ASSESS YOUR CYBERTHREAT READINESS IN AZURE

Implementing a robust cyber-resilience strategy in Azure isn't difficult, but it requires a data-centric approach. Understanding where you are today helps you to identify the biggest gaps and work to eliminate them.

	Scores		
External threats	**5** points	**3** points	**0** points
a. Where is all your **data located**? (Public cloud, colocation facility, data center, edge) **5 points** if already you have this documented **3 points** if you are in the process of documenting this **0 points** if this is not well documented	☐	☐	☐
b. Can your cloud storage automatically detect user behavior anomalies to thwart a **ransomware attack**? **5 points** if automatic detection **3 points** if manual detection **0 points** if no detection	☐	☐	☐
c. If a **hacker** were to invade, have you created immutable and indelible snapshots for rapid recovery on both structured (block) and unstructured (file) data? **5 points** if creating immutable and indelible snapshots **3 points** if creating snapshots **0 points** if relying on backups	☐	☐	☐
d. Are you able to replicate to other regions to **protect against outages** and perform nondisruptive disaster recovery tests without difficulty? **5 points** if you can with ease **3 points** if you can but with limitations **0 points** if you can'**t**	☐	☐	☐

NetApp

Internal threats	Scores		
	5 points	**3** points	**0** points
a. Do you have written **data security policies** that define clear roles and responsibilities? **5 points** if you already have this documented **3 points** if you are in the process of documenting this **0 points** if this is not well documented	☐	☐	☐
b. Have you implemented a Zero Trust architecture, and can you prevent **rogue administrators** from destroying production or backup data? **5 points** if monitoring across all of your on-premises and cloud applications **3 points** if monitoring across some of your on-premises and cloud applications **0 points** if not implemented	☐	☐	☐
c. Can you proactively detect abnormal behavior by potentially **malicious or compromised users** and automatically respond to help minimize damage? **5 points** if monitoring across all of your on-premises and cloud applications **3 points** if monitoring across some of your on-premises and cloud applications **0 points** if not monitoring	☐	☐	☐
d. Do you have the right tools to implement an effective data governance strategy to avoid scenarios like **data loss**? **5 points** if fully implemented **3 points** is partially supported **0 points** if not available	☐	☐	☐

Environmental threats	Scores		
	5 points	**3** points	**0** points
a. Do you have a well-documented and current **business continuity plan**? **5 points** if you have this already documented **3 points** if you are in the process of documenting this **0 points** if this is not well documented	☐	☐	☐
b. Are you proactively monitoring your cloud and overall IT environments to better detect anomalies, policy violations, or **system failure**? **5 points** if using AI **3 points** if monitoring without AI **0 points** if not monitoring	☐	☐	☐
c. How quickly can you **restore your mission-critical systems** from business disruption, like natural disaster outages? **5 points** if you have 15-minute RTO and RPO **3 points** if you have 24-hour RTO and RPO **0 points** if you need to call your storage provider to find out	☐	☐	☐
d. Can you automatically failover critical application and data across sites to recover from **unplanned outages**? **5 points** if able to automatically failover **3 points** if able, but the process is not automatic **0 points** if not possible	☐	☐	☐

NetApp

Score yourself

41-60 points
Congratulations, you are well on your way to becoming a fully cyber-resilient organization.

Next step: Speak to an Azure specialist in a 1:1 cyber resilience session to get help in filling those gaps so that you can thwart cyberthreats and keep your data protected and secure.

21-40 points
Well done. You have started on your cyber-resilience journey and have made lots of progress. But you're probably seeing where your limitations are, and although backup and recovery are important, they're not enough.

Next step: It's time to deploy a solution that goes beyond backup to proactively prevent threats. Check out our handy guide to help you start building true cyber resilience in Azure.

Less than 20 points
You're off to a good start—every journey needs a great beginning. But you're probably realizing that your cyber resilience needs some work.

Next step: Read our Azure cyber resilience blog, Keeping your data secure from the inside out, to better understand how and why you should build up your cyber resilience in Azure. If you're still not sure where to start, or if you have questions, contact an Azure specialist for a high-value, no-cost 1:1 strategy session.

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 enterprise-grade 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

NetApp