Zerto
a Hewlett Packard Enterprise company

Manage and Mitigate the High Cost of Ransomware

Become Ransomware Resilient 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 continue to grow. If you are not prepared for an attack, you are vulnerable to days or even weeks 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, no doubt, 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.

Replicate and Detect

To avoid downtime, data must be protected, and only real-time replication gives you the lowest recovery point objective or lowest data loss possible. But when a ransomware attack occurs, detecting that attack as quickly as possible is also critical to recovering that data quickly.

Isolate and Lock

Attackers will target backups and security measures to prevent recovery because the ability to recover quickly defeats the attack. Being able to isolate recovery data where attackers can't access it and have a recovery environment that attackers haven't compromised enables that quick, assured recovery.

Test and Recovery

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 at any time and gain confidence by testing both failover and recovery quickly.

Disaster Recovery with Zerto 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, real-time detection, recovery automation, non-intrusive DR testing capabilities, reporting, analytics, and the Zerto Cyber Resilience Vault.

Zerto Ransomware Resilience Features

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

Real-Time Encryption Detection—Zerto uniquely detects encryption as changed blocks are replicated in real time, analyzing data for encryption anomalies, and sending alerts when anomalies are found. Zerto also tags checkpoints in the recovery journal to make it easier to pinpoint when an attack began, and which recovery checkpoint should be used for safe recovery.

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 Cyber Resilience Vault

For the ultimate last line of defense against ransomware, the Zerto Cyber Resilience Vault provides isolation, air-gapping, immutability in a zero-trust architecture. Built with HPE Alletra for storage, HPE Proliant for compute, and HPE Aruba for networking, the Zerto Cyber Resilience Vault stores recovery data on production-grade hardware that can be used to run your application within minutes of detecting a ransomware attack with full confidence.

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

LEARN MORE

Free On-Demand Lab

Zerto Cyber Attack Survival Guide

Zerto Cyber Resilience Vault

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. **www.zerto.com**