# Independent Tests of Anti-Virus Software



## Single Product Test Superna Data Security Edition Commissioned by Superna

TEST PERIOD: JULY - AUGUST 2024

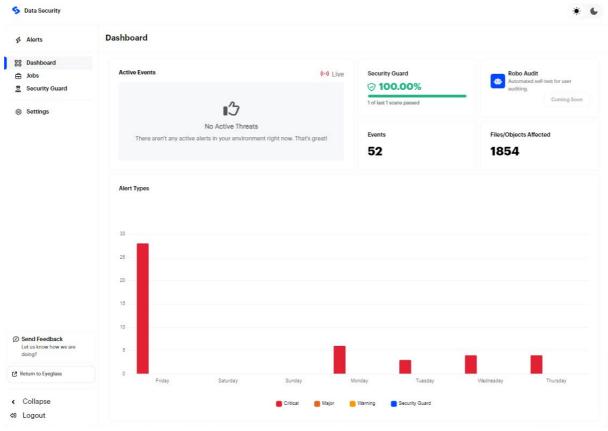
LAST REVISION: 20<sup>TH</sup> AUGUST 2024

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 Vast Data 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

🌖 Data Security

	* •
🖇 Alerts	Alerts
Dashboard	Active History
🖻 Jobs 👮 Security Guard	Show Security Guard
Settings	
Send Feedback Let us know how we are doing?	No Events
🖸 Return to Eyeglass	There aren't any events to review right now. Thats Great!
	Figure 2: Superna Data Security Edition
🌖 Data Security	* 6
∲ Alerts	Alerts
C Dashboard	Active History

<ul> <li>Jobs</li> <li>Security Guard</li> <li>Settings</li> </ul>	Filter	days [] Severity 1s Criti	ical +2			Show S	Security Guard
igi setungs	Severity 0	User 0	Threat Category 0	Items Affected 0	Source Cluster 0	State 0	Detected at 0
	CRITICAL	user2@avc2024.superna.net	Suspicious Extension	19	vast2	Locked Out	08/13/2024 3:59 AM
	CRITICAL	user1@avc2024.superna.net	Suspicious Extension	19	vast2	Locked Out	08/13/2024 3:58 AM

Figure 3: Superna Data Security Edition – Detection

## **Test Configuration**

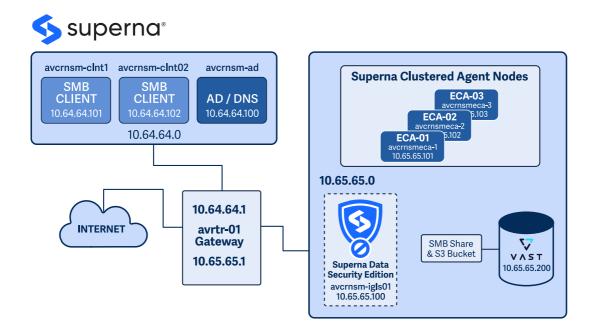


Figure 4: Infrastructure

#### **Product Versions**

- Superna Data Security Edition 2.9.0-24085
- Vast Data VMS:
  - Build: release-4-7-0-sp10-1157242-vms
  - Software version: 4.7.0.80
- Vast Data Cluster:
  - Build: release-4-7-0-sp10-1157242
  - PSNT: lb-release-4-7-0-sp10-1147242
  - Software version: 4.7.0.80

#### 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 Vast Data 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 Vast Data. 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.

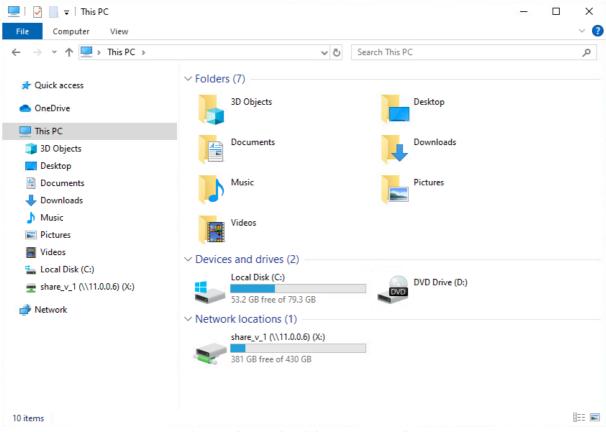


Figure 5: Share on the Windows 10 - User 1 client

#### **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.

I #FILEENCRYPTED.txt - Notepad				9 <del></del>	×
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:					
					¥
<			0		>
	Ln 1, Col 1	100%	Windows (CRLF)	UTF-8	

*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					
음을 Dashboard 글 Jobs	Active History					
Security Guard	Filter 🗸				Show S	Security Guard
③ Settings	💼 Date Is 7 days 🞚 Severity Is Criti	ical+2				
	Severity 0 User 0	Threat Category 0	Items Affected 0	Source Cluster 0	State 0	Detected at 0
	CRITICAL User2@avc2024.superna.net	Suspicious Extension	19	vast2	Locked Out	08/13/2024 3:59 AM
	CRITICAL user1@avc2024.superna.net	Suspicious Extension	19	vast2	Locked Out	08/13/2024 3:58 AM

Figure 7: Detection events in the "Alerts" section

After a few files on the connected shares were encrypted, write access on the shares was disabled for both users:

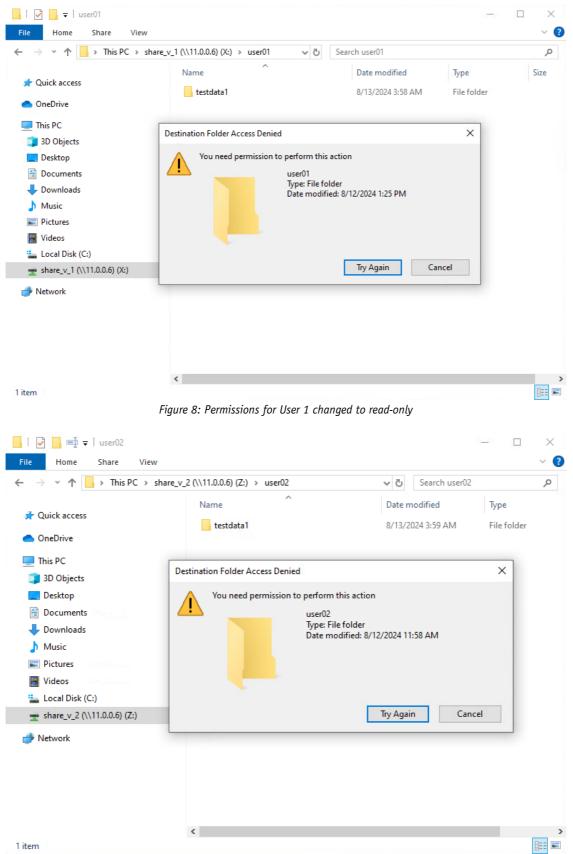


Figure 9: Permissions for User 2 changed to read-only

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

& Alerts		Suspicious Extension Activity related to file e blocked list.		State Locked Out	Detected at 08/13/2024 3:58 AM	User user1@avc	2024.superna.net
음 Dashboard 클 Jobs 호 Security Guard	Create Snapshot	Archive as Unresolvable	දි <b>ය</b> Restore User Access	Duration 8 minutes 27 seconds	Expires 3 hours 52 mi seconds	nutes 8	Source IP Address 10.64.64.101
Settings	Overview Recove	ry Manager					
	Locked Out     Severity automati	cally upgraded to CRITICAL					3.50 A
	Locked Out     Signal received; E     Locked Out	event state going to LOCKED_	OUT				3-58 A
	Write a comment						,
	igls-avc2024.supern 1723535915329	a.net-user1 Test-defaultsmb	⊳share1-17_387-			(	01/20/1970 5:45 PM 🗸
Send Feedback Let us know how we are doing?	igls-avc2024.supern 1723535915329	a.net-useri Test-defaultsmb	-share2-17_387-			0	01/20/1970 5:45 PM 👻
	🕀 Shares						
Return to Eyeglass							

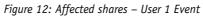
Figure 10: Automatic snapshots created by Superna Data Security Edition – User 1 Event

& Alerts	CRITICAL     Suspicious Extension     Activity related to file extensions on the     blocked list.			State Locked Out	Detected at 08/13/2024 3:59 AM	User user2@avc2024.superna.net	
끊 Dashboard 크 Jobs ፪ Security Guard	ලි Create Snapshot	급 Archive as Unresolvable	26 Restore User Access	Duration 8 minutes 54 seconds	Expires 3 hours 51 mi seconds	inutes 5	Source IP Address 10.64.64.102
Settings	Overview Recover	ry Manager					
	<ul> <li>Locked Out</li> </ul>	vent state going to LOCKED_					3-59 Al 3-59 Al
	<ul> <li>Locked Out</li> </ul>	vent state going to LOCKED_ vent state going to LOCKED_					3:50 AI
	Write a comment						>
	♂ Snapshots						
	Igls-avc2024.supern: 1723535953787	a.net-user2 test-defaultsmb	-share1-17_388-			0	I/20/1970 5:45 PM ♀
Send Feedback Let us know how we are doing?	IgIs-avc2024.supern: 1723535953788	a.net-user2 test-defaultsmb	-share2-17_388-			o	/20/1970 5:45 PM ╺
Return to Eyeglass	⊟ Shares						

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

& Alerts		Suspicious Extension Activity related to file blocked list.			Detected at 08/13/2024 3:58 AM	User user1@avc20	24.superna.net
양 Dashboard 국 Jobs 중 Security Guard	Create Snapshot	ਰ Archive as Unresolvable	26 Restore User Access	Duration 11 minutes 56 seconds	Expires 3 hours 48 min seconds	utes 39	Source IP Address 10.64.64.101
3 Settings	Overview Recov	ery Manager					
	August 13, 2024						
	Locked Out     Severity automa	tically upgraded to CRITICAL					3-50 AI
	<ul> <li>Locked Out</li> <li>Severity automatic</li> </ul>	tically upgraded to MAJOR					3-59 AI
		Event state going to LOCKED	)_OUT				3:58 AI
	Locked Out Write a comment						>
	ලි Snapshots						
	🕀 Shares						
Send Feedback	smb_policy	vast2		default			/smb/share1 🔺
Let us know how we are doing?	Permission			Client	ts		
Return to Eyeglass	NFS Read-Write						
Collapse	NFS Read-Only						

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



5 Data Security							* •
& Alerts		Suspicious Extension Activity related to file blocked list.		State Locked Out	Detected at 08/13/2024 3:59 AM	User user2@avc20	024.superna.net
88 Dashboard 글 Jobs 훐 Security Guard	Create Snapshot	ਰ Archive as Unresolvable	26 Restore User Access	Duration 13 minutes 27 seconds	Expires 3 hours 46 mi seconds	inutes 32	Source IP Address 10.64.64.102
③ Settings	Overview Recov	ery Manager					
	August 13, 2024						
	<ul> <li>Locked Out</li> <li>Signal received;</li> </ul>	Event state going to LOCKEE	LOUT				3:50 AM
	<ul> <li>Locked Out</li> <li>Signal received;</li> </ul>	Event state going to LOCKED	OUT				3:50 AM
	<ul> <li>Locked Out</li> <li>Signal received;</li> </ul>	Event state going to LOCKED	OUT				3:59 AM
	Locked Out Write a comment						>
	© Snapshots						×
	🕀 Shares						*
Ø Send Feedback	smb_policy	vast2		default			/smb/share1 🔺
Let us know how we are doing?	Permission			Clients			
🖸 Return to Eyeglass	NFS Read-Write			×			
< Collapse	NFS Read-Only						
¢n) Logout	SMB Read-Only			10.64.64.101,	10.64.64.102		

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.

CRITICAL	<b>bicious Extension</b> ity related to file extensions on t	he blocked list.	State Locked Out	Detected at 08/13/2024 3:58 AM	User user1@avc2024.superna.net
ට Create Snapshot	C Archive as Unresolvable	26 Restore User Access	Duration 17 minutes 39 seconds	Expires 3 hours 42 minutes 56 sec	Source IP Address onds 10.64.64.101
verview Recovery Mar	ager				
43 100% Total Recoverable	0% 0% Unrecoverable Recovered			Filte	er v
vast2	• Path •	Cluster 🖌 Event Type	♥ Event Time ♥ File	Name 🖌 Recover	y Source 👻 Recovery Time 🛩 Sta
	<ul> <li>/smb/share</li> </ul>	1/user01/t vast2 FILE_CREAT	'E, FILE_WR 08/13/2024 3:58 AM /sm	b/share1/user01/t user01_	base C
	<ul> <li>/smb/share</li> </ul>	1/user01/t vast2 FILE_CREAT	E, FILE_WR 08/13/2024 3:58 AM /sm	b/share1/user01/t user01_	base 🤅
	<ul> <li>/smb/share</li> </ul>	1/user01/t vast2 FILE_CREAT	'E, FILE_WR 08/13/2024 3:58 AM /sm	b/share1/user01/t user01_	base 🤅
	/smb/share	1/user01/t vast2 FILE_CREAT	E, FILE_WR 08/13/2024 3:58 AM /sm	b/share1/user01/t user01_	base 🤅
	<ul> <li>/smb/share</li> </ul>	1/user01/t vast2 FILE_CREAT	E, FILE_WR 08/13/2024 3:58 AM /sm	b/share1/user01/t user01_	base 🤤
	<ul> <li>/smb/share</li> </ul>	1/user01/t vast2 FILE_CREAT	E, FILE_WR 08/13/2024 3:58 AM /sm	b/share1/user01/t user01_	base C
	<ul> <li>/smb/share</li> </ul>	1/user01/t vast2 FILE_CREAT	E, FILE_WR 08/13/2024 3:58 AM /sm	b/share1/user01/t user01_	base C
	<ul> <li>/smb/share</li> </ul>	1/user01/t vast2 FILE_CREAT	E, FILE_WR 08/13/2024 3:58 AM /sm	b/share1/user01/t user01_	base 🤅
	<ul> <li>/smb/share</li> </ul>	1/user01/t vast2 FILE_CREAT	E, FILE_WR 08/13/2024 3:58 AM /sm	nb/share1/user01/t user01_	base 🤅
	43 Items Selected	۵	Recalculate Snapshots 🔬 Expo	rt as CSV 🔗 Recover	iase a

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:

5 Data Security			۲
	Jobs		
88 Dashboard		Preparing to recover files on vast2	
🖨 Jobs	Recovery Job S-1-5-21-2130525082-3192732430-	Preparing to recover tiles on vast2	00:00:28
2 Security Guard	2112517702-1103_1723535915210 1723537164082 FINISHED • 08/13/2024 4:19 AM	Setting up S3 access to view /smb	00:00:00
Settings	L	Recovering files	00:00:27
	Collecting Recovery Items from kafka topic all- user-events_S-1-5-21-2130525082-3192732430	$\odot$	00:00:27
	Finished - 08/13/2024 4-16 AM	Quarantine & Restore /smb/share1/user01/testdata1/file00001.txt	00:00:01
		Quarantine & Restore /smb/share1/user01/testdata1/file00001.txt.owned	00:00:02
	Recovery Job S-1-5-21-2130525082-3192732430- 2112517702-1104 1723535951326 1723536968297	Quarantine & Restore /smb/share1/user01/testdata1/file00002.txt	00:00:01
	FINISHED - 08/13/2024 4:16 AM	Quarantine & Restore /smb/share1/user01/testdata1/file00002.txt.owned	00:00:01
		Quarantine & Restore /smb/share1/user01/testdata1/file00003.txt	00:00:01
	Collecting Recovery Items from kafka topic all- user-events S-1-5-21-2130525082-3192732430	Quarantine & Restore /smb/share1/user01/testdata1/file00003.txt.owned	00:00:01
	HINISHED - 08/13/2024 4:14 AM	Quarantine & Restore /smb/share1/user01/testdata1/file00004.txt	00:00:01
		Quarantine & Restore /smb/share1/user01/testdata1/file00004.txt.owned	00:00:01
		<ul> <li>Quarantine &amp; Restore /smb/share1/user01/testdata1/file00005.txt</li> </ul>	00:00:01
		Quarantine & Restore /smb/share1/user01/testdata1/file00005.txt.owned	00:00:01
		Quarantine & Restore /smb/share1/user01/testdata1/file00006.txt	00:00:01
		<ul> <li>Quarantine &amp; Restore /smb/share1/user01/testdata1/file00006.txt.owned</li> </ul>	00:00:01
) Send Feedback		Quarantine & Restore /smb/share1/user01/testdata1/file00007.txt	00:00:01
Let us know how we are doing?		Quarantine & Restore /smb/share1/user01/testdata1/file00007.txt.owned	00:00:01
Return to Eyeglass		<ul> <li>Quarantine &amp; Restore /smb/share1/user01/testdata1/file00008.txt</li> </ul>	00:00:01
		<ul> <li>Quarantine &amp; Restore /smb/share1/user01/testdata1/file00008.txt.owned</li> </ul>	00:00:01
Collapse		<ul> <li>Quarantine &amp; Restore /smb/share1/user01/testdata1/file00009.txt</li> </ul>	00:00:01
Logout		Quarantine & Restore /smb/share1/user01/testdata1/file00009.txt.owned	00:00:01

Figure 15: Recovery complete

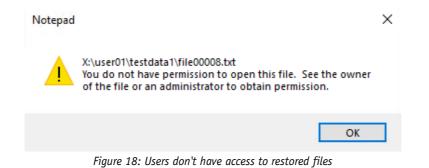
At this point, both client VMs were reverted to a clean snapshot. After verifying that the recovery of all selected files was complete, User Access was restored using the respective button in the event overview page.

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

File Home Share View			- 0 ×
			~ ?
$\leftarrow$ $\rightarrow$ $\checkmark$ $\uparrow$ $\square$ $\rightarrow$ This PC $\rightarrow$ share_v_1	(\\11.0.0.6) (X:) → user01	ch user01	م
	Name	Date modified Type	Size
📌 Quick access	testdata1	8/13/2024 4:19 AM File fold	der
OneDrive	New Text Document.txt	8/13/2024 4:22 AM Text Do	ocument 1
💻 This PC	New Text Document.txt - Notepad	- 🗆 X	
3D Objects	File Edit Format View Help		
Desktop	test		~
Documents			
🕂 Downloads			
👌 Music			
Pictures			
📑 Videos			
🏪 Local Disk (C:)			
🛫 share_v_1 (\\11.0.0.6) (X:)			
i Network			
			<b>_</b>
	<	>	
4	Ln 1, Col 5 100% Windo	ows (CRLF) UTF-8	
2 items 1 item selected 4 bytes			
	Figure 16: Write access restored for	User 1	
🛃 🔄 🛋 =   user02			- 🗆 🗙
File Home Share View			
			~ 🕐
$\leftarrow \rightarrow \checkmark \uparrow$ $\land$ This PC $\rightarrow$ share	v_2 (\\11.0.0.6) (Z:) > user02 >	ע טֿ Search user02	<b>؟</b> ~ م
	v_2 (\\11.0.0.6) (Z:) > user02 > ^^	✓ ♂ Search user02 Date modified	
← → Y ▲ This PC → share ★ Quick access	Name	Date modified	ر Type
	^		٩
<ul> <li>Quick access</li> <li>OneDrive</li> </ul>	Name ^	Date modified 8/13/2024 4:16 AM 8/13/2024 4:23 AM	ہ Type File folder Text Document
<ul> <li>Quick access</li> <li>OneDrive</li> <li>This PC</li> </ul>	Name  testdata1  New Text Document.txt  New Text Document.txt - Notepad	Date modified 8/13/2024 4:16 AM	ہ Type File folder
<ul> <li>Quick access</li> <li>OneDrive</li> <li>This PC</li> <li>3D Objects</li> </ul>	Name testdata1 New Text Document.txt New Text Document.txt - Notepad File Edit Format View Help	Date modified 8/13/2024 4:16 AM 8/13/2024 4:23 AM	ہ Type File folder Text Document
<ul> <li>Quick access</li> <li>OneDrive</li> <li>This PC</li> <li>3D Objects</li> <li>Desktop</li> </ul>	Name  testdata1  New Text Document.txt  New Text Document.txt - Notepad	Date modified 8/13/2024 4:16 AM 8/13/2024 4:23 AM	ہ Type File folder Text Document
<ul> <li>Quick access</li> <li>OneDrive</li> <li>This PC</li> <li>3D Objects</li> <li>Desktop</li> <li>Documents</li> </ul>	Name testdata1 New Text Document.txt New Text Document.txt - Notepad File Edit Format View Help	Date modified 8/13/2024 4:16 AM 8/13/2024 4:23 AM	ہ Type File folder Text Document
<ul> <li>Quick access</li> <li>OneDrive</li> <li>This PC</li> <li>3D Objects</li> <li>Desktop</li> <li>Documents</li> <li>Documents</li> </ul>	Name testdata1 New Text Document.txt New Text Document.txt - Notepad File Edit Format View Help	Date modified 8/13/2024 4:16 AM 8/13/2024 4:23 AM	ہ Type File folder Text Document
<ul> <li>Quick access</li> <li>OneDrive</li> <li>This PC</li> <li>3D Objects</li> <li>Desktop</li> <li>Documents</li> <li>Downloads</li> <li>Music</li> </ul>	Name testdata1 New Text Document.txt New Text Document.txt - Notepad File Edit Format View Help	Date modified 8/13/2024 4:16 AM 8/13/2024 4:23 AM	ہ Type File folder Text Document
<ul> <li>Quick access</li> <li>OneDrive</li> <li>This PC</li> <li>3D Objects</li> <li>Desktop</li> <li>Documents</li> <li>Downloads</li> <li>Music</li> <li>Pictures</li> </ul>	Name testdata1 New Text Document.txt New Text Document.txt - Notepad File Edit Format View Help	Date modified 8/13/2024 4:16 AM 8/13/2024 4:23 AM	ہ Type File folder Text Document
<ul> <li>Quick access</li> <li>OneDrive</li> <li>This PC</li> <li>3D Objects</li> <li>Desktop</li> <li>Documents</li> <li>Downloads</li> <li>Music</li> <li>Pictures</li> <li>Videos</li> </ul>	Name testdata1 New Text Document.txt New Text Document.txt - Notepad File Edit Format View Help	Date modified 8/13/2024 4:16 AM 8/13/2024 4:23 AM	ہ Type File folder Text Document
<ul> <li>Quick access</li> <li>OneDrive</li> <li>This PC</li> <li>3D Objects</li> <li>Desktop</li> <li>Documents</li> <li>Downloads</li> <li>Music</li> <li>Pictures</li> <li>Videos</li> <li>Local Disk (C:)</li> </ul>	Name testdata1 New Text Document.txt New Text Document.txt - Notepad File Edit Format View Help	Date modified 8/13/2024 4:16 AM 8/13/2024 4:23 AM	ہ Type File folder Text Document
<ul> <li>Quick access</li> <li>OneDrive</li> <li>This PC</li> <li>3D Objects</li> <li>Desktop</li> <li>Documents</li> <li>Downloads</li> <li>Music</li> <li>Pictures</li> <li>Videos</li> </ul>	Name testdata1 New Text Document.txt New Text Document.txt - Notepad File Edit Format View Help	Date modified 8/13/2024 4:16 AM 8/13/2024 4:23 AM	ہ Type File folder Text Document
<ul> <li>Quick access</li> <li>OneDrive</li> <li>This PC</li> <li>3D Objects</li> <li>Desktop</li> <li>Documents</li> <li>Downloads</li> <li>Music</li> <li>Pictures</li> <li>Videos</li> <li>Local Disk (C:)</li> </ul>	Name testdata1 New Text Document.txt New Text Document.txt - Notepad File Edit Format View Help	Date modified 8/13/2024 4:16 AM 8/13/2024 4:23 AM	ہ Type File folder Text Document
<ul> <li>Quick access</li> <li>OneDrive</li> <li>This PC</li> <li>3D Objects</li> <li>Desktop</li> <li>Documents</li> <li>Downloads</li> <li>Music</li> <li>Pictures</li> <li>Videos</li> <li>Local Disk (C:)</li> <li>share_v_2 (\\11.0.0.6) (Z:)</li> </ul>	Name testdata1 New Text Document.txt New Text Document.txt - Notepad File Edit Format View Help	Date modified 8/13/2024 4:16 AM 8/13/2024 4:23 AM	ہ Type File folder Text Document
<ul> <li>Quick access</li> <li>OneDrive</li> <li>This PC</li> <li>3D Objects</li> <li>Desktop</li> <li>Documents</li> <li>Downloads</li> <li>Music</li> <li>Pictures</li> <li>Videos</li> <li>Local Disk (C:)</li> <li>share_v_2 (\\11.0.0.6) (Z:)</li> </ul>	Name testdata1 New Text Document.txt New Text Document.txt - Notepad File Edit Format View Help	Date modified 8/13/2024 4:16 AM 8/13/2024 4:23 AM	ہ Type File folder Text Document
<ul> <li>Quick access</li> <li>OneDrive</li> <li>This PC</li> <li>3D Objects</li> <li>Desktop</li> <li>Documents</li> <li>Downloads</li> <li>Music</li> <li>Pictures</li> <li>Videos</li> <li>Local Disk (C:)</li> <li>share_v_2 (\\11.0.0.6) (Z:)</li> </ul>	Name testdata1 New Text Document.txt New Text Document.txt - Notepad File Edit Format View Help	Date modified 8/13/2024 4:16 AM 8/13/2024 4:23 AM	ہ Type File folder Text Document
<ul> <li>Quick access</li> <li>OneDrive</li> <li>This PC</li> <li>3D Objects</li> <li>Desktop</li> <li>Documents</li> <li>Downloads</li> <li>Music</li> <li>Pictures</li> <li>Videos</li> <li>Local Disk (C:)</li> <li>share_v_2 (\\11.0.0.6) (Z:)</li> </ul>	Name testdata1 New Text Document.txt New Text Document.txt - Notepad File Edit Format View Help test	Date modified 8/13/2024 4:16 AM 8/13/2024 4:23 AM	✓
<ul> <li>Quick access</li> <li>OneDrive</li> <li>This PC</li> <li>3D Objects</li> <li>Desktop</li> <li>Documents</li> <li>Downloads</li> <li>Music</li> <li>Pictures</li> <li>Videos</li> <li>Local Disk (C:)</li> <li>share_v_2 (\\11.0.0.6) (Z:)</li> </ul>	Name  testdata1  New Text Document.txt  New Text Document.txt - Notepad File Edit Format View Help test	Date modified 8/13/2024 4:16 AM 8/13/2024 4:23 AM	ہ Type File folder Text Document

Figure 17: Write access restored for User 2

Note: After restoring the files affected by the ransomware infection, only administrators have access to the restored files. According to Superna, this behaviour is specific to Vast and occurs because Vast does not currently provide an API for Superna Data Security Edition to reset the file permissions after a restore. In a real-world scenario, administrators would have to reset the file permissions themselves.



Comparing the SHA256 hashes of the recovered files using an administrator account confirmed that content-wise, all files were correctly restored to their state before the ransomware infection.

To prepare for testing the next ransomware sample, affected files were deleted and re-created on the Windows clients. Furthermore, existing storage snapshots on Vast were removed and fresh snapshots were created as described previously.



#### 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:

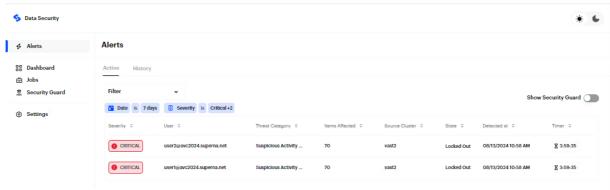


Figure 19: Custom Variant 2 detected

As during the first iteration, Superna Data Security Edition quickly removed write access to the shares both users.

S Data Security						* •
& Alerts	CRITICAL	us Activity Pattern s user action on data was detecte	ed.	State Locked C	Detected at Out 08/13/2024 10:58 AM	User user1@avc2024.superna.net
88 Dashboard	© Create Snapshot	고 Archive as Unresolvable	26 Restore User Access	Duration 3 minutes 46 seconds	Expires 3 hours 56 minutes 13 second	Source IP Address Is 10.64.64.101
③ Settings	Overview Recovery Manager					
	August 13, 2024 Locked Out Signal received: Event state gol Locked Out Signal received: Event state gol Locked Out Creating Snapshots for User av vat2 - Igle avc0024.superna.ne Write a comment	ing to LOCKED_OUT	fully created snapshot vast2 - Igle avc202	24 superna net useri Test default -smb-s	share2-17_390-1722561131797. Su	10.50 AM 10.50 AM constituity created angustor 10.50 AM
	igls-avc2024.superna.net-user1 Te	st-defaultsmb-share2-17_390-172356	1131797			01/20/1970 5:46 PM 🗸
Ø Send Feedback	igls-avc2024.superna.net-user1 Te	st-defaultsmb-share1-17_390-172356	1131797			01/20/1970 5:46 PM 🗸
Let us know how we are doing?	⊟ Shares					•
Return to Eyeglass	S User Alert History View All					
∢ Collapse ♦) Logout						

#### New storage snapshots were created for each event:

Figure 20: New storage snapshots created by Superna Data Security Edition – User 1

& Alerts	CRITICAL	CRITICAL Suspicious Activity Pattern Suspicious user action on data was detected.				User user2@avc2024.superna.net		
Dashboard Jobs	ලි Create Snapshot	C Archive as Unresolvable	26 Restore User Access	Duration 4 minutes 27 seconds	Expires 3 hours 55 minutes 32 second	Source IP Address 10.64.64.102		
Settings	Overview Recovery Manager	Overview Recovery Manager						
	August 13, 2024  Locked Out Signal received; Event state gol	ng to LOCKED_OUT				10.50 A		
	vast2 - Igls-avc2024.superna.ne	c2024.superna.net\user2 test Success	sfully created snapshot vast2 - igis-avc20	24.superna.net-user2 test-default-smb	share2-17_391-1723561135999. Su	ccessfully created snapshot 10-50 A		
	Signal received; Event state gol Locked Out Creating Snapshots for User ave	c2024.superna.net\user2 test Success	stuly created snapshot vast2 - Igle avc20	24.superna.net user2 test-default-smb	share2-17_391-1723561135999. Su	1050 A		
	Signal received, Event state gol Locked Out Creating Snapshots for User aw vast2 - Igls-avc2024.superna.ne Write a comment	c2024.superna.net\user2 test Success	dully created snapshot vast2 - igls avc20	24.superna.net-user2 test-default-smb	share2-17_391-1723561135999. Su	ccessfully created snapshot 10-59 A		
Send Feedback Let us how how we are doing?	Signal received, Event state gol Locked Out Creating Snapshots for User aw vast2 - Igle-avc2024.superna.ne Write a comment	c2024.superna.net\user2 test Success	dully created unapoliot vast2 - igle avc20	24 superna net user 2 test default-smb	share2-17_291-1722561135999. Su	ccessfully created snapshot 10-59 A		
Let us know how we are	Signal received, Event state got Locked Out Creating Snapshots for User aw vast 2 - tijle ave2024 superna.ne Write a comment Snapshots Shares	c2024.superna.net\user2 test Success	sfully created snapshot vast2 - IgIs swc20	24.superna.net user2 trest-default-smb	share2-17_391-1723561135999. Su	ccessfully created snapshot 10-59 A		

Figure 21: 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:

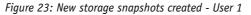
fistory						
					Show	w Security Guard 🔵
s 7 days i Severity is Critical+2	Threat Category 0	Items Affected 🗘	Source Cluster 0	State 0	Detected at 0	Timer 0
	Suspicious Activity	80	vast2	Locked Out	08/13/2024 2:27 PM 08/13/2024 2:27 PM	X 3:56:44
	AL user1@avc2024.superna.net	Uter 0     Threat Category 0       AL     userl@avc2024.superna.net     Suspicious Activity       AL     user2@avc2024.superna.net     Suspicious Activity	User 0     Threat Category 0     Items Affected 0       AL     user1@avc2024.superna.net     Suspicious Activity     80       AL     user2@avc2024.superna.net     Suspicious Activity     80	User 0 Threat Category 0 Items Affected 0 Source Cluster 0 AL usert@avc2024.superna.net Suspicious Activity 80 vast2	Uter o     Threat Category o     Items Affected o     Source Cluster o     State o       AL     userl@avc2024.superna.net     Suspicious Activity     80     vast2     Locked Out       AL     user2@avc2024.superna.net     Suspicious Activity     80     vast2     Locked Out	User 0       Threat Category 0       Items Affected 0       Source Cluster 0       State 0       Detected at 0         AL       userl@avc2024.superna.net       Suspicious Activity       80       vast2       Locked Out       08/13/2024.2.27 PM         AL       user2@avc2024.superna.net       Suspicious Activity       80       vast2       Locked Out       08/13/2024.2.27 PM

As during the previous iterations, share write access was quickly removed for both users.



S Data Security		* •
🖇 Alerts	← CRITICAL Supplicious Activity Pattern Suspicious user action on data was detected. Detected Uccked Out 08/13	ed at User /2024 2:27 PM user1@avc2024.superna.net
88 Dashboard 🖻 Jobs 8 Security Guard	English     Create Snapshot     Archive as Unresolvable     Restore User Access     4 minutes 52 seconds     2 hours 55	Source IP Address minutes 7 seconds 10.84.84.101
Settings	Overview Recovery Manager	
	Locked Out           Signal received; Event state going to LOCKED_OUT           Locked Out           Creating Stopphots for User avc2024 superna.net/usert Test Successfully created snapshot vast2 - Iglis-avc2024.superna.net/usert Test default-smb share2-17,336-1 vast2 - Iglis-avc2024.superna.net/usert Test default-smb share2-17,336-1 vast2 - Iglis-avc2024.superna.net/usert Test default-smb share2-17,336-1	2.57 FM 77235726639966. Successfully created snapshot 2.57 FM
	Locked Out Read only access set for tps [10.64.64.101] on following view policies: smb_policy Write a comment.	23795
	@ Snapshots	
	Igle avc2024.superna.net usert Test default-smb share2-17,395-1723573663996	01/20/1970 5:46 PM 👻
Send Feedback Let us know how we are doing?	tgle avc2024.superna.net usert Test delault-smb sharel+17,395-1723573663995	01/20/1970 5:46 PM ♥
-		
🖄 Return to Eyeglass	S User Alert History View All	

#### New storage snapshots were created for each event:



Alerts	CRITICAL	ous Activity Pattern us user action on data was detect	ted.	State Locker	Detected at d Out 08/13/2024 2:27 PM	User user2@avc2024.superna.net
Dashboard Jobs Security Guard	Create Snapshot	回 Archive as Unresolvable	26 Restore User Access	Duration 5 minutes 39 seconds	Expires 3 hours 54 minutes 20 seconds	Source IP Address 10.64.64.J02
Settings	Overview Recovery Manage	F				
	vast2 - Igls-avc2024.superna.n	vc2024.superna.net\user2 test Success	afully created snapshot vast2 - igits ave202 . smb.policy	4.superna.net user2 test-default-smb	share2-17,394-1723573663990. Suc	coessfully created snapshot 2.271
	Signal received; Event state ge Locked Out Creating Snaphots for User a vast?- jdjs ave2024.superna.n Locked Out Read only access set for ips (1) Write a comment	vc2024.superna.net\user2 test Success net-user2Read More	: snb.policy	M.auperna.net user2 test-default-smb	share2-17_394-1723573663993. Suc	2:081 constituity created snapshot 2:071 2:071 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2:072 2
	Signal received; Event state ge Locked Out Creating Supphotos for User a Vast2 - Iglia ave2004.superna.n Locked Out Read only access set for tps (1) Write a comment	wc2024.supperna.net(uner2 text Success net-uner2Read More 0.64.64.102] on following view policies	: smb_policy 73663983	M.auperna.net user2 test-default-smb	share2-17,394-1723573663990. Suc	constuly created snapshot 2.071 2.071
Send Foedback Let us know how we are doang?	Signal received; Event state ge Locked Out Creating Supphotos for User a Vast2 - Iglia ave2004.superna.n Locked Out Read only access set for tps (1) Write a comment	vc2024 supprena nefQueer? test Buccesse et user?Read More 0.64.64.102] on following view policies. Lest default- smb share2-17,394-172357	: smb_policy 73663983	4.superna.net user2 test-default-smb	share2-17,394-1722573663993. Suc	constituity created snapshot 2:271 2:271

Figure 24: 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 Compliance<sup>1</sup>

NIST Framework Attribute	How Superna Data Security Edition Complies	NIST Compliance Status
Identify	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



<sup>&</sup>lt;sup>1</sup> 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)

