REQUEST A DEMO

Zerto
a Hewlett Packard Enterprise company

CYBERATTACK SURVIVAL KIT

Unlock Cyber Resilience with Rapid Recovery

NEXT

REQUEST A DEMO

CYBER RESILIENCE:

Defend Your Business from Financial Impact and Reputation Damage

Ransomware... Not If, but When and How Severe?

Ransomware attacks have been escalating for years and continue to rise in volume and severity. Cybercriminals have used malicious code to wreak havoc on businesses and are constantly inventing new and unexpected methods to spread malware and encrypt critical data. When it hits your business, vital data gets encrypted, and recovering from the attack could cost millions in reputational damage and lost revenue. Ransom costs continue to increase, and attacks continue to specialize. No organization is immune to a ransomware attack.

So, just how prevalent is the ransomware concern among businesses?

> Ransomware affected 66% of organizations in 2023.[1]
>
> Ransomware is expected to attack a business, consumer, or device every two seconds by 2031[2]

With alarming statistics and news headlines of ransomware attacks increasing, it's not a matter of if an attack will happen—it's a matter of when and how severe it will be.

Things get even scarier when you look at the cost of these attacks.

> The average ransom payment almost doubled from $812,380 in 2022 to $1,542,333 in 20233.[1]
>
> The total cost of ransomware in 2031 will be $265 billion.[4]

It's clear: ransomware is not only growing more frequent, but more costly as well.

Organizations like yours have long focused on preventing cyberattacks on their data centers and users. But as business has evolved rapidly, your data now resides in disparate locations (on-premises and in the cloud), in different workloads, and in the hands of more users than ever. To meet more demanding service levels in this evolving threat landscape, your strategy must take cyber recovery just as seriously as prevention.

If you know an attack will happen, then you need multiple layers of defense that include recovering your data.

[1,3] *2023 Ransomware Report: Sophos State of Ransomware*

[2,4] *Global Ransomware Damage Costs Predicted to Exceed $265 Billion by 2031 (cybersecurity ventures.com)*

REQUEST A DEMO

DETECT RANSOMWARE IN REAL TIME

When Ransomware Attacks, Speed Matters

You've been hit by a ransomware attack, and reacting quickly is vital to reducing the impact of the attack. But how can you react if you don't know the attack has begun? Being able to detect when an attack begins and data is starting to become encrypted gives you the ability to act quickly. If you have lengthy delays to scan a backup, your data may already be encrypted, and the malware's reach is ever increasing.

Real-time encryption detection can help minimize the scale or blast radius of ransomware's impact phase. Some businesses may misunderstand how much and how fast ransomware typically encrypts, but the numbers tell the story.

Analysis

An internal analysis of 116 globally diverse ransomware attacks, spanning 43 different ransomware variants, uncovered that a median dataset of 183.5 GB was compromised. A separate study from Splunk, *An Empirically Comparative Analysis of Ransomware Binaries*, found the average ransomware can encrypt a gigabyte of data in 47.7 seconds. This means that in a typical attack, the full encryption detonation would be estimated to take 2 hours and 26 minutes.

Unfortunately, waiting for a nightly backup to run and then scanning those copies means the average ransomware has already finished encrypting the entire dataset 12–24 hours beforehand—in a race against time, the attackers are miles down the road before there'd be any alerts that there's an issue.

With Zerto

Zerto, on the other hand, can detect and alert within seconds. If ransomware is detected within 15 seconds, for example, not only is the average ransomware not finished encrypting, but it would've only managed to encrypt about 300 MB out of the 183.5 GB—about a 99.8% savings in the amount of locked data.

The sooner you can detect, the sooner you can take action: that's why real-time encryption detection has real-world ramifications.

Read the Data Sheet—Real-Time Ransomware Detection

Read the Gorilla Guide to Real-Time Ransomware Detection and Recovery—Gorilla Guide to Real-Time Ransomware Detection and Recovery

REQUEST A DEMO

SAFEGUARDING IN A VAULT

Isolate and Lock Data with Immutability and Air Gapping

One key difference between a cyberattack like ransomware and a more typical disaster scenario is that a ransomware attacker will actively attempt to prevent recovery. Attackers will target recovery data for encryption or deletion so that the only way to recover is to pay the ransom. Safeguarding recovery data is essential to ensuring recovery in the worst-case scenario of attackers having compromised your recovery tools.

One way data can be protected is by making it immutable so that attackers cannot change or delete that data. Immutability is often used on static data copies that are stored in an unchanging state in remote locations like cloud storage. Even so, attackers have found ways to attack immutable data copies by altering the policies that made them immutable or artificially altering the system times. For greater protection, a cyber vault is needed.

What is a Cyber Vault?

A well-designed cyber vault can protect recovery data by making it inaccessible to attackers with air gapping and immutability built on a zero trust architecture. Ideally, the vault can only be managed by direct physical access within the data center, so it's fully protected from network intrusions. Cyber vault architecture is meant to provide an air-gapped cleanroom where recovery can begin quickly and safely during the forensic phase after a ransomware attack has hit.

The Zerto Cyber Resilience Vault combines Zerto with HPE Alletra Storage, HPE Proliant compute, and HPE Aruba networking to provide a fully isolated, zero trust architecture. This architecture enables every level of recovery, from individual files to entire sites, with the isolated vault being the ultimate failsafe. Zerto gives users the ability to recovery in minutes or hours from most types of attacks. With the Zerto Cyber Resilience Vault, you are protected from every level of cyberattack with isolated, air-gapped, and immutable copies of your data in a production-grade compute and storage environment.

Learn more about the Zerto Cyber Resilience Vault—Cyber Resilience Vault

Watch a Short Video—Understanding the Zerto Cyber Resilience Vault on Vimeo

REQUEST A DEMO

CYBERATTACK RECOVERY SCENARIOS

Recover What is Needed

Cyberattacks like ransomware can come in many shapes and sizes. They can affect only files and folders, virtual machines, or they can affect whole sites and multiple sites. While having a vault in place gives you recovery failsafe, many attacks can be recovered. These five videos cover some of the wide range of recovery options with Zerto.

Ransomware Recovery After File Encryption

This video looks at a small-scale attack that has encrypted files and folders on a VM and discusses how Zerto can provide instant file restores.

Ransomware Recovery After File Encryption (v2 on Vimeo)

Ransomware After VM Encryption

This video looks at an attack that has compromised an entire VM and discusses how Zerto can provide instant VM restores.

Ransomware Recovery After VM Encryption (v2 on Vimeo)

Ransomware Recovery After Application Infection

This video looks at an attack that has infected all VMs that comprise a multi-VM app stack and how Zerto can recover using orchestrated failovers to a peer site.

Ransomware Recovery After Application Infection (v2 on Vimeo)

Ransomware Recovery After Site Infection

This video looks at an attack that has compromised the infrastructure at all on-premises sites and how Zerto can recover using orchestrated failovers to a cloud DR site.

Ransomware Recovery After Full Site Infection (v2 on Vimeo)

Ransomware Recovery After Multi-Site Infection

This video looks at an attack that has fully infected all on-premises and cloud infrastructure and how Zerto can recover using portable immutable copies that can be re-attached to any new or existing Zerto deployment.

Ransomware Recovery After Multi-Site Infection (v2 on Vimeo)

REQUEST A DEMO

A TALE OF TWO RANSOMWARE ATTACKS

A Before and After

About TenCate: This multinational textile company, based in the Netherlands, experienced ransomware attacks twice. The first attack occurred prior to implementing Zerto, and the second one occurred after the Zerto implementation. Their experience recovering from ransomware using backups the first time versus Zerto the second time reveals the power of Zerto for fast, nondisruptive ransomware recovery.

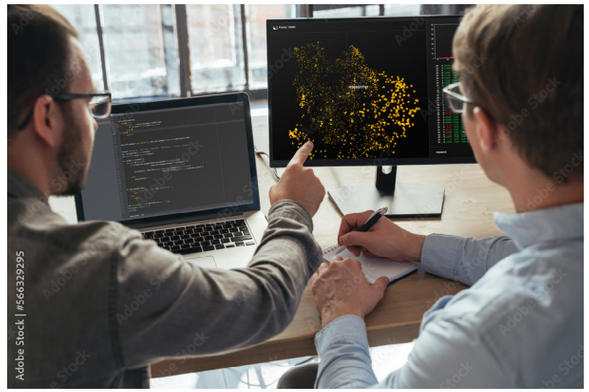
TenCate spent weeks recovering after a first attack with their legacy backup solution. After adopting Zerto, recovery from a second attack took just 10 minutes—with virtually no data loss.

Before

One of TenCate's manufacturing facilities was hit with CryptoLocker. All of the file servers were infected. At this point, TenCate's only recovery method was restoring from disk. As a result of this attack, TenCate experienced 10 hours of data loss and was not able to recover for two weeks.

After

Directories on a file server in a manufacturing facility were hit by a more advanced form of CryptoLocker. TenCate only experienced 10 seconds of data loss and was able to recover in under 10 minutes.



After adopting Zerto, TenCate recovered from a second ransomware attack in just 10 minutes with virtually no data loss.

REQUEST A DEMO

BUILD YOUR CYBER RESILIENCE STRATEGY

Take a Proactive Stance Now

Prevention of cyberattacks isn't always possible, but mitigating the threat certainly is. Zerto enables you to defend your business from the lasting effects of cyberattacks like ransomware. When you are in control of your business data, you are no longer vulnerable to the hacker's demands. Forget about paying the ransom and recreating lost work. With real-time encryption detection, immutability, air gapping in a secure vault, and flexible, orchestrated recovery, Zerto helps to minimize data loss and downtime in the event of a ransomware attack.

Try Zerto Recovery from Ransomware with an On-Demand, Hands-On Lab—myZerto Labs: MyZerto

EXPLORE OUR LAB

Read a Technical White Paper—Ransomware Technical White Paper

WHITE PAPER

Learn more about Zerto for Cyber Resilience—Malware & Ransomware Recovery

LEARN MORE

Watch an On-Demand Webinar—Building a Cyber Resilience Vault with Zerto

WATCH THE WEBINAR

Contact Us for More Information

CONTACT US

BACK