Assess your cyberthreat readiness

Ransomware. Data exfiltration. System failure. Cyberthreats come in all shapes and sizes. True cyber resilience is all about keeping your business running, no matter what comes your way.

You'll see some vendors like Pure go all in on recovery. And although recovery is critical, it's not the whole story. What would you rather do: Clean up the feathers in the henhouse after the fox has torn through it, or keep the hens safe with the fox locked outside?

Take a moment to assess your readiness to protect against cyberthreats, to detect emerging trouble, and to get back to business with intelligent analytics and rapid recovery. You may spot some openings in your henhouse that need patching.

	Scores		
External threats	**5** points	**3** points	**0** points
a. Can your storage mitigate **malware attacks** by automatically blocking more than 3,000 known malicious file extensions? **5 points** if automatic blocking of all malicious extensions **3 points** if manual blocking or blocking of only some malicious extensions **0 points** if no blocking	☐	☐	☐
b. Can your storage automatically detect file system 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 your IT, 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. Do you have access to intelligent health checks and recommendations to prevent **unauthorized data access?** **5 points** if intelligent health checks **3 points** if partial health checks **0 points** if no health checks	☐	☐	☐

NetApp

	Scores		
Internal threats	**5** points	**3** points	**0** points
a. Have you implemented a Zero Trust architecture and can you prevent **rogue administrators** from destroying production or backup data? **5 points** if fully protected **3 points** if partially protected **0 points** if not implemented			
b. Can you proactively detect abnormal behavior by potentially **malicious or compromised users** and automatically respond to help minimize damage? **5 points** if proactively monitoring **3 points** if partially monitoring **0 points** if not monitoring			
c. 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** if partially supported **0 points** if not available			
d. Can you prevent the deletion of backup data by **insider threats** to enable recovery from cyberattacks? **5 points** if fully able to prevent **3 points** if partially able to prevent **0 points** if unable to prevent			

	Scores		
Environmental threats	**5** points	**3** points	**0** points
a. Are you proactively monitoring your IT environment to better detect bottlenecks, policy violations, or **system failure**? **5 points** if using AI **3 points** if monitoring without AI **0 points** if not monitoring	☐	☐	☐
b. Are you able to test your disaster recovery or backup solution automatically without disrupting operations, so you can recover quickly if a **site failure** occurs? **5 points** if automatic non-disruptive testing **3 points** if manual non-disruptive testing **0 points** if disruptive testing	☐	☐	☐
c. Can you securely and efficiently replicate data to other regions to protect against **natural disaster** outages? **5 points** if reliably able to replicate **3 points** if if able, but it's difficult **0 points** if not possible	☐	☐	☐
d. Can you automatically fail over critical application and data across sites to recover from **unplanned outages**? **5 points** if able to automatically fail over **3 points** if able, but it's not automatic **0 points** if not possible	☐	☐	☐

Score yourself

0-20 points

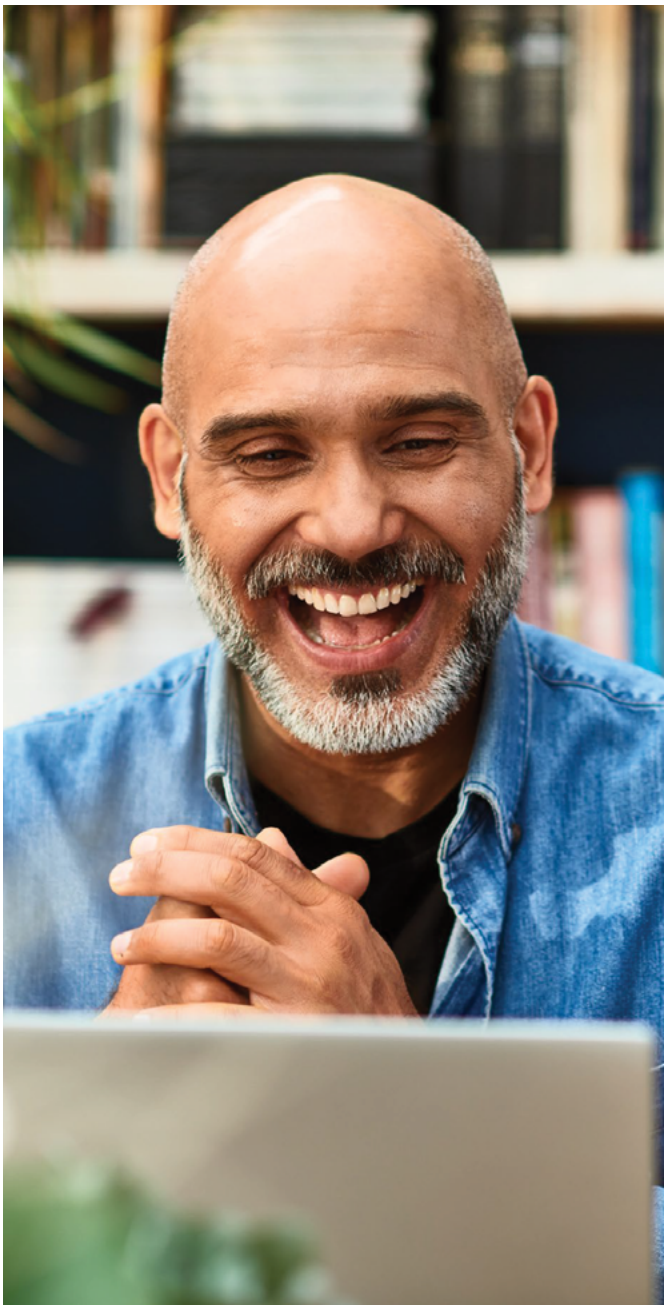
Congratulations! You are well on your way to true cyber resilience. In performing this assessment, you probably still identified opportunities for improvement. Our cyber-resilience specialists would love to help you fill those gaps so that you can thwart cyberthreats and keep your data protected and secure.

21-40 points

Well done. You have started 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. It's time to deploy a solution that goes beyond backup to proactively prevent threats. We have a handy guide to help you start building true cyber resilience.

41-60 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, and recovery-focused vendors like Pure just can't offer the comprehensive solutions that you need to protect your data. You need a solution with a Zero Trust architecture that can detect threats immediately with automated anomaly detection and can help you quickly recover with tamperproof snapshots and intelligent forensics. Not sure where to start? Take a look and see which vendor is right for you.



NetApp

+1 877 263 8277