

Cyber resilience: Manage and mitigate the high cost of cyber threats

Prepare for, respond to and recover from a cyber attack

The IDC report, State of Disaster Recovery and Data Protection Readiness: 2021, clearly shows the growing threat of facing a cyber-attack, such as ransomware, specifically the threat of data loss and significant business disruptions. Out of the organizations surveyed, IDC found that:

- **95%** experienced a malicious attack in the past 12 months
- **43%** of which suffered unrecoverable data loss
- **63%** suffered a data-related business disruption

Cyber-attacks are here to stay, with new variants and technical methods expanding every day. The result is these attacks are growing in both severity and volume. Traditional cyber security strategies aren't evolving fast enough nor protecting us in a business world expecting 24/7 availability.

Therefore, organizations are shifting their cybersecurity strategies towards cyber resilience. Instead of focusing exclusively on securing network parameters, many are shifting towards mitigating risk across global, hybrid-cloud environments.

Cyber resilience is preparing for, responding and recovering from a cyber-attack. It's not just about prevention anymore. Rather, it's about consistently ensuring the integrity of your critical data. Cyber resilience spans your people, process and technology.

People & process: Building a strong process and culture focused on cyber resilience

Without the right framework, you are completely susceptible to any form of cyber-attack. Modern IT organizations adopt a specific framework, such as the NIST framework, to ensure they have the right processes for every step of their cyber security approach. This includes processes and methodologies for threat protection, detection, identification, and recovery.

Having the right preparation is crucial, but equally important is deploying the right data recovery technology, such as with Zerto, a Hewlett Packard Enterprise company, that employs continuous data protection (CDP) as part of its platform.

[Access the Cyber Attack Survival Kit for more resources to help you build a strategy to focus on cyber resilience.](#)

KEY HIGHLIGHTS

Recovery in seconds

Recover entire sites, applications, VMs and files with granularity and within seconds

Application consistency

Restore entire multi-VM applications quickly from the same checkpoint for a consistent recovery

Short & long-term retention

Use Zerto's journaling technology across short- and long-term retention periods

Continuous non-disruptive testing

Perform recovery testing with no impact to production in an isolated environment with additional reporting capabilities

Data forensics

Isolate your data in a separate network and ensure its integrity before restoring back to production

Continuous data protection in an era of cyber threats

The IDC State of Data Protection and Disaster Recovery: 2021 survey also found that 80% of respondents have had to rethink data protection due to the sudden emergence of work from home, among other factors. Why? Because traditional recovery solutions haven't evolved. The nature of snapshot backup technology leads to time gaps, data loss, and lengthy recovery times that are a disruption to your entire organization.

The Zerto difference: Continuous data protection

Continuous stream of recovery points: The Elastic Journal combines the granular journal technology with long-term repositories, providing a continuous stream of recovery points from any point in time going back just seconds, to hours, months, or even years.

Application consistency: Protect and recover entire application stacks with guaranteed consistency through Virtual Protection Groups. Consistency is maintained across multiple virtual machines (VMs) no matter where they are running in your infrastructure.

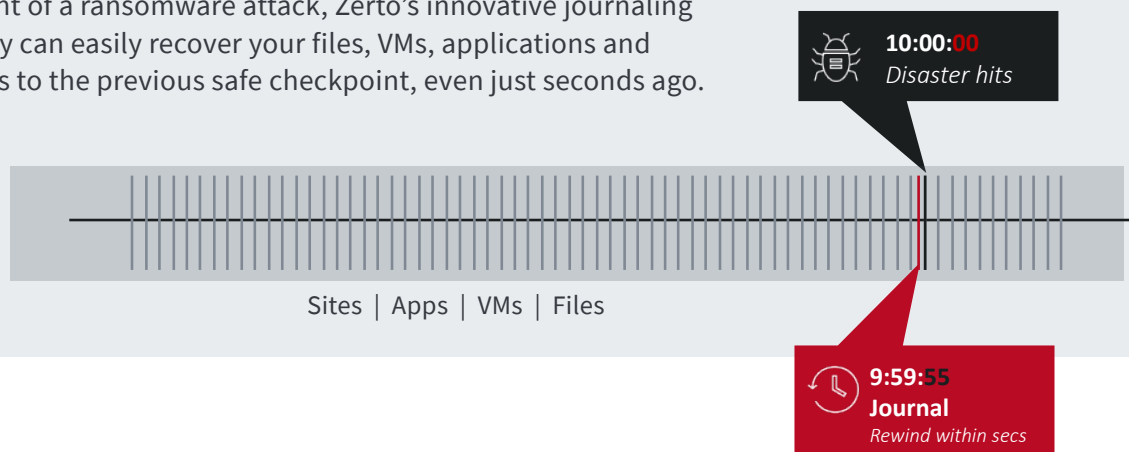
Continuous non-disruptive testing: Zerto's IT Resilience Platform™ enables orchestrated and automated disaster recovery testing, carried out any time, with just four simple clicks.

During our last ransomware attack, we were able to stop it within 15 minutes and be back up and running within 3 hours! Without Zerto, we would have had to pay the ransom and we still don't know if we'd be able to get our data back.

RUBYANNE O'BRYAN
Systems Administrator
ClearPath Mutual

Ransomware recovery in seconds

In the event of a ransomware attack, Zerto's innovative journaling technology can easily recover your files, VMs, applications and entire sites to the previous safe checkpoint, even just seconds ago.



SCHEDULE A DEMO



TAKE A TOUR

About Zerto

Zerto, a Hewlett Packard Enterprise company, empowers customers to run an always-on business by simplifying the protection, recovery, and mobility of on-premises and cloud applications. Zerto's cloud data management and protection platform eliminates the risks and complexity of modernization and cloud adoption across private, public, and hybrid deployments. The simple, software-only platform uses continuous data protection at scale to converge disaster recovery, backup, and data mobility. Zerto is trusted by over 9,500 customers globally and is powering offerings for Microsoft Azure, IBM Cloud, AWS, Google Cloud, Oracle Cloud, and more than 350 managed service providers. www.zerto.com

Copyright 2021 Zerto. All information may be subject to change.