DELL Technologies

Enhance cyber protection, simplicity and resilience.

The Dell 2022 cybersecurity readiness checklists

Know where your cybersecurity stands.

Know where it needs to get.

Your organization depends on always-accessible, always-safe data—from application servers to multi-cloud to your virtual desktop infrastructure (VDI). With confidence in the security of every element in your technology infrastructure, your organization can minimize costly downtime and stay focused on innovation and growth.

Use these checklists to assess the current state of your cybersecurity readiness. When you know your organization's strengths and vulnerabilities, you know the best next steps for comprehensive data security across your full IT ecosystem.

Protect data and systems checklist

Enhance cyber resiliency checklist

Overcome security complexity checklist

Modern Cyber Security for Enhanced IT Resiliency

Enhance cyber resiliency checklist

Blocking cyber threats is an essential component of any data security plan, but if you stop at prevention—your data **is not** fully secure. You must also include cyber-resilience solutions and strategies to recover and protect data, and minimize data loss and costly downtime, should a breach ever occur. Answers these questions to determine the cyber resilience of your organization:

YES	NO	
☐	☐	**Is your overall security posture based on a zero-trust architecture?**
☐	☐	Are your existing data protection methods sufficient to cope with today's malware and ransomware threats? (Dell Technologies internal studies suggest that over 60% of organizations are concerned about this risk.*)
☐	☐	Does your organization practice the 3-2-1 backup methodology?
☐	☐	Are recovery plans routinely tested?
☐	☐	Has your organization ascertained the amount of time its operations would be disrupted in the event of a cyber attack? Is it weeks, days or minutes?
☐	☐	Does your organization base its security model on the notion of continually blocking/preventing as many threats as possible, or that an attack is ultimately inevitable?
☐	☐	Has your organization implemented systems and processes that focus on minimizing the operational disruption and/or financial impact that an attack may cause?
☐	☐	Has your organization implemented an air-gapped data vault where "known-good" data is stored?
☐	☐	What type of threat detection capabilities do you have in place? Are they managed internally or by a third party?
☐	☐	Does your organization utilize AI-based pattern anomaly detection?
☐	☐	Is end-to-end data encryption in place?
☐	☐	What is the organization's backup and system snapshot process?

* Dell Technologies Global Data Protection Index

Overcome security complexity checklist

Complexity is the enemy of security. When your Security Operations Team is managing security solutions for endpoints, servers, networks, storage, and cloud, the risks, costs, and inefficiencies can mount quickly. You can't afford to simply add layer upon layer of security tools or the maintenance that comes with them. Answer these questions to determine if security complexity is making your data and systems vulnerable:

YES	NO	
☐	☐	**Is your overall security posture based on a zero-trust architecture?**
☐	☐	What is your current security spend, both on internal and external (third-party) capabilities?
☐	☐	Does your organization routinely analyze its internal and third-party security providers to ensure effectiveness and value?
☐	☐	Has your organization ensured the appropriate level of redundancy in its security capability? Have extraneous or low-value elements been eliminated?
☐	☐	Has your organization taken advantage of potential synergies by rationalizing the number of security vendors?
☐	☐	Have you hired an outside expert to assess your overall security posture and propose enhancements?
☐	☐	If your organization is using multiple data protection vendors, have you determined the potential higher cost of data loss versus that of a single vendor? (Dell studies indicate that the cost can be as much as four times as high in a multi-vendor scenario.)
☐	☐	Does your organization utilize any automation or orchestration tools to help with either detection and/or recovery?

Learn More about our solutions and contact a Dell Sales Rep today.

Call your authorized Dell Partner for more information.

Take the Cyber Assessment