Unitrends Healthcare BCDR Checklist

THE HEALTHCARE INDUSTRY HAS UNDERGONE RAPID DIGITAL TRANSFORMATION, OFFERING OPPORTUNITIES FOR INNOVATION AND GROWTH AS WELL AS CHALLENGES IN MEETING UPTIME DEMANDS AND PROTECTING A RAPIDLY GROWING DATA SET. PATIENT OUTCOMES DEPEND ON APPLICATION AVAILABILITY.

TO OPTIMIZE DATA PROTECTION IN HEALTHCARE, IT TAKES KNOWLEDGE OF THE UNIQUE CHALLENGES OF THE INDUSTRY — FROM PROTECTING HIGHLY PROPRIETARY EHR CONTENT AND MEETING 24X7X365 UPTIME REQUIREMENTS TO FENDING OFF INCREASINGLY POPULAR AND TARGETED RANSOMWARE ATTACKS TO SUPPORTING LARGE NUMBERS OF UNSAVVY, NON-TECHNICAL USERS.

SAFEGUARDING PATIENT DATA IS AS IMPORTANT AS PROVIDING UPTIME AND AVAILABILITY OF APPLICATIONS AND SERVICES. OVER THE LAST DECADE, 70 PERCENT OF THE US POPULATION HAS BEEN AFFECTED BY HEALTHCARE DATA BREACHES.[1] IF YOUR ORGANIZATION RELIES ON INTERACTIVE WEBSITES, ONLINE PATIENT PORTALS OR THIRD-PARTY BILLING SERVICES, IT'S CRITICAL TO ENSURE REQUIRED PHYSICAL, NETWORK AND PROCESS-RELATED SECURITY MEASURES ARE DOCUMENTED, IMPLEMENTED AND FOLLOWED.

This checklist is broken down into five categories to help you understand the different options that exist in the market today. With hundreds of vendors and technologies emerging in storage, infrastructure, data management and continuity, there's a broad range of strategies to consider as you determine the right business continuity and disaster recovery (BCDR) solution for your organization.

01 — **PROTECTION FOR ALL WORKLOADS**

02 — **AVOIDING DOWNTIME AND DATA LOSS**

03 — **SAFEGUARDING DATA FROM RANSOMWARE, CYBERTHREATS AND OTHER SECURITY CONSIDERATIONS**

04 — **REGULATORY COMPLIANCE**

05 — **SUPPORT FOR NON-SAVVY USERS**

[1] https://www.prnewswire.com/news-releases/230-954-151-us-healthcare-records-lost-or-stolen-between-2009-2019--study-by-privacyaffairs-finds-301126158.html

© 2021 UNITRENDS // ALL RIGHTS RESERVED // WWW.UNITRENDS.COM

Protection for All Workloads

	CAPABILITY	DESCRIPTION
☑	Fewer Point Products	A multi-vendor protection strategy increases IT complexity, risk and cost. Reducing the number of point solutions means managing fewer licenses and service agreements, and cuts management and technician time.
☑	Purpose-Built Appliance	A purpose-built turnkey data protection solution is easier to install, upgrade, service and manage.
☑	Wide Coverage of Protected Assets	To reduce the number of point products you need to rely on, your backup solution should be able to natively support hundreds of versions of operating systems, hypervisors and applications. Choose a single solution that provides complete protection for medical and business records whether they're stored on physical, virtual, NAS or cloud targets.
☑	Policy-Based Management	Admins should have the choice of how backups are scheduled, either by entering a specific schedule or using intelligent policy-based scheduling technology.
☑	Data Reduction	Data reduction (deduplication, compression) reduces the overall size of files and eliminates redundancy among stored blocks, making movement, management and storage more efficient.
☑	RESTful API	A RESTful API can easily integrate with other applications.
☑	Support for Hyperscale Clouds	Today's solution should easily integrate with hyperscale clouds such as AWS or Azure to protect IaaS workloads, store backups for long-term retention requirements and enable disaster recovery.
☑	Purpose-Built Cloud	A cloud provider that offers a dedicated cloud can provide turnkey solutions specifically tuned to meet the needs for long-term retention and disaster recovery. Key functions are delivered as a service thereby, reducing the reliance on internal IT to develop DR as a core IT competency.

© 2021 UNITRENDS // ALL RIGHTS RESERVED // WWW.UNITRENDS.COM

Avoiding Downtime and Data Loss

	CAPABILITY	DESCRIPTION
☑	Flexible Recovery Options	Your solution should be flexible in both how you can recover assets and where you can recover the data to. Look for solutions that support a wide range of recovery modes including physical-to-virtual (P2V), V2V, V2P and replicas.
☑	Instant Recovery From Local Disasters	If a server, VM or data center rack goes offline or fails, your appliance should be able to orchestrate failover to bring applications back up from your most recent backup with a near-zero RTO.
☑	Bare Metal Recovery	Bare metal restores enable application recovery across servers from different vendors and hardware configurations.
☑	Data Loss Prediction	Backup solutions with intelligent tools help simulate different disasters and outage scenarios to determine what types of and how much data would be lost in a downtime event so you can refine your strategy and ensure RPOs are being met.
☑	Application Downtime Prediction	BCDR platform equipped with deep application testing capability, helps to identify, simulate and test the multiple steps required to recover complex applications to ensure RTOs and uptime SLAs are being met.
☑	Manage Protection of Multiple Sites	A single user interface should provide you with a global view to manage protection of on-premise assets, remote offices, SaaS apps and endpoint devices.

© 2021 UNITRENDS // ALL RIGHTS RESERVED // WWW.UNITRENDS.COM

Safeguarding Data From Ransomware, Cyberthreats and other Security Considerations

	CAPABILITY	DESCRIPTION
☑	AES Encryption	AES encryption secures data privacy both at-rest and in-flight. In addition to data backups, office email should be secured and any Personal Health Information (PHI) sent via email should be encrypted. Any removeable storage devices (HDDs, USB drives) should be encrypted. Staff should be trained adequately in encryption procedures.
☑	Ransomware Prevention	Consider a solution written in hardened Linux. Ransomware targets Windows applications and common utilities (i.e. VSS writers) due to their popularity and the fact that Windows is an open architecture.
☑	Threat Detection	Your solution should use machine learning to detect in near real-time an active infection. Artificial Intelligence (AI) establishes a baseline of heuristics such as change rate prediction, data entropy and randomness to identify anomalies in data that antivirus and Firewalls don't catch. Automatic notifications alert admins, enabling them to take immediate action to slow the spread and speed recovery efforts.
☑	Anti-Phishing Defense	Empower employees to defend against phishing and account takeover attacks. Solutions that provide visual cues (i.e. banner notification), alert employees to external senders, spoofed and/or imitated users and enable them to quarantine suspicious emails, which helps to automate workflows and feedback loops to streamline IT review.
☑	Physical Security	Computers and servers should be in secured, locked locations. An alarm system should be in place for after-hours security as well as continuous visual security for office systems.
☑	Password Protection	Computers and servers should be password protected. Passwords should not be viewable by visitors and office goers.

© 2021 UNITRENDS // ALL RIGHTS RESERVED // WWW.UNITRENDS.COM

Regulatory Compliance

	CAPABILITY	DESCRIPTION
☑	Long-Term Data Retention	Depending on your state, you may be required to retain medical records for several years after last contact or until a patient who's a minor reaches a certain age. Your solution needs to be able to accommodate long-term data retention, whether locally, to a cloud location, or a secondary target (i.e. NAS device or tapes).
☑	Role-Based Access Control	When dealing with highly proprietary data, not all backup and recovery users may require access. A solution that limits the scope and capabilities of admins and other users ensures that backup schedules and/or recoveries are only performed by authorized personnel.
☑	Immutable Audit Logs	Immutable logs and routine monitoring ensure that the data being managed by your backup and recovery systems is being appropriately handled and accessed by staff.
☑	Internal Anomalous Monitoring & Detection	Secure servers, data and network with an AI-augmented solution that identifies threats such as misconfigurations, unauthorized logins, new devices being added to the network, gaps in backups and admin rights being granted that firewall and antivirus can't detect.

© 2021 UNITRENDS // ALL RIGHTS RESERVED // WWW.UNITRENDS.COM

Support for Non-Savvy Users

	CAPABILITY	DESCRIPTION
☑	Intuitive User Interface (UI)	A modern, simple UI should be a priority. Operating your backup system should be possible without the need to frequently consult a manual or guide. Substitutes and managers can quickly and seamlessly stand in when primary admins are unavailable.
☑	File Recovery	Healthcare IT often supports unsophisticated users prone to mistakes (Doctors, Nurse, Admins) who may click dangerous links or delete files. Your solution should make it intuitive and easy to find and restore individual files from backups with only a few clicks. Indexed search capabilities and self-service recovery (with role-based access control) enable quick recovery, and in some cases may not require IT intervention.
☑	Purpose-Built SaaS Protection	Native data protection tools for SaaS applications such as O365, G Suite and Salesforce often can't meet the RTO and RPO required today. A purpose-built solution protects cloud-based applications to minimize loss of data and productivity with granular, point-in-time recovery.

UNITRENDS HAS A LONG HISTORY OF HELPING IT PROFESSIONALS WORKING IN HEALTHCARE ORGANIZATIONS PROTECT THEIR ASSETS. HOSPITALS, ACUTE CARE FACILITIES, CLINICS AND MEDICAL LABS ACROSS THE WORLD LEVERAGE UNITRENDS' PORTFOLIO OF TURNKEY, CLOUD-EMPOWERED BACKUP APPLIANCES TO PROVIDE CONTINUITY ACROSS ALL WORKLOADS. AGILE AND CUSTOMIZABLE, UNITRENDS OFFERS UNMATCHED FLEXIBILITY TO HELP MEET AN ORGANIZATION'S NEEDS OF TODAY AND TOMORROW. UNITRENDS PROVIDES UNPARALLELED PROTECTION FOR PHYSICAL, VIRTUAL AND CLOUD-BASED SYSTEMS AUGMENTED WITH AI AND AUTOMATED, APPLICATION-LEVEL RECOVERY TESTING SO YOU KNOW YOU CAN RECOVER SYSTEMS, DATA AND APPLICATIONS WITH 100 PERCENT CONFIDENCE.

ARE YOU READY TO SEE HOW UNITRENDS CAN HELP YOUR ORGANIZATION? GET STARTED TODAY!

ABOUT UNITRENDS

Unitrends makes efficient, reliable backup and recovery as effortless and hassle-free as possible. We combine deep expertise gained over thirty years of focusing on backup and recovery with next generation backup appliances and cloud purpose-built to make data protection simpler, more automated and more resilient than any other solution in the industry.

Learn more by visiting unitrends.com or follow us on LinkedIn and Twitter @Unitrends.

UNITRENDS
A Kaseya COMPANY

© 2021 UNITRENDS // ALL RIGHTS RESERVED // WWW.UNITRENDS.COM