Is your organization ransomware proof?

How to use DRaaS as your silver bullet against ransomware attacks

FLEXENTIAL®

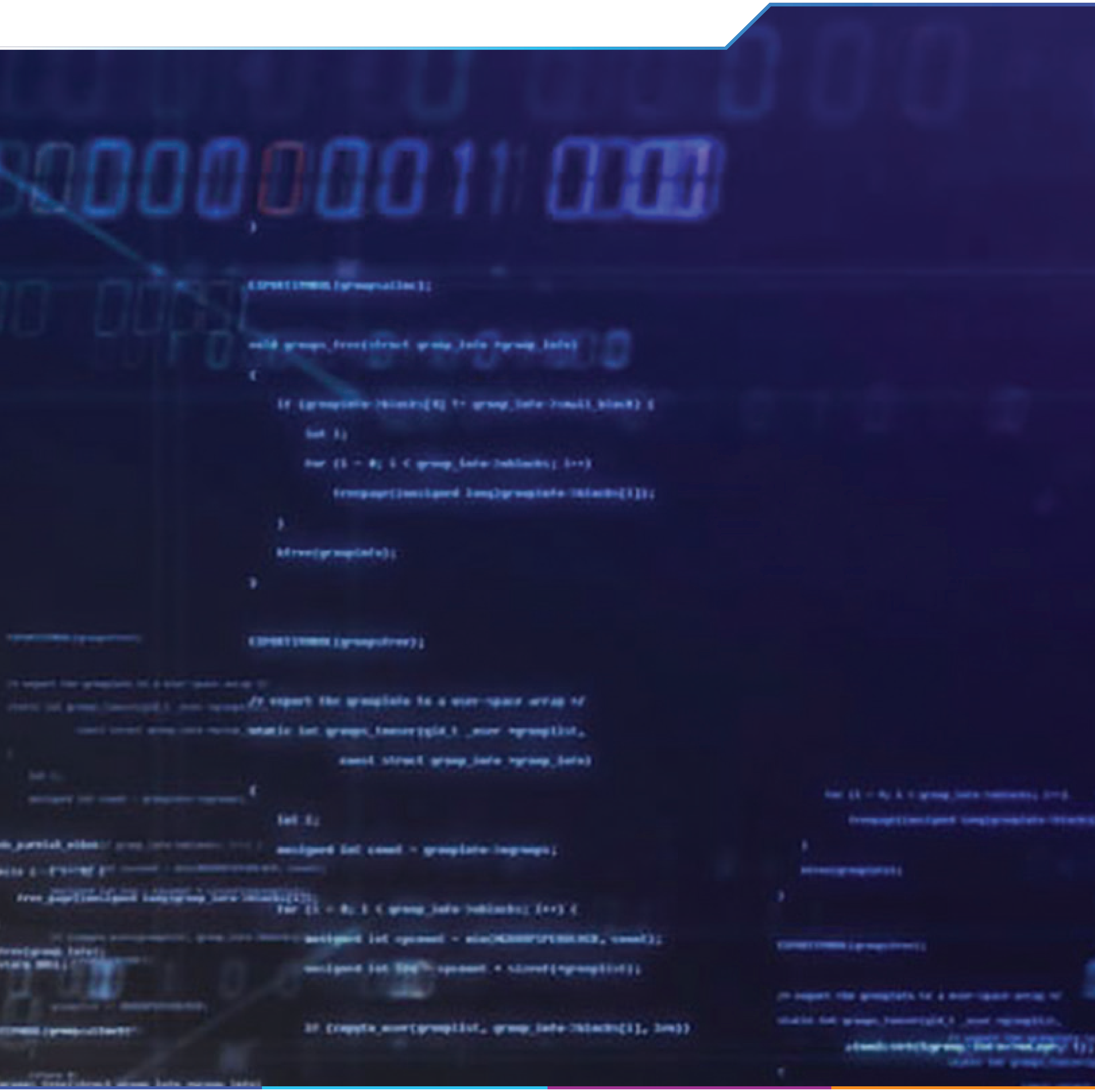


Table of Contents

Introduction

An organization will fall victim to a ransomware attack every 11 seconds by the end of 2021, according to a Cybersecurity Ventures report, and effectively protecting your data and IT environment seems to get more complex by the day.

Gone are the days when traditional backups sufficed. With the adoption of digital IT transformation strategies, organizations rely on more dynamic solutions to safeguard their complex IT environment and protect their mission-critical data, applications and workloads against disruptions and threats like cyberattacks.

While malware, breaches, phishing and other cyberattacks have been on the rise for years, the dramatic explosion in ransomware attacks is shaking the IT security landscape. Cybersecurity Ventures predicts that ransomware will cost the world $20 billion annually by 2021. This statistic is particularly alarming given ransomware's ability to quietly encrypt data, undetected—potentially for weeks or even months. Ransomware can put organizations with recovery windows of only hours of strategy more vulnerable to data loss. This failback period may not be enough to restore files and minimize data loss associated with a well-concealed ransomware attack.

This presents a disturbing scenario and liability for any business and begs the question: How can a business ensure the rapid and accurate recovery of its files without extensive data loss? A solution such as disaster-recovery-as-a-service (DRaaS), which is able to replicate days' worth of data, rather than hours, for up to 30 days is a powerful first step.

An organization will fall victim to a ransomware attack every 11 seconds by the end of 2021.

The lowdown on ransomware

In 2020, Forrester predicts that data will continue to be "weaponized" and monetized by ransomware attackers as they continue to be financially rewarded for their hostage-taking efforts.

This threat does not discriminate. It impacts all businesses—across industries and without regard for size.

Ransomware is a form of malware that encrypts files and then demands the victim pay a ransom to restore the files.

Case and point: In 2019, a massive ransomware attack crippled the City of Baltimore for more than a month, with losses amounting to more than $18 million. In addition to the high monetary cost, the government is also likely experiencing substantial intangible costs due to citizens' loss of trust in the government's ability to safeguard their data.

Also, in 2019, multiple healthcare providers fell victim to ransomware, with one paying $75,000 to recover its files.

The point is that no business is immune to a ransomware attack. So what is a ransomware attack and how does it work?

Ransomware is a form of malware that encrypts files and then demands the victim pay a ransom—often payable in bitcoin for anonymity—to restore the files.

The most prevalent form of ransomware attack occurs when a user opens a seemingly legitimate attachment or clicks a link in an email, unknowingly releasing the ransomware. The ransomware then infects their computers with malicious software that encrypts files and folders on local drives, attached drives, backup drives and other computers on the network.

Users and organizations are generally not aware they have been infected until they are unable to access their data or until they receive ransom demands. Clearly, this can be catastrophic to a business as it can impact the safety of sensitive or proprietary information, disrupt regular operations, incur financial losses for restoring systems and files, and potentially damage an organization's reputation.

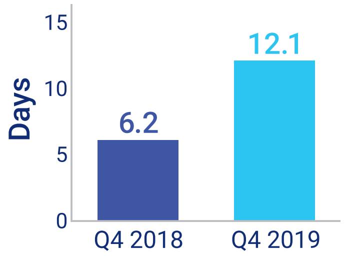
The threats in our midst

As the saying goes, data is the lifeblood of a business, and with ransomware becoming a very real, daunting reality, businesses need to be prepared to prevent attacks and fight back when necessary.

First of all, how can a business maintain operations seamlessly after an attack?

While continuous data protection can be an integral piece of this solution, how long the data is retained is a compelling issue. Data has commonly been retained for a segment of hours. While this may be enough for the run-of-the-mill power outage that is immediately identified—allowing the recovery process to be quickly set into motion—there is an increasing number of situations, including ransomware attacks, where going back more than a few hours is necessary to recover operations.

AVERAGE DOWNTIME DUE TO A RANSOMWARE ATTACK



Ransomware's ability to quietly encrypt data for days leaves businesses vulnerable: They can pay the ransom or lose the data. Even if the ransom is paid, there is no guarantee that the data will be returned. Remember, we are dealing with bad guys here. It is truly a lose-lose situation.

To address looming threats like ransomware attacks and to better protect their data and business continuity, organizations need to be able to retain a sufficient timespan of data to return to the replication point just before the incident. To achieve this, they must think about failback in terms of days, not mere hours.

Businesses need a failback window of days, not hours

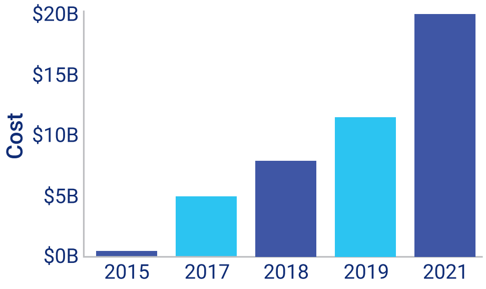
Today, more than ever, organizations need to get the most out of their DRaaS solution. In Q4 2019, the average downtime caused by a ransomware attack was 12.1 days—nearly double what it was at the same time last year.

A flexible failback window that can roll back days to heighten not only recovery capabilities but also the testing environment is critical. Being limited to hours of recovered data makes a company extremely susceptible to data loss.

Organizations have a lot to lose if their data is not properly protected. Ransomware reportedly may have cost U.S. organizations more than $7.5 billion last year, up from $325 million in 2015. Cybersecurity Ventures predicts that number will reach $20 billion in 2021.

Businesses with high downtime costs, or strict regulatory and compliance requirements are particularly at risk. The financial and healthcare industries and government institutions fall right into this mix. With extensive regulations dictating the security and management of their data, these organizations face steep fines and even more menacing business consequences if they are not prepared to effectively handle any threat to data, systems and applications availability.

PREDICTED AVG GLOBAL COST OF RANSOMWARE



Source: Cybersecurity Ventures

Companies with stronger disaster recovery capabilities are less likely to need to pay a ransom for their data because they can effectively restore their files with minimal data loss, rendering the ransom threat void.

The benefits of a failback of days also improves testing capabilities by enabling longer, more interactive and complete testing to be conducted. Companies that can create sandbox environments can test patches, test-drive enhancements and gain improved insights into the performance of their DR environment without impacting the production environment.

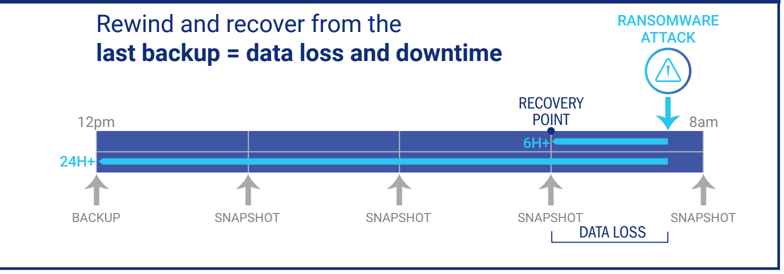
With a variety of business-crippling events present in the business world and the clear need for high-performance, comprehensive testing capabilities, what is available to satisfy this critical need? Enter extended journaling.

Extended journaling

Extended journaling, which is a feature of the Flexential DRaaS product, offers customers cost-effective options and the flexibility to build tailored disaster recovery programs, while ensuring rapid recovery of mission-critical applications and minimal data loss in the event of a ransomware attack. It's designed with flexibility, secure and cost-effective extended journaling that allows up to 30 days of data replication history. By delivering a deeper retention period, extended journaling improves continuous data protection and offers greater flexibility in recovering business applications to a specific period in time.

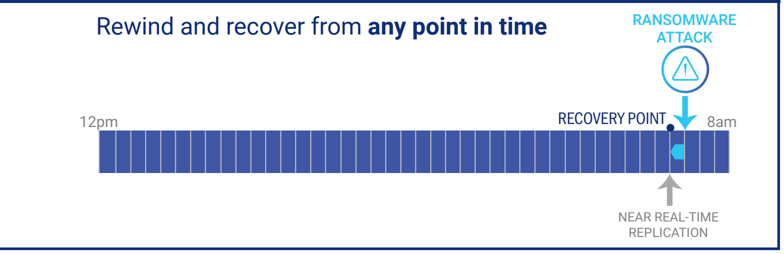
TRADITIONAL DATA PROTECTION SOLUTIONS

Rewind and recover from the **last backup = data loss and downtime**



THE FLEXENTIAL DRaaS SOLUTION

Rewind and recover from **any point in time**



Backed by the redundancy of Flexential's geographically diverse data center locations and the resiliency of its high-performing, reliable interconnection services, extended journaling enables organizations to protect their data and enrich their testing capabilities for a heightened level of preparedness.

Up to 30 days of data replication history

Extended journaling offers up to 30 days of replication history, enabling the cost-effective recovery and testing of servers protected in the Flexential Recovery Cloud. With multiple checkpoints every hour, the service offers up to thousands of recovery points to deliver a granular level of restore so that organizations can precisely pinpoint the recovery point and capably balance what they need to restore the data with the amount of data that will be lost.

> Ransomware may have cost U.S. organizations more than $7.5 billion last year.

To ensure the most robust data protection, customers can choose the journal length that best suits their unique needs. The length of this journaling history does not impede recovery speed, allowing businesses to maintain their expected recovery time objectives (RTO) for each virtual protection group (VPG).*

**A VPG is a collection of virtual machines that facilitates the efficient management of your disaster recovery environment.*

Self-service for ease of use and ultimate flexibility

Designed to be an easy-to-use, self-service capability with substantial flexibility, extended journaling offers customers real-time visibility into their DRaaS environment. Individual VPGs can be easily monitored and managed through the portal, enabling direct access to the operations driving the replication process.

Customers have the flexibility and power to manipulate their settings from the customer portal through a user-friendly dashboard, giving them greater control over their disaster recovery environment. Through the self-service dashboard, a business can monitor the status of its recovery cloud, the total amount of recovery data in its recovery environment, the recovery and testing history of the VPGs and more—putting control of their VPG solution in their own hands.

Customers can also manage virtual machines with an interface tool to tune the journaling length of individual or all virtual machines to meet current or evolving needs. The failback window can be set across all VPGs—or individually for each VPG protected in the recovery cloud—to support any disaster recovery or testing need, optimized financial spend, efficiency and application rollback.

While extended journaling is designed to be self-service, Flexential is available around-the-clock to support customers and help them get the most out of their disaster recovery testing plan.

Addressing a broader spectrum of disaster conditions

Threats are an unfortunate but inevitable part of doing business. The success of business continuity and compliance is a direct result of a business' level of preparation for an attack.

Given the security and redundancy built into the Flexential Recovery Cloud, supplementing it with extended journaling is a powerful step toward protecting business data.

Extended journaling pushes competences further to decrease the potential for significant data exposure. Its 30-day replication journal can handle the threat of corrupted or lost data associated with any ransomware attack.

More complete testing for improved performance

Tremendous testing benefits are also available because of the extended replication window. When testing is limited to a set number of hours, organizations may only have time to handle their most compulsory needs, leaving other initiatives underused or untouched.

Testing within a less restrictive environment enables more complete, interactive testing—allowing end users to be more involved in the testing process. The ability to perform more business-enabling analyses gives businesses the ability to assess new features and applications, better understand their capabilities during and after an attack, effectively check virtual machines and patches, and conduct any other strategic initiatives without disrupting the production environment. This improved testing environment increases the level of preparedness to drive even greater value from the Flexential solution.

Conclusion

As threats continue to evolve, organizations need to keep pace with the services and capabilities that protect their workloads and enhance their operations. Extended replication windows are one way to do this. By offering days—not hours—of replication history, the extended journaling capability from Flexential allows companies to quickly recover from an attack with minimal data loss. Additionally, a disaster recovery solution focused on days enables a more comprehensive testing environment that drives business direction and acumen. Focusing DRaaS on supplying days of replication is the critical step today's businesses need to take to get the most out of their recovery strategy.

About Flexential
Flexential solves IT infrastructure challenges for enterprises tasked with meeting the most stringent security, compliance and resiliency demands. We take a consultative approach that recognizes one size does not fit all and that requirements often change over time. Tailored solutions built on our highly connected national colocation platform, spanning 21 markets, and robust portfolio of cloud, data protection, managed and professional services, flex over time to accommodate evolving hybrid IT requirements.