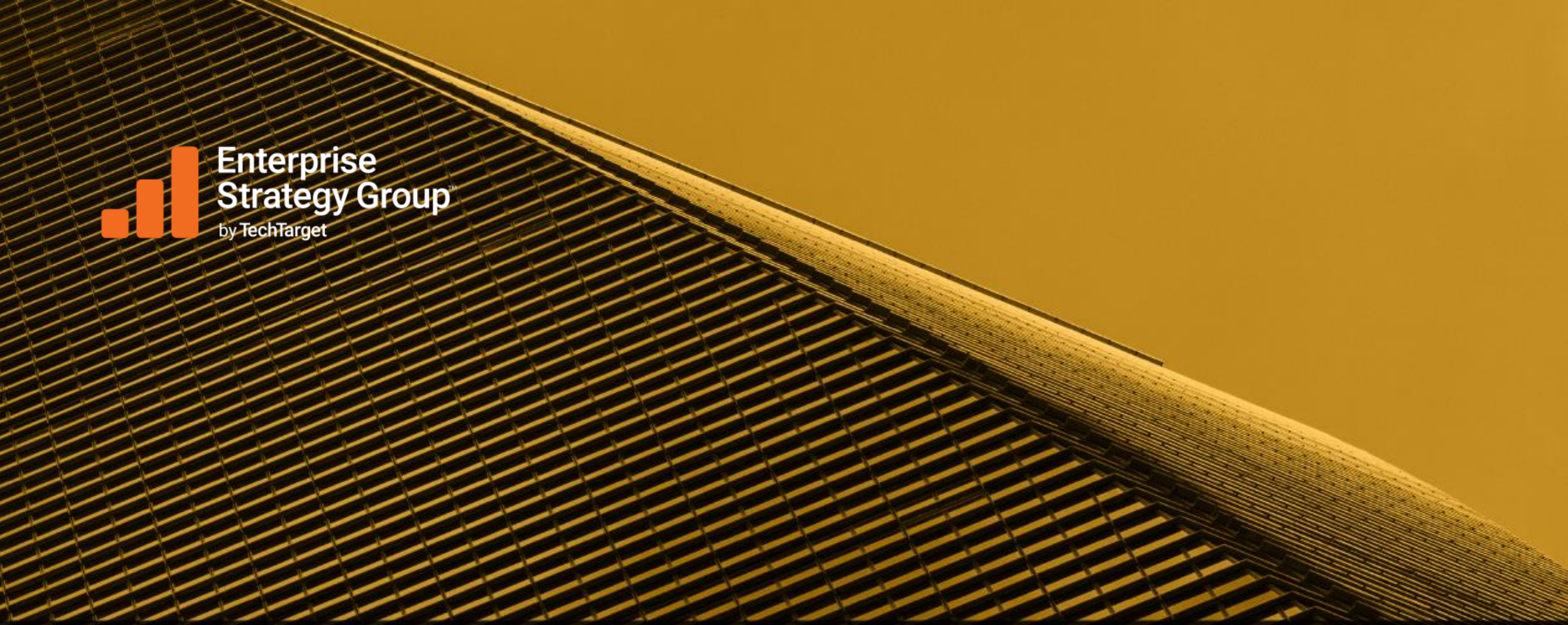


TECHNICAL VALIDATION

NetApp BlueXP Ransomware Protection

Comprehensive Ransomware Protection for NetApp Storage

By Justin Boyer, IT Validation Analyst
Enterprise Strategy Group

March 2024

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

Contents

Introduction

This Technical Validation from TechTarget's Enterprise Strategy Group details our evaluation of the NetApp BlueXP ransomware protection service. We evaluated how BlueXP enables robust ransomware protection for NetApp users, saving security and IT teams time, improving their effectiveness, and delivering faster response and recovery times in the face of ransomware attacks.

Background

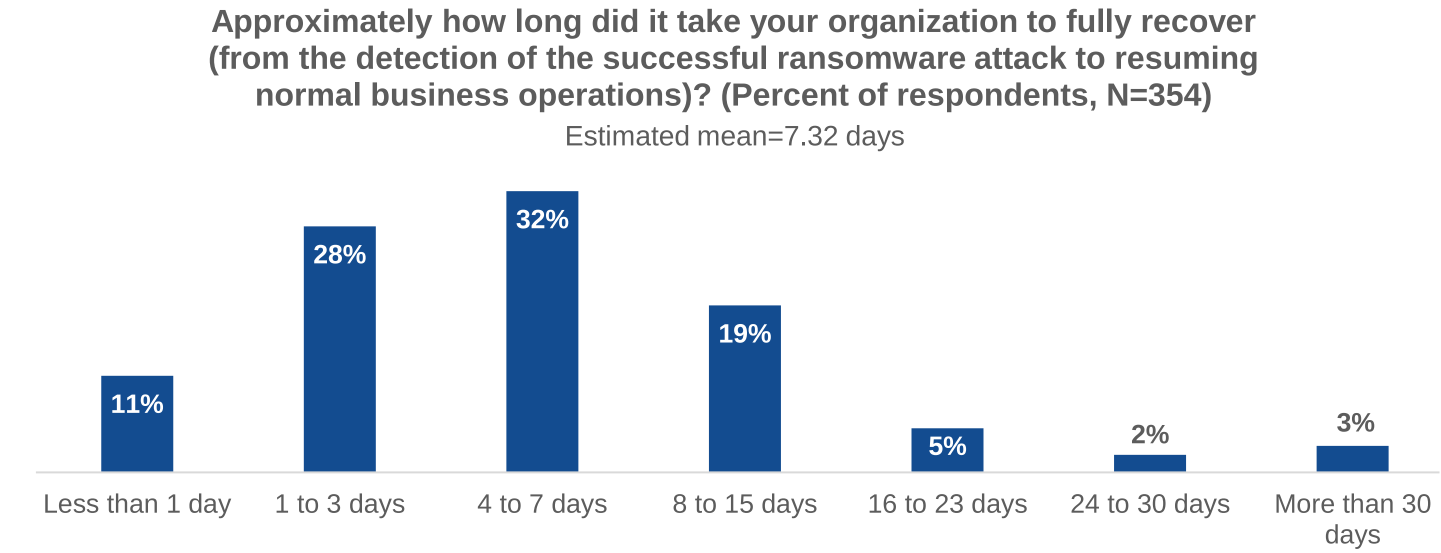
The volume and criticality of a business's data have grown, making it a tempting target for attackers. While some attackers want to steal an organization's data outright, others decide to make it inaccessible and hold it for ransom. Either way, malicious actors are hoping to get a pay day from unsuspecting and unprepared companies.

Research conducted by Enterprise Strategy Group shows that ransomware attacks are a not a matter of if, but of when. Seventy-five percent of survey respondents indicated that they've experienced a ransomware attack, successful or unsuccessful, in the past 12 months, with another 37% reporting that they've had multiple successful ransomware attacks in the same period.[1]

Ransomware leaves organizations dead in the water, without the ability to perform critical business functions and generate revenue. Additionally, recovery can be difficult and time-consuming.

Figure 1 shows how long organizations said it takes them to recover after a successful ransomware attack. Eighty-nine percent of respondents indicated it takes at least a day to recover, and 29% said it takes more than a week. Across all respondents, the estimated mean time to recovery was 7.32 days.

Figure 1. Time to Full Operational Recovery From Point of Ransomware Detection



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

Organizations need a solution that can protect their data, detect attacks, and quickly recover if an attack succeeds.

[1] Source: Enterprise Strategy Group Complete Survey Results, *2023 Ransomware Preparedness: Lighting the Way to Readiness and Mitigation*, November 2023. All Enterprise Strategy Group research references and charts in this Technical Validation are from this survey results set.

NetApp BlueXP Ransomware Protection

NetApp BlueXP ransomware protection is a service offered to NetApp customers that provides robust ransomware protection for data stored within their NetApp storage. BlueXP ransomware protection features protection, response, and recovery capabilities and offers a holistic ransomware defense technology at the storage layer.

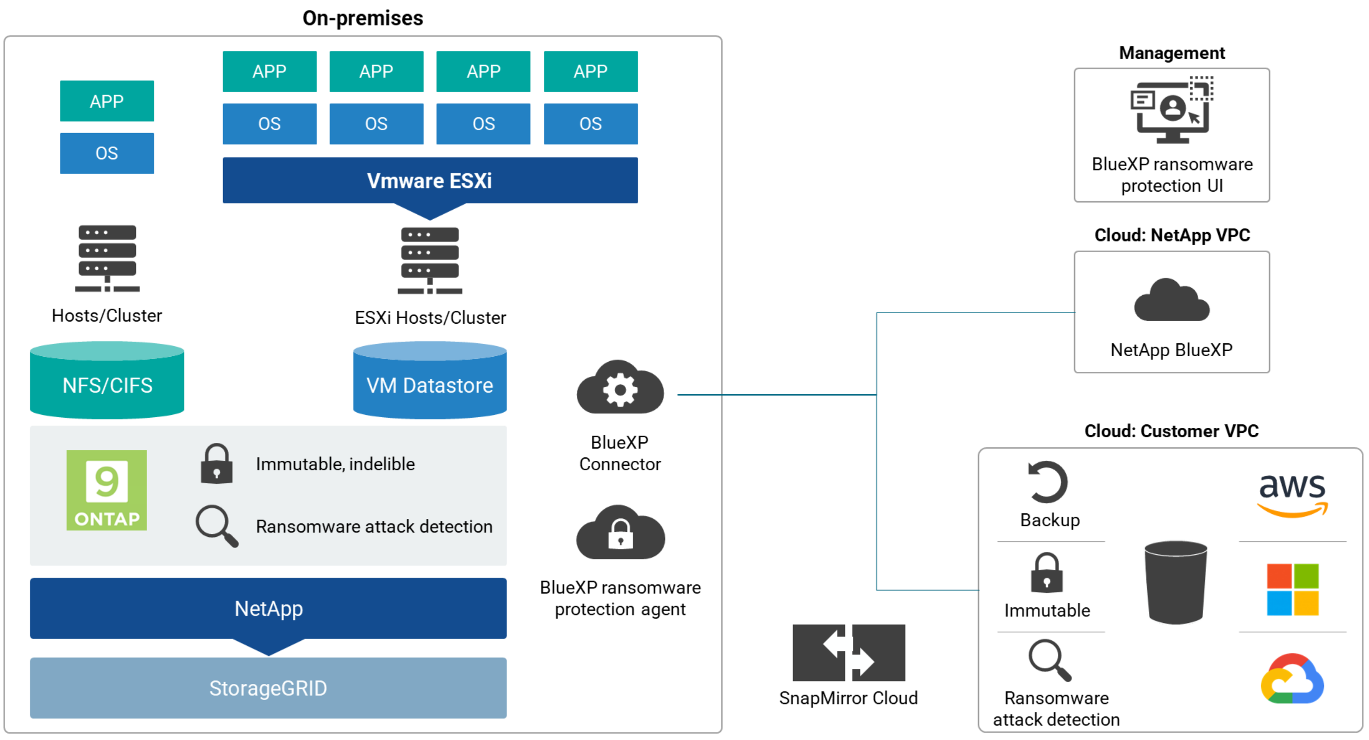
BlueXP ransomware protection provides a single control plane to coordinate and execute a comprehensive, workload-centric ransomware defense, covering all functions of the NIST framework: govern, identify, protect, detect, respond, and recover.

BlueXP ransomware protection automatically identifies data types within NetApp storages, maps the data to workloads, and analyzes workload risk. It proposes protection policies that align protection level with workload importance and applies these protection policies with one click.

Once protection is in place, BlueXP ransomware protection uses AI/ML-powered anomaly detection on both primary and secondary storage to increase the speed and accuracy of attack detection. Upon detecting an attack, BlueXP ransomware protection takes immutable and indelible snapshot copies to minimize further impact and business disruptions (see Figure 2).

BlueXP ransomware protection also helps organizations recover workloads easier and faster by recommending a restore point and orchestrating the workflow for application-consistent recovery of all workload data.

Figure 2. NetApp BlueXP Ransomware Protection



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

Enterprise Strategy Group Technical Validation

Enterprise Strategy Group evaluated NetApp BlueXP ransomware protection to validate how it assists organizations in ransomware preparedness, how its anomaly detection capabilities help identify potential attacks and respond accordingly, and how BlueXP ransomware protection helps organizations recover quickly in the event of a successful attack.

Assisting With Ransomware Preparedness

Enterprise Strategy Group validated BlueXP ransomware protection's ability to assist organizations in preparing their environment to defend against ransomware attacks.

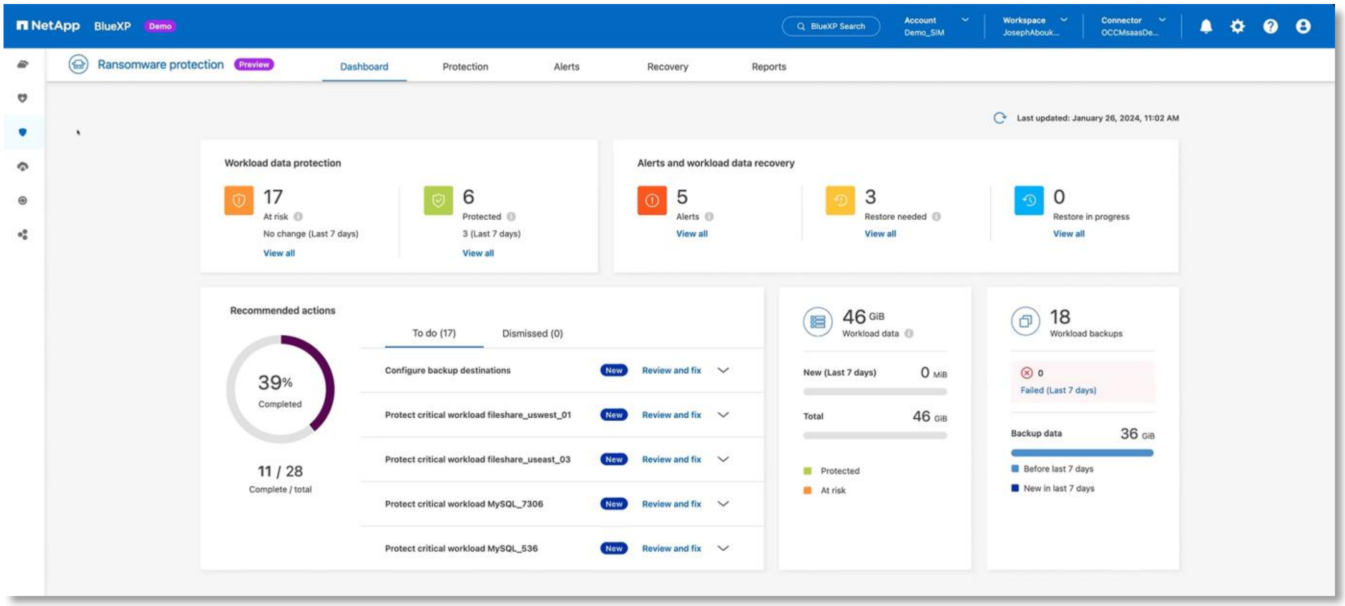
Enterprise Strategy Group Testing

As shown in Figure 3, the BlueXP ransomware protection dashboard provides an overview of protection, alerts, and recommendations. The top-left box displays an overview of workload data protection. A workload in the context can be a database, application, virtual machine (VM), or file share—essentially any entity that holds or uses business data. Workloads marked as "At risk" currently don't have a ransomware protection policy applied to it. Those that do are counted under the "Protected" category.

The top right of the dashboard features alerts and tools for workload data recovery. On-device storage protection software detects anomalies in real time and flags them. These may or may not be attacks, but they'll show up in the dashboard for investigation. When an anomaly has been remediated, a restore may be necessary. The current number of restores needed and in progress are also presented here.

The bottom of the dashboard features a list of recommended actions that will make the organizations' workload data more secure. These protections aren't only for backing data up but also include real-time anomaly detection and malicious file blocking. The bottom panels also display how much data and how many backups BlueXP ransomware protection is currently managing.

Figure 3. BlueXP Ransomware Protection Dashboard



Last updated: January 26, 2024, 11:02 AM

Workload data protection

17 At risk — No change (Last 7 days) — View all

6 Protected — 3 (Last 7 days) — View all

Alerts and workload data recovery

5 Alerts — View all

3 Restore needed — View all

0 Restore in progress — View all

Recommended actions

39% Completed

11 / 28 Complete / total

To do (17) | Dismissed (0)

Configure backup destinations	New	Review and fix
Protect critical workload fileshare_uswest_01	New	Review and fix
Protect critical workload fileshare_useast_03	New	Review and fix
Protect critical workload MySQL_7306	New	Review and fix
Protect critical workload MySQL_536	New	Review and fix

46 GiB Workload data

New (Last 7 days): 0 MiB

Total: 46 GiB

18 Workload backups

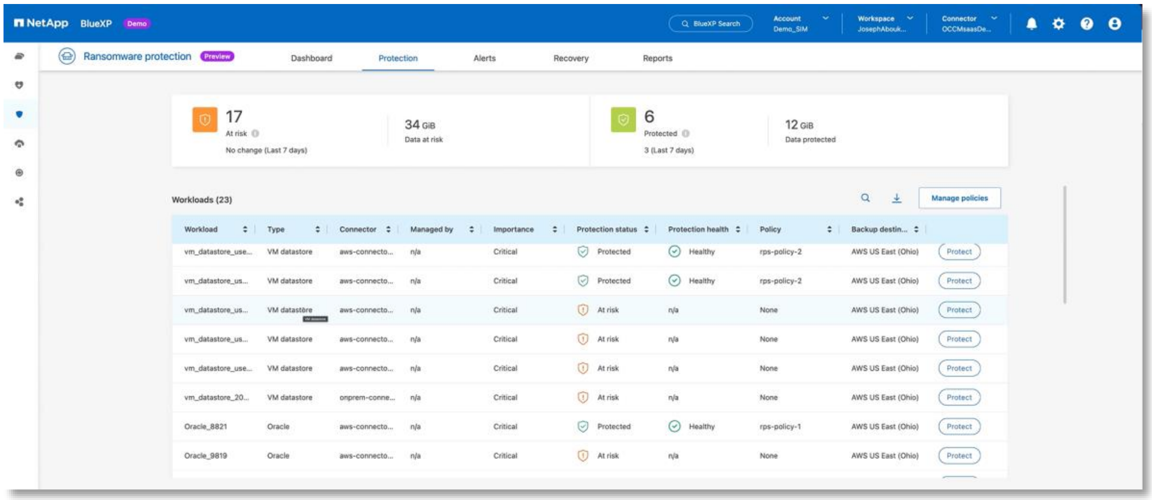
0 Failed (Last 7 days)

Backup data: 36 GiB

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

The Protection module of BlueXP ransomware protection enables administrators to view and protect workloads. As shown in Figure 4, BlueXP ransomware protection displays a list of discovered workloads and whether they're currently covered by ransomware protection. It also displays the policy applied and protection health, indicating either that the policy is working or that it needs attention.

Figure 4. Workload Protection Interface



17 At risk
No change (Last 7 days)

34 GiB Data at risk

6 Protected
3 (Last 7 days)

12 GiB Data protected

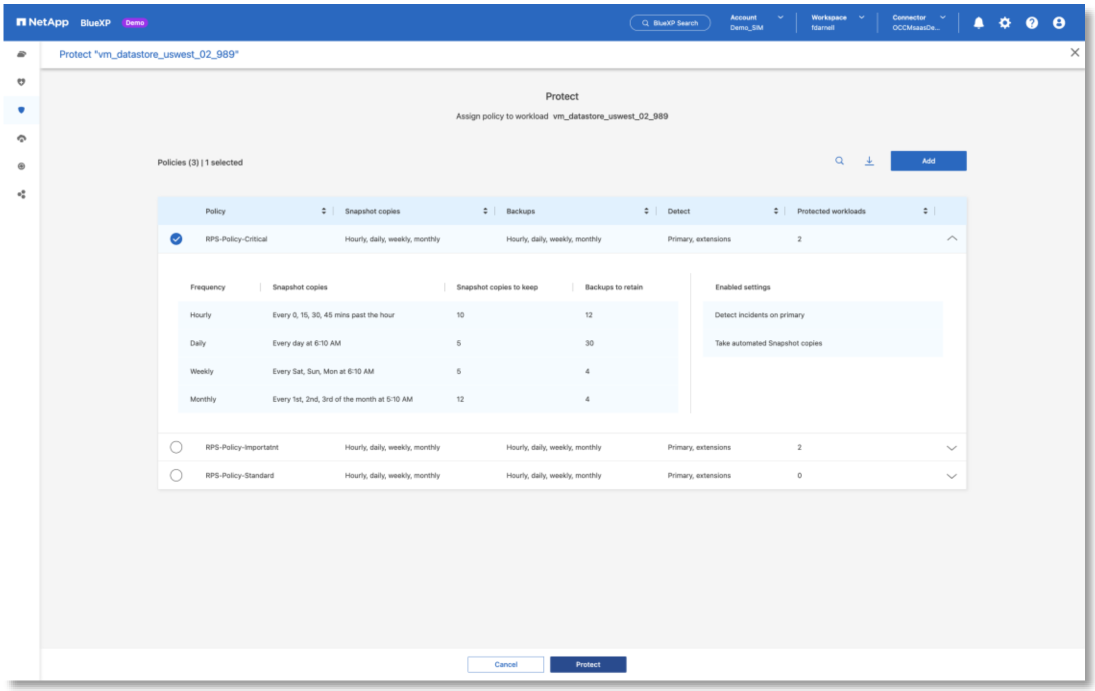
Workloads (23)

Workload	Type	Connector	Managed by	Importance	Protection status	Protection health	Policy	Backup destin...	
vm_datastore_use...	VM datastore	aws-connecto...	n/a	Critical	Protected	Healthy	rps-policy-2	AWS US East (Ohio)	Protect
vm_datastore_us...	VM datastore	aws-connecto...	n/a	Critical	Protected	Healthy	rps-policy-2	AWS US East (Ohio)	Protect
vm_datastore_us...	VM datastore	aws-connecto...	n/a	Critical	At risk	n/a	None	AWS US East (Ohio)	Protect
vm_datastore_us...	VM datastore	aws-connecto...	n/a	Critical	At risk	n/a	None	AWS US East (Ohio)	Protect
vm_datastore_use...	VM datastore	aws-connecto...	n/a	Critical	At risk	n/a	None	AWS US East (Ohio)	Protect
vm_datastore_20...	VM datastore	onprem-conne...	n/a	Critical	At risk	n/a	None	AWS US East (Ohio)	Protect
Oracle_8821	Oracle	aws-connecto...	n/a	Critical	Protected	Healthy	rps-policy-1	AWS US East (Ohio)	Protect
Oracle_9819	Oracle	aws-connecto...	n/a	Critical	At risk	n/a	None	AWS US East (Ohio)	Protect

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

Enterprise Strategy Group walked through the process of protecting a previously at-risk workload through the Protection module. After clicking the **Protect** button on a workload, we were taken to the Protect screen (Figure 5).

Figure 5. Applying Protection Policy With One Click



Protect "vm_datastore_uswest_02_989"

Protect

Assign policy to workload vm_datastore_uswest_02_989

Policies (3) | 1 selected

	Policy	Snapshot copies	Backups	Detect	Protected workloads
●	RPS-Policy-Critical	Hourly, daily, weekly, monthly	Hourly, daily, weekly, monthly	Primary, extensions	2
○	RPS-Policy-Importatnt	Hourly, daily, weekly, monthly	Hourly, daily, weekly, monthly	Primary, extensions	2
○	RPS-Policy-Standard	Hourly, daily, weekly, monthly	Hourly, daily, weekly, monthly	Primary, extensions	0

Frequency	Snapshot copies	Snapshot copies to keep	Backups to retain
Hourly	Every 0, 15, 30, 45 mins past the hour	10	12
Daily	Every day at 6:10 AM	5	30
Weekly	Every Sat, Sun, Mon at 6:10 AM	5	4
Monthly	Every 1st, 2nd, 3rd of the month at 5:10 AM	12	4

Enabled settings
Detect incidents on primary
Take automated Snapshot copies

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

The Protect screen presents a list of potential policies used to safeguard the selected workload. A policy defines the frequency at which snapshots are taken, how many snapshot copies to keep, and how many backups to retain. These options enable organizations to implement business continuity policies, ensuring that the right backups are always available in the event of a successful attack.

The Protect screen also displays the enabled settings on the policy for added protection, such as autonomous ransomware protection, automatic snapshots if it detects something anomalous, and malicious file blocking. These added features actively protect workload data while ensuring the data can be restored if necessary.

Why This Matters

According to Enterprise Strategy Group research, across all survey respondents the mean amount of data impacted by successful ransomware attacks was reported to be about 1.3 petabytes (PB). Organizations today hold massive amounts of data that are critical to their business operations. Successful ransomware attacks prevent the business from operating and halt revenue production. However, businesses can't protect data unless they know where it is and how it is protected.

Enterprise Strategy Group validated how BlueXP ransomware protection assists organizations in preparing for ransomware attacks. BlueXP ransomware protection discovers workloads stored within NetApp storage and displays a risk overview on the dashboard. The dashboard also features alerts on protected workloads and suggestions on how to make the environment more secure. We walked through the process of protecting a workload through the Protection workflow, applying a policy that includes snapshot and backup timing, retention, and activation of real-time protection.

With BlueXP ransomware protection, organizations can quickly discover, view, and protect their workloads with a few clicks. Administrators have flexibility to define and apply policies to various workloads based on their business impact if compromised. Additionally, BlueXP ransomware protection goes beyond backups and provides actionable alerts in real time for suspicious behavior. With BlueXP, organizations can view overall risk across their NetApp workloads, understanding where their data is and whether it is vulnerable.

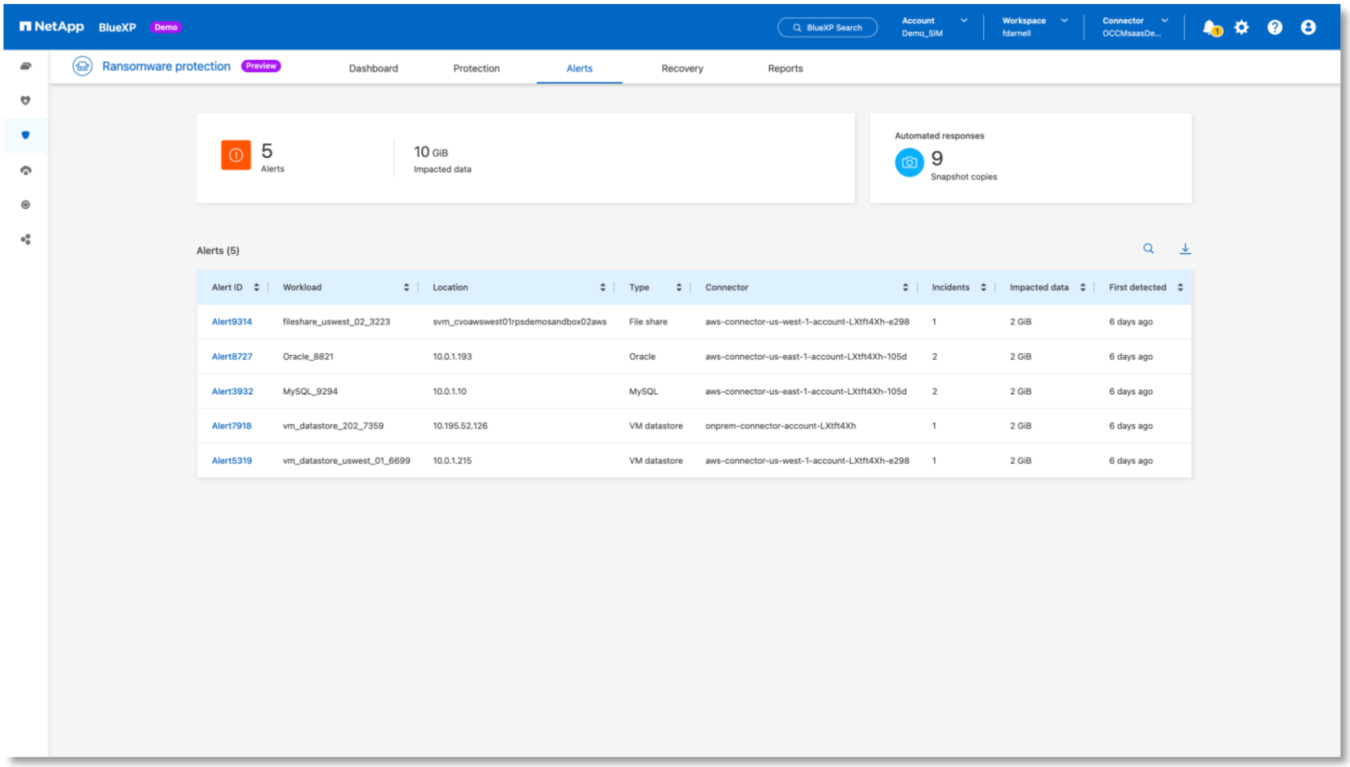
AI-powered Anomaly Detection

Enterprise Strategy Group validated BlueXP ransomware protection's real-time AI/ML-powered anomaly detection and protection that leverages ONTAP on-box capabilities.

Enterprise Strategy Group Testing

Enterprise Strategy Group walked through the alert remediation workflow, reviewing how BlueXP ransomware protection reacts when it sees a potential ransomware attack in progress. After navigating to the Alerts tab, we viewed a list of alerts, along with various data points (see Figure 6). BlueXP ransomware protection reports the workload on which the alert was found, along with its location, type, number of incidents, and the amount of data affected. These alerts indicate that suspicious activity has occurred, as detected by BlueXP ransomware protection's AI/ML-powered anomaly detection. From here, the alerts can be investigated to determine if they are actual attacks or something else.

Figure 6. Displaying Potential Attacks for Review



5
Alerts

10 GiB
Impacted data

Automated responses
9
Snapshot copies

Alerts (5)

Alert ID	Workload	Location	Type	Connector	Incidents	Impacted data	First detected
Alert9314	fileshare_uswest_02_3223	svm_cvoawswest01rpsdemosandbox02aws	File share	aws-connector-us-west-1-account-LXtft4Xh-e298	1	2 GiB	6 days ago
Alert8727	Oracle_8821	10.0.1.193	Oracle	aws-connector-us-east-1-account-LXtft4Xh-105d	2	2 GiB	6 days ago
Alert3932	MySQL_9294	10.0.1.10	MySQL	aws-connector-us-east-1-account-LXtft4Xh-105d	2	2 GiB	6 days ago
Alert7918	vm_datastore_202_7359	10.195.52.126	VM datastore	onprem-connector-account-LXtft4Xh	1	2 GiB	6 days ago
Alert5319	vm_datastore_uswest_01_6699	10.0.1.215	VM datastore	aws-connector-us-west-1-account-LXtft4Xh-e298	1	2 GiB	6 days ago

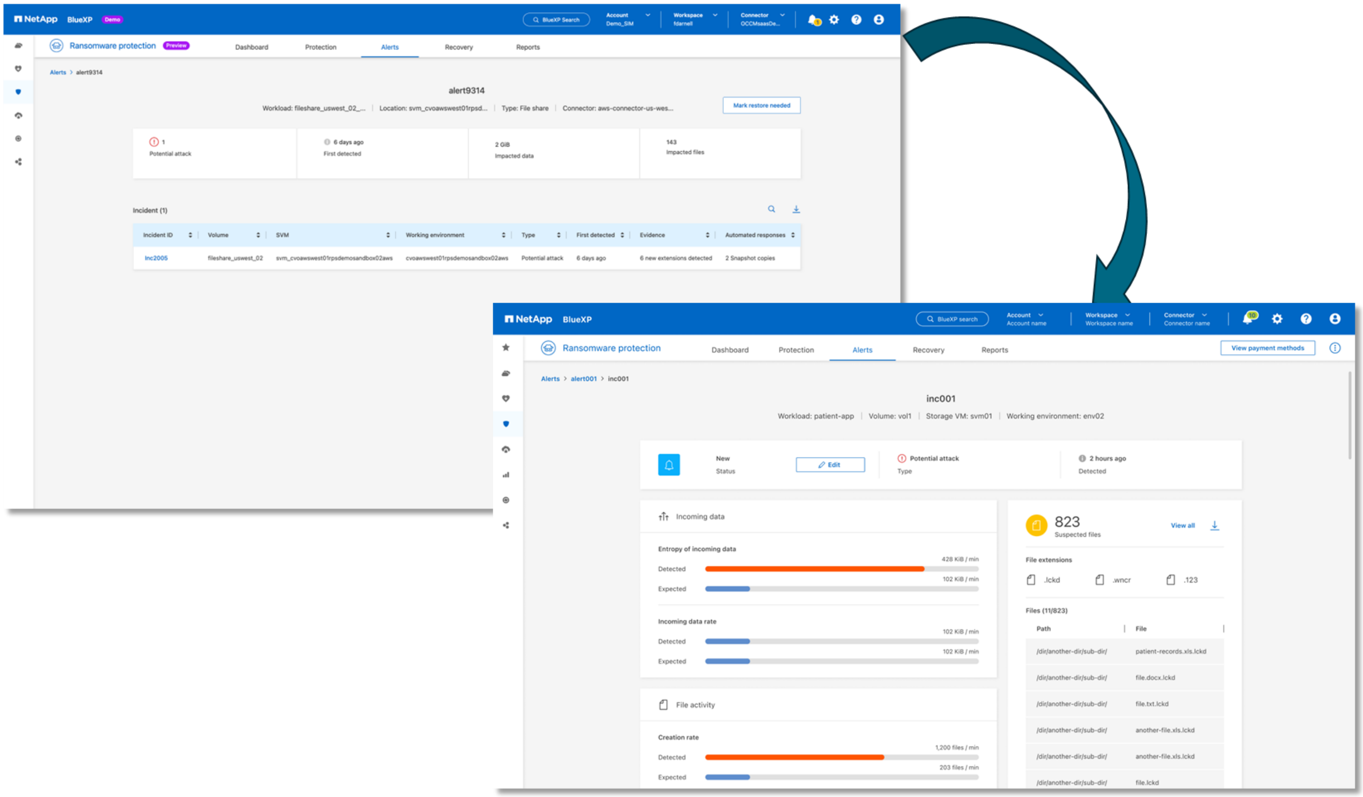
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Next, we stepped through the process of viewing alert details to determine what triggered the alert. As shown in Figure 7, we clicked on **Alert 9314** to view its details. This alert has one incident noted that is labeled as a potential attack. Incidents may also be labeled "Warning" if BlueXP ransomware protection determines that it warrants attention but doesn't indicate an attack in progress.

The Evidence column provides the reason why the anomaly detection decided to raise an alert. In the case of Alert 9314, six new extensions that were previously never used before within this volume appeared, indicating that a malicious actor could be encrypting files or that an employee could be using it in an unapproved manner. This page also indicates that two snapshot copies were made automatically in response to the alert, ensuring that, if it was an attack, safe data is available for restoration.

After clicking into the specific incident, we viewed the incident detail page. This page displays various signals used to determine that an alert was necessary. The left side of the page highlights several triggers that warrant consideration, such as a change in the entropy of incoming data and file creation, renaming, and deletion rates. On the right side, you can see how many files were affected and the specific extensions seen by the anomaly detection system. The bottom-right section lists the impacted files. A visual inspection of these impacted files may lead to confirmation of an attack or the determination that this is expected activity.

Figure 7. Drilling Into Incident Details and Viewing Impacted Files



Alerts > alert9314

alert9314

Workload: fileshare_uswest_02_... | Location: svm_cvoawswest01rpsd... | Type: File share | Connector: aws-connector-us-wes...

1 Potential attack	6 days ago First detected	2 GiB Impacted data	143 Impacted files

Incident (1)

Incident ID	Volume	SVM	Working environment	Type	First detected	Evidence	Automated responses
Inc2005	fileshare_uswest_02	svm_cvoawswest01rpsdemosandbox02aws	cvoawswest01rpsdemosandbox02aws	Potential attack	6 days ago	6 new extensions detected	2 Snapshot copies

Alerts > alert001 > inc001

inc001

Workload: patient-app | Volume: vol1 | Storage VM: svm01 | Working environment: env02

New Status	Potential attack Type	2 hours ago Detected

Incoming data

Entropy of incoming data

Detected 428 KiB / min

Expected 102 KiB / min

Incoming data rate

Detected 102 KiB / min

Expected 102 KiB / min

File activity

Creation rate

Detected 1,200 files / min

Expected 203 files / min

823 Suspected files

File extensions: .lckd .wncr .123

Files (11/823)

Path	File
/dir/another-dir/sub-dir/	patient-records.xls.lckd
/dir/another-dir/sub-dir/	file.docx.lckd
/dir/another-dir/sub-dir/	file.txt.lckd
/dir/another-dir/sub-dir/	another-file.xls.lckd
/dir/another-dir/sub-dir/	another-file.xls.lckd
/dir/another-dir/sub-dir/	file.lckd

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

Why This Matters

Enterprise Strategy Group research shows that successful ransomware attacks aren't uncommon among respondents. Seventy-five percent of respondents reported having at least one successful ransomware attack in the past 12 months, with 37% experiencing more than one. Fast detection is essential to protecting an organization's data. No matter what type of data an organization holds, they will be a target eventually.

Enterprise Strategy Group validated that BlueXP ransomware protection's real-time detection and alerting helps organizations to see and respond to attacks quickly. We viewed specific alerts, what triggered them, and what actions BlueXP ransomware protection took to protect the data. Upon seeing suspicious behavior, BlueXP ransomware protection creates snapshot backups automatically to ensure that there will be a safe backup option for recovery.

Ransomware attacks have become part of the normal day-to-day reality for cybersecurity and IT teams. Malicious actors are looking for easy targets, regardless of company size or industry. BlueXP ransomware protection helps NetApp customers quickly identify and remediate potential attacks with fast detection, provides clear information on why alarms are raised, and enables automatic backups to aid in recovery, preparing organizations to face the inevitable.

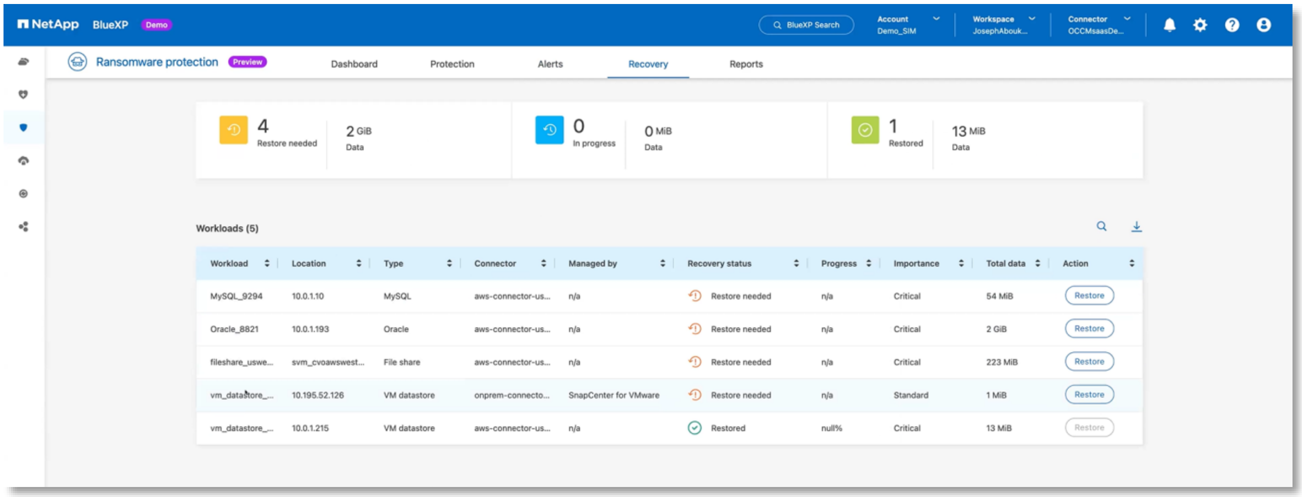
Guided Recovery

Enterprise Strategy Group validated BlueXP ransomware protection's ability to assist in quickly recovering from any successful ransomware attacks.

Enterprise Strategy Group Testing

Once an alert is remediated and any immediate necessary actions are complete, an administrator may choose to restore the affected data. Enterprise Strategy Group navigated to the Recovery tab to view the workloads that have been marked for recovery. This list view, as shown in Figure 8, displays pertinent information, such as the workload name, location, recovery status, importance, and total data affected. From here, an administrator can choose to restore the workload from a snapshot by clicking the **Restore** button for the specific workload.

Figure 8. Reviewing Workloads That Need to Be Restored



4 Restore needed | 2 GiB Data
0 In progress | 0 MiB Data
1 Restored | 13 MiB Data

Workloads (5)

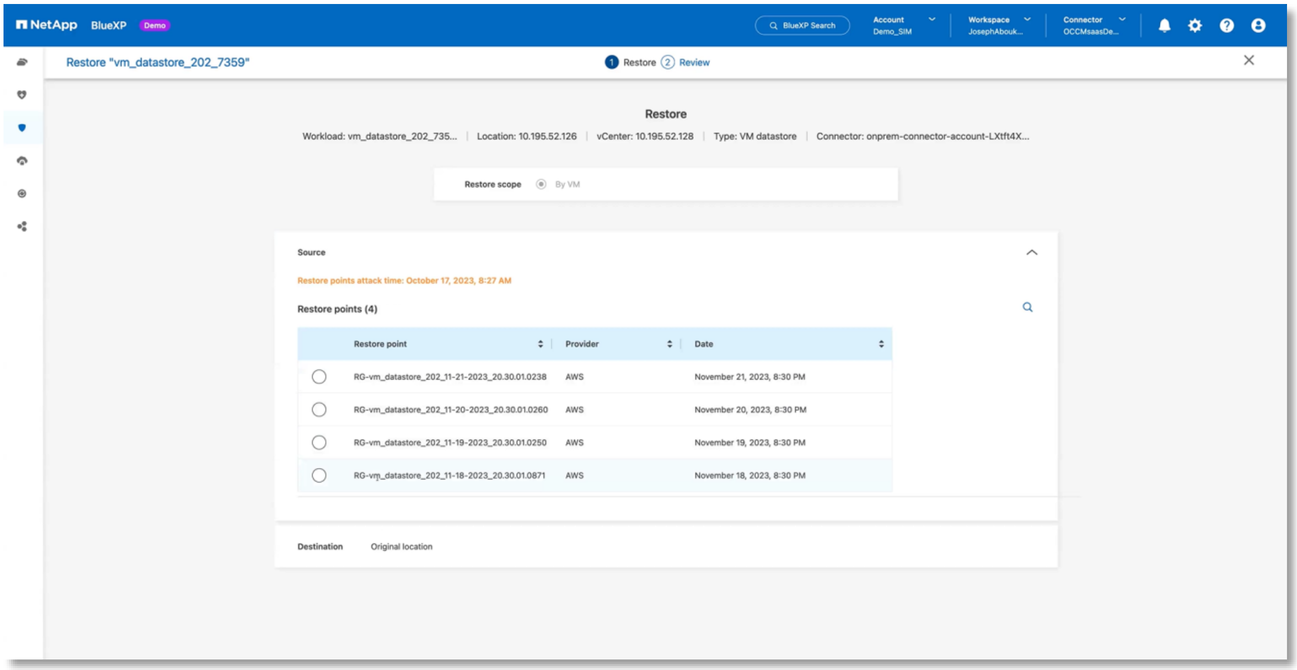
Workload	Location	Type	Connector	Managed by	Recovery status	Progress	Importance	Total data	Action
MySQL_9294	10.0.1.10	MySQL	aws-connector-us...	n/a	Restore needed	n/a	Critical	54 MiB	Restore
Oracle_8821	10.0.1.193	Oracle	aws-connector-us...	n/a	Restore needed	n/a	Critical	2 GiB	Restore
fileshare_uswe...	svm_cvoawswest...	File share	aws-connector-us...	n/a	Restore needed	n/a	Critical	223 MiB	Restore
vm_datastore_...	10.195.52.126	VM datastore	onprem-connecto...	SnapCenter for VMware	Restore needed	n/a	Standard	1 MiB	Restore
vm_datastore_...	10.0.1.215	VM datastore	aws-connector-us...	n/a	Restored	null%	Critical	13 MiB	Restore

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

Next, we chose to restore a VM managed by SnapCenter for VMware, enabling VM-consistent recovery. VMs managed this way can be restored to their previous state, with all applications and data as they were when the snapshot was taken. This enables the VM to be restored and working without reconfiguring the VM in any way.

As shown in Figure 9, the Restore screen displayed the list of restore points available for this VM workload. It also showed the exact time of the suspected attack, enabling us to choose the appropriate restore point taken before the attack.

Figure 9. Viewing the List of Snapshots to Use for Restoration



Restore "vm_datastore_202_7359"

Restore

Workload: vm_datastore_202_735... | Location: 10.195.52.126 | vCenter: 10.195.52.128 | Type: VM datastore | Connector: onprem-connector-account-LXtft4X...

Restore scope ● By VM

Source

Restore points attack time: October 17, 2023, 8:27 AM

Restore points (4)

	Restore point	Provider	Date
○	RG-vm_datastore_202_11-21-2023_20.30.01.0238	AWS	November 21, 2023, 8:30 PM
○	RG-vm_datastore_202_11-20-2023_20.30.01.0260	AWS	November 20, 2023, 8:30 PM
○	RG-vm_datastore_202_11-19-2023_20.30.01.0250	AWS	November 19, 2023, 8:30 PM
○	RG-vm_datastore_202_11-18-2023_20.30.01.0871	AWS	November 18, 2023, 8:30 PM

Destination Original location

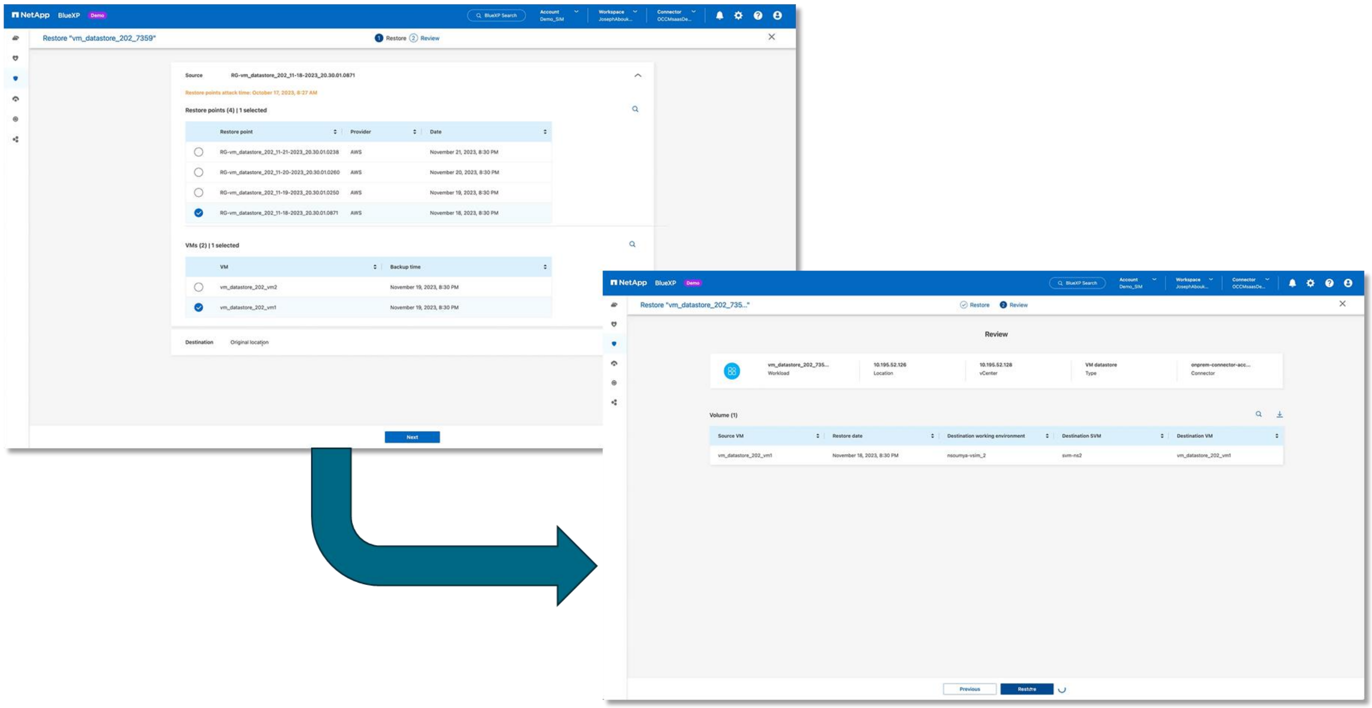
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

After choosing a restore point, we were presented with the VM backups and chose which VM backup to restore (Figure 10). Since we were restoring a VM, we could not change the destination. Other workload types enable users to choose to restore to a secondary location if desired. It is also possible to restore from a snapshot for even faster recovery.

Once we chose the VM and clicked **Next**, we were presented with a summary of the activity we were about to take, including the workload and VM information for confirmation. After clicking the **Restore** button at the bottom of the screen, BlueXP ransomware protection began the restoration process.

BlueXP ransomware protection uses a series of workflows to seamlessly restore workloads without human intervention. Once the restoration process is underway, BlueXP ransomware protection handles all of the details to ensure application consistency and health, fully restoring all data volumes behind the scenes. When restoring other workload types, such as file shares or applications, organizations can elect to restore them more granularly (i.e., by file or by volume).

Figure 10. Choosing a Restoration Point and Restoring a Workload



Source RG-vm_datastore_202_11-18-2023_20.30.01.0871

Restore points attack time: October 17, 2023, 8:27 AM

Restore points (4) | 1 selected

	Restore point	Provider	Date
○	RG-vm_datastore_202_11-21-2023_20.30.01.0238	AWS	November 21, 2023, 8:30 PM
○	RG-vm_datastore_202_11-20-2023_20.30.01.0260	AWS	November 20, 2023, 8:30 PM
○	RG-vm_datastore_202_11-19-2023_20.30.01.0250	AWS	November 19, 2023, 8:30 PM
✓	RG-vm_datastore_202_11-18-2023_20.30.01.0871	AWS	November 18, 2023, 8:30 PM

VMs (2) | 1 selected

	VM	Backup time
○	vm_datastore_202_vm2	November 19, 2023, 8:30 PM
✓	vm_datastore_202_vm1	November 19, 2023, 8:30 PM

Destination Original location

Review

Workload	Location	vCenter	Type	Connector
vm_datastore_202_735...	10.195.52.126	10.195.52.128	VM datastore	onprem-connector-acc...

Volume (1)

Source VM	Restore date	Destination working environment	Destination SVM	Destination VM
vm_datastore_202_vm1	November 18, 2023, 8:30 PM	nsoumya-vsim_2	svm-ns2	vm_datastore_202_vm1

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

Why This Matters

When a ransomware attack occurs, restoration and recovery are essential to ensure that ransoms don’t have to be paid. Enterprise Strategy Group research indicates that most companies (56%) that have been victims of a successful ransomware attack paid the ransom, with a further 57% saying they experienced and paid further extortion fees beyond the initial ransomware demand. Clearly, organizations need a way to restore their affected data to prevent having to pay to decrypt business-critical files.

Enterprise Strategy Group validated that BlueXP ransomware protection provides the tools necessary to recover from a ransomware attack with minimal downtime. After remediating an alert, we walked through the restoration process. We chose which restore point to use based on the time of the attack and restored a virtual machine to working order with application states and data intact. BlueXP ransomware protection does this with workflows behind the scenes and no manual intervention.

With many successful ransomware attacks shutting companies down for days or weeks, damaging revenue, and pushing many to pay the ransom to prevent further costs, organizations need a solution to quickly recover from attacks. BlueXP ransomware protection continually takes snapshots of data and provides the tools necessary for IT admins to restore data with minimal human intervention. If an attack happens, organizations won’t have to pay and will be able to restore business functions within minutes instead of days or weeks.

Conclusion

Ransomware has become a consistent threat to organizations of all sizes and industries. Attackers have noticed that unprepared companies are willing to pay ransomware recovery fees—and even more exorbitant fees after the fact—to get their businesses back up and running. Enterprise Strategy Group research indicates that ransomware attacks are not a matter of if, but of when, with three-quarters of organizations surveyed having experienced a ransomware attack in the past 12 months.

To successfully combat the growing hoard of ransomware attackers, organizations need a comprehensive plan to address the possibility of attack, along with the tools to implement it. Eighty-four percent of organizations surveyed take extra measures to protect their data backups in the event of a ransomware attack. Organizations need a solution to discover, detect, protect, and recover from attacks.

BlueXP ransomware protection provides NetApp customers with the tools required to protect the workloads in their NetApp storage infrastructure. Enterprise Strategy Group validated that BlueXP ransomware protection discovers all workloads—databases, apps, virtual machines, and file shares—and provides a risk overview and suggestions to improve it. BlueXP ransomware protection protects workloads by taking regular scheduled snapshots, watching for anomalous activity with its AI/ML-powered detection engine, blocking malicious file extensions, and seamlessly restoring affected workloads in the case of a successful attack.

BlueXP ransomware protection by NetApp helps organizations prepare for and recover quickly from an inevitable ransomware attack, enabling them to have confidence that they will never have to pay a ransom for NetApp storage workloads. If you use NetApp for your storage needs, Enterprise Strategy Group recommends you consider BlueXP ransomware protection for your environment.

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