
DELL Technologies
Fortify your enterprise with modern security
Protect your enterprise with a holistic strategy.

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

Protect data and systems checklist

From remote laptops and desktops to cloud and on-premises servers and storage, your organization depends on every IT infrastructure element to stay productive and innovate. But each device, network endpoint and system can introduce opportunities for intended or unintended systems breaches that leave your data vulnerable. Answer these questions to determine if your data is secure across your full IT ecosystem:

YES	NO	
☐	☐	**Is your overall security posture based on a zero-trust architecture?**
☐	☐	Does your organization's security capability cover the end-to-end IT ecosystem, including devices, applications and systems?
☐	☐	Does your organization manage one security policy that applies to both internal and external providers?
☐	☐	Has your organization assessed and addressed risks in its IT supply chain, accounting for security, integrity, quality and resilience?
☐	☐	Can your organization track devices/endpoints and lock or wipe them in the case of theft or unauthorized use?
☐	☐	Do your vendors (or internal DevOps) have appropriate measures in place to protect the process by which new products, features and services are developed (secure development lifecycle)?
☐	☐	Has your organization assessed the new and potentially greater risks posed by increased remote work?
☐	☐	Are endpoint security measures in place both above and below the OS?
☐	☐	Thinking holistically, is your current security capability bolted on or built in? Siloed or unified? Threat centric or context centric?
☐	☐	Are personnel and physical security technologies and processes in place? Are they routinely reviewed and updated?

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?

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?

Strengthen your organization's security posture.

As organizations expand their security capabilities and become more mature and cyber resilient, overcoming complexity is crucial to ongoing success. Dell is a trusted partner in modern security. We deliver the expertise and end-to-end tools to help you achieve these three core outcomes:

Protected data and systems
Select Dell as a trusted security partner with the scale and resources to provide advanced tools and intrinsic capabilities holistically across an organization's IT spectrum.

Enhanced cyber resiliency
Plan, prepare and practice mature resiliency programs to protect critical data and apps and to lessen the impact of cyber attacks.

Reduced security complexity
Utilize automation, consolidate security tools and make use of Dell security experts to intelligently scale.

Dell stops at nothing to help our customers build their breakthrough. Our modern security approach is designed to help ensure that an organization's environment is secure and resilient, so they can focus on their core competency, build their breakthrough and advance human progress.

DELL Technologies

About Dell Technologies

Dell Technologies helps organizations and individuals build their digital future and transform how they work, live and play. The company provides customers with the industry's broadest and most innovative technology and services portfolio for the data era.

Learn more at www.dell.com/securitysolutions

Sources

1 Dell Global Data Protection Index, 2021.

2 Based on Dell internal analysis, August 2017.

3 ESG review commissioned by Dell, "Analyzing the Economic and Operational Benefits of the Dell EMC Data Protection Portfolio," evaluating the economic value of the Dell EMC data protection portfolio, September 2020. Actual results will vary.