Enterprise Strategy Group by TechTarget

TECHNICAL VALIDATION

Proactive Cybersecurity for Unstructured Data with RackTop

Protection from Ransomware, Data Exfiltration, and Malicious Insiders

By Craig Ledo, IT Validation Analyst
Enterprise Strategy Group

March 2023

Contents

Introduction

This Technical Validation from TechTarget's Enterprise Strategy Group (ESG) documents the detailed evaluation of the RackTop BrickStor Security Platform (SP), including proactive data security, all-in-one Cyberstorage protection, and ease of use.

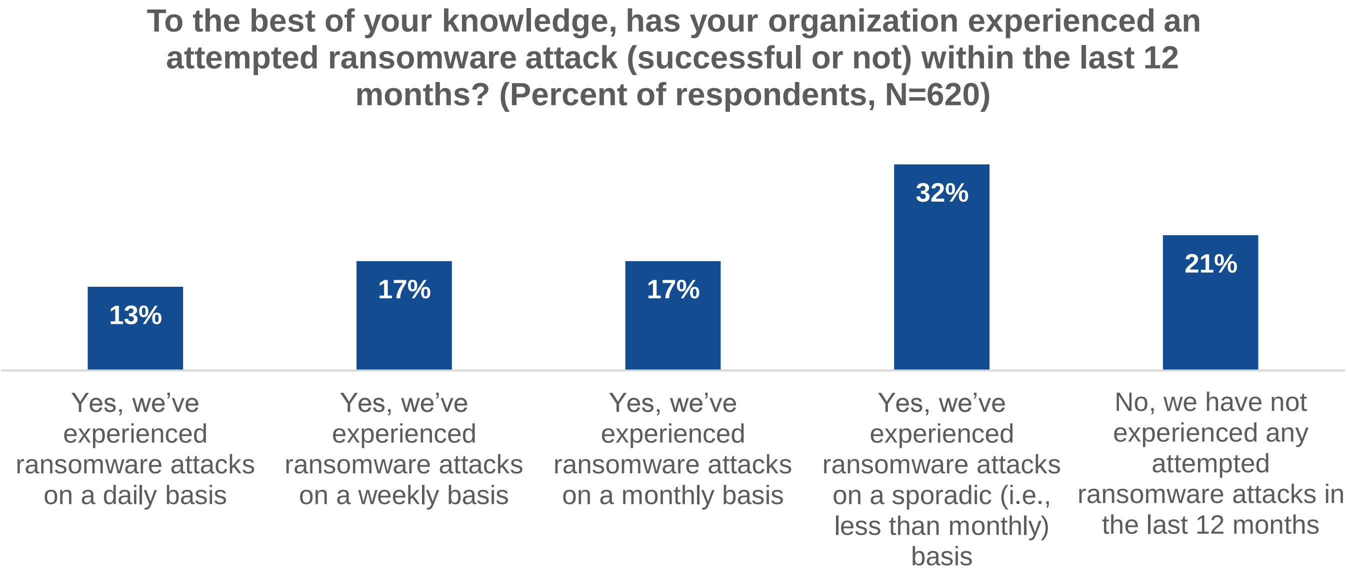
Background

Ransomware attacks continue to be top of mind for organizations and IT leaders since data is critical to the business. In addition, ransomware attacks have led to tremendous business costs, including downtime, people time, device costs, network cost, lost opportunities, ransom paid, and so on. Unfortunately, many organizations still underestimate the strategic value of augmenting data security.

Enterprise Strategy Group research shows that 79% of respondent organizations reported that they experienced a ransomware attack within the last year, including 17% that said they experienced attacks on a monthly basis, 17% that were attacked weekly, and 13% that were targeted daily. 32% of the respondents experienced ransomware attacks more sporadically (see Figure 1).[1]

This is why it's critical for organizations to implement strong defenses against ransomware attacks and to address attacks before, during, and after they occur, especially since organizations may be revisited by these criminals.

Figure 1. 79% of Organizations Reported That They Experienced a Ransomware Attack within the Last Year



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

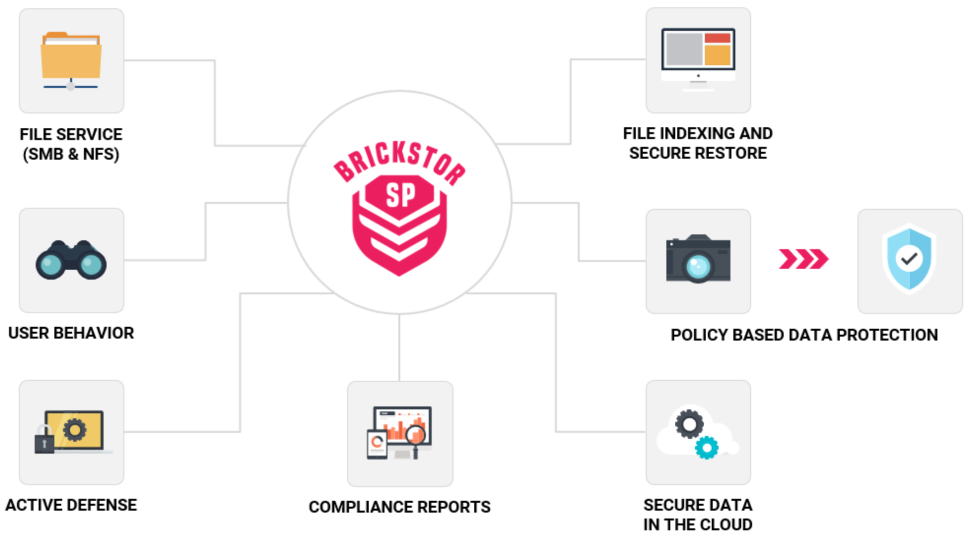
[1] Source: Enterprise Strategy Group Research Report, *The Long Road Ahead to Ransomware Preparedness*, June 2022.

RackTop Solution Overview

RackTop provides a Cyberstorage solution, BrickStor SP, which stores and actively defends unstructured data from ransomware, data theft, and insider threats (see Figure 2). The BrickStor SP software can be deployed on-premises, at the edge, or in the cloud to actively secure data anywhere. The solution delivers Cyberstorage capabilities in a single product, which includes a data-centric zero trust architecture. This architecture places critical protections close to the data in order to uniquely identify, protect, detect, respond to, and recover from advanced persistent threats (APTs). In addition, the data security stack addresses the entire data continuum, including minimizing the threat window, actively detecting and stopping data-oriented attacks, and facilitating remediation and recovery. RackTop BrickStor SP has many key benefits, including that it:

- Uses open standards, uses a modern user interface, and can be implemented in any modern IT environment and maintained by IT generalists.
- Includes data protection capabilities that orchestrate data versioning, replication, retention, and disposition.
- Eliminates complex and disparate tools, resulting in a unified, simple to manage, and secure data protection solution.
- Includes a secure data archive with transparent tiering to S3-compatible object solutions.
- Can be deployed in front of existing enterprise storage capacity, as a turnkey appliance, or as a virtual machine.
- Provides advanced user behavior auditing and analysis, as well as automatic incident reporting.
- Can share data securely using common file protocols (SMB, NFS).
- Is compliance-ready (SOX, NIST, RMF, HIPAA) and integrates with SIEMs, SOARs, and third-party APIs.

Figure 2. RackTop BrickStor SP Solution Overview



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Enterprise Strategy Group (ESG) Technical Validation

ESG performed a technical validation of the RackTop BrickStor SP, including proactive data security, all-in-one Cyberstorage protection, and ease of use.

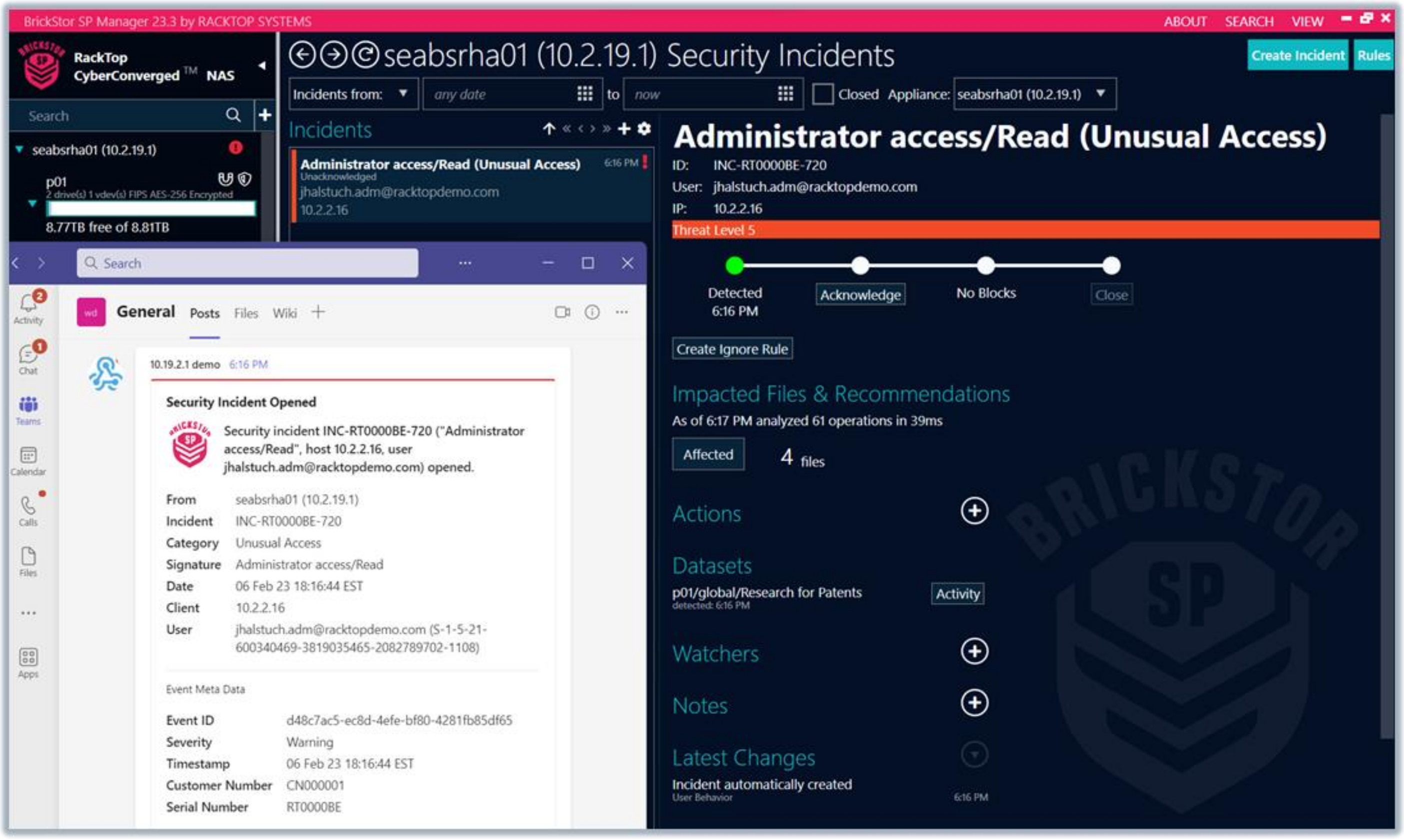
Proactive Data Security

Enterprise Strategy Group (ESG) validated RackTop's proactive data security capabilities, including data security for primary and secondary data; protection against cyber-attacks, insider threats, malware, and data theft; and immutable snapshots. Proactive data security should include limiting or blocking an attack, which is always better than recovering from one.

RackTop proactively monitors normal accounts and privileged accounts (e.g., admin accounts). For example, if the system detects an unusual access (e.g., administrator access/read) or security incident, an alert will be sent to the security team to investigate (see Figure 3). The security team can also drill into the incident to see which files were affected.

In addition, users can create security incident rules (see "Create Ignore Rule" button in Figure 3).

Figure 3. Proactive Security Incident Detection



seabsrha01 (10.2.19.1)
p01
2 drive(s) 1 vdev(s) FIPS AES-256 Encrypted
8.77TB free of 8.81TB

Administrator access/Read (Unusual Access) 6:16 PM
Unacknowledged
jhalstuch.adm@racktopdemo.com
10.2.2.16

10.19.2.1 demo 6:16 PM

Security Incident Opened

Security incident INC-RT0000BE-720 ("Administrator access/Read", host 10.2.2.16, user jhalstuch.adm@racktopdemo.com) opened.

From	seabsrha01 (10.2.19.1)
Incident	INC-RT0000BE-720
Category	Unusual Access
Signature	Administrator access/Read
Date	06 Feb 23 18:16:44 EST
Client	10.2.2.16
User	jhalstuch.adm@racktopdemo.com (S-1-5-21-600340469-3819035465-2082789702-1108)

Event Meta Data

Event ID	d48c7ac5-ec8d-4efe-bf80-4281fb85df65
Severity	Warning
Timestamp	06 Feb 23 18:16:44 EST
Customer Number	CN000001
Serial Number	RT0000BE

Administrator access/Read (Unusual Access)

ID: INC-RT0000BE-720
User: jhalstuch.adm@racktopdemo.com
IP: 10.2.2.16
Threat Level 5

Impacted Files & Recommendations
As of 6:17 PM analyzed 61 operations in 39ms
Affected 4 files

Datasets
p01/global/Research for Patents
detected: 6:16 PM

Latest Changes
Incident automatically created 6:16 PM
User Behavior

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

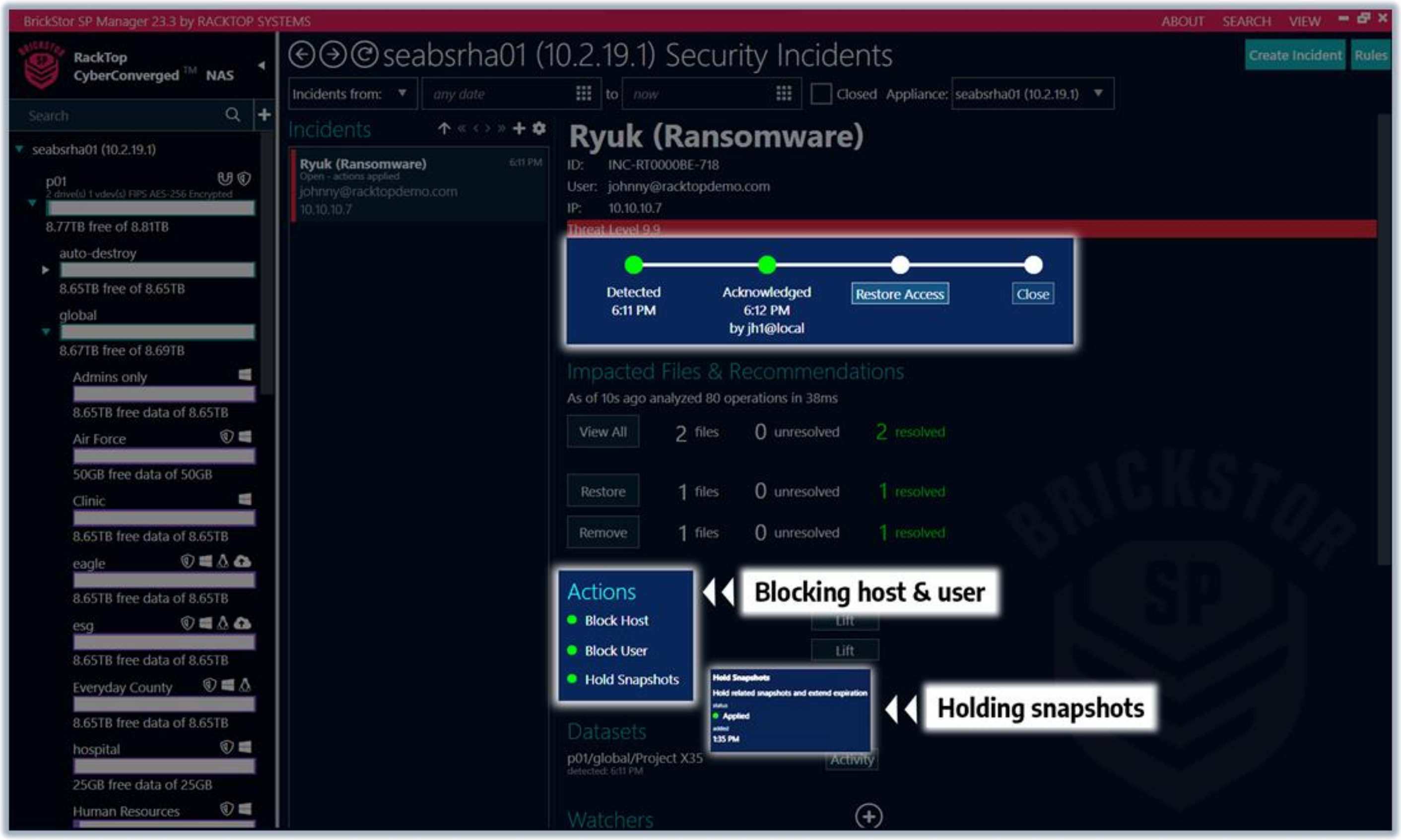
During the demonstration, a Ryuk ransomware attack was detected (see Figure 4). The user can take action on this ransomware incident by acknowledging the attack, investigating it, restoring access, and then closing the incident. In addition, the user can:

- **Block Host**: Block host IP from accessing shares.
- **Block User**: Block user from accessing shares.

In addition to immutable snapshots, users can hold related snapshots and extend expiration preventing administrative or accidental destruction.

Again, the security team can drill into the incident to see which files were affected and remove (i.e., delete file or quarantine file) or recover (i.e., restore) the appropriate files.

Figure 4. Security Incident Resolution



Ryuk (Ransomware)

ID: INC-RT0000BE-718
User: johnny@racktopdemo.com
IP: 10.10.10.7
Threat Level 9.9

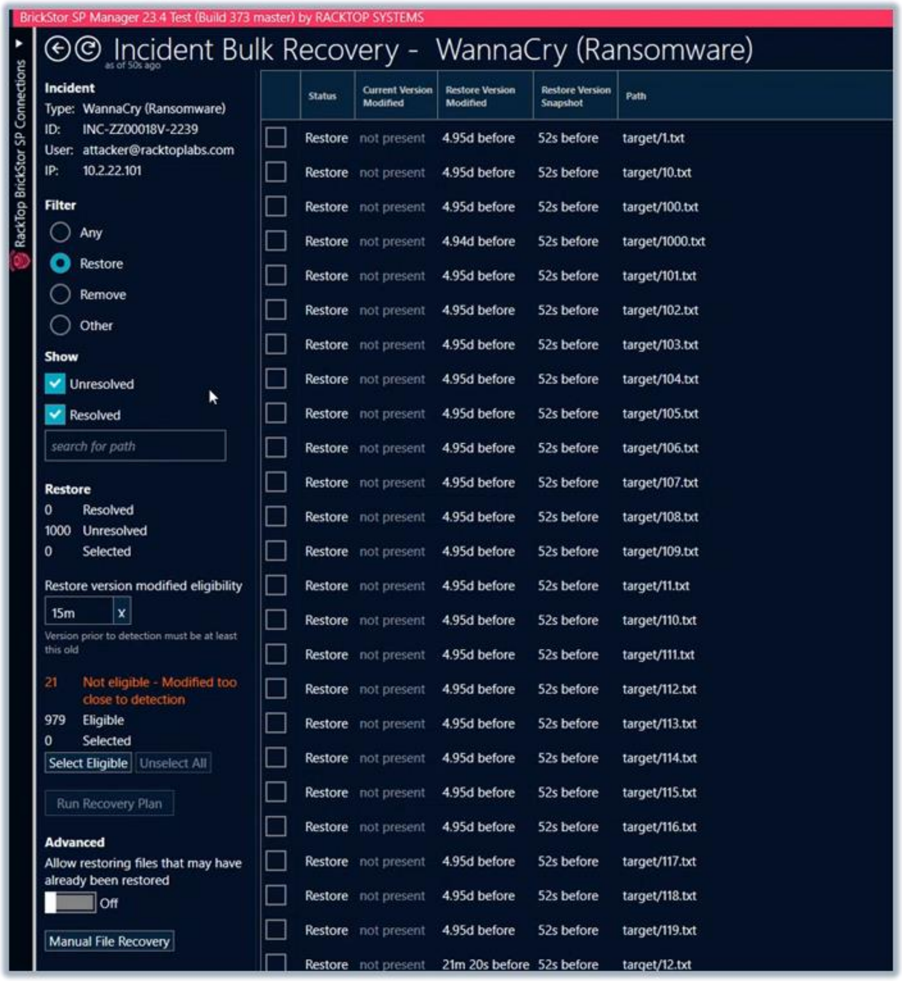
As of 10s ago analyzed 80 operations in 38ms

View All 2 files 0 unresolved 2 resolved
Restore 1 files 0 unresolved 1 resolved
Remove 1 files 0 unresolved 1 resolved

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Removing and recovering files can all be quickly managed from this user interface (see Figure 5). The incident management window analyzes and recommends what files should be removed and restored based by the user for rapid return to service.

Figure 5. Recovery and Removal of Files



BrickStor SP Manager 23.4 Test (Build 373 master) by RACKTOP SYSTEMS

Incident Bulk Recovery - WannaCry (Ransomware)

as of 50s ago

Incident
Type: WannaCry (Ransomware)
ID: INC-ZZ00018V-2239
User: attacker@racktoplabs.com
IP: 10.2.22.101

Filter
○ Any
● Restore
○ Remove
○ Other

Show
☑ Unresolved
☑ Resolved

search for path

Restore
0 Resolved
1000 Unresolved
0 Selected

Restore version modified eligibility
15m x
Version prior to detection must be at least this old

21 Not eligible - Modified too close to detection
979 Eligible
0 Selected

Select Eligible | Unselect All

Run Recovery Plan

Advanced
Allow restoring files that may have already been restored
Off

Manual File Recovery

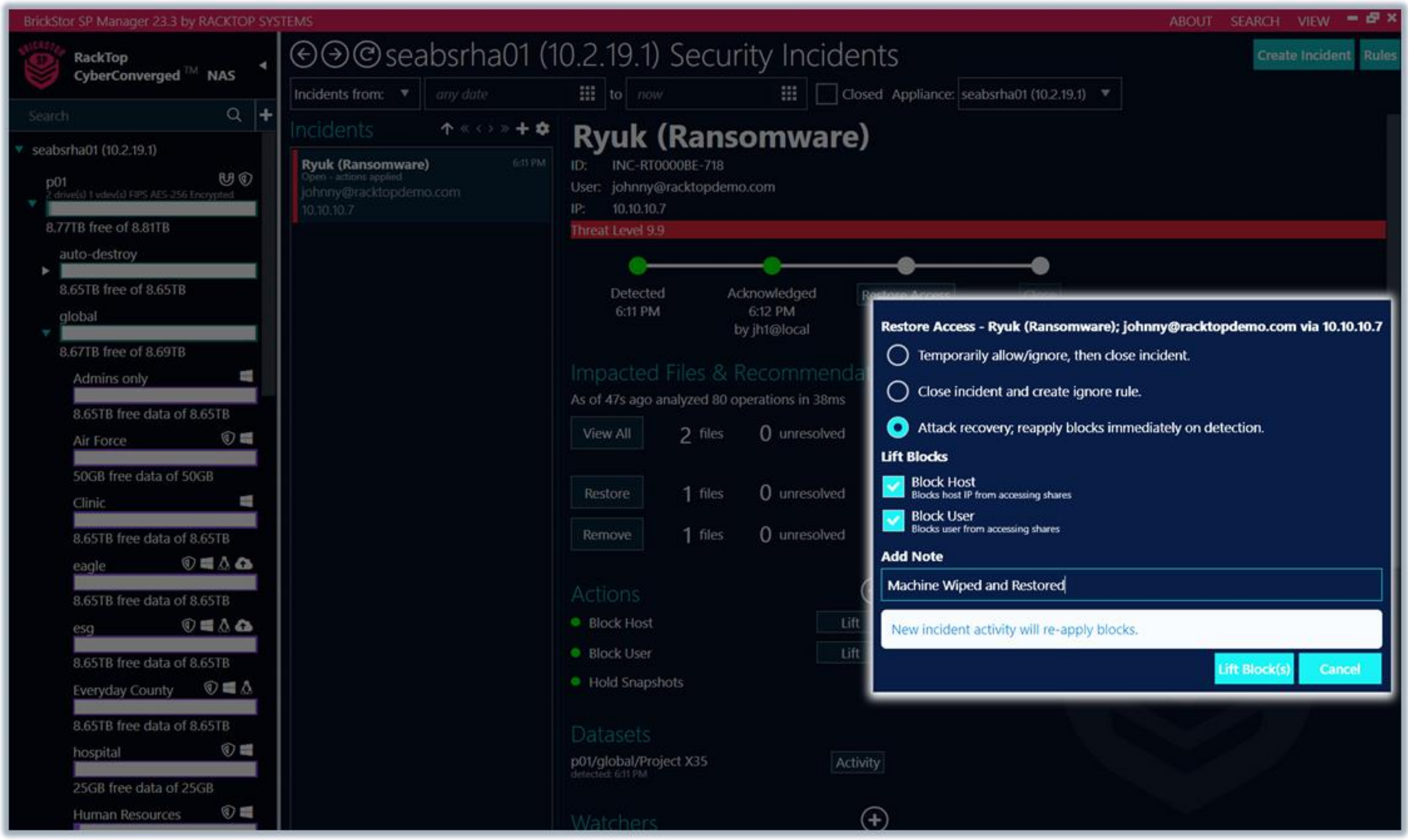
	Status	Current Version Modified	Restore Version Modified	Restore Version Snapshot	Path
□	Restore	not present	4.95d before	52s before	target/1.txt
□	Restore	not present	4.95d before	52s before	target/10.txt
□	Restore	not present	4.95d before	52s before	target/100.txt
□	Restore	not present	4.94d before	52s before	target/1000.txt
□	Restore	not present	4.95d before	52s before	target/101.txt
□	Restore	not present	4.95d before	52s before	target/102.txt
□	Restore	not present	4.95d before	52s before	target/103.txt
□	Restore	not present	4.95d before	52s before	target/104.txt
□	Restore	not present	4.95d before	52s before	target/105.txt
□	Restore	not present	4.95d before	52s before	target/106.txt
□	Restore	not present	4.95d before	52s before	target/107.txt
□	Restore	not present	4.95d before	52s before	target/108.txt
□	Restore	not present	4.95d before	52s before	target/109.txt
□	Restore	not present	4.95d before	52s before	target/11.txt
□	Restore	not present	4.95d before	52s before	target/110.txt
□	Restore	not present	4.95d before	52s before	target/111.txt
□	Restore	not present	4.95d before	52s before	target/112.txt
□	Restore	not present	4.95d before	52s before	target/113.txt
□	Restore	not present	4.95d before	52s before	target/114.txt
□	Restore	not present	4.95d before	52s before	target/115.txt
□	Restore	not present	4.95d before	52s before	target/116.txt
□	Restore	not present	4.95d before	52s before	target/117.txt
□	Restore	not present	4.95d before	52s before	target/118.txt
□	Restore	not present	4.95d before	52s before	target/119.txt
□	Restore	not present	21m 20s before	52s before	target/12.txt

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Once the user has removed and/or recovered the files and removed any malware, etc., access can then be restored, including lifting blocks (e.g., Block Host and Block User). Figure 6 shows how access can be restored, including the following options:

- Temporarily allow/ignore, then close incident.
- Close incident and create ignore rule.
- Attack recovery, bulk/manually reapply blocks immediately on detection.

Figure 6. Restoring Access



Ryuk (Ransomware)

ID: INC-RT0000BE-718
User: johnny@racktopdemo.com
IP: 10.10.10.7
Threat Level 9.9

As of 47s ago analyzed 80 operations in 38ms

Restore Access - Ryuk (Ransomware); johnny@racktopdemo.com via 10.10.10.7

○ Temporarily allow/ignore, then close incident.

○ Close incident and create ignore rule.

● Attack recovery; reapply blocks immediately on detection.

Lift Blocks

☑ Block Host
Blocks host IP from accessing shares

☑ Block User
Blocks user from accessing shares

Add Note

Machine Wiped and Restored

New incident activity will re-apply blocks.

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Why This Matters

According to Enterprise Strategy Group (ESG) research, more than half (56%) of organizations that have been victimized by a successful ransomware attack also admit to having paid a ransom to regain access to data, applications, or systems. However, paying the ransom does not guarantee the recovery of data. Only 14% reported getting all of their data back post-payment.[2] Also, traditional data protection schemas which consist of daily full backups can take hours, if not days, to recover.

ESG validated that RackTop's Cyberstorage solution provides unified file services, plus detects and prevents cyber-attacks on data before they impact the business. Proactively limiting or blocking (e.g., block host, block user) an attack before it impacts the business is always better than recovering from one.

[2] Source: Enterprise Strategy Group Research Report, *The Long Road Ahead to Ransomware Preparedness*, June 2022.

All-in-One Cyberstorage Protection

Enterprise Strategy Group (ESG) validated RackTop's all-in-one solution for Cyberstorage security. RackTop replaces legacy solutions and includes new storage and data protection technologies that are designed to actively defend unstructured data from cyber-attacks. BrickStor SP addresses all three phases of a cyber-attack:

- **Before**: Cyber-hygiene.
- **During**: Active defense.
- **After**: Remediation and recovery.

Specifically, with its Cyberstorage platform to actively defend data, BrickStor SP addresses the five functional areas of the NIST Cybersecurity Framework: **Identify, Protect, Detect, Respond, and Recover**.

- Before: BrickStor's user and entity behavior analysis (UEBA) and security orchestration automation and response (SOAR) **identify** fingerprints (or baseline behaviors) to **protect** data in the event of a ransomware attack or other data breach.
- During: Each file transaction is evaluated in real time to **detect** and **respond** to anomalous behaviors that might encrypt or extort data. As soon as unusual behavior is detected, BrickStor SP can respond and stop attacks in real time to enable organizations to recover files instantly.
- After: The **recover** function supports the timely return to service to reduce the impact from a cybersecurity incident.

BrickStor SP can evaluate trust for each file operation without negatively affecting user experience or application performance. BrickStor SP also satisfies all the requirements of the data pillar for the CISA Zero Trust Maturity Model. So, organizations can adopt a data-centric zero trust architecture seamlessly, while meeting the requirements of the Cybersecurity Executive Order and the CISA Zero Trust Maturity Model without having to change workflows or user behaviors.

Why This Matters

Enterprise Strategy Group (ESG) created a ransomware preparedness segmentation model that placed survey respondents into one of four stages of maturity based on their organization's technology and processes in place across the five NIST categories. ESG believes that these five categories speak significantly to overall ransomware preparedness. Using this segmentation model, 15% of respondent organizations are classified as ransomware preparedness leaders. Nearly one in four (23%) fall into the maturing category, one-third (33%) are aspiring, and 29% are still novices.[3]

ESG believes the BrickStor SP architecture provides an all-in-one solution that places critical protections close to the data in order to uniquely identify, protect, detect, respond, and recover from cyber-threats. This solution could help any organization significantly improve their ransomware preparedness.

Ease of Use

Enterprise Strategy Group (ESG) validated RackTop's ease of use. The RackTop solution is 100% agentless and operates on-premises, at the edge, or in the cloud. And in most instances, it can be installed in a few minutes and protecting data in less than 1 hour.

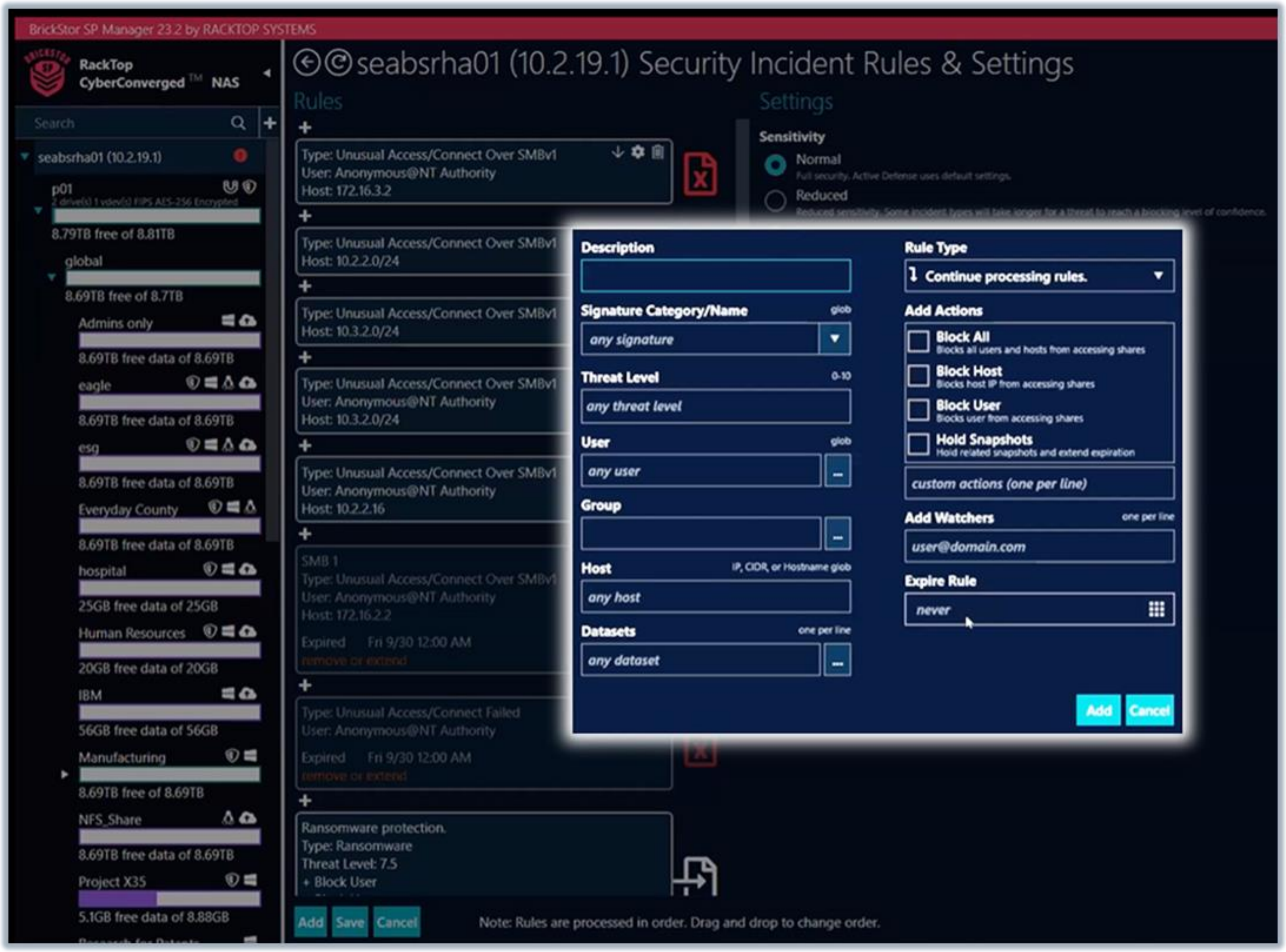
Users can customize the security incident rules, which include the following information: description, signature/category name, threat level, user, group, host, data sets, rule type, add actions (block all, block host,

[3] Source: Enterprise Strategy Group Brief, *State of the Ransomware Preparedness Market*, December 2022.

block user, hold snapshots), add watchers, and expire rule (see Figure 7). In addition, users can also customize the settings as follows:

- **Normal**: Full security. Active defense uses default settings.
- **Reduced**: Reduced sensitivity. Some incident types will take longer for a threat to reach a blocking level of confidence.
- **Low**: Notify only. Incidents are created, but actions such as block will not occur.
- **Off**: Active defense disabled. Threat detection and blocking will not occur.

Figure 7. Security Incident Rules and Settings



BrickStor SP Manager 23.2 by RACKTOP SYSTEMS

RackTop CyberConverged™ NAS

seabsrha01 (10.2.19.1) Security Incident Rules & Settings

Rules

Type: Unusual Access/Connect Over SMBv1
User: Anonymous@NT Authority
Host: 172.16.3.2

Type: Unusual Access/Connect Over SMBv1
Host: 10.2.2.0/24

Type: Unusual Access/Connect Over SMBv1
Host: 10.3.2.0/24

Type: Unusual Access/Connect Over SMBv1
User: Anonymous@NT Authority
Host: 10.3.2.0/24

Type: Unusual Access/Connect Over SMBv1
User: Anonymous@NT Authority
Host: 10.2.2.16

SMB 1
Type: Unusual Access/Connect Over SMBv1
User: Anonymous@NT Authority
Host: 172.16.2.2
Expired Fri 9/30 12:00 AM
remove or extend

Type: Unusual Access/Connect Failed
User: Anonymous@NT Authority
Expired Fri 9/30 12:00 AM
remove or extend

Ransomware protection.
Type: Ransomware
Threat Level: 7.5
+ Block User

Add | Save | Cancel

Note: Rules are processed in order. Drag and drop to change order.

Settings

Sensitivity
● Normal
Full security. Active Defense uses default settings.
○ Reduced
Reduced sensitivity. Some incident types will take longer for a threat to reach a blocking level of confidence.

Description:

Signature Category/Name (glob): any signature

Threat Level (0-10): any threat level

User (glob): any user

Group:

Host (IP, CIDR, or Hostname glob): any host

Datasets (one per line): any dataset

Rule Type: Continue processing rules.

Add Actions
□ Block All — Blocks all users and hosts from accessing shares
□ Block Host — Blocks host IP from accessing shares
□ Block User — Blocks user from accessing shares
□ Hold Snapshots — Hold related snapshots and extend expiration

custom actions (one per line)

Add Watchers (one per line): user@domain.com

Expire Rule: never

Add | Cancel

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

The BrickStor SP Manager also includes compliance reports that help organizations meet cybersecurity and regulatory frameworks. There are 25 categories of compliance reports, including data encryption, key management, privileged access management, administrator auditing, user behavior auditing, and data retention. Some of the compliance reports demonstrated included:

- **Access by Permission Type**: Access types granted to users, groups, and shares.
- **Access by User/Group**: Shares a user/group can access.
- **Host Based Permissions**: Permissions granted to share clients.
- **Host Based Access by Host**: Shares a client can access.
- **Host Based Access by Permission Type**: Access granted to share clients.

Compliance reports can be exported to PDF, CSV, or printed.

Why This Matters

Enterprise Strategy Group (ESG) research shows that while the majority of organizations do have some kind of incident response capabilities in place, only 13% have formal retainer agreements with incident response firms. Almost two-thirds (63%) of organizations are staffing response functions with their own incident responders, while more than half (53%) are also depending on managed detection and response providers to help.[4] The use of managed detection and response providers has quickly become a core strategy for security teams to overcome skills and coverage shortages.

ESG reviewed RackTop's installation and setup procedure and determined it is very easy to get the solution configured and up and running. In addition, it is very easy to address security issues using the solution's incident response and management user interface.

Conclusion

Ransomware attacks are one of the most challenging events a data-driven organization can experience. They disrupt organizations and can lead to immense recovery costs and damage to organizations' reputations. And with the rise of newer double and triple extortion-based attacks (which both steal and encrypt data), reliance on data protection and backup solutions alone is no longer sufficient. Organizations are constantly struggling to stay one step ahead of attackers. If attackers do find their way in, organizations need to be able to rely on their cybersecurity processes to identify, protect, detect, respond, and recover.

Enterprise Strategy Group (ESG) verified that the RackTop software-defined data storage solution demonstrates robust proactive data security capabilities in an all-in-one Cyberstorage package that is easy to use. BrickStor SP can be deployed as new capacity or on top of existing storage capacity to create high-performance secure network-attached storage. ESG validated that RackTop's BrickStor SP software-defined Cyberstorage, including unstructured data fortified with advanced security and compliance features, demonstrated simple and secure protection of an organizations' data.

Every organization should have a ransomware protection plan that includes a proven data security vendor that understands the multitude of challenges and has built a solution that incorporates zero trust principles into technology that detects and prevents attacks on data before it impacts the business. If your organization is looking for a solution that provides all-in-one proactive data security that is easy to use, ESG believes the BrickStor SP software-defined Cyberstorage solution is worth serious consideration. Plus, RackTop offers a 90-day Jumpstart program to try BrickStor SP for free.

[4] Source: Enterprise Strategy Group Research Report, *The Long Road Ahead to Ransomware Preparedness*, June 2022.

About Enterprise Strategy Group
Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community. © TechTarget 2023.

✉ contact@esg-global.com
🖥 www.esg-global.com