DELL Technologies

The Dell 2022 Ultimate Cybersecurity Checklist

Know where your cybersecurity stands.

Know where it needs to get.

Your enterprise depends on always-accessible, always-safe data—from application servers to your virtual desktop infrastructure (VDI). With confidence in the data security of every element in your technology infrastructure, your business can focus on innovation and growth.

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

Endpoint security checklist

Server security checklist

VDI-cloud security checklist

Storage security checklist

Cyber and disaster recovery checklist

Modern Cyber Security for Enhanced IT Resiliency

Endpoint security checklist

Laptops. Desktop computers. Tablets. Cell phones. Network endpoints keep businesses humming. They also introduce opportunities for security breaches—intended or unintended. Robust endpoint security has these prevention and recovery measures in place:

IN PLACE	DON'T HAVE	
□	□	Device Theft Protection
□	□	System Boot Security
□	□	Malware Protection
□	□	Bootloader Integrity Check
□	□	Unverified/Corrupt BIOS Installation Prevention
□	□	Lost or Stolen Device Recovery
□	□	Hardware-Enforced Protection
□	□	BIOS Configuration and Rootkit Protection
□	□	Device Login with Password
□	□	Additional Authentication Factors
□	□	Bluetooth Device Proximity Automatic Lock
□	□	Password Recovery
□	□	Credential Protection
□	□	Hardware-Isolated Authentication Factors
□	□	Integrated Policy and Identity Protection
□	□	Common Criteria and FIPS Certification
□	□	Recovery of Files from Cloud
□	□	Antivirus Scan
□	□	Phishing and Malware Filter
□	□	Data-at-Rest Encryption
□	□	Trusted Application Verification
□	□	User Authorization for Apps
□	□	Permanently Erased Data on Drives
□	□	Prevention of Unauthorized Use of Drives
□	□	Data Protection from Physical Impact

Server security checklist

Servers hold vital and sensitive enterprise information, from the accessible data used in applications (operational and client) to archival storage. This makes servers a tempting target. Robust encryption, continuous monitoring, powerful backups and more are powerful defenses. What do you have in place?

IN PLACE	DON'T HAVE	
□	□	Risk Assessment Completed (by device)
□	□	Employee Training & Education
□	□	Access Control in Place
□	□	Server Permissions
□	□	Termination Policy in Writing
□	□	Incidence Response Plan
□	□	Disaster Recovery Plan
□	□	Yearly Review
□	□	Unique User IDs for Each Employee
□	□	Automatic Logoff
□	□	Encrypted Onsite Data Storage
□	□	Encrypted Offsite Data Backups
□	□	Corporate Grade Firewall
□	□	Corporate Grade Antivirus
□	□	Spam Email Filter
□	□	Encrypted Remote Access (VPN, Mobile?)
□	□	Remote Wiping of Data
□	□	Regular Patching & App Updates

IN PLACE	DON'T HAVE	
□	□	Complete Network Documentation
□	□	24/7 Network Monitoring
□	□	Secure Server Room
□	□	Secure Workstation Areas
□	□	Complete Inventory of Assets & Devices
□	□	Decommissioned Workstation Process
□	□	Network Anomaly Monitoring (internal & external)
□	□	Continuous Network Threat Detection (with real-time alerts)
□	□	Controller Integrity Validation (config changes, firmware, code)
□	□	Centralized Management, Data Aggregation, Alerts & Reporting

VDI-cloud security checklist

VDI-cloud security is a comprehensive set of policies, processes and tools used to protect data and applications running on private and public cloud infrastructures. How defensive is your VDI-cloud security?

IN PLACE	DON'T HAVE	
□	□	Early detection of compliance and security violations.
□	□	Scan IaC templates in the IDE.
□	□	Scan Dockerfiles for vulnerabilities.
□	□	Scan app manifests for insecure configurations.
□	□	Scan source code repositories for package vulnerabilities.
□	□	Trigger scans when developers make pull requests.
□	□	Develop tests based on threat modeling to identify hot spots.
□	□	Scan containers & secure registries.
□	□	Scan container images for vulnerabilities and malware.
□	□	Detect and alert on secrets leakage in container images.
□	□	Sign images and build metadata in the CI/CD pipeline.
□	□	Maintain dedicated test environments to validate security tests.
□	□	Maintain private registries for development artifacts.
□	□	Maintain pre-production registries for production deployment artifacts.
□	□	Ensure the use of signed images throughout the process.
□	□	Encrypt container images for confidentiality.

Storage security checklist

With data volume rising exponentially, secure storage is critical to your operations and your brand. Robust storage security doesn't happen without a comprehensive protection plan that provides backup, isolates and recovers data and detects unusual access patterns. Answer these questions to assess storage security vulnerabilities:

IN PLACE	DON'T HAVE	
		Where do you store your data?
□	□	PC, Laptop, Workstation (endpoint device)
□	□	External Hard Drive
□	□	Network Drive
□	□	Remote Storage (cloud)
		Where do you store your backup?
□	□	PC, Laptop, Workstation (endpoint device)
□	□	Removable Media
□	□	External Hard Drive
□	□	Network Drive
□	□	Remote Storage (cloud)
		How will you create/sync your backup copy?
□	□	Automatic System Tools
□	□	Manual
		What kind of backup will you run?
□	□	Full
□	□	Incremental
□	□	Differential

IN PLACE	DON'T HAVE	
		How will you protect access to your data?
□	□	User ID/Password
□	□	Limited Network Access
□	□	Role-Based Access Rights
		How will you protect your systems?
□	□	Antivirus Software
□	□	A Systematic Plan for Updating/Patching All Applications & OS
□	□	Firewall
□	□	Anti-Intrusion Software
□	□	Restricted Physical Access
		How will you protect the integrity of data?
□	□	Data transferred over the network will be encrypted.
□	□	Access to data related to my research is accessible only by those who are authorized to access it.
□	□	I have a plan for validating the integrity of my data.

Cyber and disaster recovery checklist

Cyber recovery ensures data integrity across your full IT infrastructure. Disaster recovery prioritizes restoring the most important data first, so business operations and services continue uninterrupted. Both are essential. Explore whether your cyber recovery and disaster recovery plans keep your data safe and restore operations fast.

Verify the data breach

IN PLACE	DON'T HAVE	
□	□	Identify affected systems or hardware (lost laptop or USB).
□	□	Determine whether incident was internal/external, malicious attack or an accident.
□	□	Determine whether the incident exposed data.
□	□	Determine elements possibly at risk, such as name, date of birth or Social Security number.
□	□	Identify the system, application and information compromised.

Contain and mitigate the data breach

IN PLACE	DON'T HAVE	
□	□	Identify and take action to stop the source/entity.
□	□	Takes affected machines offline.
□	□	Segregates affected system.
□	□	Deletes the "hacking" tool.
□	□	Determines what other systems are under threat.
□	□	Prompts what additional measures need to be implemented (passwords, admin rights, access codes, etc.).

Recovery tools

IN PLACE	DON'T HAVE	
□	□	Backup of all infrastructure: servers, endpoints, storage systems and cloud data.
□	□	Storage of a backup copy in the cloud via a cloud service provider and a secure subscription service.
□	□	Data encryption for data sent to the cloud backup service provider data center.
□	□	Incremental backups (as data changes) after initial backup.
□	□	Detection and backup of new/changed files to minimize the impact on performance and user productivity.
□	□	Data de-duplication support to improve performance and reduce storage and bandwidth requirements.
□	□	Use of backups captured as a point-in-time snapshot to restore data to its previous state from any previous point in time.

DELL Technologies

Knowledge is cybersecurity power.

Ready to deepen your cyber resiliency?

Take the Cyber Resiliency Assessment and get your data security roadmap.

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

Call your authorized Dell Partner for more information.

Take the Cyber Assessment