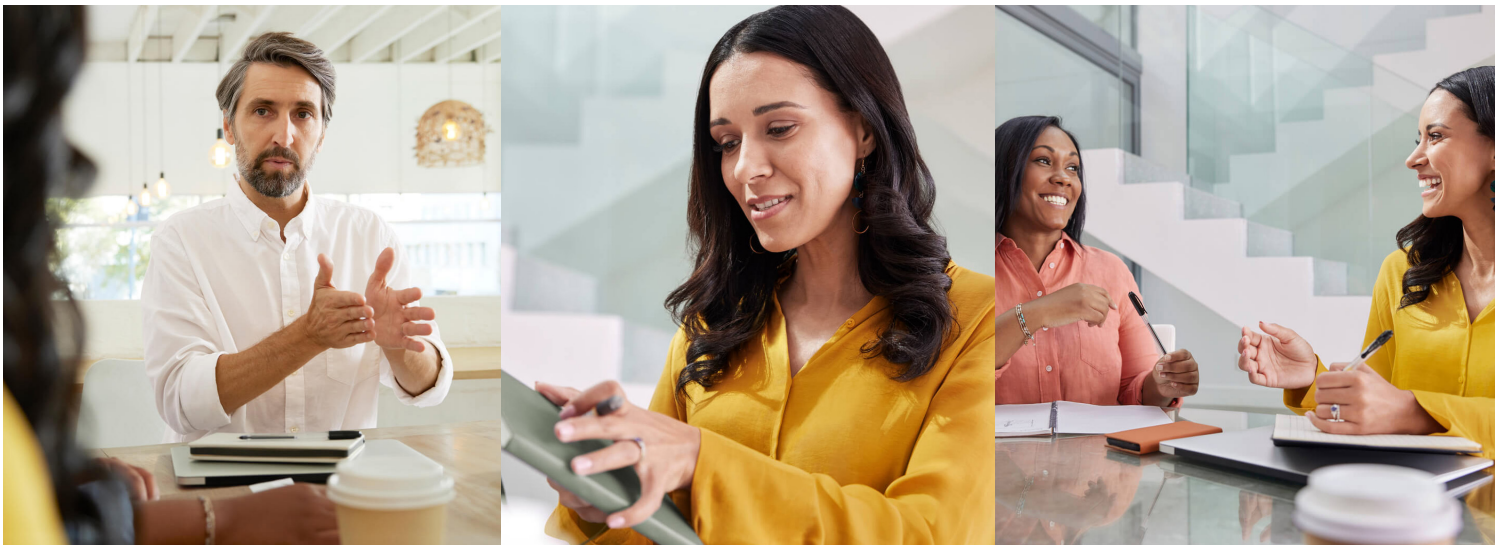
HPE GreenLake

The right kind of continuous data protection is the key to business survival

A new approach



Continuous data protection is emerging as a best practice to enable swift recovery from ransomware and other disasters.

Lessons for leaders

- There is a straight trade-off between cost and the ability to recover from disasters quickly.
- Paying ransom to a ransomware attacker is no guarantee of data recovery.
- Systems are available to enable fast and thorough data recovery after an attack or other disaster.

The best outcome from a ransomware attack is to block it before it gains entry. But that can't be your whole strategy. You need to plan for recovery from the attacks that will invariably make it through.

Ransomware recovery has to be as fast as possible so the business at large can get back up and running. Classic IT data recovery solutions are suitable for small, isolated recovery operations, but for large ones, these solutions are too slow and often not reliable enough. A new approach, called continuous data protection, allows for fast recovery from even significant data losses.

The ransomware pandemic persists

A recent Enterprise Strategy Group (ESG) survey of midmarket organizations[1] found that ransomware attacks are extremely common: 47% of respondents experienced attacks on at least a monthly basis in 2021 and 73% suffered at least one successful attack. Further, 53% of victims of successful ransomware attacks reported that this included sensitive infrastructure configuration data. This scenario not only exposes details that could enable future attacks but also complicates recovery.

[1] "The Long Road Ahead to Ransomware Preparedness," ESG eBook

The cost of a successful attack can be huge and is in proportion to the amount of data loss and the time before recovery. How much money is lost to ransomware is a difficult number to nail down, as victims often are not happy to share details. But Cybersecurity Ventures says the losses from ransomware[2] in 2021 were $20 billion, and it predicts that number will hit $265 billion in 2031.

Even in the best case, ransomware can cause hours of downtime. As well, ransomware attacks can cause customers to lose confidence and the event can expose the company to additional, costly compliance audits.

The limits of conventional data recovery

For these and other reasons, backup and recovery is now serious business. Organizations are using various on-premises and cloud-based backup facilities to mitigate risk, and these strategies continue to evolve. For many years, conventional wisdom held that if you had backups, at least you could recover, even after a delay. However, attackers began encrypting or corrupting backups as well. As a result, many organizations now have to air gap backups to protect them from corruption.

In the ESG survey, 47% of respondents said they use a third-party tool to validate the integrity of backups to ensure they are usable for recovery. The more concerned survey participants were that their backups could be compromised, the more likely they were to use third-party solutions. Almost nobody said they left backups where any intruder could find them: 49 percent of respondents take extra measures to protect all of their backups, and 97 percent take such steps to protect at least some backups.

Recovery tools are not just about ransomware. There are other disasters to plan for, such as failures of applications and services, natural disasters that take down facilities, and outages from mistakes, similar to what Rogers Communications, a large Canadian telecom, recently suffered.[3]

Phil Goodwin, research vice president for the infrastructure systems, platforms, and technology group at IDC, says the implementation of disaster response is more common than ever, with smaller application- and workload-specific events being handled as part of the disaster response process. Goodwin calls these micro disasters.

Data becomes unrecoverable for many reasons, and solutions geared toward just one of them will not always solve the problem. The use of outdated technologies and inadequate backup practices can result in unrecoverable data. An IDC survey[4] lists several noteworthy reasons for data being unrecoverable, including:

- Backup system failure: 49%
- Corrupted/encrypted data due to malware/ransomware: 46%
- Data loss occurring in the gap between backups: 45%
- Human error: 35%
- Lost or damaged tapes: 29%

All of these factors point to the need for an automated, isolated, and continuous system.

Immediate ransomware response

An IT disaster recovery plan needs to consider two subtly different numbers that come into play during an attack:

- Recovery-time objective (RTO) is the maximum acceptable amount of time that can pass from the point at which business is disrupted by the attack until business operations are restored.
- Recovery-point objective (RPO) is the age of the files that must be recovered in the event of an outage before recovery becomes difficult or impossible. RPO is an important number for calculating your backup frequency. An RPO of one hour means you are willing to accept an hour of data loss at most. Even that may seem high, but if you aren't backing up continuously, every backup solution includes the acceptance of some level of risk.

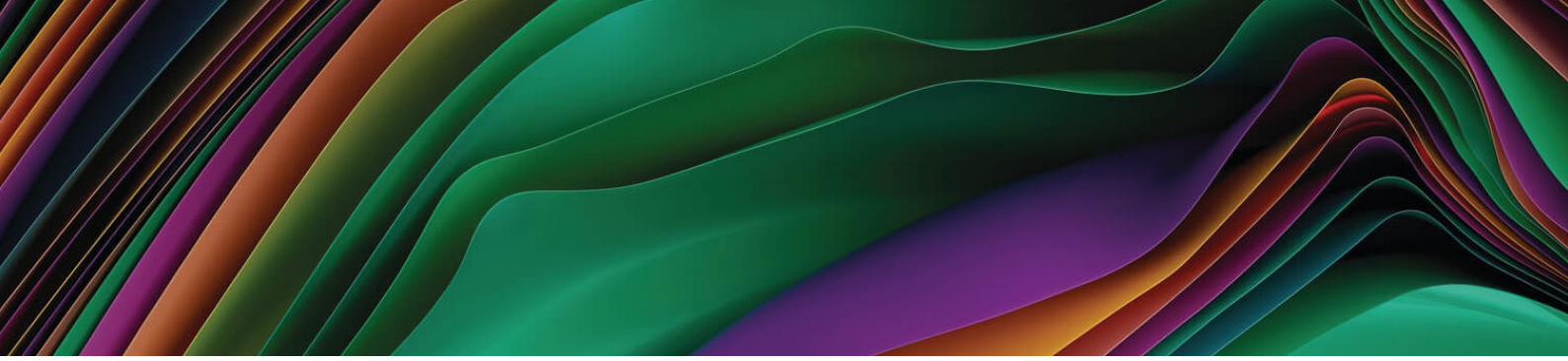
Ransomware recovery can make RTO and RPO calculations hard for various reasons. You can reasonably estimate downtime if a particular application or server goes down absent an attack, but recovering from a ransomware attack is much more complicated.

As the IDC survey data shows, restoring from backup is not a great situation even when backups are intact. It is common for backups to be unusable or for the recovery system to fail as it is running. These problems become evident during thorough testing, but the data shows that few organizations test restoration thoroughly and frequently enough.

[2] "Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031," Cybercrime Magazine

[3] "CRTC ordering Rogers to explain in detail what caused massive network outage," Canadian Broadcasting Company, 2022

[4] "The State of Data Protection and Disaster Recovery Readiness: 2021," IDC white paper



Part of the reason for this is that the restoration process itself can be very lengthy. Stories abound of victims that chose to pay a ransom because recovery with the decryption key appeared to be faster than restoring from backup. Surveys show that most organizations are at least partly prepared to pay ransom and have cryptocurrency accounts just for that purpose.

And yet, paying the ransom and hoping to decrypt all your data is not a road to a quick recovery. A high percentage of organizations do pay the ransom,[5] but a third of those that paid were still unable to recover all their data.[6]

Continuous data protection

The ideal solution to these problems is one that continuously backs up and provides the fastest recovery possible. Continuous data protection (CDP) is a solution that delivers always-on replication of data combined with detailed journaling. You start with a complete backup from a known good state, called a gold backup, and CDP automatically backs up all changes to the data, along with when they occurred. This means you can either perform a full restore from the gold backup, plus all the changes, or more likely, roll back to a particular point in time by undoing any changes since that point.

As long as the backups are protected, recovery from an attack that modifies data should be complete and fast, at least relative to restoring conventional backups. To meet fast-as-possible goals, CDP is implemented on disk- or flash-based storage instead of the usual tape. This makes it expensive, but the knowledge that you can recover quickly and keep business moving makes the cost easier to justify.

Because CDP backups are stored on disk and only modified data is backed up, restore processes are considerably faster than full backups, primarily when a time rollback is performed.

CDP hardware is usually deployed in the data center near the devices it is backing up. If an organization has a requirement for off-site backup, it can usually be accommodated as a secondary backup method.

CDP solves some of the biggest problems with conventional backup, namely the fact that data written since the last backup may be lost. Both recovery points and recovery times are effectively minimized because little, if any, data will be lost in the event of a disaster and recovery is faster than with any other recovery method.

[5] "More organizations are paying the ransom. Why?," Help Net Security, April 11, 2022

[6] "Paying the ransom is not a good recovery strategy," Help Net Security, May 24, 2022

a50006811ENW