

E-BOOK

# NetApp and Google Cloud: Solving the challenges that will help you get the most from your cloud journey

**Cyber resilience:** How to take an inside-out approach to overcoming data protection and data security challenges in the cloud

 **NetApp** | Google Cloud





# We can't wait to show you what's in store for you on your Google Cloud journey.

## But first, let's start with a confession.

At NetApp, we're cloud obsessed. That's why one of the things we love to do is solve cloud challenges. It gets our engineering engines revving, satiates our appetite for new possibilities, and paves the way for us to create innovative solutions for problems of any size.

That's why we work so well with Google Cloud. At our core, we are technology engineers that love to solve problems. NetApp's deep expertise in all things data—data management, data protection, data migration—perfectly complements the scale, agility, and analytics of Google Cloud. Our partnership is a testament to the power of working together and listening to each other, to our market, and most importantly, to you – our customers.







From the deployment of key workloads to unplanned outages and big cloud bills, when you run into challenges on your cloud journey, we listen, solve problems, and show you the way forward. Whether you need a solution that's already available (but maybe you didn't know it was out there) or something more customized, our partnership with Google Cloud empowers you to accelerate time-to-market while building better technology.

We know some of you may not be as cloud obsessed as we are. That's okay; it's why we made this guidebook. This is the place where you can get excited about your cloud future while improving your cloud present. Discover new capabilities, find the answers to your cloud conundrums, and get started on the next step in your journey, knowing

that at every point along the way you're supported by the smartest people in the Google Cloud and NetApp universe.

Throughout this guidebook, you'll find unique cloud journeys that feature specific challenges and a recurring theme that can't be overstated:

*Helping you expertly navigate all the things in and around Google Cloud that mean the most to you and your business.*

After going through this guidebook, you'll see the opportunities that arise from having the full weight of NetApp and Google Cloud in your corner – in the hybrid cloud and wherever your journey takes you.

**– The NetApp Google Cloud Team**





# How to navigate this guidebook

## Choose your path

You'll get to choose between two paths up ahead: one for those born in the cloud and one for those who started in the data center. Take the path that best describes your circumstance.

### Born in the cloud

Your business lives in the public cloud and doesn't have a second home on-premises. PaaS, SaaS, IaaS, DaaS—you fully embrace the as-a-service model. Pay-as-you-go (PAYGO) is your bread and butter. At heart, you're looking to build innovative applications with the newest technologies, faster, smarter, and more efficiently than ever before.

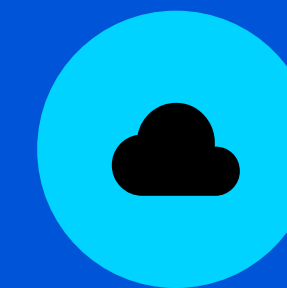
### On-premises to the cloud

You set off on your cloud journey only to find it's not as straightforward as you'd hoped. You're facing legacy hardware, expensive third-party software licenses—and you haven't even migrated half of your data to the cloud. To you, "emerging technologies" is a euphemism for "emerging complexities." In this case, what you really want is what you really need: to augment everything you do on-premises with competitive advantages that can only be claimed in the cloud.

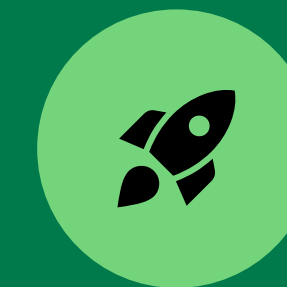
## Now you're in control

Watch for the icon that most closely matches your scenario to follow the path that best aligns to your priorities and challenges. This will help you to identify the best solutions for you to consider.

## Ready to get started? Let's go!



**Born in the cloud**



**On-premises to the cloud**



# Constructing the pillars of data protection and data security in your cloud environment



Uptime, regional availability, ransomware, natural disasters, unfettered user access—your organization's data is at risk.

There are solutions, but what's needed is a global approach. A shift in mindset. A cover-all-bases-ahead-of-time method of dealing with your cloud environment insecurities while keeping your customer data secure.

In other words, the old sports adage is true: The best defense is a good offense. You need a data-centric approach to data protection and security that is prepared to overcome the obstacles standing in your way of becoming a cyber-resilient enterprise.





**More data**

With data exploding at a 40-50% compound annual growth rate (CAGR), you're likely feeling the pressure of having to protect a rapidly expanding data storage footprint. It doesn't help that almost 80-90% of that data is unstructured, untouched, and flying under your organization's radar. In other words, your data is a sitting duck, a vulnerability, a cybercriminal network's idea of a "goldmine."

**More cyberthreats**

Most organizations (72%) saw a significant uptick in the volume, sophistication, and impact of cyberattacks last year.<sup>1</sup> This speaks to a fundamental principle of risk management: not all risks can be eliminated, but they can be effectively mitigated. "How?" is the \$1.4 million dollar question (which is the average cost of remediating a ransomware attack).

**More downtime**

As the IDC observes, "Petabyte-scale deployments are becoming commonplace"—and here comes the kicker: "traditional backup methodologies can no longer cope with such data volumes."<sup>2</sup> And when the cost of downtime hits \$9,000 per minute, there are nine thousand reasons to have rapid data recovery on hand if something goes wrong.

Faced with these challenges, organizations need a cyber resilience solutions portfolio that proactively anticipates threats and allows you to bounce back quickly when (not if) an attack happens.





## NetApp's pillars of cyber resilience

### Data protection

- Data availability. Always-redundant everything, with efficient data mirroring.
- Data recovery. Extremely fast and efficient granular backup and archive on-premises or in the cloud.

### Data security

- Threat detection. Monitoring, detection, alerting, and prevention of new and existing threats.
- Threat remediation. Quick response to and recovery from cyberattacks, with minimal disruption.

Let's explore the reasons why your enterprise needs enhanced data protection and data security capabilities. We'll look at the challenges you might run into along the way. And we'll discuss how—together—NetApp and Google Cloud can help you become a cyber-resilient enterprise.





# Let's start with your priorities

- 🚀 Data center costs →
- 🚀 Data center departure →
- 🚀 ☁ Global security measures →
- 🚀 ☁ Always-available data →
- 🚀 ☁ Data protection and security →
- 🚀 ☁ Avoiding GDPR penalties →





# Let's start with your priorities

## Data center costs

### Data center departure

### Global security measures

### Always-available data

### Data protection and security

### Avoiding GDPR penalties



## Data center costs

The aging hardware in your data center is getting too expensive. Continually refreshing that hardware is costly, wasteful, and may not use the most efficient servers in your data center. And it takes way too long to requisition parts if something is missing, breaks, or needs an upgrade.

What challenges might I face?



# Let's start with your priorities

 Data center costs 

 Data center departure

  Global security measures 

  Always-available data 

  Data protection and security 

  Avoiding GDPR penalties 



## Data center departure

Your expensive data center is about to expire and the task of meeting your company's cloud mandate is just waiting to be tackled. At this point, it's become obvious that traditional backup and recovery methods are not as quick, effective, or comprehensive as your systems need. Simply put, some big (and long overdue) changes are in order.

What challenges might I face?



# Let's start with your priorities

🚀 Data center costs ➔

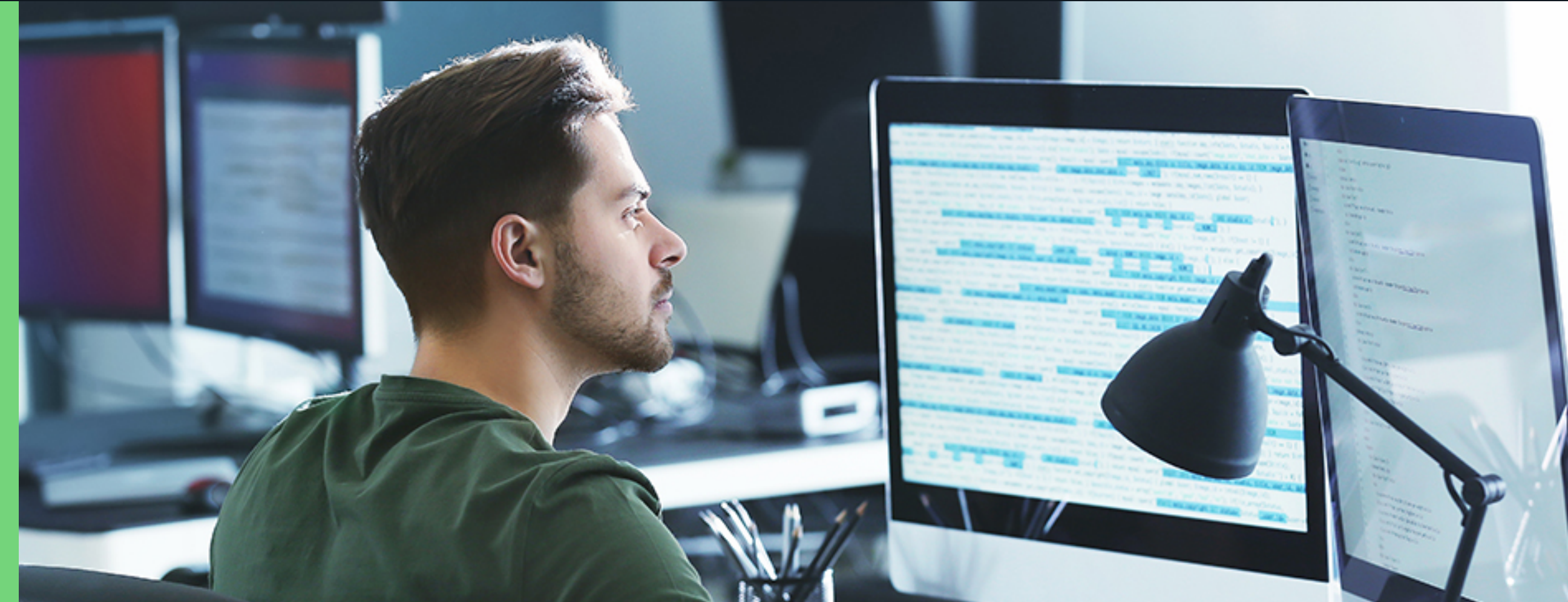
🚀 Data center departure ➔

🚀 ☁ Global security measures

🚀 ☁ Always-available data ➔

🚀 ☁ Data protection and security ➔

🚀 ☁ Avoiding GDPR penalties ➔



## Global security measures

The security of your data—which is accessed by professionals around the world—is a significant concern. You want to be able to say that your systems will never go down, that you're insusceptible to data loss, and that you've got redundant systems with efficient data mirroring. Not being able to say any of that with confidence means you're ready to enforce global security measures.

What challenges might I face?



# Let's start with your priorities

 Data center costs 

 Data center departure 

  Global security measures 

  Always-available data

  Data protection and security 

  Avoiding GDPR penalties 



## Always-available data

Your workforce is all over the place, which is why you've got data in different regions. It needs to be available and easily accessible; your data should always be ready to use at the level of performance you and your global team require—no matter where it's located—especially when a potential downtime-causing disaster strikes your data.

What challenges might I face?



# Let's start with your priorities

🚀 Data center costs ➔

🚀 Data center departure ➔

🚀 ☁ Global security measures ➔

🚀 ☁ Always-available data ➔

🚀 ☁ Data protection and security

🚀 ☁ Avoiding GDPR penalties ➔



## Data protection and security

The World Economic Forum found that cyberattacks increased by 125% in 2021.<sup>3</sup> More recent analysis shows that protecting your perimeter from external threats and insulating your systems from internal threats are imperative to maintain business continuity.<sup>4</sup> You need new toolsets and skills to shield your data—not just from cybercriminals targeting you and your customers' data, but from human error and former employees as well.

What challenges might I face?



# Let's start with your priorities

 Data center costs 

 Data center departure 

  Global security measures 

  Always-available data 

  Data protection and security 

  Avoiding GDPR penalties



## Avoiding GDPR penalties

The business implications of government regulations for data protection have you thinking about how your company stores an enormous amount of personal information about website visitors, shoppers, employees, and users. You need to know what you have, where it is, and if you should even have it—all while ensuring that PII within the company isn't shared with anyone who doesn't have proper clearance.

What challenges might I face?



# Challenges

- Hybrid cloud security expert →
- Manual threat monitoring →
- Staying compliant →
- Cloud skills gap →
- Privacy issues →
- Backup and recovery →





# Challenges

## Hybrid cloud security expert

  Manual threat monitoring 

  Staying compliant 

  Cloud skills gap 

  Privacy issues 

  Backup and recovery 

## Hybrid cloud security expert

How do you fill the knowledge and resource gaps that arise when your on-premises team becomes a cloud team? You've got new security concerns now. Your data in the cloud not only needs to be secure in its new home, but also when it's on the move and every time anyone touches it around the world. Will your data center experts get up to speed with networking, authentication, encryption, and multifactor authentication in the cloud?

[Back to priorities](#)[What is the solution?](#)



# Challenges

 Hybrid cloud security expert 

  Manual threat monitoring

  Staying compliant 

  Cloud skills gap 

  Privacy issues 

  Backup and recovery 

## Manual threat monitoring

You can tell your security is lacking. Yes, your team is industrious, smart, and resourceful. But their powers are limited, and security threats only multiply with time. How much damage can be done before anyone notices? It's hard to know in advance. All you can say for certain is that:

- a) U.S. businesses lost \$6.9 billion in 2021 to cybercriminals,<sup>5</sup> and
- b) you don't want to be one that tips this figure over into 7 billion.

[Back to priorities](#)

[What is the solution?](#)





# Challenges

- Hybrid cloud security expert →
- Manual threat monitoring →
- Staying compliant**
- Cloud skills gap →
- Privacy issues →
- Backup and recovery →



















## Staying compliant

As unstructured data accumulates across your cloud or hybrid cloud environment, you may lose track of confidential information and visibility into how well it's protected. Does it meet government regulations? Should you even have it at all? If not, how do you dispose of it properly? If you had the ability to discover, classify, and govern your data anywhere it resides, you could remove these questions from your list of concerns.

[Back to priorities](#)[What is the solution?](#)



# Challenges

-  Hybrid cloud security expert 
-   Manual threat monitoring 
-   Staying compliant 
-   Cloud skills gap
-   Privacy issues 
-   Backup and recovery 



## Cloud skills gap

You may (or may not) know a lot about cloud, but what you do know is that you're not a cloud-regions expert. It's not obvious if you should choose to store your data in one region over another, or if one region offers better coverage and services for your specific needs. Do cloud-region experts exist? If so, where do you find one? You need to know because you're in charge of closing this knowledge gap.

[Back to priorities](#)[What is the solution?](#)



# Challenges

- Hybrid cloud security expert →
- Manual threat monitoring →
- Staying compliant →
- Cloud skills gap →
- Privacy issues
- Backup and recovery →



















## Privacy issues

Think back to six months ago when one of your best programmers left the job because ... well, it's not why they left that matters. What matters is you just found out that they still have access to sensitive company information. This discovery raises a potentially costly question that comes with penalties: Who else might have access to your files that shouldn't?

[Back to priorities](#)[What is the solution?](#)



# Challenges

-  Hybrid cloud security expert 
-   Manual threat monitoring 
-   Staying compliant 
-   Cloud skills gap 
-   Privacy issues 
-   Backup and recovery

## Backup and recovery

Replacing a single file may require replacing the entire volume from the backup. Full restorations take a long time. Creating a dummy environment to see if the backup is dependable is also time-consuming. The goal is to get back up and running as quickly and efficiently as possible. However, there are so many steps required to bounce back quickly, they're slowing down you and your business.

[Back to priorities](#)[What is the solution?](#)



# Solutions

  Step 1. Protect



  Step 2. Detect



  Step 3. Recover





# Solutions

  Step 1. Protect

  Step 2. Detect



  Step 3. Recover



## Step 1

### Protect

Classify your data with an AI-driven toolkit for enhanced governance and privacy.

Map your data landscape



Encrypt it but don't throw away the key



Back to priorities

Back to challenges

Onward to resources





# Solutions



## Step 1. Protect



## Step 2. Detect



## Step 3. Recover



### Step 1

## Protect

Classify your data with an AI-driven toolkit for enhanced governance and privacy.

Map your data landscape

Encrypt it but don't throw away the key



Use AI-driven capabilities to discover, classify, and govern your data across your entire data estate. File shares, object storage, databases—you can scan both cloud and on-premises data from every source and see where the risks are hiding.

With an AI solution that discovers and classifies your data for you, you gain unprecedented visibility into your hybrid cloud environments. It also means you'll satisfy compliance requirements for data usage audit reporting to save time and money.

Let a digital advisor take it from there. NetApp® Active IQ® performs health checks and can point out any best-practice gaps that need corrective action. Active IQ will also detect issues before they become problems and reduce time spent on storage operations. Fun evidence-based fact: after implementing Active IQ, users were able to resolve issues 2x faster.

[Back to priorities](#)

[Back to challenges](#)

[Onward to resources](#)





# Solutions

## Step 1. Protect

## Step 2. Detect



## Step 3. Recover



### Step 1

## Protect

Classify your data with an AI-driven toolkit for enhanced governance and privacy.

Map your data landscape



Encrypt it but don't throw away the key

When you think about the doors to your sensitive data, you want to know who holds the keys. For end-to-end protection, enterprises need to enforce encryption policies that cover data, whether it's moving or sitting in storage.

### Data encryption at rest—always.

Every volume is encrypted at rest using AES-256 encryption. All user data written to media can only be decrypted with a per-volume key.

### Data encrypted in transit

Data in transit can be encrypted at the NAS protocol layer to ensure secure data transport. Secure private networks with optional protocol end-to-end encryption.

### Customer-managed encryption keys (CMEK)

CMEK functionality gives you the option to encrypt your per-volume keys with a per-project, per-region master key that's hosted in Google Key Management Service (KMS).

Now that your data is safe under lock and encryption key, the next step is thwarting potential cyberattacks ahead of time.

Back to priorities

Back to challenges

Onward to resources





# Solutions

  Step 1. Protect



  Step 2. Detect

  Step 3. Recover



## Step 2

### Detect

Uncover security vulnerabilities with enhanced attack pre-emption capabilities.

Know who's touching your data



Fortify your storage  
operating system



Keep the overhead to  
a minimum



Back to priorities

Back to challenges

Onward to resources





# Solutions



Step 1. Protect



Step 2. Detect



Step 3. Recover



## Step 2

### Detect

Uncover security vulnerabilities with enhanced attack pre-emption capabilities.

Know who’s touching your data

Fortify your storage operating system



Keep the overhead to a minimum



The beauty of role-based access control (RBAC) is that you’ll never have to ask, “Who’s that creeping in my files?” RBAC is like a badge reader that only permits access to software and resources that users need based on their role (storage admin, backup admin, application owner, etc.). Anything you don’t want them to see or touch will be out of sight, out of mind, and out of (potentially malicious or accidentally damaging) reach.

[Back to priorities](#)

[Back to challenges](#)

[Onward to resources](#)





# Solutions



Step 1. Protect



Step 2. Detect



Step 3. Recover



## Step 2

### Detect

Uncover security vulnerabilities with enhanced attack pre-emption capabilities.

Know who’s touching your data



Fortify your storage operating system

Keep the overhead to a minimum



Go with a storage operating system that follows a “Zero Trust Model” and treats all traffic within your environment as hostile unless proven otherwise. NetApp protects your data with built-in capabilities, such as space-efficient, immutable snapshot copies. These capabilities provide rapid and granular data recovery and prevent encryption by malware. When a malicious actor is trying to delete or encrypt data, a Snapshot™ copy provides a recovery point that takes you back to a happier time—before any damage took place.

[Back to priorities](#)

[Back to challenges](#)

[Onward to resources](#)





# Solutions



Step 1. Protect



Step 2. Detect



Step 3. Recover



## Step 2

### Detect

Uncover security vulnerabilities with enhanced attack pre-emption capabilities.

Know who's touching your data



Fortify your storage operating system



Keep the overhead to a minimum

Close your skills gap with the automated ease of emerging technologies. Let AI do the proactive detective work for you (and your team). This way, you won't have to depend on your admin to spot unusual user behavior that's indicative of ransomware or rogue users. You can also receive automated alerts that notify you when attacks or mass deletions are detected, allowing you to address—and resolve—issues in record time.

[Back to priorities](#)

[Back to challenges](#)

[Onward to resources](#)





# Solutions

 Step 1. Protect 

 Step 2. Detect 

 Step 3. Recover

Step 3

## Recover

Restore data rapidly and accelerate application uptime to bounce back faster.

You’ve protected your data and got AI-driven eyes on your entire data estate. All good, right? Alas, the logic of Murphy’s law never falters: “Anything that can go wrong will go wrong.” And when it does, you want—scratch that, *need*—to develop and implement a plan that:

- a) maintains your resilience in the face of disruption, and
- b) will restore any capabilities or services that were impaired during this “cybersecurity incident.”

Let’s put that plan into action.

Stop, drop, and SnapLock



Bouncing back to business



Back to priorities

Back to challenges

Onward to resources





# Solutions

  Step 1. Protect



  Step 2. Detect



  Step 3. Recover

## Step 3

### Recover

Restore data rapidly and accelerate application uptime to bounce back faster.

Stop, drop, and SnapLock

Bouncing back to business



Hackers often get access to an IT environment and then look for backup copies of the data they want to corrupt. They will try to delete the backup copies while encrypting production data to extort money in exchange for the encryption key. SnapLock™ prevents hackers (or rogue administrators) from deleting your data. It makes indelible data copies that can't be changed or deleted within the scheduled retention period.

Your backup copies are protected against intentional (and accidental) deletion and all the headaches that come with it. Now let's take the final step to achieving cyber resilience.

Back to priorities

Back to challenges

Onward to resources

#### About SnapLock

SnapLock is a feature of ONTAP® that provides WORM (write once, read many) file locking, which can be used for many purposes: corporate data retention policies, HIPAA compliance, or SEC compliance, where data must be retained for certain amounts of time.





# Solutions

  Step 1. Protect



  Step 2. Detect



  Step 3. Recover

## Step 3

### Recover

Restore data rapidly and accelerate application uptime to bounce back faster.

Stop, drop, and SnapLock



Bouncing back to business

With **ONTAP SnapRestore®**, you can restore petabytes of data locally or remotely in minutes.

- Neutralize the impact of the security incident on your business without breaking your budget.
- Block malicious user accounts and apply file-level forensics to identify which files you want to restore.
- Store backups in low-cost Google Cloud archival storage once you’ve completed the initial backup so you won’t have to worry about TCO.

Once you’ve completed the initial backup, you’ll only be charged for changes to data blocks. And that will be that—you’ll have bounced back to business in minutes with nothing but serious cost savings to show for it. Revenge against cybercriminals is a dish best served with lower TCO.

Back to priorities

Back to challenges

Onward to resources





# Next steps

We've explored the priorities that put you on this cloud adventure.

We've outlined some challenges that you can expect to encounter—or maybe already have encountered—along the way.

And we've given you options to consider on your path forward, as well as the benefits waiting for you on the other side.

All that's left is to show you how NetApp and Google Cloud deliver the data protection and data security capabilities you need to evolve into a cyber-resilient enterprise.

**To learn more about the products and services discussed on this cloud adventure, visit:**

Page: See the NetApp Google Cloud cyber-resilience overview



5 reasons: NetApp for ransomware protection



Blog: Safe and sound in the cloud



Blog: Data leak prevention best practice



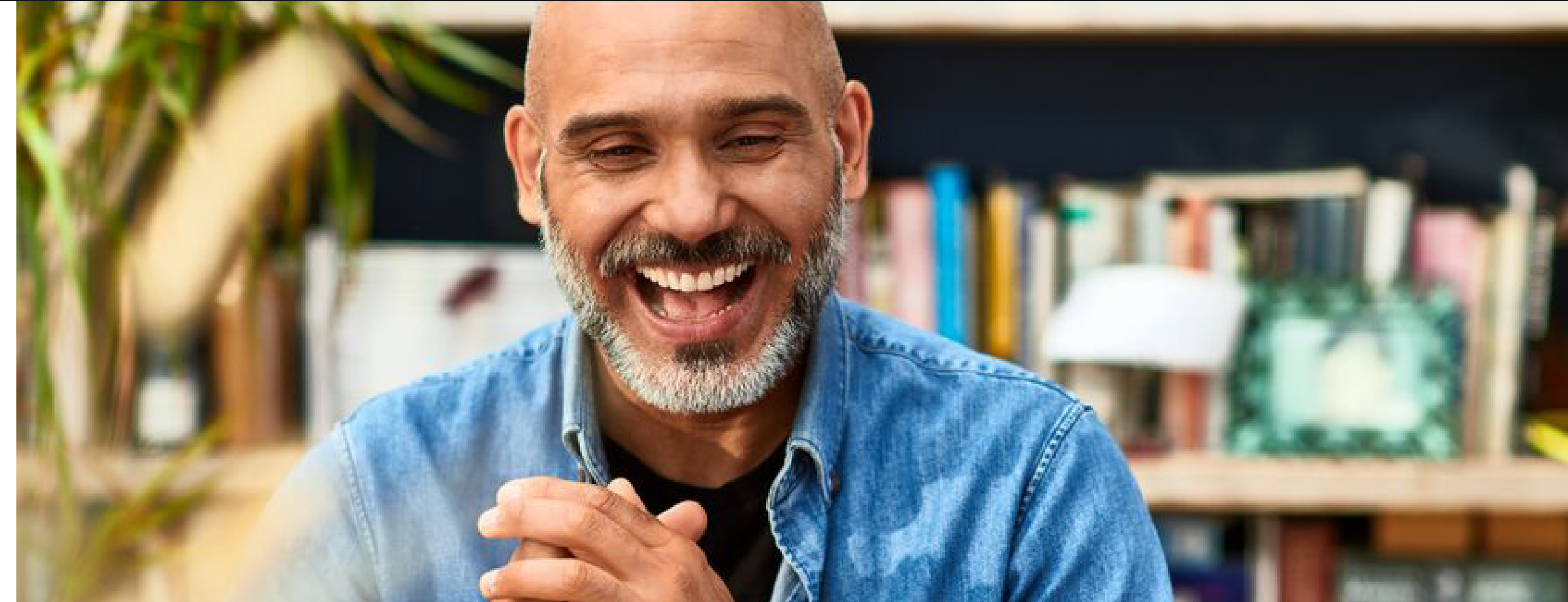
Video: Managing data in Google Cloud with Cloud Volumes ONTAP



IDC Report: Meeting the high availability requirements in digitally transformed enterprises



E-book: Disaster recovery in Google Cloud with Cloud Volumes ONTAP



## Get started

Want to engage in a more detailed discussion about your cyber-resilience strategy? Get in touch with your sales representative or talk security with a NetApp cloud architect.

Speak to a NetApp and Google Cloud security specialist

Ask NetApp Pro Services about data, compliance, and ransomware protection services



- 1
- The State of Ransomware 2022
- 2
- IDC, Worldwide Data Replication and Protection Software Forecast, 2019–2024: Rough Waters Ahead, 2020
- 3
- Global Cybersecurity Outlook
- 4
- Ransomware Attacks on the Rise in 2022
- 5
- Alarming Cyber Statistics for Mid-Year 2022 That You Need to Know
- 6
- The Zero Trust Model in an Impenetrable Nutshell



**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