E-BOOK

Safeguard your data from the inside out: Choosing the right cyber-resilience infrastructure

NetApp

Contents

```
package com.ds.ucd.be.becore.solr;

import ...

public final class LocationUtils {

    /**
     * Parses Point from it's String representation.
     * @param locationString - String that represents location, as 2 double
     * @return org.springframework.data.solr.core.geo.Point instance
     */
    public static Point parseLocation(String locationString) {
        Preconditions.checkNotNull(locationString,  errorMessage: "Location St
        Preconditions.checkArgument(locationString.contains(","),  errorMessa
        locationString = locationString.trim();

        if (locationString.contains(" ,")) {
            locationString = locationString.replaceAll( regex: " ,",  replaceme
        }

        if (locationString.contains(", ")) {
            locationString = locationString.replaceAll( regex: ", ",  replacemen
        }

        String[] location = locationString.split( regex: ",");
        Preconditions.checkArgument( expression: location.length >= 2,  errorMessa
        double lat = Double.parseDouble(location[0]);
        double lon = Double.parseDouble(location[1]);

        return new Point(lat, lon);
    }
}
```

You need more than backup

Ransomware, system failures, compromised credentials, and natural disasters: Cyberthreats attack your data from every direction. Internal, external, and environmental threats abound.

In today's environment, security doesn't mean securing just the perimeter and endpoints.

And effective protection? It's more than confirming that your data is backed up to another location.

If you're building a dream team to help keep your organization's most important asset—its data—safe against these threats, you need a superhero squad that's ready to safeguard your hybrid multicloud environment from end to end.

When ransomware strikes, do you want a partner who says, "Don't worry, I'll be here to help clean up the mess when the attack is over"?

Or do you want a dream team that can:

- **Protect.** Proactively protect your data to minimize damage
- **Detect.** Automatically detect threats and isolate them before they wreak havoc
- **Recover.** Help you recover data, workloads, and applications in minutes—rather than taking days

Building true cyber resilience requires the right technologies, which means going beyond simply relying on backups to restore data after a ransomware attack takes you offline. The best cyber-resilience solutions are built-in and protect you from data loss and downtime, proactively detecting potential threats and enabling quick recovery of data in minutes if something sinister strikes.

Cyber resilience: The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use cyber-resources

In NetApp terms: A comprehensive approach to deliver IT and to keep serving customers during any type of cyberevent

How do you choose the right solutions for cyber resilience?

So, how do you choose the right solution to modernize your cyber-resilience toolkit? Solutions that offer backup are important, but today's environment demands more. The cyber-resilience dream team goes beyond backup and provides the solutions that you need to protect, to detect, and to recover from cyberthreats in your hybrid multicloud environment. What should you look for when selecting a solution?

To help you select the right solution, you need to answer these four questions:

- **How will the solution be deployed?**
- **Will the solution help prevent cyberattacks?**
- **Will the solution deliver a consistent customer experience?**
- **Will the solution simplify operations and lower my TCO?**

How will the solution be deployed?

First, you need to decide how your solution will be deployed. Where do your data, workloads, and applications reside: on premises, in the cloud, or both?

On premises. Protect and secure your data, applications, and workloads in the data center with solutions that continuously monitor for threats, block recognized malware attempts, and give you the control to recover from an attack in minutes.

In the cloud. Look for solutions that protect your data in the cloud on your hyperscaler of choice. Avoid lock-in, and choose solutions that provide the same level of cyber-resilience support on AWS, Microsoft Azure, Google Cloud, or private cloud.

Both. True cyber-resilience solutions protect your data no matter where it resides. Leading solutions bring their full capabilities to all layers of complex hybrid cloud environments.

NetApp has the only enterprise-grade storage services that are embedded natively in the world's biggest public clouds. And our unified control plane makes it easier than ever to store, manage, and protect your data across a hybrid multicloud environment.

> "We recently experienced a ransomware event, and when we saw what Cloud Insights ransomware detection provides, we were sold."
>
> —Director of IT, Transportation Company

Will the solution help me prevent cyberattacks?

IT teams are under pressure to get solutions to market even faster, offer new IT innovations that increase performance and efficiency, and take the customer experience to the next level. Developing an effective cyber-resilience infrastructure helps your company protect its most valuable asset—now and in the future.

So, what do you look for? Make sure that your solution delivers these key features and capabilities:

- Protect against threats with continuous monitoring that identifies anomalous user behavior and storage performance.
- Automatically contain compromised user credentials and block known malware extensions to prevent malicious attacks.
- Securely and efficiently replicate data to other regions to protect against outages.
- Create smart, immutable, and indelible snapshots for rapid recovery on both structured (block) and unstructured (file) data.
- Deliver multilayered, sophisticated cyber-resilience support across the hybrid cloud and the world's largest clouds.

> "We want our users to be unaware of IT and just be able to access and store their data—today, tomorrow, or 5 years from now. NetApp solutions just run, and the data is safe. We can meet the high demands of a data-driven hospital with a small team. That's worth a mint."

—Maria Strey, Head of IT, Klinikum Freising

Will the solution deliver a consistent customer experience?

Have you ever spent days on restoring key applications and data or dealing with irate customers and workers who can't access what they need to get critical work done? Users don't have time to waste—and every minute that workers lose productivity or that customers can't access their data affects the bottom line.

It's critical that your cyber-resilience solutions keep your data, workloads, and applications online. So, what do you look for to keep your systems protected and your critical resources online?

Make sure that your solution delivers these key features and capabilities:

- Automatically fail over critical applications and data across sites to recover from unplanned outages to keep your customers connected at all times.
- Securely and efficiently replicate data to other regions to protect against natural-disaster outages to eliminate downtime that impacts your customer experience.
- Perform intelligent health checks and make recommendations to prevent unauthorized data access to keep critical customer data protected.

> "This is the most reliable ransomware protection we've found. One of our critical applications looks a lot like ransomware to other tools, and false positives have halted business more than once. Not so with Cloud Insights, which has been able to distinguish the difference between business as usual and an actual threat."

—Director of IT, Finance Company

Will the solution simplify operations and lower my TCO?

Built-in, rather than bolted-on, cyber-resilience solutions offer effective protection against ransomware and other emerging threats. If your only defense against ransomware is relying on backup, the minutes of downtime and the costs of restoring your data quickly add up. Ransomware attacks or data breaches can damage your bottom line, and simply relying on backups isn't enough to mitigate the damage to your revenue or reputation:

- Damage from ransomware attacks is anticipated to top $30 billion globally in 2023.[1]
- The average cost of dealing with a ransomware attack is $1.8 million.[2]
- Today, around 77% of businesses rely on backup software for data recovery.[3] With a 37% failure rate for backups and a 34% restore failure rate, relying on backups alone can be a risky proposition.[4]
- Data is growing by 50% per year.[5]

> "We had a ransomware attack, and the only data I could recover was on NetApp."
>
> —Leader of IT

So, what do you look for to help you move beyond relying on individual IT teams to spot threats and to help you streamline the costs associated with potential threats?

You should make sure that your solution delivers these key features and capabilities:

- Reduce IT costs by relying on AI tools that detect threats early with continuous monitoring for compromised users or file system anomalies, respond automatically, and thwart attacks, freeing up your staff to focus on innovation.
- Simplify operations and reduce the need for specialized cybersecurity staff with automatic responses such as the ability to identify and block more than 3,000 known malicious file types.
- Reduce the costs associated with restoring data with smart, immutable, and indelible snapshots that enable rapid recovery of structured (block) and unstructured (file) data.

Build cyber resilience into your hybrid cloud

Do NetApp® cyber-resilience tools protect you if your IT team manages data on premises? In the cloud? In a hybrid environment? At the edge?

Absolutely.

Because our cyber-resilience solutions are data-centric by design, your data is secure, resilient, and available no matter where it resides—on premises, at a remote location, or in the cloud. NetApp cyber-resilience solutions span your entire data estate, and key features make it easy for you to reap the benefits of the cloud.

You can:

- Migrate seamlessly to the cloud with NetApp Cloud Volumes ONTAP®, the leading enterprise-grade storage management solution that integrates with AWS, Azure, and Google Cloud.
- Scale your secure storage into the petabytes for diverse use cases, including file services, databases, DevOps, and other enterprise workloads.
- Use the NetApp BlueXP™ unified control plane to build, protect, and govern your entire hybrid multicloud data estate.
- Get hands-on help at any time from NetApp Data Migration Services for cloud to design your strategy and to execute the migration.

NetApp cyber resilience: Where data protection meets data security

While many of our competitors tell their customers that backup is the best protection against ransomware threats, we do more. NetApp approaches cyber resilience from the inside out.

Just as an automobile manufacturer designs the safety features of a car around the passengers, NetApp designs its protection and security solutions around your data.

Our portfolio of solutions includes powerful, robust data management; intelligent data and user monitoring; and professional services to help you at any stage of your preparation and management.

Across the hybrid cloud, NetApp technology protects and secures for cyber resilience:

- **Data availability.** Redundant everything combined with efficient data mirroring.
- **Data recovery.** Fast, efficient granular backup and archiving, on premises or in the cloud.
- **Threat detection.** Monitoring, detection, alerting, and prevention of known and newly discovered threats.
- **Threat remediation.** Rapid response and recovery to minimize disruption.

For many of our competitors, including Pure Storage, their response to threats such as ransomware focuses on backups. Backups are critical, but they're not enough to address the variety of cyberthreats. Restoring from a backup, as opposed to a local snapshot, requires data movement. The greater the damage from a cyberattack, the greater amount of data to be restored or moved and therefore the more time to restore. The longer it takes to detect the attack, the more damage and potential data loss as you will have to go further back in time to recover clean data.

Rapidly changing, multifaceted threats have put every single company at risk. The adoption of technologies that combat ransomware, build in redundancy, and deeply integrate protection and security is now imperative for business and technology leaders across the board.

NetApp cyber-resilience solutions:

- **Protect.** Prevent attacks and minimize data losses and downtime before they cost you big.
- **Detect.** Proactively identify attacks as they happen.
- **Recover.** Quickly restore data, workloads, and applications in minutes.

Proactively detect threats before they strike

Don’t leave detection of ransomware to chance or a deluge of help-desk tickets from angry users. Avoid the struggle of trying to identify threats manually and the chaos that can arise when you’re left to rely only on backups.

Instead, you need ways to identify and fix security vulnerabilities, discover ransomware, and use AI and machine learning to detect and to respond to threats in real time. You must be able to:

- Proactively detect abnormal behavior by potentially compromised users and automatically respond to minimize damage.
- Identify potential security gaps and prevent unauthorized data access by following remediation recommendations from automated health checks.
- Get automatic notifications when alarming behaviors occur—and get clear insights into which data is affected.
- Prevent malware attacks by automatically blocking more than 3,000 known malicious file extensions.

Always verify, never trust

A critical step is to develop an underlying architectural approach that makes it far more difficult for internal or external threats to succeed. By requiring verification for each attempt to access data, log in, or make a change, Zero Trust architecture brings a new level of security to your cyber-resilience efforts. Storage solutions that don’t support cyber resilience at this level are leaving the door open to threats.

Features to implement this protection should:

- Access the tools to deploy Zero Trust architecture, such as multifactor authentication, role-based access control, comprehensive logging, and auditing.
- Prevent damage from compromised credentials by using native NetApp ONTAP multi-admin verification (MAV). With MAV, more than one administrator must authorize critical storage actions such as the deletion of volumes and NetApp Snapshot™ copies, or even admin account creation.
- Manage user access with advanced access management and permissions controls that follow policy-based guidelines by user type, data type, and more.
- Detect anomalies in real time to identify compromised user accounts or possible rogue behavior based on permissions and policies.

Quickly recover when threats do strike

Effective cyber resilience helps you recover rapidly if ransomware breaches all your other defenses. Eliminate the need for your team to spend hours or days on restoring data—or waiting for physical tape to arrive—with features that:

- Create smart, immutable, and indelible snapshots for rapid recovery on both structured (block) and unstructured (file) data.
- Develop logical internal air gaps that also protect your structured and unstructured data from compromised administrator credentials or rogue administrator attacks.
- Support near-zero recovery point objective (RPO) and recovery time objective (RTO) solutions if a system failure occurs.
- Securely and efficiently replicate your data to other regions to protect against natural-disaster outages.
- Automatically fail over your critical applications and data across sites to recover from unplanned outages.
- Use snapshots to recover from any damage that occurs and to get your data, workloads, and applications back online in minutes rather than taking hours or days.
- Alert your IT and business leaders about concerning IT activities.
- Include forensic capabilities that provide deep and smart analytics after a cyber hit to identify the scope and root cause.

Take your cyber resilience to the next level

Don’t leave ransomware protection to backups alone. You need a solution that’s ready to protect you from end to end.

With NetApp solutions, you can build cyber resilience across your entire hybrid multicloud environment and have the tools to fight ransomware attacks and other cyberthreats from the moment that they’re detected.

Our data protection and data security solutions are built-in—not bolted-on—to help you proactively detect potential threats. And if a cyberthreat does strike, NetApp solutions help minimize your data loss and downtime and help you quickly recover data, applications, and workloads in minutes.

Learn more about NetApp

→ Explore solutions for ransomware protection

→ Connect with a cyber-resilience specialist

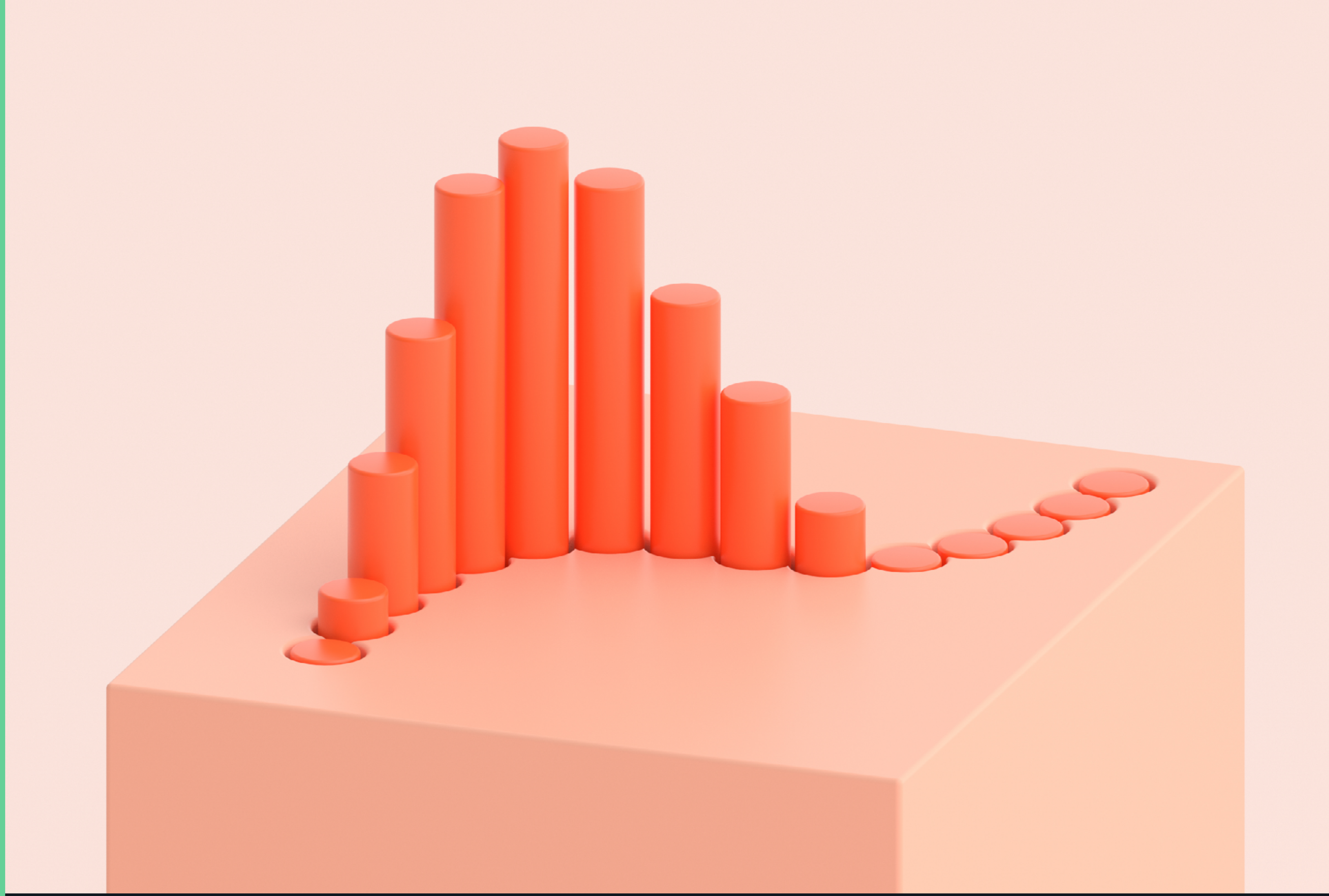
[1] - International Association of Privacy Professionals (IAPP), "Ransomware attacks on the rise in 2022," August 30, 2022.

[2] - Sophos, "The State of Ransomware 2021," April 2021.

[3] - Gartner Peer Insights, Cyber Resilience survey.

[4] - Veeam, "Data Protection Trends Report," March 2021.

[5] - IDC, "Worldwide Data Replication and Protection Software Forecast, 2019–2024: Rough Waters Ahead," July 2020.



About NetApp
In a world full of generalists, NetApp is a specialist. We're focused on one thing, helping your business get the most out of your data. NetApp brings the enterprise-grade data services you rely on into the cloud, and the simple flexibility of cloud into the data center. Our industry-leading solutions work across diverse customer environments and the world's biggest public clouds.

As a cloud-led, data-centric software company, only NetApp can help build your unique data fabric, simplify and connect your cloud, and securely deliver the right data, services, and applications to the right people—anytime, anywhere.

NetApp

+1 877 263 8277