Independent Tests of
Anti-Virus Software

Single Product Test

Commissioned by Superna

TEST PERIOD: NOVEMBER 2020
LANGUAGE: ENGLISH
LAST REVISION: 13TH NOVEMBER 2020

WWW.AV-COMPARATIVES.ORG

Introduction

This report has been commissioned by Superna.
The product Superna Eyeglass 2.5.7-20153 has been tested in November 2020.

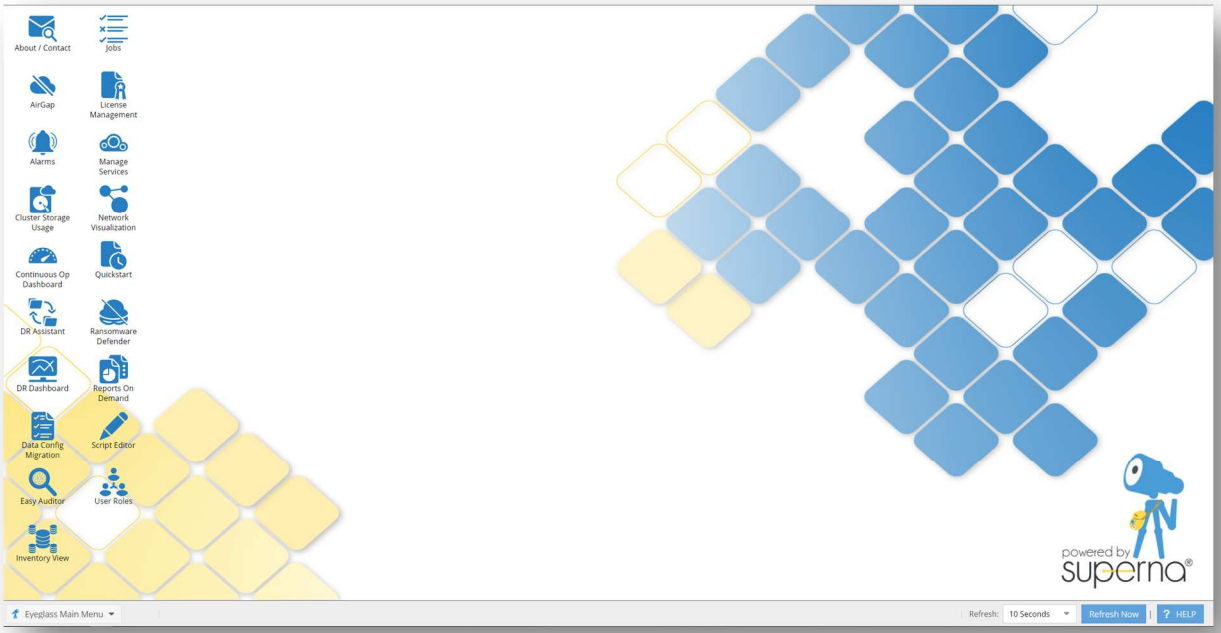

Figure 1: Superna Eyeglass - Webinterface

Superna Eyeglass Ransomware Defender 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 with this.

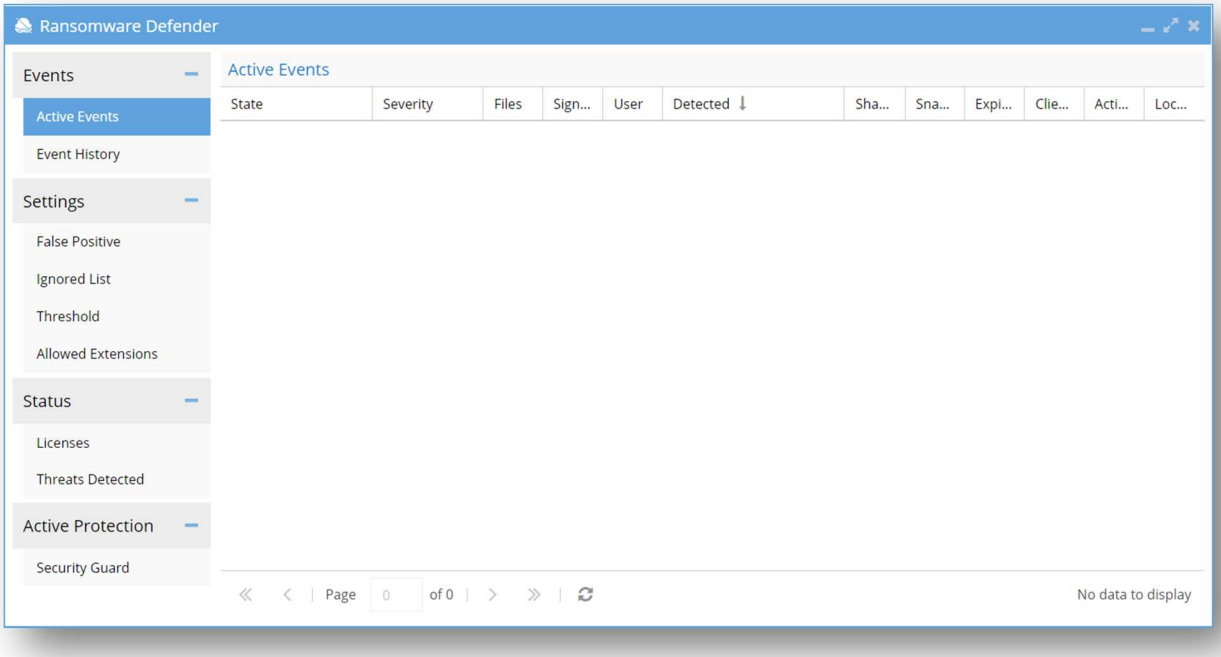

Figure 2: Ransomware Defender

Ransomware Defender 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. A notification is immediately sent to the administrator when ransomware activity is spotted and a user is blocked. 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.

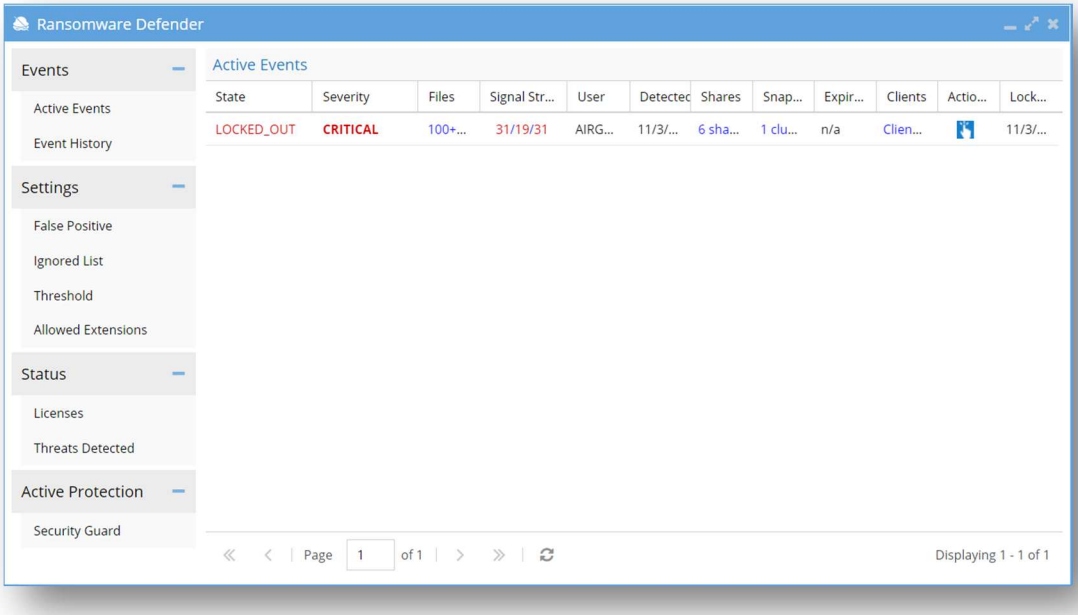

Figure 3: Ransomware Defender – Detection

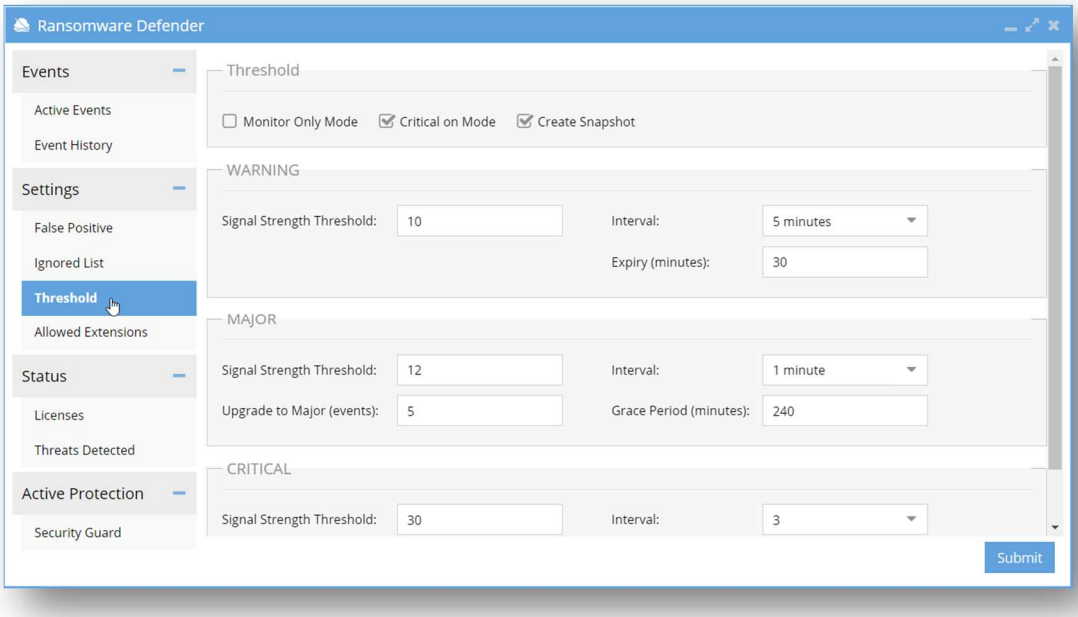

Figure 4: Ransomware Defender – Threshold

Ransomware Defender integrates AirGap Cyber Vault capabilities with the ability to suspend data copy operations automatically when the source data is under threat. Superna's Rapid Recovery allows the offline data to be usable in < 2 hours regardless of the size of the data set protected. The Rapid recovery also restores SMB and NFS share definitions.

The deployment was provided in the form of OVF templates for the VMware vSphere platform. A web-based interface was provided to manage the product.

Test Configuration

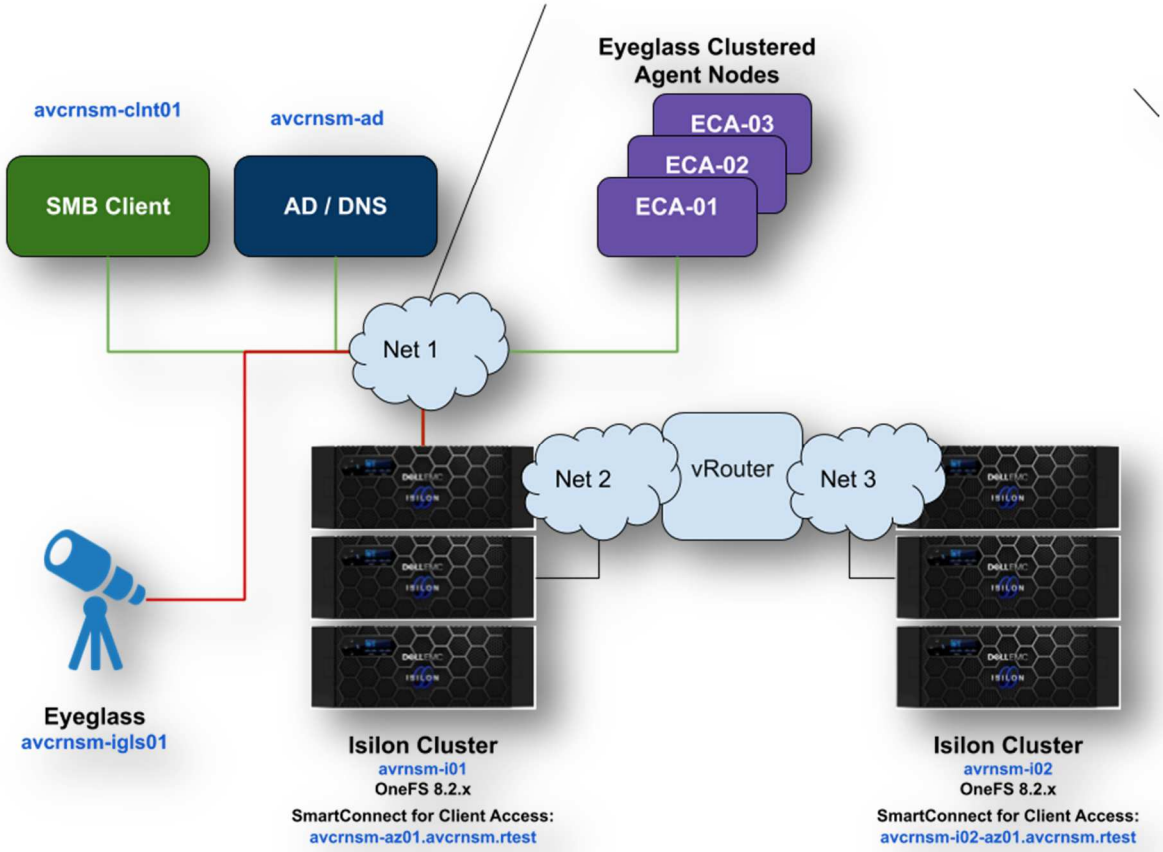

Figure 5: Infrastructure

Test scenario

Two ransomware samples will be executed manually on a client with connected shares. Superna Eyeglass Ransomware Defender will be in "Enforcement Mode".

Shares

Four shares are mapped to the cluster avrnsm-i01 (cf. Figure 5: Infrastructure) as network drives to the client before the sample will be executed. The shares' content was provided by Superna containing different types of documents.

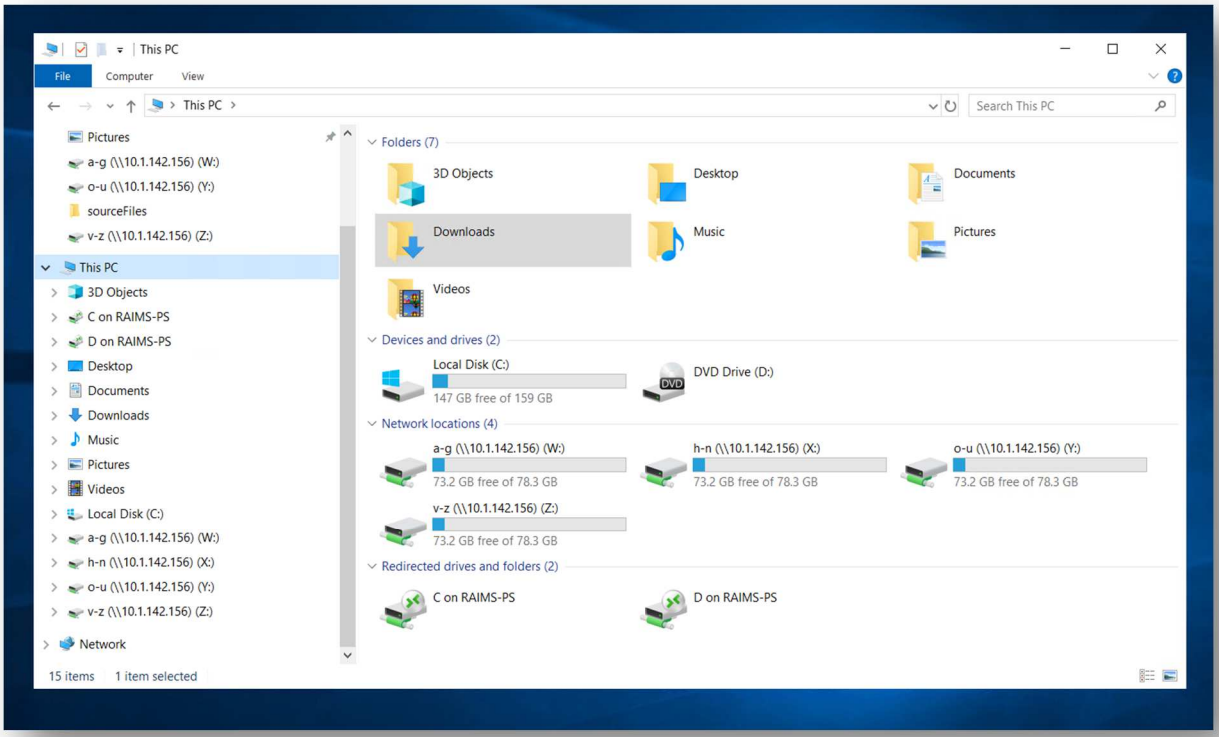

Figure 6: Shares on Windows 10

Client

Windows 10 64-bit English

Sample Selection

Two ransomware sample families, Wasted Locker and DoppelPaymer, will be used. These ransomware families had been chosen by Superna as known variants that attack network attached drives.

Test Result

The samples encrypted several files on the client and the storage cluster. The number of encrypted files on the cluster before detection and user lockout is dependent on the user behavior threshold settings.

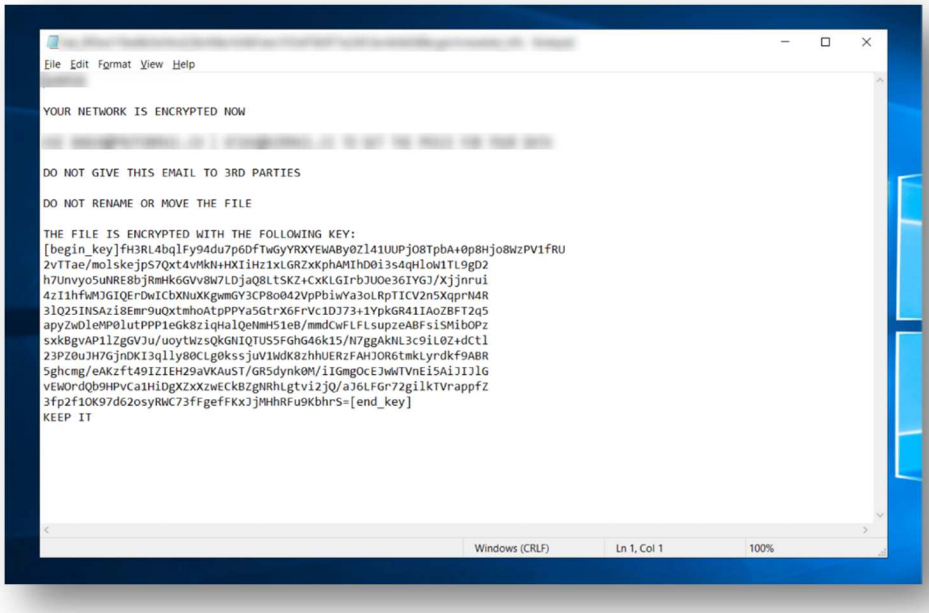

Figure 7: Wasted Locker

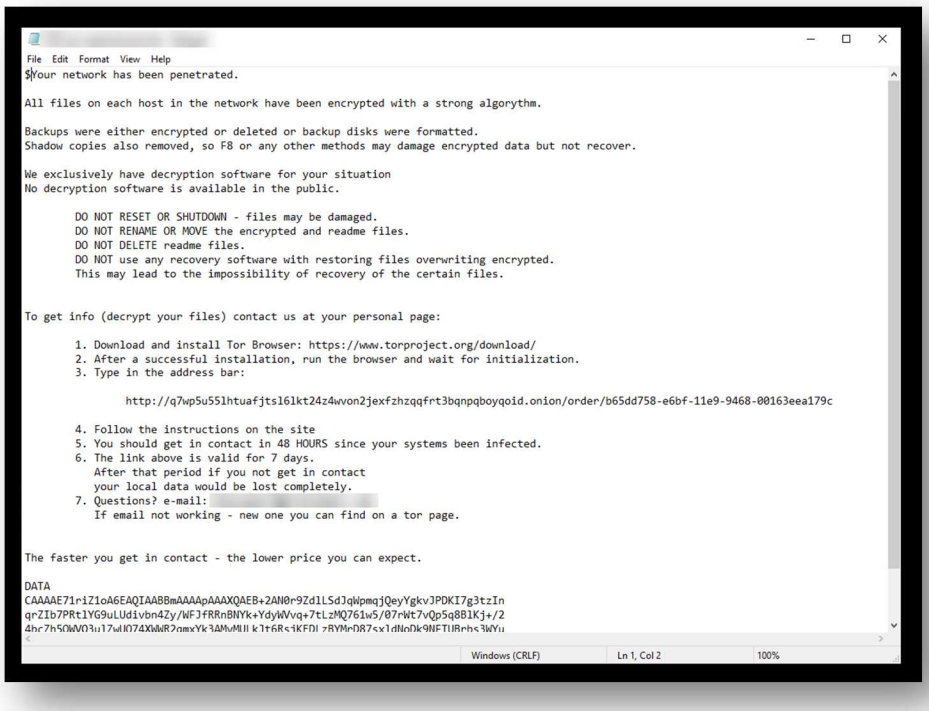

Figure 8: DoppelPaymer

Superna Eyeglass Ransomware Defender worked as expected and locked the user out from the storage cluster, halting the propagation of file encryptions after reaching the threshold. On the client the four shares were no longer accessible.

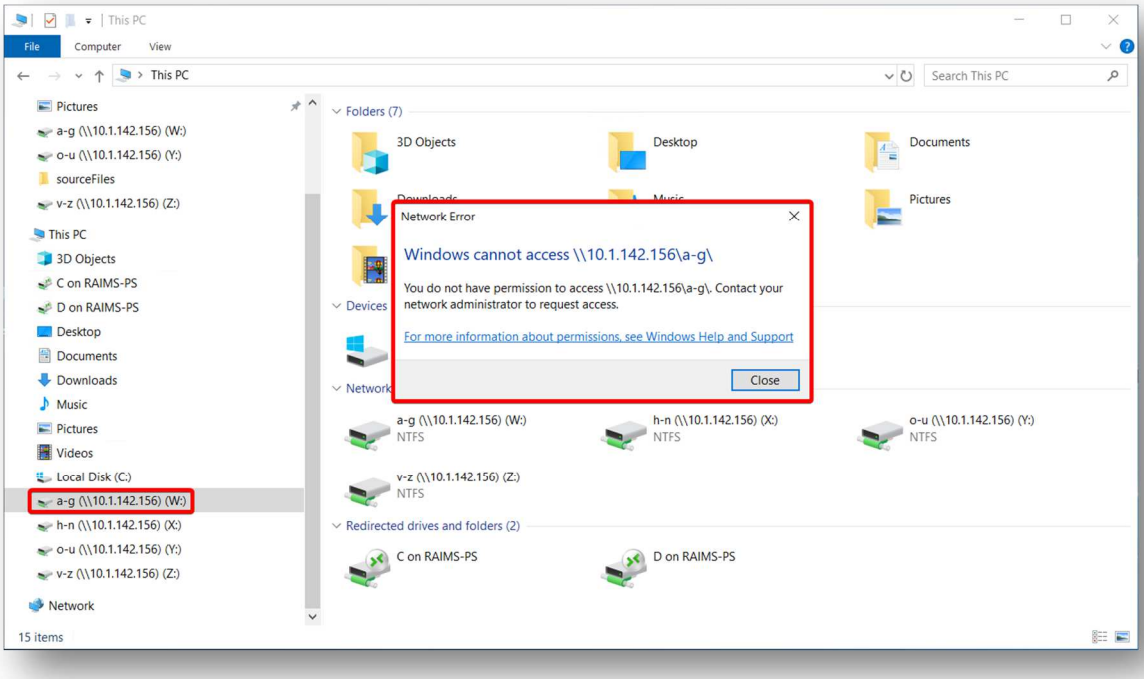

Figure 9: User locked out of Shares

Ransomware Defender shows the lockout within Active Events on the Eyeglass web interface. The user has the ability to resolve the Action, which will lead to enable access to the shares.

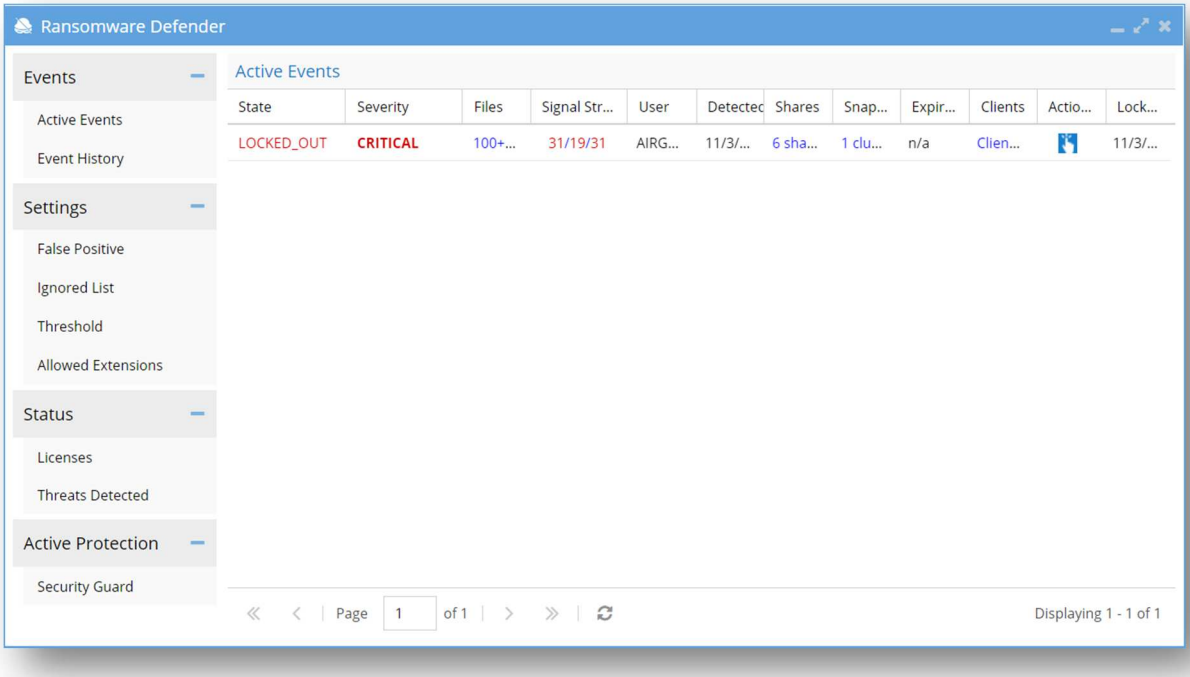

Figure 10: Ransomware Defender - User locked out from shares

The storage device has filesystem snapshots applied by Superna that allows data recovery in a multi-user infection attack scenario.

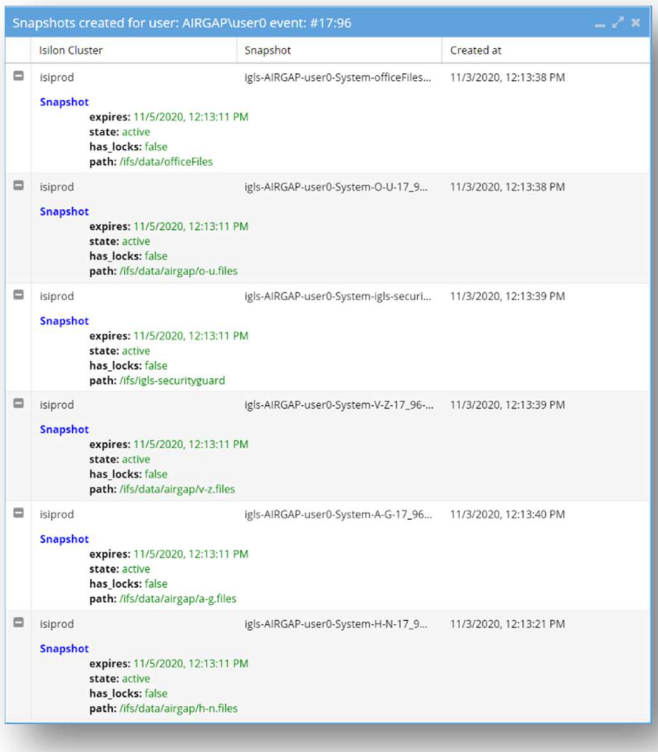

Figure 11: Snapshots

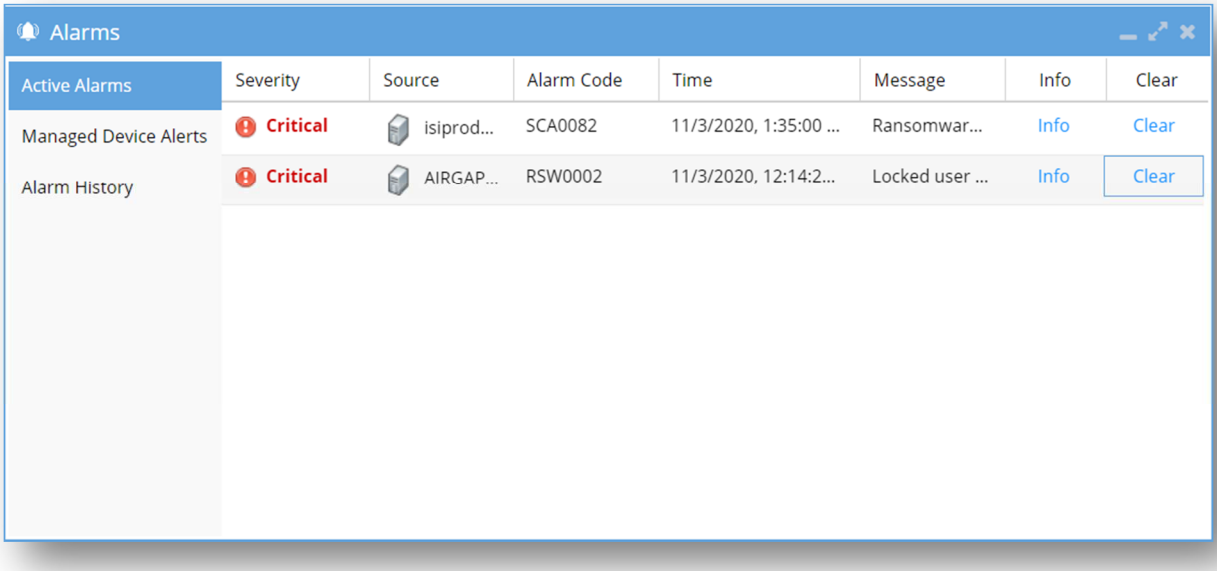

Figure 12: Superna Eyeglass - Alarms

AirGap stopped replication to the Cyber vault copy of the offline data until the Active Security Event is resolved.

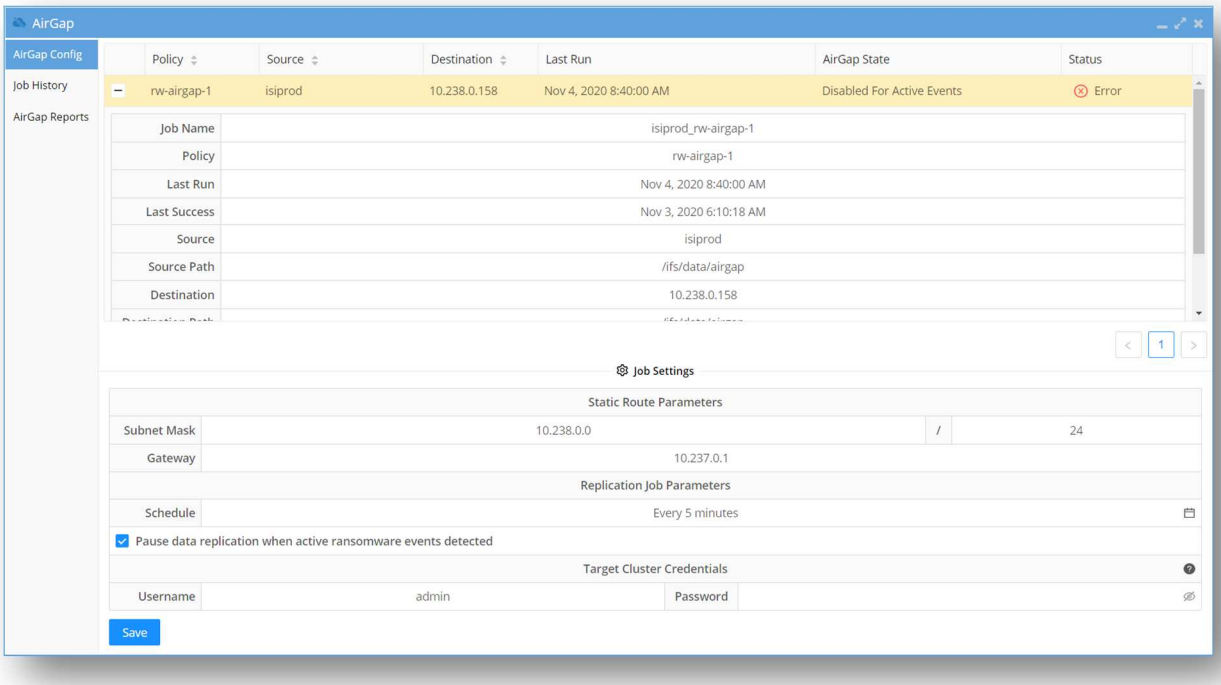

Figure 13: AirGap - Disabled after Ransomware Detection

Superna Ransomware Defender also allows a restore user access function once the file system restore has been completed.

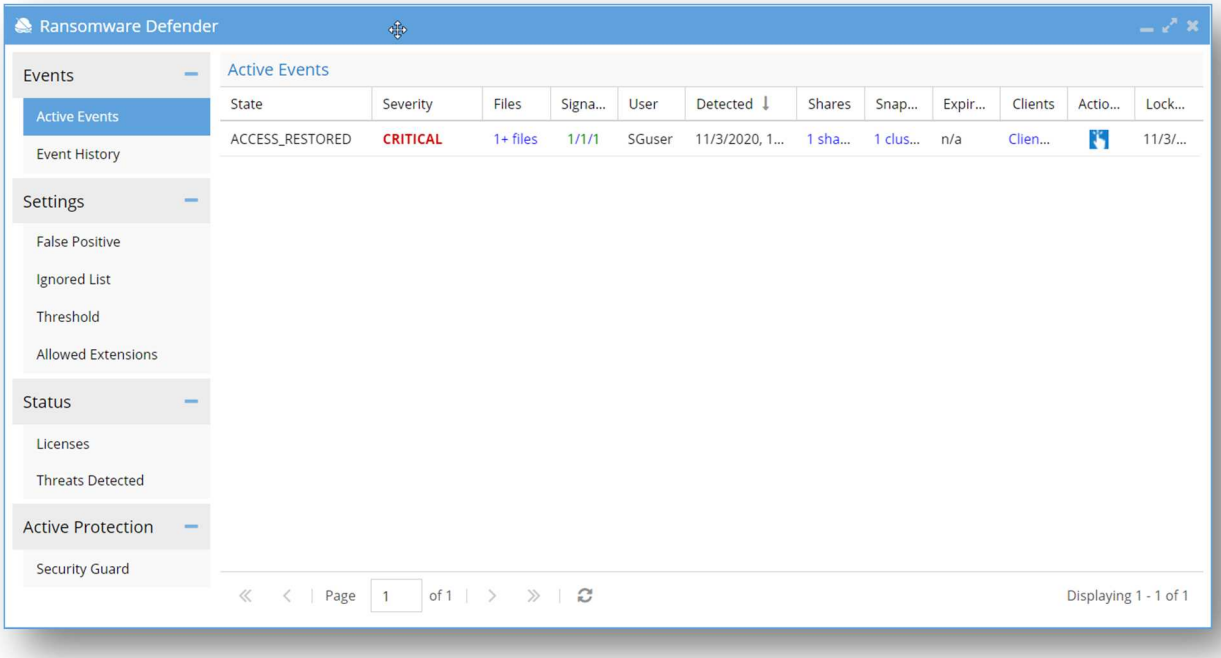

Figure 14: Access Restored

Copyright and Disclaimer

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

AV-Comparatives
(November 2020)