

E-BOOK

Cyber resilience: Protect your data from the inside out with NetApp and Azure

 **NetApp** |  Microsoft Azure



Overview

- 3 Journey to the center of the IT organization
- 5 With threats everywhere you look, where do you start?
- 6 Chart your course to greater cyber resilience
- 7 **Identify:** Take stock of your environment
- 8 **Protect:** Put your defenses in place
- 9 **Detect:** Stay one step ahead
- 10 **Respond:** Know what to do in a crisis
- 11 **Recover:** Get back to normal in no time
- 12 Build a modern approach to cyber resilience from the inside out
- 13 A cyber-resilience plan in action with NetApp
- 17 A data-centric cyber-resilience plan no matter where data resides
- 18 Your cyber-resilience plan is just a few clicks away



Journey to the center of the IT organization

In today's world, where data is the lifeblood of organizations and cyberattacks are increasingly common, the alignment between data protection and data security teams has become essential.

It's no longer sufficient to rely solely on tools that are a step or two from the data. To mitigate the damage or loss of your most valuable asset, you need a deeply integrated and comprehensive data defense strategy.

A new approach to cybersecurity

For the past few decades, IT teams have used the “castle-and-moat” approach to cybersecurity, because that's what was available.

Today, there's a smarter approach: ***cyber resilience***.

Cyber resilience combines data protection with data security. Even if an intruder breaches the perimeter or an insider takes malicious action, your data remains uncompromised because it's safeguarded by built-in rather than bolted-on protection and security features.



Why does cybersecurity matter?

Previous cybersecurity measures aren't keeping pace with ever-evolving criminal tactics. Today:

- ❌ Most security strategies revolve around stopping the enemy at the gate by fortifying the perimeter.
- 🌐 Companies aren't defending just one gate. They're responsible for hundreds, thanks to the proliferation of endpoints, bring-your-own-device policies, and the rise of remote work.
- 🎯 It's now easier than ever for criminals to compromise organizations that are already too overwhelmed to thoroughly monitor complex network environments.

And many organizations forget that the goal isn't to prevent intrusions; prevention is only one of several facets of a cyber-resilience strategy. The main goal is to **protect your data**.



Cyber resilience

The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use cyber-resources.¹

In other words: Prepare for every eventuality.

With threats everywhere you look, where do you start?

Does your cyber-resilience strategy start with what matters most?

The stakes are higher than ever, and ransomware attacks have become a when-not-if reality of modern computing.

✓ With 66% of organizations hit by ransomware in the last year,² attackers are getting even better at holding data hostage.

✓ About one-third of organizations end up paying to get their encrypted data back after experiencing a ransomware attack.³

✓ The average cost to deal with a ransomware attack is up to US\$1.4 million and climbing.⁴

✓ Double-extortion ransomware attacks are on the rise, which means that organizations are at risk not only of losing their data, but also of having it leaked to the public.⁵

But do you have to live in fear of the next ransomware attack? No. You can unfear ransomware and **activate cyber resilience** by taking a data-centric approach to cybersecurity.

This approach means starting as close to the data as possible, rather than at the perimeter.



Chart your course to greater cyber resilience

If you're going to travel to the center of your IT organization to better protect your data, a little preliminary work is in order. Fortunately, others have already ventured forth and left some helpful guideposts:



Even with these markers to guide you, building a comprehensive cyber-resilience plan is still challenging and expensive. Your team has to juggle limited resources, fill in skills gaps, incorporate regulatory requirements, and jockey for attention with other priorities.⁶ Cyber resilience can quickly become exhausting—and forgotten.

Here's how to work your way through each step.



Identify:

Take stock of your environment

Identify what needs to be protected and rank each item by importance. Here are some questions to consider.

Do you know where your data resides and what data types exist in your environment?

For each type of data, is it sensitive, and who has access permissions?

Which systems are essential to maintaining business operations?

What role does each technology play in your business operations, and how could it potentially be exploited by a malicious actor?

Are information flows documented?

How are roles and responsibilities related to cybersecurity activities assigned?

What is your plan for threat identification and risk management?⁷

What are your current data protection and security solutions?

In other words, you need to assess your current data protection and security. You also need to classify different types of data, determine where the types are located, and evaluate their permissions.



Challenges associated with the Identify stage

The Identify stage is time consuming and IT leaders already have a tremendous number of day-to-day infrastructure and data management tasks on their plates. Just inventorying an entire IT infrastructure, especially without automation tools, can consume a significant amount of time.

If this inventory exercise isn't conducted with a specific plan or standardized classification protocols, it can create an even more confusing set of data that teams have trouble deciphering and operationalizing.



Protect: Put your defenses in place

In the Protect stage, you build your walls.

Encrypt your data, conduct regular backups, make sure that access controls are in place, implement perimeter defenses like firewalls, update vulnerable operating systems and applications, and train users about cybersecurity best practices.⁷

This stage involves blocking malicious users, quarantining potentially bad data, preventing additional data from being written to a disk, creating granular immutable copies that thwart infection, and preventing data deletion with indelible backups.



Challenges associated with the Protect stage

The Protect stage encompasses some of the latest changes in the approach to cybersecurity. Although organizations have been using firewalls and network intrusion tools for decades to protect their IT environments, the new reality of massive amounts of data has complicated these strategies. IT teams must answer challenging questions like:



How can you encrypt large amounts of data that's being generated faster than it can be inventoried?



How can you ensure access control without severely compromising user experience (potentially leading to lower productivity levels or unsafe workarounds)?



How can you be certain you've covered everything, given the number of blind spots you've uncovered?



What regular testing are you conducting of your data protection technologies to make sure that you can successfully recover your data if a threat occurs?

Detect: Stay one step ahead

Prevention is the best cure. Put systems in place that identify suspicious activity before it becomes an existential threat, including:

- Updated detection processes
- Regularly monitored logs to detect and address anomalous activity
- A thorough understanding of regular data flows, so that you can spot unusual activity that might signal data theft
- The ability to not just detect, but also gauge the impact (or “blast radius”) of a breach⁷

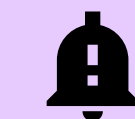
In other words, you need to monitor user behavior for suspicious activity and detect anomalies in data behavior.



Challenges associated with the Detect stage



Manage alert overwhelm: Possibly the greatest challenge of the Detect stage is the amount of noise that organizations must filter out. Cybersecurity teams and security operations centers are overwhelmed with threat alerts, which they often have to work through manually.



Automate threat triage: Teams need a way to automatically investigate and eliminate false and low-priority alarms, so they can dedicate their attention to the trickier alerts.



Increase detection speed: Cybersecurity teams also need a way to detect these threats faster, so they can respond before serious damage is done. In particular, they need immediate notice of unauthorized access with compromised credentials before a bad actor can encrypt a significant amount of data.

Respond:

Know what to do in a crisis

Threats evolve alongside security measures. Therefore it's important to continually put your plans to the test in three steps.

1

All team members must know their responsibilities, including general cybersecurity best practices and their specific roles in an emergency.

2

Update plans as threats evolve and as lessons are learned in the aftermath of attacks.

3

Share all plan updates with other stakeholders, both internal and external, so that there's a cohesive response if an attack occurs.⁷



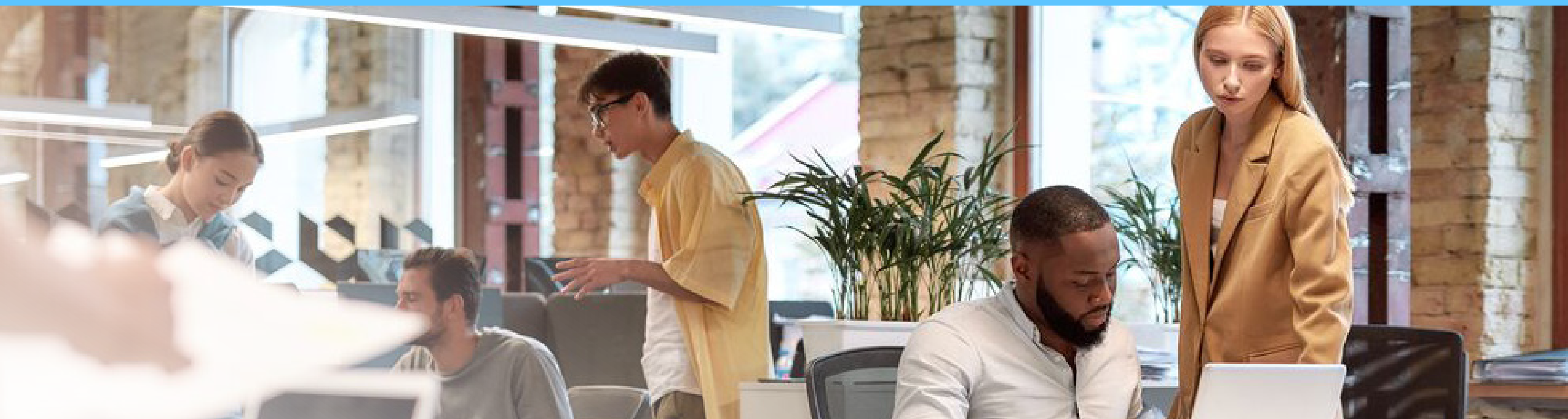
Challenges associated with the Respond stage

Acing the Respond step requires an overview of your systems, so you can evaluate where your data is, monitor what kind of activity is happening in your environment, and update your plans accordingly.

This is a time-intensive activity for organizations that are already overwhelmed with day-to-day infrastructure and data management needs.

And the truth is that any effective response needs to be faster than the time it takes for individuals to manually execute a plan, no matter how well prepared.

Cybersecurity teams need automated tools that follow predetermined steps—such as taking a data snapshot—as soon as the system detects suspicious activity.



Recover:

Get back to normal in no time

If a cyberattack interrupts business operations, you need to be able to get back up and running quickly. It's imperative to know:

- What information will need to be shared?
- Who will need access to this information?
- How will you make sure that these stakeholders get the information they need in a timely manner?
- How will you communicate the breach to the public, informing people whose information might have been compromised?
- What steps you need to take to communicate with regulatory bodies?

In the Recover stage, you want to reduce downtime by restoring data quickly, bringing uncompromised applications back online, and applying intelligent forensics to identify the source of the threat.



Challenges associated with the Recover stage

In the aftermath of an attack, it can take valuable time to identify what's been compromised and how much. But you need to get this information quickly to manage both the internal response and the external optics.

These five parts of a cyber-resilience plan—Identify, Protect, Detect, Respond, and Recover—are supported by the NetApp® cyber-resilience solution. But many organizations are invested in a patchwork of cybersecurity tools that can make even the thought of shifting to another provider overwhelming.

With NetApp you don't have to be overwhelmed by this shift. You can introduce a ransomware solution that serves as either a full-scale solution or a complement to your existing investments.



Build a modern approach to cyber resilience from the inside out

Let's take a closer look at building a modern approach to cyber resilience for your business, including the solutions that can address the common challenges just described. NetApp cyber-resilience solutions approach these challenges from the inside out, with security and protection solutions designed around your data.

NetApp's portfolio of solutions for Azure includes powerful, robust data management, intelligent data and user monitoring, and professional services to help organizations at every stage of their preparation and management.

When your data becomes your primary focus, it's easier to tackle your cyber-resilience needs. Your first step is understanding your current state by working through the following questions.



Prevention is the best cure. Put systems in place to identify suspicious activity before it becomes an existential threat. Ask yourself:

- Where is my data located? In the cloud? On the premises? At the edge? In multiple regions?
- What kind of data do I have?
- What kinds of permissions does my data have?
- How can I quickly identify and block malicious activity?
- How can I make sure that all my data is safe while I determine the blast radius of an attack?
- How can I bring my data and applications back online, in minutes, if an attack occurs?
- How can I investigate the source of a threat so that I have enough information to prevent future similar attempts?
- How can I build protection directly within or around my data so that it can “self-protect” quickly—while we’re identifying and addressing a threat?
- How can I monitor user behavior for suspicious activity across my global network?

By answering all of these questions, you create the skeleton for a data-centric cyber-resilience plan that can help your organization prepare for ransomware attacks.

Perhaps you answered “unknown” to some of these questions. NetApp offers professional services that not only give you answers but also provide the tools you need to execute your new ransomware protection and recovery plan.

A cyber-resilience plan in action with NetApp

NetApp Cloud Volumes ONTAP® for Azure and Azure NetApp Files are designed to address the needs of IT and security teams to protect and secure data across on-premises and Azure environments. Built on NetApp ONTAP storage management software, Cloud Volumes ONTAP and Azure NetApp Files integrate with NetApp data services that enhance visibility, detect threats, and automate response and recovery.

“We recently experienced a ransomware event, and when we saw what Cloud Insights ransomware detection provides, we were sold.”



Director of IT, Transportation Company





Identify

Your team needs to know what kind of data you have, whether it is sensitive, and where that data is located in order to plan how to protect it. NetApp BlueXP™ classification uses artificial intelligence algorithms for data discovery, mapping, and classification to deliver this information.

Also, BlueXP observability provides visibility across your on-premises and Azure infrastructure, enabling your team to monitor and secure your entire environment. And it's a good thing, too, because your defenses are about to be put to the test.



Protect

Consider this scenario. One morning, your New York–based IT team comes into work and learns that someone in the London office has clicked an unfriendly email link.

Even though no one was around to physically monitor this attack, NetApp FPolicy, part of ONTAP and supported for use with Cloud Volumes ONTAP for Azure, used its Zero Trust data protection to block known malicious file extensions.

Nevertheless, these hackers persist. They use a compromised user account to infect files through a zero-day malware exploit. More malware taps into several compromised user accounts to encrypt data—slowly, in the hope of avoiding detection.

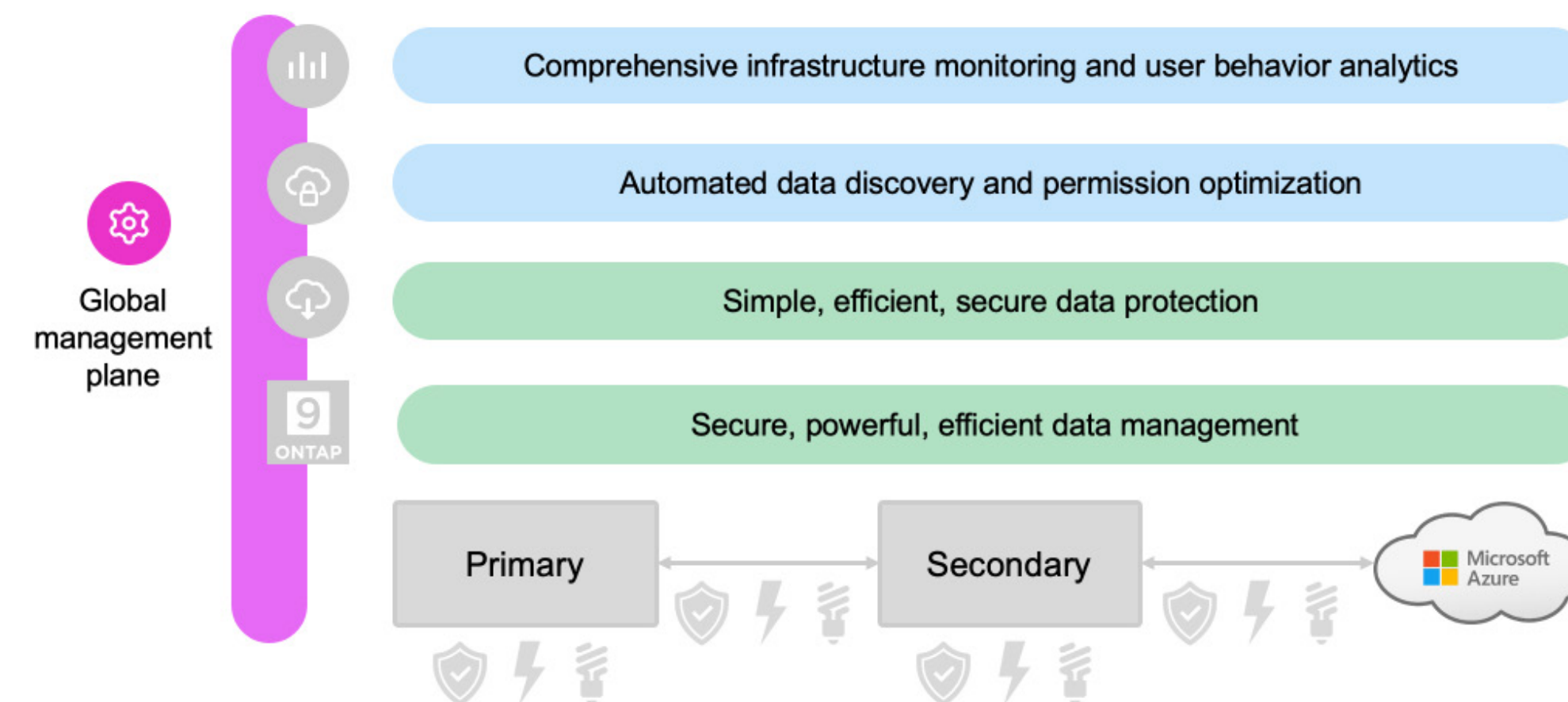


Detect and Respond

Spotting and combating all of this activity would be difficult for a few individuals to accomplish, especially if they're juggling other responsibilities in a different time zone. But the IT team has BlueXP observability, which integrates with Cloud Volumes ONTAP for Azure, to monitor and spot user behavioral anomalies. Even if the team doesn't notice the attack, BlueXP does and instantly creates a NetApp Snapshot™ copy to protect the data.

Your primary volume may be susceptible to encryption, but your Snapshot copies are immutable, and when combined with BlueXP backup and recovery, deliver a secure and effective data protection strategy. Write once, read many (WORM) cloud storage, powered by the SnapLock® feature of ONTAP, provides indelible copies that can be used for secure data retention and as a logical air gap.

Observability can also identify the source of the attack and automatically block the compromised user account to prevent further damage and help prevent data exfiltration.





Recover

With BlueXP classification and observability services, you can apply intelligent file forensics to identify what data was affected and by whom, enabling you to focus your data recovery efforts, reducing downtime.

Your IT team can then proceed to restore data rapidly—terabytes in minutes—by using NetApp tools. Logs can be exported to leading security information and event management (SIEM) software for further analysis.

And despite the high drama of the moment, the entire team can rest easy. Data recovery was never in question because NetApp uses WORM cloud storage powered by the SnapLock feature of ONTAP to lock files to prevent data deletion.

A data-centric cyber-resilience plan no matter where data resides

Does this scenario still apply if your IT team manages data on premises? In the cloud? In a hybrid environment? At the edge? Absolutely yes to all.






Because cyber resilience is data-centric by design, your data is always fully secure, resilient, and available no matter where it resides—on premises, at a remote location, or in the cloud. The NetApp cyber-resilience solution spans your entire data estate, including Azure and on premises.

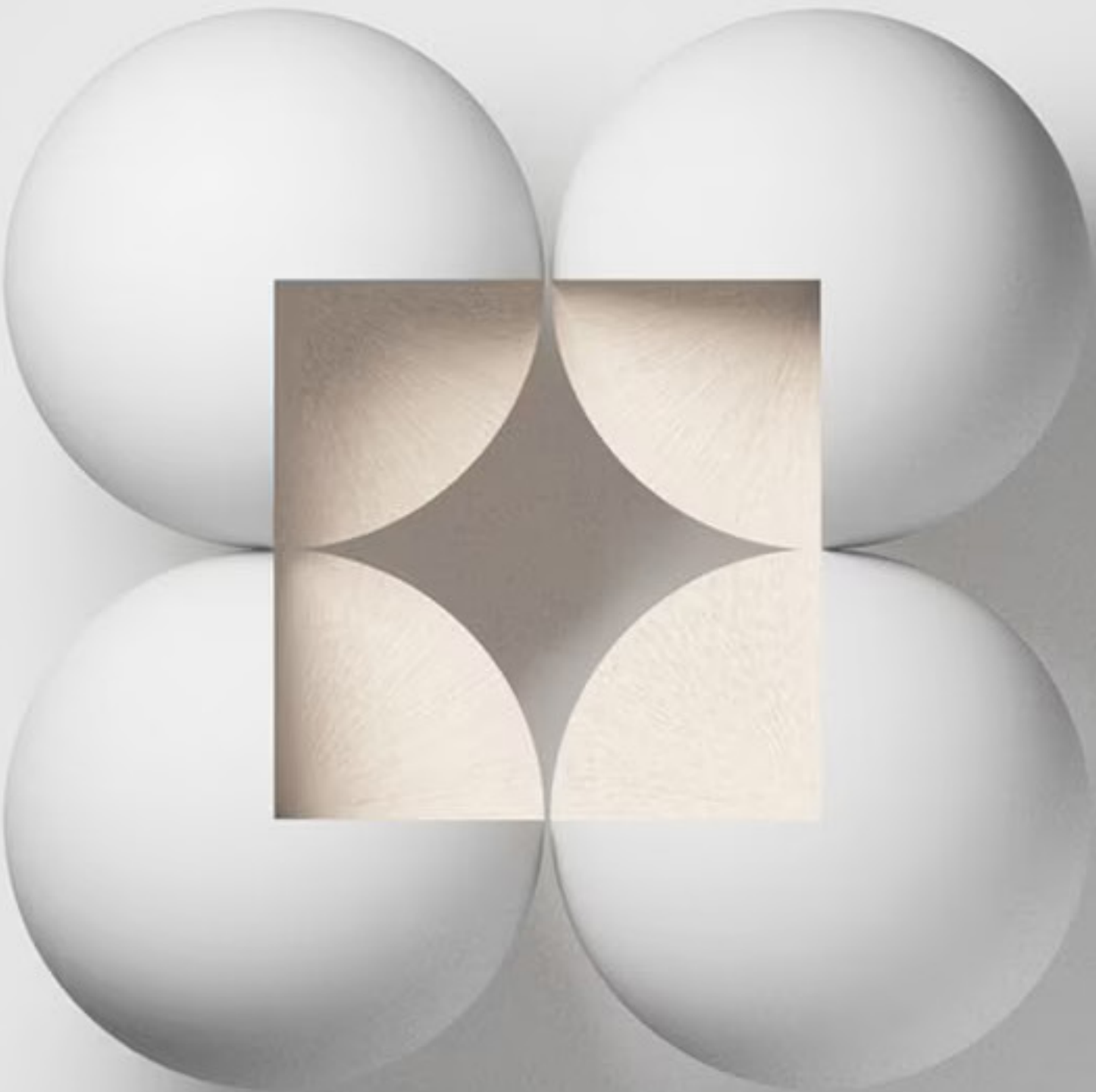
Make the most of your existing investment

The data-centric NetApp cyber-resilience solution can assist with all five stages of the plan outlined here. But your organization might have already invested in cybersecurity tools. ONTAP software features can integrate with many existing cybersecurity investments, so you can close gaps instead of starting over from the beginning.

Protect		Detect	Recover	
Identify	Protect	Detect	Respond	Recover
<p>Thwart ransomware attacks and prevent unplanned data loss:</p> <ul style="list-style-type: none">• Block malicious files (FPolicy)• Establish rapid, granular recovery points (Snapshot™)• Efficiently replicate data for backup and disaster recovery (SnapMirror®)• Create a logical air gap and flexible secure data retention (SnapLock®)• Identify and correct security exposures on your storage system (Active IQ® Digital Advisor)• Learn normal user file access behavior (BlueXP™ observability)• Categorize and locate sensitive data (BlueXP classification)• Identify file access permissions (BlueXP classification)		<p>Quickly identify threats before they become a problem:</p> <ul style="list-style-type: none">• Trigger alerts based on storage behavior (BlueXP)• Detect data and storage anomalies (BlueXP ransomware protection)• Visibility into unusual user director performance metrics (file system analytics)• Identify change in user file access patterns (BlueXP observability)• Detect attempted mass file deletions (BlueXP observability)	<p>Restore data rapidly and accelerate application uptime:</p> <ul style="list-style-type: none">• Recover data in minutes, locally or remotely (SnapRestore®)• Apply file level forensics (syslog)• Initiate NetApp® Snapshot™ recovery point (BlueXP observability)• Block malicious user accounts (BlueXP observability)• Provide forensic data to identify which files to restore (BlueXP observability)	
Secure access with end-to-end encryption, multifactor authentication, role-based access				

Your cyber-resilience plan is just a few clicks away

-  [Schedule a 1:1 cyber-resilience strategy session](#)
-  [Read our e-book on real stories of data loss](#)
-  [Take the self-assessment—Where does your security strategy stand?](#)
-  [Read up on Azure ransomware protection](#)
-  [See the NetApp cyber-resilience overview for Azure](#)



1. National Institute for Standards and Technology, [Developing Cyber-Resilient Systems](#), December 2021.
2. Sophos News, [The State of Ransomware 2022](#), April 20, 2022.
3. Statista, “[Methods of organizations compromised by ransomware to get their encrypted data back as of February 2021](#),” 2021.
4. Sophos News. [The State of Ransomware 2022](#), April 20, 2022.
5. Deloitte, [Double extortion incidents](#), October 2020.
6. Infosec, [NIST CSF: Implementing NIST CSF](#), February 19, 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.



+1 877 263 8277