Why 2022 is the year for your customers to review their BC/DR strategy

Over the past two years, I.T. has undergone a huge transformation. A staggering 96% of all organizations are accelerating usage of cloud to adapt to changing business models in a global economy. As legacy systems are stretched across multiple platforms, organizations must adopt new approaches to business continuity and disaster recovery (BC/DR) to ensure data is completely protected. Transformational technologies put in place to support distributed enterprises during the pandemic were put to the test, and they're here to stay.

2022 is the year to review your customers BC/DR strategy, and here's the top three reasons why you should implement a comprehensive data protection platform like Unitrends Unified BC/DR.

#1: Unified BC/DR has the completeness to protect all workloads regardless of where they live

According to findings in Unitrends 2021 State of BCDR Survey, approximately 30% of workloads are being delivered via the cloud. Infrastructure-as-a-Service (IaaS) accounted for 53% of these workloads while another 47% were delivered via SaaS applications. Overall, the percentage of organizations that plan to move to a fully cloud-hosted model is anticipated to increase by 70% over the next two years.

As environments are increasingly distributed and growing in complexity, you need a BC/DR solution that's able to unify different approaches to workload protection under a single pane of glass, in part simplifying complex systems and reducing the space between jumping through different UIs and consoles to manage different workloads.

Unified BC/DR resolves to:

- Holistically supports a plethora of data protection approaches. Whether your workloads exist on-premises, on remote endpoints or in cloud hosted SaaS applications, you can protect them all by utilizing Unitrends flexible licencing models accommodating all backup sources and target on a single platform. Unitrends UniView enables you to manage all of them holistically from a single user interface.
- Enable customized global alerts to cut through the noise across your platform and prioritize resolving issues that directly impact recoverability as it relates to your SLAs (RTO and RPO). Powered from the cloud, the global alerting system alerts administrators to incidents even when a local appliance may not be able to do so directly.
- Reverse proxy into modularized components (such as individual appliances) through SSO from the global interface, reducing login attempts across the platform and speeding up time to resolution.

#2: Unified BC/DR leverages artificial intelligence and automation to remediate risks and threats with speed and agility

The attack surface for threat actors to target organizations with cyberattacks is incredibly broad. In a landscape rife with cyberthreats, using a solution that leverages artificial intelligence and automation helps to reduce the frequency and impact of occurrences of data loss and downtime.

The combination of automation and AI serves to simplify complex tasks, provide deep levels of visibility into activity within your environment, and help guard employees against human error and cybercrime.

Unified BC/DR resolves to:

- Provide you with 100% confidence in recoverability by automating recovery testing. Testing has always been a challenge since many organizations don't have the resources to regularly test recoverability. Unitrends Recovery Assurance helps users orchestrate tiered, application-level recovery testing against multiple systems to fully certify recoverability of all workloads with all dependencies, data and services validated in an isolated sandbox.
- Protect end users from advanced phishing threats. By injecting purposeful security integrations into our SaaS backup solution, organizations are provided front-end protection against cybercrime

with in-depth anti-phishing defence, including warning banners and click-to-quarantine suspicious emails, while proactive dark web monitoring alerts to credential compromise and exposure enabling IT to secure accounts at risk before an attack occurs.

- Reduce the time you spend troubleshooting backups. Unitrends Helix brings automation technology to serve the infrastructure use-case. Helix, powered from the cloud, is constantly on the lookout for remediation opportunities to autonomously solve issues related to your environment (such as VSS errors) and backup appliances before they can negatively impact backups.

#3: Unified BC/DR provides a secure, hardened platform immune from Microsoft based attacks

A ransomware attack is launched every 11 seconds and attackers are craftier than ever before, implementing nefarious techniques such as dormancy and un-decodable encryption. Often, by the time a victim realizes something is wrong, it's too late. With most attacks targeting Windows based systems, the operating system of your backup solution can make you more vulnerable.

Combating ransomware requires a multi-pronged approach, from end-user training and awareness, proactive network monitoring, antivirus, firewalls, anti-phishing defences and a purposeful hardening of your backup infrastructure.

Unified BCDR resolves to:

- Provide a secure backup appliance written on a hardened Linux kernel. The Linux OS lies outside of the Windows attack surface and camouflages backup files from malware hunting for Windows-based extensions. Additional controls, such as role-based access control, help secure the backup environment from unwarranted access.
- Able secure, off-site data retention and disaster recovery using immutable cloud storage. Immutable cloud infrastructure means that once written to the target, no source can modify, delete, or otherwise change your data. Your local appliance can read the data and import it back from the Unitrends cloud for recovery at any time with no additional data egress charges.
- Detect sleeper ransomware and slow-burning infections with machine learning. Equipped on every appliance, machine learning establishes baseline patterns of behaviour by measuring several heuristics within backup data. When symptoms present themselves that match the behaviour of clients infected by ransomware, alerts are immediately sent to administrators and displayed on the appliance dashboard, while the appliance flags suspected backups to prevent them from being used in a recovery attempt.

Assess your BCDR strategy today!

To see (in under 5-minutes) how your current solution stacks up against Unified BC/DR, take our Survey.

Claim your free BC/DR Assessment report

Links:

UniView: UniView Single Pane Management Data Sheet

Recovery Assurance: Recovery Assurance Data Sheet

Unitrends Helix: Helix Self-Healing Backups Data Sheet

State of BCDR Survey: Peer Insights Global Survey Report