# Manage and Mitigate the High Cost of Ransomware

## Get Ransomware Ready with Zerto

Ransomware is one of the most dangerous threats to organizations around the world, and both the threat and the cost of ransomware attacks are continuing to grow. If you are not prepared for an attack, you are vulnerable to hours or days of downtime, data loss, and damaging news coverage. To stay competitive, or even survive doing business in the next decade, you must treat ransomware as not just another cybersecurity threat, but as a true disaster.

Ransomware prevention is important but, regardless of how many preventative measures you have in place, the prevalence of ransomware means experiencing an attack is inevitable. Preparation and choosing the right disaster recovery solution is crucial when, not if, a ransomware attack happens.

**Cyber security experts predict that by 2031 ransomware will grow in frequency and in cost to the world economy.**

## $265 Billion
*Cost of ransomware attacks*

## 2 Seconds
*Ransomware attack occurrence*

*Source: David Braue, "Global Ransomware Damage Costs Predicted to Exceed $265 Billion by 2031." Cybercrime Magazine. Jun. 3, 2021.*

### Recover systems and data within minutes of an attack

One of the biggest costs of a ransomware attack is downtime as organizations are disrupted by loss of access to critical data and systems. Reducing downtime to minutes nearly eliminates these costs.
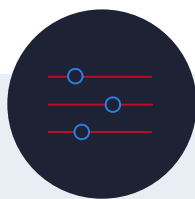
### Recover data to a point seconds before an attack

Data loss can equate directly to loss of intellectual property, productivity, and revenue. Eliminate days or hours of data loss by enabling recovery to a point seconds before an attack.

### Lower risk with instant, non-disruptive testing

A recovery plan is only as good as your ability to execute it successfully. Testing disaster recovery plans without disrupting your production environment lets you test often at any time and gain confidence by testing both failover and recovery quickly.

# Zerto Disaster Recovery Beats Ransomware

Zerto, a Hewlett Packard Enterprise company, enables the best recovery time objectives (RTO) and recovery point objectives (RPO) at scale for organizations around the world. Zerto stands out from other recovery solutions by using continuous data protection with unique journaling technology, application-consistent recovery, immutable data copies, recovery automation, multi-platform agility, non-intrusive DR testing capabilities, reporting, and analytics.

## Zerto Ransomware Recovery Features

**Continuous Data Protection**—Zerto replicates all data changes in real time to a journal where recovery checkpoints are created every five seconds. This recovery journal can be local, remote, or both, enabling fast recovery of individual files, virtual machines, containers, entire applications, and sites to a point seconds before a ransomware attack.

**Application Consistent Recovery**—Zerto logically groups virtual machines and containers to combine all workloads in an application, a department, a site, or any combination you need. A virtual protection group (VPG) keeps data consistent across all workloads in the group, so you can recover applications from ransomware with confidence.

**Immutable Data Copies**—Ransomware often targets snapshots and backups to prevent easy recovery, making a ransom payment more likely. With Zerto, copies of the journal can be made immutable to protect them from ransomware encryption and ensure recovery.

**Multi-Platform Agility**—Ransomware often targets specific operating systems or hypervisor platforms. Zerto provides additional protection against ransomware encryption of recovery data via support for and replication across multiple on-premises and cloud platforms.

**Failover and Recovery Automation**—Recover within minutes in just a few clicks, whether recovering a single file, one or more applications, or an entire site. Zerto's automation and orchestration recover virtual machines and containers and their data together in virtual protection groups so that applications are back online quickly following an attack with minimal manual interaction needed.

**Non-Disruptive DR Testing**—Test recovery scenarios often without disrupting your production environment. You can test recovery of individual applications or entire sites with built-in test reports to prepare for a ransomware attack and meet compliance requirements. And when an attack hits, you can move the test recovery into an isolated environment to ensure your recovery data is free of ransomware before rolling it back into production.

**Zerto Reporting and Analytics**—Zerto Analytics, built into the solution, provides one single, comprehensive view of your entire multi-site, multi-cloud environment. Zerto Analytics reporting gives you confidence that you are prepared for a ransomware attack and can even assist in pinpointing when the attack started.

## Zerto
a Hewlett Packard Enterprise company

### TenCate's Ransomware Experience
**READ CASE STUDY**

**BEFORE ZERTO:**
2 weeks
*recovering*
12 hours
*data loss*

**AFTER ZERTO:**
<10 minutes
*recovery time*
seconds
*data loss*

"Honestly, in the recent attack, I was kind of laughing during the recovery. I knew I had a way out with Zerto. I was confident, and my heart didn't sink. I chose a recovery point a few minutes before the infection, tested for the VM being clean and connected the vNIC – back to work. Didn't go home worried, stressed, or depressed."

Jayme Williams
**Sr. Systems Engineer, TenCate**

## TRY ZERTO NOW

Get out of ransomware jail. Protect 10 VMs, right now, for free.

🖥 | **TRY IT FREE**

🖥 | **READ CYBER ATTACK SURVIVAL GUIDE**

RITM0058086