TECHNICAL VALIDATION

Nutanix Data Lens

Data Analytics for Ransomware Resilience

By Tony Palmer, Practice Director, Validation Services
Enterprise Strategy Group

October 2023

This Enterprise Strategy Group Technical Validation was commissioned by Nutanix and is distributed under license from TechTarget, Inc.

Contents

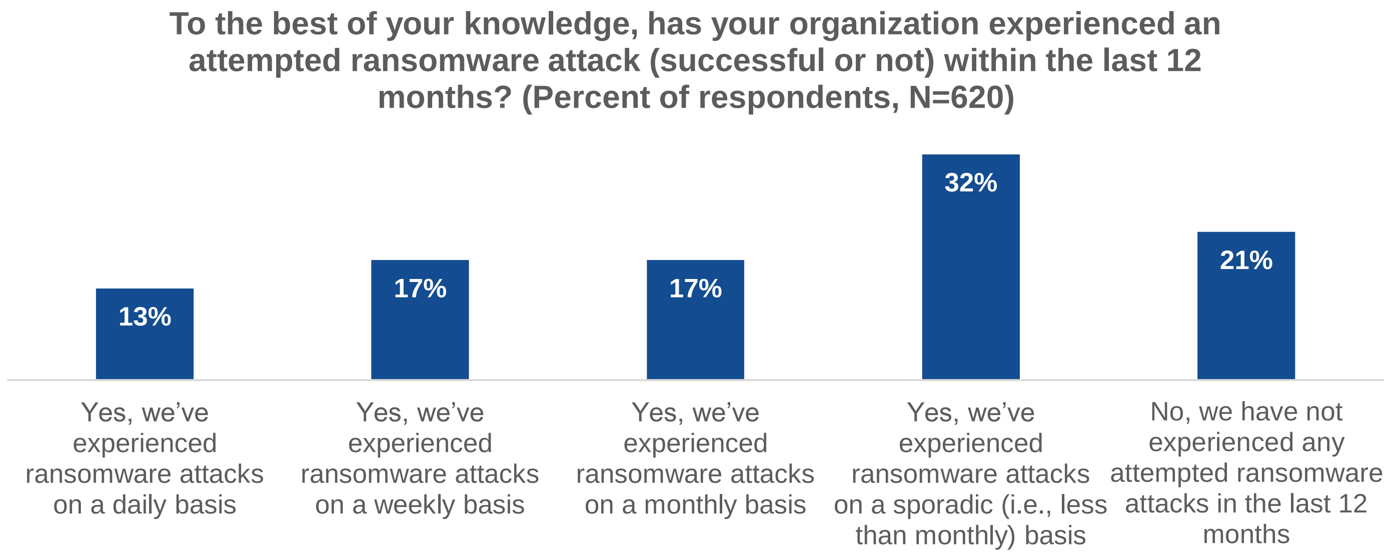
Introduction

TechTarget's Enterprise Strategy Group has examined Nutanix Data Lens and validated its ability to provide data security and data lifecycle management while supporting audits and compliance. Of particular interest is our evaluation of how Data Lens provides rapid detection of and response to active ransomware attacks.

Ransomware Challenges

Ransomware is pervasive and represents a serious threat to organizations of every size across industries. Recent Enterprise Strategy Group research revealed that most organizations have had to deal with ransomware attacks over the past 12 months. Specifically, 79% of organizations reported experiencing ransomware attacks at some point over the past 12 months, while 47% cited experiencing probing attacks on at least a monthly basis, including 13% that said they were targeted daily (see Figure 1).[1]

Figure 1. Rate of Ransomware Attacks



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

Among that population, nearly three-quarters (73%) report that they have been financially or operationally impacted by these attacks, making them "successful." It should also be noted that 32% of organizations report having been successfully hit more than once, making ransomware both a significant and recurring source of business disruption. It's important to note that many organizations don't report ransomware attacks, so this number is likely higher.

Without an industry reference architecture or blueprint for ransomware protection, many organizations are building their own strategies and processes to respond. A common foundation for these strategies is the NIST Cybersecurity Framework—standards, guidelines, and best practices to manage cybersecurity-related risk. NIST designed the framework to provide a prioritized, flexible, and cost-effective approach to promote the protection and resilience of IT infrastructure. To achieve true ransomware resiliency, an organization needs all of the functions defined in the framework: identify and detect attacks; protect from damage; determine the scope and respond; and recover operations quickly.

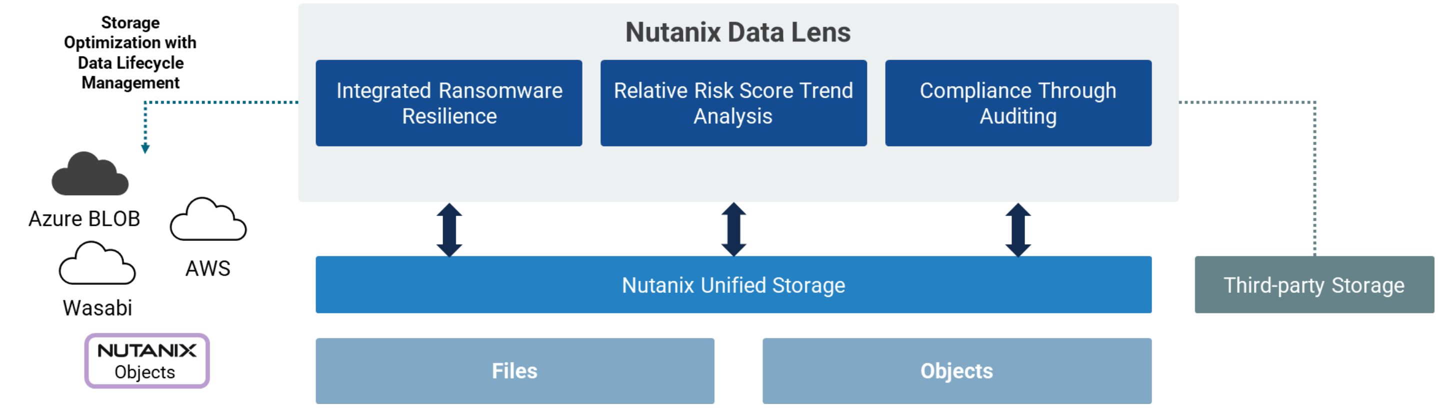
[1] Source: Enterprise Strategy Group Research Report, *The Long Road Ahead to Ransomware Preparedness*, June 2022. All Enterprise Strategy Group research references and charts have been taken from this research report.

Nutanix Data Lens

Nutanix Data Lens is a software as a service (SaaS) data security and governance solution designed with ransomware resilience and data analytics for unstructured data on Nutanix Cloud Platform. Data Lens uses global data visibility to provide proactive assessment and mitigation of data security risks. It identifies anomalous activities, audits user behavior, and ensures efficient data lifecycle management, while enabling organizations to adhere to compliance requirements.

Data Lens includes a 20-minute containment window, within which threats will be detected and blocked automatically by policy for a faster return to normal operations. It's important to note that time is a critical asset when responding to an active attack and this offers organizations a significant head start on response.

Figure 2. Nutanix Data Lens


Storage Optimization with Data Lifecycle Management
Nutanix Data Lens
Integrated Ransomware Resilience
Relative Risk Score Trend Analysis
Compliance Through Auditing
Azure BLOB
AWS
Wasabi
NUTANIX Objects
Nutanix Unified Storage
Third-party Storage
Files
Objects

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

Data Lens integrates and orchestrates multiple techniques and technologies to deliver ransomware resilience: detection of threats using both known signatures and pattern-based behavioral analysis; blocking of suspicious files and activity; monitoring of activity; generation of alerts on anomalies; and 1-Click recovery. As shown in Figure 2, Data Lens also provides data analytics and lifecycle management. Data age analytics identifies the frequency of access to determine which data is hot, warm, or cold. Smart Tiering optimizes primary storage efficiency and reduces the overall attack surface by moving warm and cold data into appropriate Amazon S3 and Azure Blob buckets, and space-efficient snapshots enable higher performance on backups and recovery. Data Lens also enables organizations to confidently meet audit and compliance requirements by providing detailed visibility into user activity using audit trails and customizable activity reporting. Data Lens provides options for many of the controls required by regulatory frameworks.

Enterprise Strategy Group Technical Validation

Enterprise Strategy Group examined how Nutanix Data Lens helps enterprises detect active threats, automatically respond by blocking compromised accounts and clients, and accelerate the post-attack recovery process.

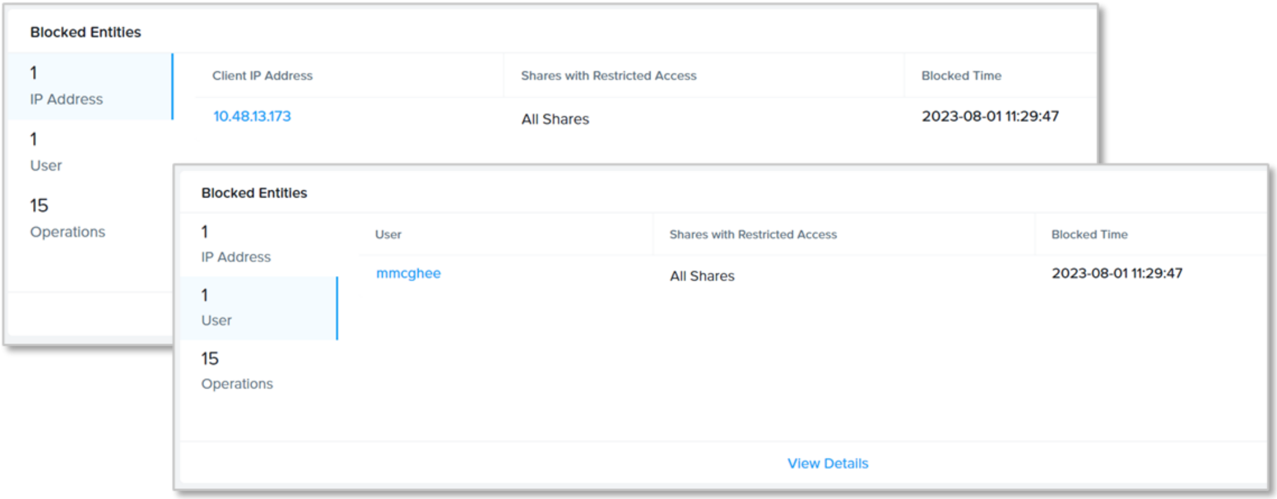
Ransomware Resilience

To validate ransomware resilience, we walked through a test that generated activity consistent with ransomware attacks and verified the time to detect, respond, and recover. We used a script to emulate activities commonly seen in ransomware attacks. On a system with elevated credentials, we launched a script that encrypted files out of place and then deleted the originals.

Enterprise Strategy Group Testing

The script kicked off at 11:15 a.m. and began its process of encrypting files and deleting the originals. Data Lens detected the activity at 11:29, just 14 minutes after the script began encrypting and renaming files. It automatically blocked access for both the user account and the underlying IP address (see Figure 3), and then it generated and sent an alert.

Figure 3. Ransomware Detected and Blocked



Blocked Entities

1 IP Address
1 User
15 Operations

Client IP Address	Shares with Restricted Access	Blocked Time
10.48.13.173	All Shares	2023-08-01 11:29:47

Blocked Entities

1 IP Address
1 User
15 Operations

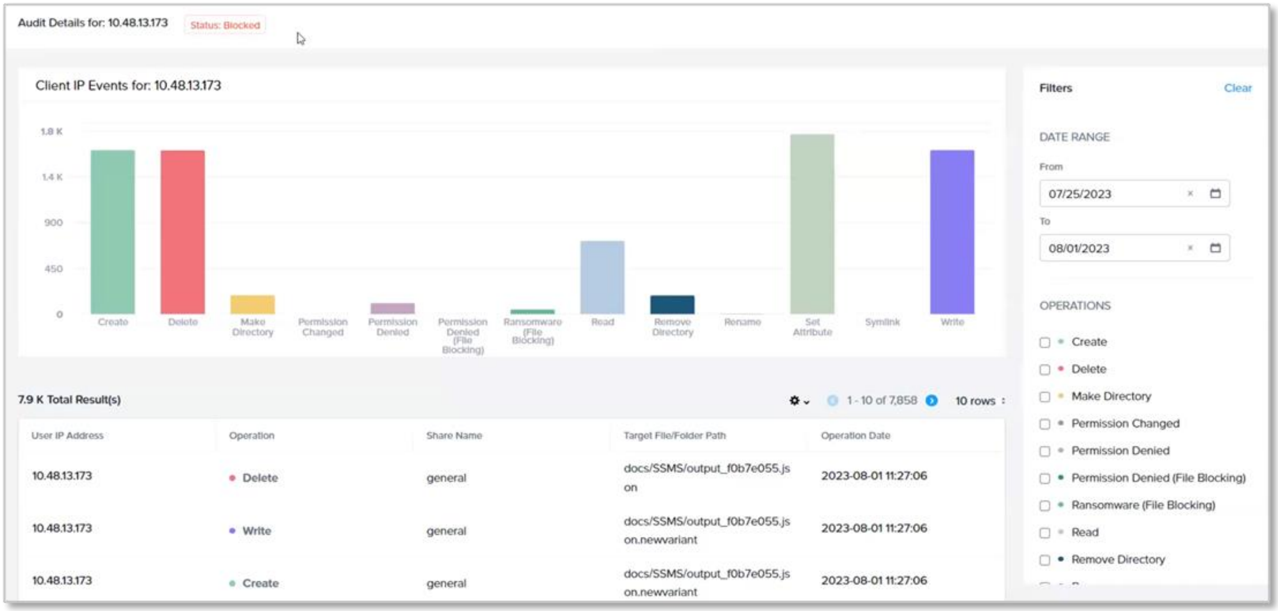
User	Shares with Restricted Access	Blocked Time
mmcghee	All Shares	2023-08-01 11:29:47

View Details

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

Data Lens provides detailed auditing of the activity, showing the anomalous volume of file creation, deletion, attribute changes, and writes, as shown in Figure 4.

Figure 4. Client Audit Details



Audit Details for: 10.48.13.173 Status: Blocked

Client IP Events for: 10.48.13.173

7.9 K Total Result(s)

1 - 10 of 7,858 10 rows

User IP Address	Operation	Share Name	Target File/Folder Path	Operation Date
10.48.13.173	● Delete	general	docs/SSMS/output_f0b7e055.json	2023-08-01 11:27:06
10.48.13.173	● Write	general	docs/SSMS/output_f0b7e055.json.newvariant	2023-08-01 11:27:06
10.48.13.173	● Create	general	docs/SSMS/output_f0b7e055.json.newvariant	2023-08-01 11:27:06

Filters Clear

DATE RANGE
From 07/25/2023
To 08/01/2023

OPERATIONS
- □ ● Create
- □ ● Delete
- □ ● Make Directory
- □ ● Permission Changed
- □ ● Permission Denied
- □ ● Permission Denied (File Blocking)
- □ ● Ransomware (File Blocking)
- □ ● Read
- □ ● Remove Directory

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

Why This Matters

Recovery point objectives (RPOs) and recovery time objectives (RTOs) matter because lost data is often lost money and may represent a key transaction that can never be reproduced. Overall, organizations are reporting that they are likely to lose hours of data, with nearly half (46%) stating that they believe it would take them six hours or more to recover from a ransomware event and resume mission-critical operations. Organizations need to contain an attack before beginning the recovery process, and responding quickly is critical to minimize damage and enable faster recovery.

Enterprise Strategy Group validated that Nutanix Data Lens detected ransomware activity and blocked access to files from the impacted user and their machine within 14 minutes of the start of an attack, effectively shutting it down. Because Data Lens monitors and analyzes activity, it's not dependent on malware signatures and can also use behavioral patterns to detect attacks.

The ability to detect and block attacks quickly not only reduces damage but also helps reduce RPO and RTO by allowing an organization to begin recovery actions faster.

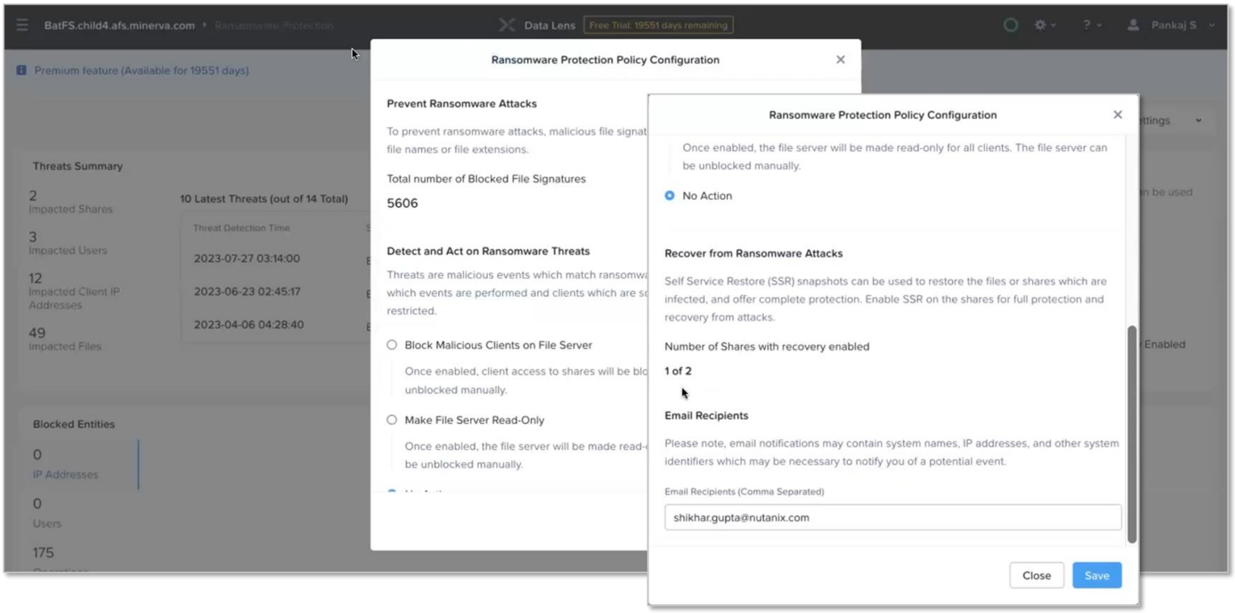
Enabling Rapid Recovery with Data Lens

Enterprise Strategy Group examined how Nutanix Data Lens uses data analytics to identify the most recent known good snapshot and enable rapid, 1-Click recovery after a ransomware attack.

Enterprise Strategy Group Testing

Data Lens ransomware protection policies control how the platform responds to attacks. Organizations can customize detection actions (e.g., block malicious clients or make the file server read-only) and recovery responses, as shown in Figure 5.

Figure 5. Ransomware Protection Recovery Policies



BatFS.child4.afs.minerva.com
Ransomware Protection
Data Lens
Free Trial: 19551 days remaining
Pankaj S
Premium feature (Available for 19551 days)
ttings
n be used
Enabled
Close
Save

Threats Summary

2 Impacted Shares

3 Impacted Users

12 Impacted Client IP Addresses

49 Impacted Files

10 Latest Threats (out of 14 Total)

Threat Detection Time
2023-07-27 03:14:00
2023-06-23 02:45:17
2023-04-06 04:28:40

Blocked Entities

0 IP Addresses

0 Users

175

Ransomware Protection Policy Configuration

Prevent Ransomware Attacks

To prevent ransomware attacks, malicious file signat file names or file extensions.

Total number of Blocked File Signatures

5606

Detect and Act on Ransomware Threats

Threats are malicious events which match ransomwa which events are performed and clients which are sc restricted.

○ Block Malicious Clients on File Server

Once enabled, client access to shares will be blo unblocked manually.

○ Make File Server Read-Only

Once enabled, the file server will be made read-only for all clients. The file server can be unblocked manually.

● No Action

Recover from Ransomware Attacks

Self Service Restore (SSR) snapshots can be used to restore the files or shares which are infected, and offer complete protection. Enable SSR on the shares for full protection and recovery from attacks.

Number of Shares with recovery enabled

1 of 2

Email Recipients

Please note, email notifications may contain system names, IP addresses, and other system identifiers which may be necessary to notify you of a potential event.

Email Recipients (Comma Separated)

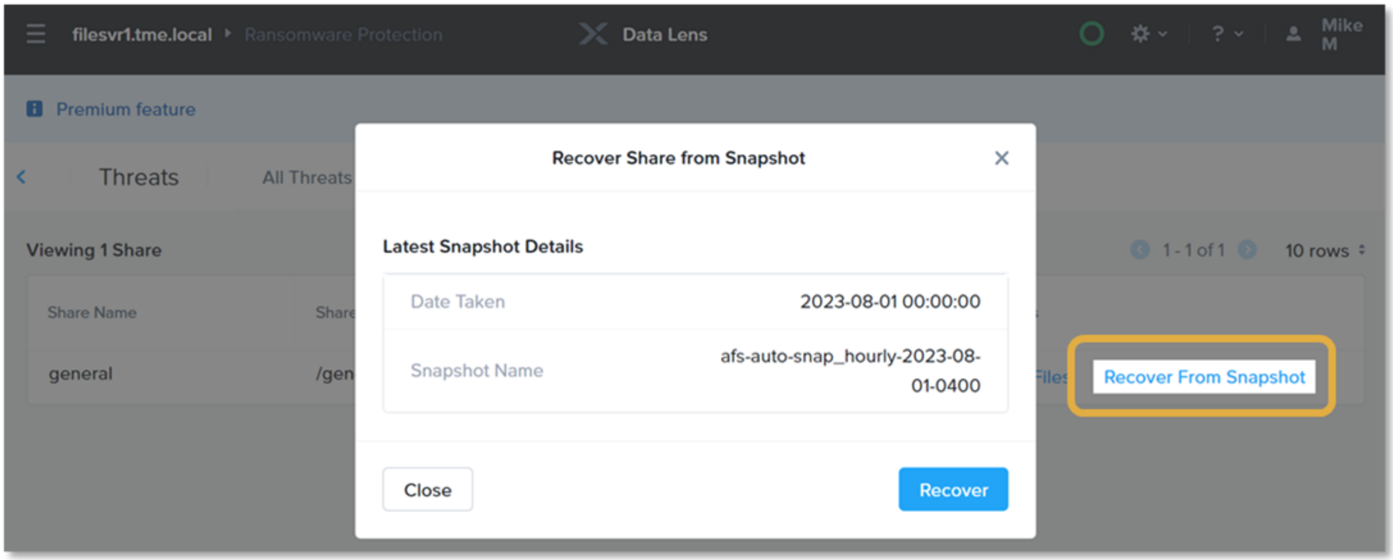
shikhar.gupta@nutanix.com

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

Organizations that use Self-Service Restore (SSR) snapshots can leverage them for granular, rapid recovery; users can select specific files or an entire share for restore, as appropriate.

As shown in Figure 6, Data Lens identifies the last known good snapshot and enables 1-Click Recovery, where all manual recovery activities are automated.

Figure 6. 1-Click Recovery



Recover Share from Snapshot

Latest Snapshot Details

Date Taken: 2023-08-01 00:00:00

Snapshot Name: afs-auto-snap_hourly-2023-08-01-0400

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

Why This Matters

Nearly three-quarters (73%) of organizations surveyed by Enterprise Strategy Group report that they have been financially or operationally impacted by ransomware attacks in the last 12 months, with nearly a third (32%) reporting multiple successful attacks. What is needed is a solution that can stop successful attacks while they're in progress and provide rapid recovery.

Enterprise Strategy Group validated that Nutanix Data Lens ransomware protection policies give organizations a robust and flexible set of automatic options for responding to ransomware attacks in progress, while making recovery as easy as selecting the most recent known good snapshot taken before the start of the attack and clicking *Recover*.

The ability to rapidly recover from attacks helps organizations resume normal operations, minimizing financial, operational, and reputational damage.

Conclusion

According to Enterprise Strategy Group research, 79% of respondents identified ransomware as at least one of their top-five business priorities. Organizations are stepping up their focus on and investment in ransomware preparedness. The scale of what is required to limit the impact of a successful attack requires ongoing engagement from line-of-business, IT, and security teams working together to reduce the risk of attack, increase readiness to recover, and resume business operations to minimize disruption and monetary impact.

Enterprise Strategy Group's analysis validated the capabilities of Nutanix Data Lens to provide detection and protection before, during, and after an attack. In our tests, Data Lens detected ransomware activity within 14 minutes of the start of the attack and automatically blocked all shares at the user and machine level in order to stop the attack in its tracks. Data Lens automatically identifies the latest known good snapshots to use for all affected shares and 1-Click Recovery enables organizations to restore all of them from one place, a significant time saver.

Nutanix Data Lens is a powerful new layer of protection organizations should consider adding to their cyber resilience toolkit. When—not if—malware does get through an organization's first lines of defense, Data Lens can detect and stop an attack very quickly and identify known good restore points, helping to make the process of recovery smoother, more efficient, and faster.

If your organization needs a solution that can identify and detect ransomware attacks in progress and block them quickly to minimize damage so you can focus on responding and recovering faster, Enterprise Strategy Group recommends a close look at Nutanix Data Lens.

Information contained in this publication has been obtained by sources TechTarget considers to be reliable but is not warranted by TechTarget. This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

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