0	Items Affected o	Source Cluster 😋	State 0	Detected at $\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$	Timer c
	CRITICAL	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.

🖇 Alerts	CRITICAL Suspicious Activity Pattern Suspicious user action on data was detected.			State Locked Out	State Detected at User Locked Out 08/16/2024 1:53 PM user1@avc2024.superna.m			
B Dashboard Jobs Security Guard	© Create Snapshot	Archive as Unresolvable	උ ස් Restore User Access	Duration 6 minutes 45 seconds	Expires 3 hours 53 minutes 20) seconds	Source IP Address 10.64.64.101	
3 Settings	Overview Recovery Mai	nager						
	 Locked Out 							
	user1@avc2024.superna. To Lockout Signal received; Event st	VC-Qsim: successfully locked share	e :share_q_2 for user user1@avc2	024.superna.net. AVC-Qsim: suo	cessfully locked share :shar	e_q_1 for user	1.53 P	
	Saved locked out shares C Locked Out Lockout access result: Al user1@avc2024.superna. To Lockout	VC-Qsim: successfully locked share .net.	e :share_q_2 for user userl@ewc2	1024.superna.net; AVC-Qsim: suo	cessfully locked share :shar	e_q_1 for user	1.53 PI	
Send Feedback Let us know how we are doing?	Saved locked out shares Clocked Out Lockout access result: A Userl@evc2024.superna. To Lockout Signal received; Event st Write a comment C Snapshots	VC-Qsim: successfully locked share .net.		024.superna.net. AVC-Qsim: suo	cessfully locked share :shar		1.53 P	

New storage snapshots were created for each event:



3 Alerts	CRITICAL Suspicious Activity Pattern Suspicious user action on data was detected.			State Locked	State Detected at User Locked Out 08/16/2024 1:53 PM user2@avc2024.supernation		
문 Dashboard 크 Jobs 문 Security Guard	(c) Create Snapshot	T Archive as Unresolvable	2ස් Restore User Access	Duration 10 minutes	Expires 3 hours 49 minutes 59 se	Source IP Addres	35
3 Settings	Overview Recovery Ma	anager					
	August 16, 2024						
	Locked Out 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.						
	Creating Snapshots for U				c2024.superna.netshare_q_1-1	17_411-1723830817539.	1:53 F
	Creating Snapshots for U	User avc2024.superna.net\user2 te apshot AVC-Qsim - igls-user2@avc2			c2024.superna.netshare_q_1-1	17_411-1723830817539.	
	Creating Snapshots for I Successfully created sna Locked Out Saved locked out shares	apshot AVC-Qsim - igls-user2@avc			2024.superna.net-share_q_1-1	17_411-1723830817539.	
	Creating Snapshots for I Successfully created snu Locked Out Saved locked out shares Locked Out	apshot AVC-Qsim - igls-user2@avc; s WC-Qsim: successfully locked shar	2024.superna.netshare_qRea	d More			1:53 F
	Creating Snapshots for 1 Successfully created snu Locked Out Saved locked out shares Locked Out Lockout access result: A	apshot AVC-Qsim - igls-user2@avc; s WC-Qsim: successfully locked shar	2024.superna.netshare_qRea	d More			1:53 F 1:53 F 1:53 F
	Creating Snaphots for I Successfully created inv Saved locked Out Saved locked Out shares Occeed Out Lockout access result: A user/20avc/2024 superva	apshot AVC-Qsim - igls-user2@avc; s WC-Qsim: successfully locked shar	2024.superna.netshare_qRea	d More			1:53 F 1:53 F
Send Foedback Let us know how we are doing?	Creating Snaphots for I Successfully created and Locked Out Saved locked out shares Locked Out Lockout access result: A user?awer?2024 surverse Write a comment	apshot AVC-Qsim - igls-user2@avc; s WC-Qsim: successfully locked shar	2024.superna.net-share_qReas	d More			1:53
et us know how we are	Creating Snaphots for 1 Successfully created and Locked Out Locked Out Locked access result: A user?dawc?024 surverse Write a comment	apshot AVC-Qaim - igis-user2@avcl s WC-Qaim: successfully locked shar a net	2024.superna.net-share_qRea e :share_q 2 for user user2@avc?	d More		hare_q.1 for user	1:53 F 1:53 F

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
ldentify	Threat identified by username and IP address	Compliant
Protect	Stops the threat with user lockout in real time	Compliant
Detect	Detect malicious ransomware file attack and raise an alert to the user	Compliant
Respond	Create automated Snapshots to protect SMB shares and create new restore points for a multiuser attack	Compliant
Recover	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.



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)

