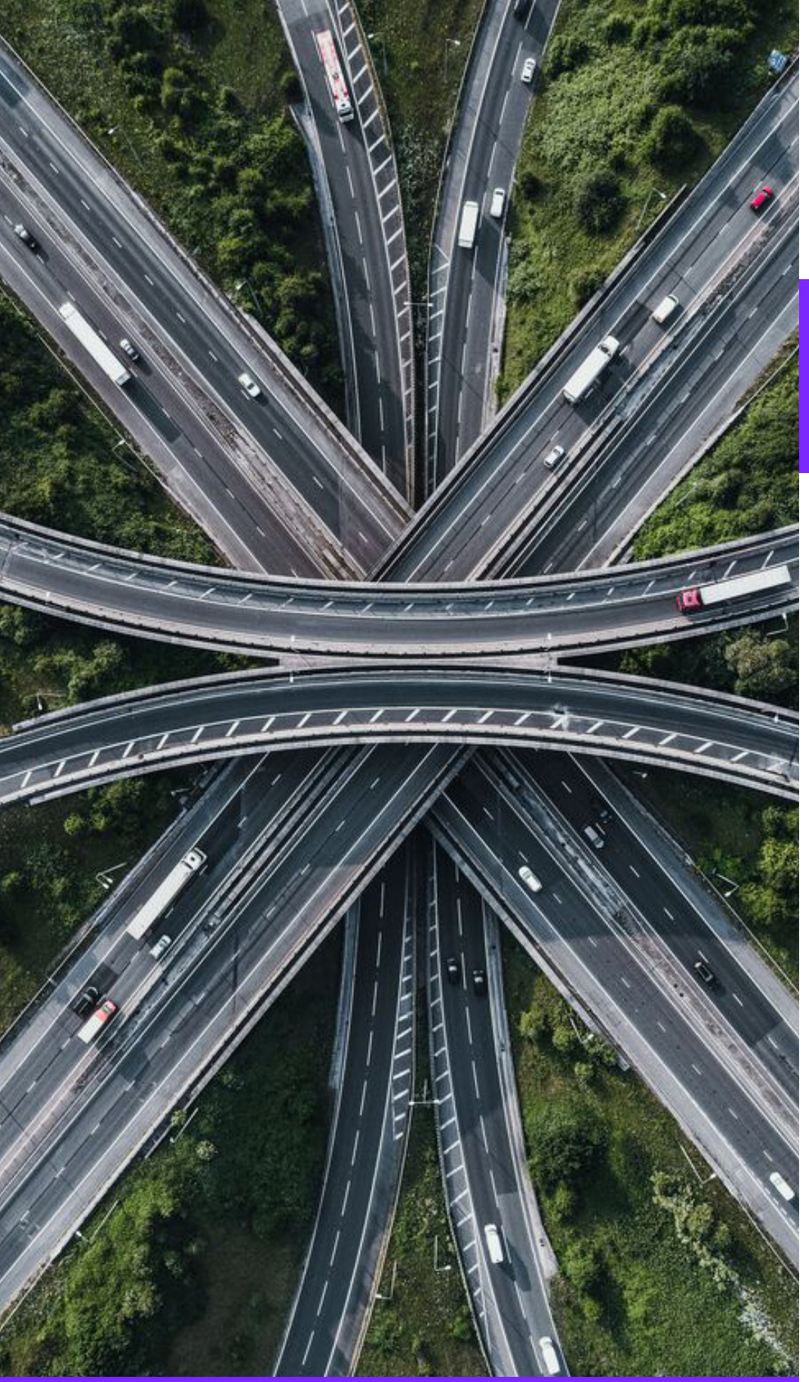
NetApp

6 CYBERSECURITY QUESTIONS TO KEEP YOUR DATA SECURED AND PROTECTED



NetApp

CONTENTS

Now, more than ever, your data needs protecting	3
What data do you have?	4
Where is your data, and who has access to it?	5
Who oversees each of your data environments?	6
How are you addressing human error and insider threats?	7
What internal knowledge exists but isn't being acted on?	8
Is your disaster response plan up to date?	9
Unstoppable cyber resilience starts with the most secure storage on the planet	10

NetApp

NOW, MORE THAN EVER, YOUR DATA NEEDS PROTECTING

Threats to your data can come from anywhere and from anyone. Threats include evolving AI-powered cyberincidents that use sophisticated methods to exploit your security vulnerabilities. Multiplatform data environments only compound the problem. Data spread across clouds and networks creates challenges and gaps that can affect productivity and put valuable data at risk.

It's not *if* but *when* you will experience a data breach. In 2022, 66% of organizations across the Americas, EMEA, and Asia Pacific were affected by ransomware.[1]

Data must be both secured and protected through an intelligent data infrastructure, which means adopting a datacentric approach where security happens from the inside out rather than the outside in. This method prioritizes the protection of the data itself rather than securing only the systems and network infrastructure that support it.

As IT environments continue to modernize and expand, the traditional lines that determine who is responsible for which data function are blurring—both within internal IT and among external partners such as cloud providers. Ultimately, securing and protecting data in a cross-platform, multi- and hybrid cloud world requires a cross-IT approach that considers the critical role data plays in modern organizations.

Exploring the following six questions will help you build an intelligent data infrastructure strategy for unified data storage that protects and secures data while minimizing workflow disruptions.

1
WHAT DATA DO YOU HAVE?

Whether it comes from generative AI creating new content, developers building and launching proprietary intellectual property (IP) and new apps, customers using those apps, or employees adding to systems of record with their day-to-day workloads, organizations are constantly generating new data at an unprecedented pace.

This fast-paced data generation also encompasses a wide variety of critical assets, including customer data, financial records, IP, employee information, operational metrics, market research, sensitive business communications, and big data analytics. These elements are the crown jewels of any company, representing invaluable resources that go beyond the scope of generative AI content.

Data is your company's most valuable asset, but not all data is created equal. It must be prioritized for protection through an intelligent data infrastructure. This prioritization includes adopting a systematic approach to categorizing each data type by its sensitivity, criticality, and value to your organization. Building this prioritization structure is critical when creating an effective data recovery plan to combat ransomware attacks and other potential data loss scenarios. Similarly, data such as employee or customer information, or banking and credit card details, needs focused governance and greater protection. Determining how to prioritize different data types requires a clear picture of the existing data you hold, the new data you are generating, and the value associated with each of your organization's data types.

How to gain visibility into your organization's data:

- **Conduct a comprehensive data audit.** Look at all current, active, and historical data. Also validate the accuracy and completeness of all data.
- **Classify and categorize your data.** Create categories that make sense for your industry and your organization.
- **Identify data that is high value, low value, and undetermined.** Also pinpoint vulnerable data and data that is subject to regulations.
- **Label data based on confidentiality and sensitivity levels.** Highest on this list should be toxic data, which is sensitive data that, if disclosed, could lead to regulatory compliance violations or damage to your organization's reputation.
- **Establish a data hierarchy.** Make strategic choices about the various levels of security and protection that each data category requires in your intelligent data infrastructure.
- **Delete data that is no longer necessary or relevant.** Outdated or inaccurate data is a potential liability.

Datacentric versus traditional Zero Trust

Whereas traditional Zero Trust controls who can access data, datacentric Zero Trust protects the data itself, no matter where it is or who is trying to access it.

By applying Zero Trust principles directly to data, organizations can achieve a higher level of security and ensure the confidentiality, integrity, and availability of their data regardless of its location or the networks it traverses.

Control your data access

Apply the Zero Trust principle of "least privilege" by using role-based access control (RBAC) to limit people's access to only the data they need to do their jobs and nothing more.

NetApp

2
WHERE IS YOUR DATA, AND WHO HAS ACCESS TO IT?

Once you know what data you have in your intelligent data infrastructure, you need to identify every place it exists and everyone who has access to it. In addition to being important for overall data security, where your data is stored is especially crucial for highly regulated industries that have to meet strict governmental requirements for data governance and compliance.

Tracking where your data resides and who has access to it may not be easy. Just as data sprawls and expands over time, so does the number of people who have access to various systems. Open-ended permissions are constantly being granted to employees, vendors, and contractors. This type of shortsightedness creates massive vulnerabilities and has been the cause of numerous high-profile breaches.

Organizations often overlook third-party relationships, in which external entities are given access but don't necessarily practice good security hygiene. All it takes is one mistake by an outside vendor to trigger a data breach. A Zero Trust strategy addresses such potential vulnerabilities by requiring that anyone who needs access must be authenticated and continuously validated.

How to effectively and compliantly control data access:

- **Find out whether your company embraces a datacentric Zero Trust architecture.** If so, learn how far into that journey you are and identify what data might still be vulnerable until a Zero Trust framework is complete.
- **Have more conversations with your security teams.** Implementing a Zero Trust security architecture is their domain, but data leaders must be part of the conversation and influence exactly how Zero Trust is used to protect data.
- **Take stock of who has access.** Find out who is using which apps and which networks are accessing what in your intelligent data infrastructure. Look at both internal and external parties. Know that internal sources are not more trustworthy by default.
- **Reduce access sprawl.** Make it a companywide policy to revoke outdated permissions on a regular basis.
- **Know your regulatory requirements.** Many governments limit whether data can be stored outside of the country of origin or transmitted between entities across country borders.

Companies that restrict data are twice as likely to avoid insider attack.[2]

3
WHO OVERSEES EACH OF YOUR DATA ENVIRONMENTS?

In organizations that embrace a hybrid cloud model for data use and storage, things can get complicated quickly. You may have complete control over your on-premises data, but different clouds handle security and protection differently. When data and apps are outside of direct control, new vulnerabilities appear. Every additional level of complexity adds risk. Cloud vulnerabilities account for a growing share of cyberattacks, so knowing how data is secured and protected on each of your platforms is essential.

It is crucial to close gaps created by multiple data platforms. To close these gaps, you need to establish internal data policies that are strictly and consistently applied across all your data environments. These policies should cover the complete data lifecycle, from how data is gathered and stored to how it is processed and disposed of. Along with all internal considerations, your organization's data policies should embrace external compliance standards set by industry associations, government agencies, and other stakeholders.

How to establish accountability and consistent data standards:

- **Determine accountability.** Accurately analyze who is accountable for each internal and external environment, including data and apps. Accountability varies across different public and private clouds, so make sure that you know what your organization is responsible for and what it is not. Don't make assumptions.
- **Establish clear protocols and assign stakeholders.** Standardize how data is handled throughout your organization, and clearly define who is responsible for enforcing these standards for each environment.
- **Identify vulnerabilities across the lifecycle.** Analyze the data lifecycle in each environment, including how data is gathered, how it is stored, how it is processed, and how it is disposed of. This information will help you to standardize data policy, which is key for effective security and protection.

82% of breaches occur in the cloud, and 39% of cloud security breaches span multiple environments.[3]

4
HOW ARE YOU ADDRESSING HUMAN ERROR AND INSIDER THREATS?

People aren't perfect. Whether due to simple mistakes or intentional acts, human factor threats can be hard to detect and highly damaging. Adding to the challenge is the increasing scarcity of cybersecurity talent. Security teams are stretched thin, which can limit their effectiveness in addressing insider threats.

Storage infrastructure teams can help strengthen an organization's defense with the right data protection strategies, systems that use AI for early detection, and automation tools focused on detecting insider threats. By leveraging advanced detection and automating data protection workflows that include local and remote backups, backup monitoring, and disaster recovery capabilities, the threat response of your intelligent data infrastructure is accelerated, and data teams are freed up to focus on more strategic problems.

How to better protect your data against the human element:

- **Establish clear policies regarding data access.** Review the effectiveness and implementation of these policies regularly.
- **Leverage smart automation.** Look for ways to automate data management and protection tasks in your intelligent data infrastructure. Automation can reduce your risks by reducing the burden on an overworked IT security team. When humans are bogged down in repetitive tasks, they can make mistakes.
- **Implement AI-powered tools.** Solutions that leverage artificial intelligence and machine learning can more quickly and accurately identify potentially malicious activity. They can also take effective action a lot faster.

74% of data breaches are the result of human action, including social engineering attacks, errors, or misuse.[4]

5
WHAT INTERNAL KNOWLEDGE EXISTS BUT ISN'T BEING ACTED ON?

In many organizations, the IT department structure walls off teams in their own silos. Whether intentional or not, this isolation often means that specialized knowledge goes unshared, limiting its usefulness to just a few people.

Instead of security specialists and infrastructure leaders collaborating to optimize data security and protection, they stay isolated in small groups—focused on their own work at the expense of the larger data picture. Insights are lost, vulnerabilities are missed, and your data is put at unnecessary risk.

How to maximize internal knowledge sharing to optimize data security and protection:

- **Cross-pollinate between teams.** Build an environment where security and infrastructure teams collaborate to create an overall stronger data environment.
- **Schedule regular check-ins and working sessions.** Bring together key members of your IT, application, infrastructure, and security teams. Address current challenges and imagine scenarios that you might face in the future.
- **Map out your overall workflow from protection to detection to recovery.** Looking at the full picture can help facilitate collaboration, improve gap identification, and reinforce accountability.
- **Evolve to a proactive stance.** Look at what projects are on the horizon and determine ways you can get a jump start with things like resourcing and planning.
- **Take an inside-out approach to security and protection.** Make data the lead character by establishing a data-first approach to security and protection.
- **Share innovations in data storage.** Security teams need as much insight as they can get into where data sits. When SecOps teams understand the latest data storage systems and capabilities, they can employ innovative methods to protect and secure data.

6
IS YOUR DISASTER RESPONSE PLAN UP TO DATE?

What happens when customers lose access to apps, when employees can't access data or information, or when cybercriminals hold your data hostage? A comprehensive disaster response and recovery plan is a critical part of data protection. While limiting overall downtime is important, getting your most essential data back online should be your highest priority. Getting back online rapidly will help you minimize the financial impact of a disaster on your bottom line and mitigate potential damage to your organization's reputation.

Building on the initial data audit mentioned earlier, you need to determine which of your data is the most critical to your operations. This information allows an efficient response that lets you focus your restoration efforts on those areas first. By establishing a data recovery hierarchy from the outset, you can generate a clear step-by-step plan that limits the effect of a disaster on your organization.

How to keep your response plan current to minimize disruptions to your intelligent data infrastructure:

- **Prioritize what data is most valuable.** This information defines the order in which applications and data will be restored.
- **Know who is responsible for what and when.** Make sure that everyone knows their role when the moment of truth arrives, from executives to engineers to systems administrators.
- **Run simulated disaster events.** Simulations after reveal vulnerabilities and areas for improvement. They also build readiness, so your team can react quickly and confidently when an event occurs.
- **Evaluate and review your plan at least once a year.** Don't wait until something happens to get it right.

A single minute of downtime can cost large organizations as much as $9,000-and it can be significantly more in industries like finance and healthcare.[5]

UNSTOPPABLE CYBER RESILIENCE STARTS WITH THE MOST SECURE STORAGE ON THE PLANET

As the intelligent data infrastructure company, only NetApp can help you build a unified data storage environment that delivers maximum security and protection while minimizing overall downtime—any data, any workload, any environment.

With NetApp, you'll know what kind of data you have, everywhere it's stored, and who has access. These comprehensive data insights can help you establish clear responsibilities for data management, address human error and insider threats, break down barriers to shared knowledge, act on that knowledge, and keep your disaster plans up to date.

[1] Sophos. "The State of Ransomware 2023." May 2023.

[2] GetApp. GetApp's 5th Annual Data Security Report: U.S. Businesses Gaining Ground Amid Ongoing Threats. September 26, 2023.

[3] UpGuard. "What is the Cost of a Data Breach in 2024?" January 23, 2024.

[4] Verizon Business. 2023 Data Breach Investigations Report. June 6, 2023.

[5] Forbes. "The True Cost Of Downtime (And How To Avoid It)." April 10, 2024.

Take the next step

Schedule a session to explore how NetApp can transform how your company capitalizes on cybersecurity.

Get an executive briefing →

NetApp

Contact us

About NetApp

NetApp is the intelligent data infrastructure company, combining unified data storage, integrated data services, and CloudOps solutions to turn a world of disruption into opportunity for every customer. NetApp creates silo-free infrastructure, harnessing observability and AI to enable the industry's best data management. As the only enterprisegrade storage service natively embedded in the world's biggest clouds, our data storage delivers seamless flexibility. In addition, our data services create a data advantage through superior cyber resilience, governance, and application agility. Our CloudOps solutions provide continuous optimization of performance and efficiency through observability and AI. No matter the data type, workload, or environment, with NetApp you can transform your data infrastructure to realize your business possibilities. www.netapp.com