RAMSOMWARE – How to Protect and Recover Your Data From this Growing Threat

WHITE PAPER

Contents

Introduction

Ransomware is a growing threat to every organization on the planet; it seems we cannot go a day without seeing another high-profile ransomware attack being detailed in mainstream media.

Cyber-criminals are innovating at a phenomenal pace in this growing 'industry' because they have the funds to do so. In fact many cyber-criminal groups have more funds than most enterprises.

The disruption these attacks are causing to businesses is huge with billions of dollars' worth of revenue being lost due to system outages caused via ransomware attacks.

Research has shown that a 41% increase in attacks has occurred since the beginning of 2021 with a staggering 93% increase year over year.

All the stats show the threat of ransomware is real and growing.

From *Ransomware Pulse Survey 2021 - Research Study by Evaluator Group,* shown in Figure 1, 56% of respondents indicated having spent against data protection over the last 12 months due to the rise in ransomware.

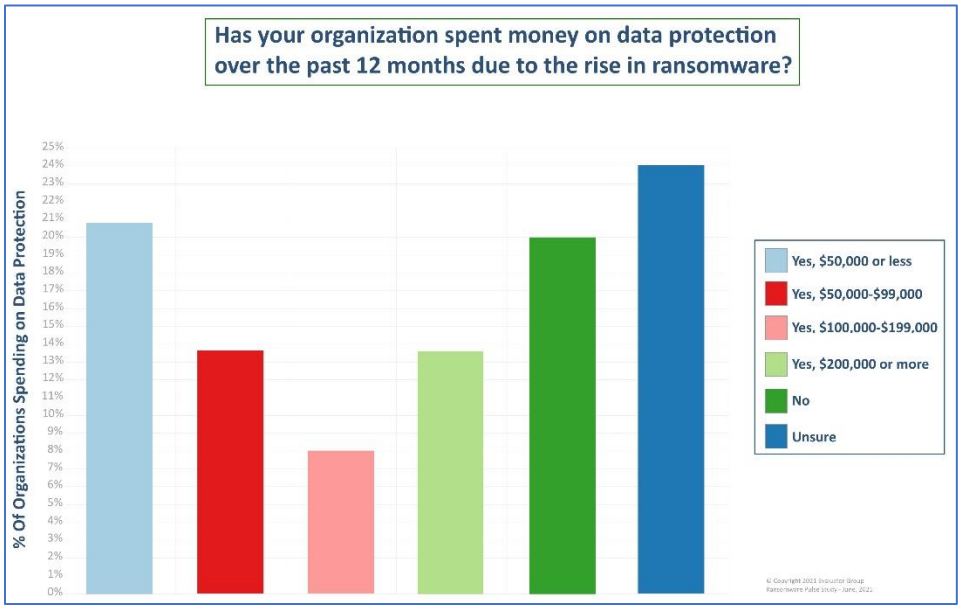

Figure 1. Data Protection Spend Over the Past 12 Months

Looking ahead, a vast 87% of respondents indicated that they plan to spend, or have budgeted to spend, against technologies for ransomware protection and prevention over the next 12 months.

The goal of this white paper is to highlight the growing threat of ransomware and detail what you can do to ensure your data is protected and recoverable in the event of ransomware attack taking place. Don't be another victim - read on and make sure you take all the steps necessary to prepare, prevent, protect, and enable recovery from ransomware.

How Does Ransomware Get In?

Companies are getting hit via ransomware every day, but how does it get in? Some of the most common ways ransomware is getting in is via the following methods:

1. Phishing emails that launch ransomware attacks via inline links, links in attachments, or fake attachments.
2. Browsing unknown links and websites.
3. Downloading and accidentally running infected software.
4. Inserting or connecting an infected disk, disc, or drive.
5. Operating system based vulnerabilities if the OS is not patched to the latest levels.
6. Plugin based vulnerabilities if plugins are not patched to the latest levels.
7. Infrastructure vulnerabilities (network, storage etc.) if not patched to the latest levels.

That list is continually expanding as more vulnerabilities are found.

There are currently many more remote workers due to the current global situation with COVID-19. This also results in a higher level of risk to organizations with most home networks undeniably easier to hack into than office networks.

Hackers are becoming increasingly sophisticated and once they are in, they may sit dormant for a period, planting attacks, watching activity, and waiting to execute at a later date, thus making recovery from an attack more complex, meaning organizations are more likely to pay the ransom.

A common comment I hear is 'we have network edge or endpoint protection, so we are safe.' Sadly, that is wrong. Whilst edge and endpoint protection solutions are a necessity and do a great job in attempting to prevent many methods of attack – including phishing, outbreaks via traps on unknown links and downloads, and blocking deployments via disk, disc, or drive – they do not protect against every form of outbreak, nor do they protect your data.

Ransomware uses many ways to get into systems and networks and often sits dormant waiting for the right time to strike. This can be after an extended period of time to increase the likelihood that backups will only recover the content that was encrypted but not the access for the attackers, so they can repeat the process again causing more pain, downtime, revenue loss and reputational impact resulting in lost business.

How to Protect and Recover your Data from Ransomware

A robust data protection solution is an absolute necessity, as it always has been and always will be. Data is the lifeblood of the vast majority of companies globally and a data protection solution should be seen as a required insurance policy. In the event of a ransomware attack, user error, hardware failure, natural disaster or any other unforeseen circumstance occurring, your business can then recover data to the applicable point in time.

For a data protection solution to be robust it needs to be built on a solid architecture. As one of the leading providers of data protection solutions for over 20 years with over 700 global customers, the team at Catalogic knows a thing or two about designing a data protection solution with a solid architecture. Here are our 5 key technical recommendations to consider when architecting a data protection solution enable protection and recovery from ransomware:

1. **3-2-1-1 Ransomware Protection Rule**
   What's this, an 8-a-side football/soccer formation? Maybe but it's also a strategy to follow to ensure your backups are available to recover your data from. The 3-2-1 backup rule is a time-honoured strategy for data protection that states that your business should have at least the following:
   - 3 copies of your data
   - 2 copies stored on different storage media types
   - 1 copy offsite or in the cloud on ideally immutable air-gapped or immutable media
   - 1 verified as recoverable

   Without backups to recover from, and the offsite copy that ransomware cannot reach, you may be forced to pay the ransom to get your data back.

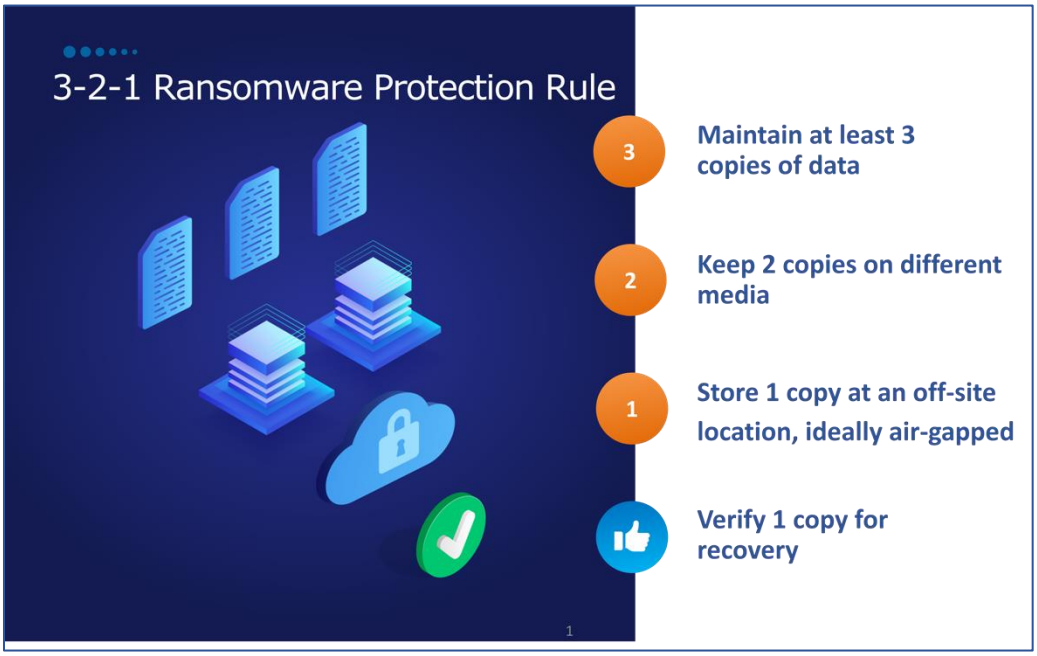

Figure 2. 3-2-1-1 Ransomware Protection Rule

2. **Instant Recoverability from Immutable Snapshots**
   The biggest pain for most businesses when looking at recovering from ransomware attacks is the time it takes to recover. Recovery procedures are often complex and slow. Slow recoveries result in larger revenue and reputational impact to businesses whilst systems are down. Data protection solutions should be focused on delivering security, speed and simplicity. With DPX we have the 3 S's fully covered:
   - **Security –** When a backup is completed it is stored as an immutable (read-only) snapshot. The immutability protects the integrity of the backup data, ensuring it is not overwritten or deleted until the backup retention time passes.
   - **Speed –** We can enable instant access recoveries, meaning regardless of the amount of data stored – be it GBs, TBs or PBs – DPX can instantly spin up a copy of your data as a writeable snapshot. These copies can be used for recovery, disaster recovery testing, reporting, DevOps, patch testing and more.

- **Simplicity –** Consumer technologies such as mobile applications and cloud storage are a major driver behind this shift to simplicity. Many backup solutions are not simple to architect, deploy and use. They involve complex command lines and need propeller heads to look after the software. Catalogic DPX is different than the competition here because it offers a simple to use, HTML UI where it's very easy to see and understand what's occurring, drive backup and restores, and provide simple concise reports to show the state of your data protection environment.

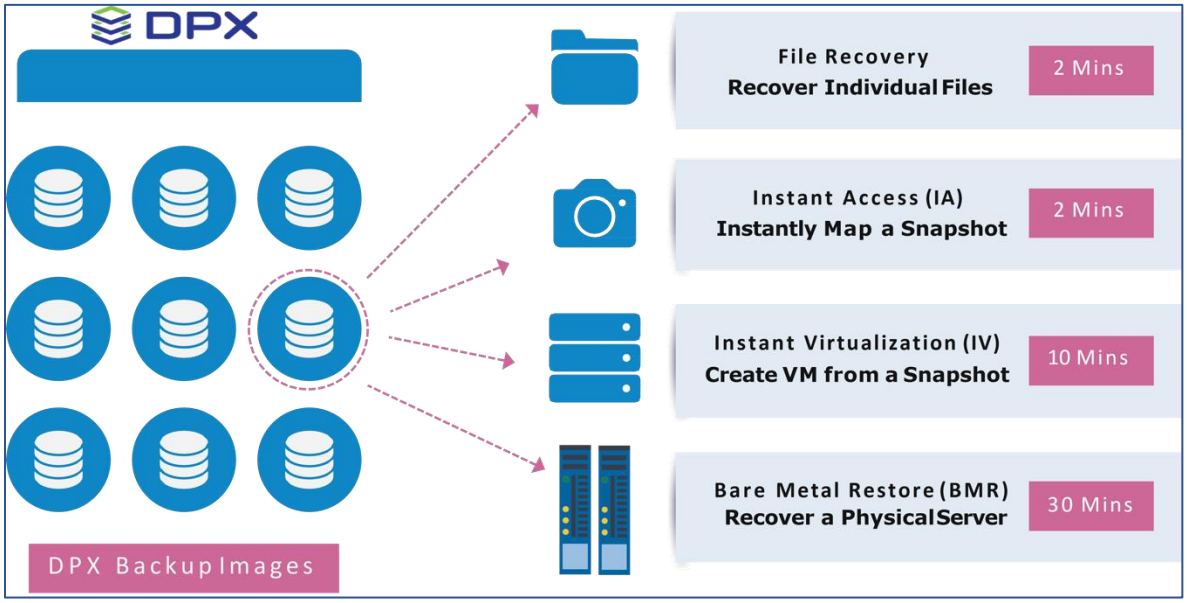

Figure 3. Catalogic DPX Provides Fast and Flexible Recovery

3. **Setting Retention Periods to Enable Granular Point-In-Time Recovery**

Sounds simple, right? However, when was the last time your businesses reviewed the retention periods set upon your backup solution? Why were they set like that again? Ah, because they always have been. Ask yourself the question – is that the correct retention period for that data now?

The average ransomware attack takes from 60 to 120 days to move from the initial security breach to the execution of the actual ransomware attack, meaning a lot of organizations already have hackers hidden in their networks waiting to strike. Therefore, a quick granular point in time recovery of the encrypted data isn't going to resolve the problem as the hacker will just strike again. The breach needs reviewing to work out what executed the attack and remove access for the hacker, as well as quickly restoring the encrypted data. This is why retention periods are so important as it presents the option to recover the breached data back to a good known state prior to hackers being present in the network. All business-critical data regardless of your industry should be stored for 120 days or more. That is more than the 30-, 60-, or 90-days standards a lot of businesses have implemented over the years.

It is critical that backups are run regularly, and data snapshots or point-in-time copies of data be taken as often as possible. You can then turn back the clock and recover as close as possible to the time the data was encrypted or damaged by ransomware and get the infected areas of your environment back to a good known state prior to hackers being present.

Retaining more data doesn't necessarily mean a bucket load more storage is needed. Catalogic DPX vStor enables data reduction via compression and deduplication to ensure your storage is optimally used. Catalogic is not a hardware vendor and has no hidden agenda to sell hardware, unlike some of our competitors. As shown in Figure 4, you can use any block storage behind DPX vStor and offload copies from vStor to many cloud providers including S3 storage in AWS, Azure, Backblaze, Cloudian, MinIO, Scality, and Wasabi, or that old airgap favorite tape. Tape continues to make strides forward in terms of its storage capacities and speed.

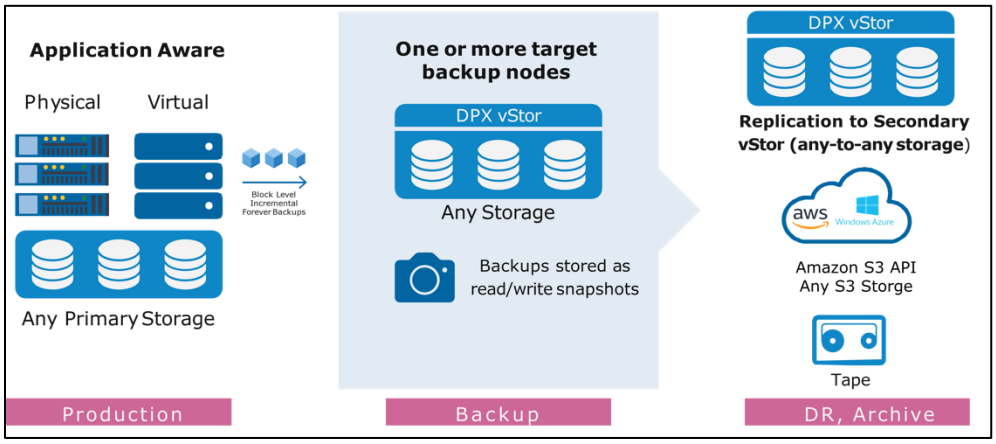

Figure 4. DPX vStor Architecture with Backup Storage Options

4. Application-Aware Backups with Verification

Applications that use databases requires additional attention if their data is protected only by the database files themselves. When a disaster or ransomware hits, a multi-step process is needed to recover applications to a point where they can be used again with minimal disruption to the business. It is therefore important to have an application-aware backup that also protects application meta data and ensures that the application servers can successfully be recovered. If you run regular application recovery verification tests, you know with relative certainty that the data and applications can be restored and up and running again quickly.

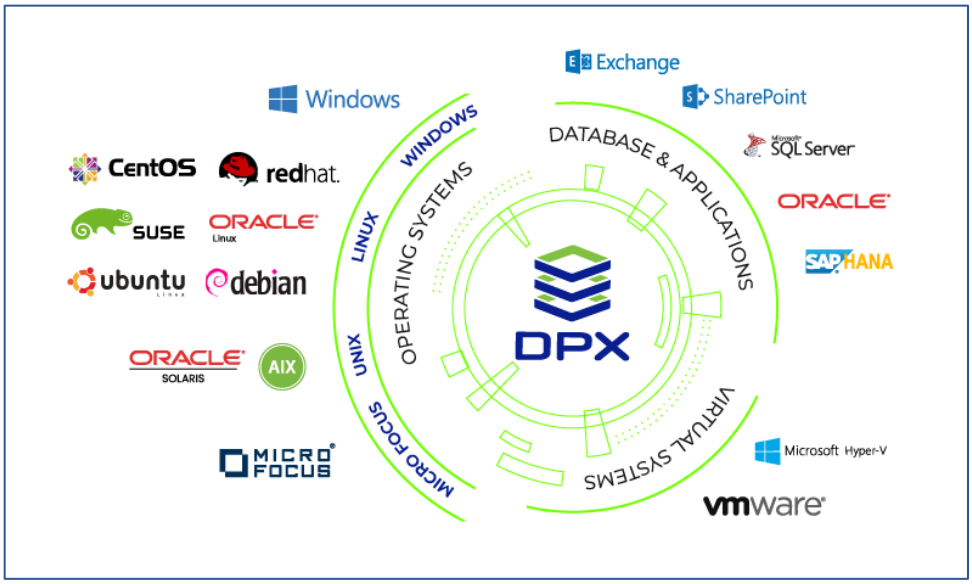

Figure 5. Application-Aware Backups

5. **Real-Time Reporting to Provide Awareness that Ransomware Could be Present**
   In normal operations incremental data backup sizes have relatively small amounts of changes between full backup cycles. When ransomware hits and data is encrypted, the incremental backups sizes suddenly become much more like a full backup, as shown in Figure 6.

   Modern data protection products can track these changes and report if backup sizes are unexpectedly much larger and alert the backup/security administrator of this anomaly. Not only can this help identify an attack in progress, it also helps identify the point in time that a rapid data recovery can be done from.

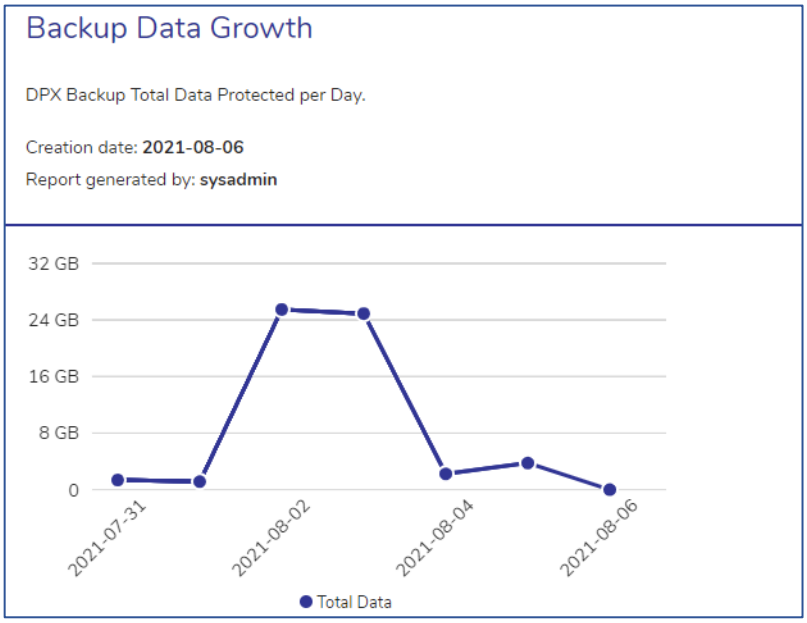

Figure 6. Real-time Reporting of Data Backup Sizes

We continue to evolve Catalogic DPX to add advanced features that ensure you can protect and recovery your data from the growing threat of ransomware.

Ransomware Recovery Checklist

Success in most walks of life can be attributed to having a plan in place. To enable quick and successful recovery from a ransomware attack, here are some of our high-level recommendations in the format of a simple checklist.

Checklist

⇒ Implement basic security fundamentals across your business.
⇒ Prepare for a ransomware attack – create a business continuity/recovery plan.

Ransomware Attack Commences

⇒ Don't panic - isolate the device where the attack Is being facilitated from and isolate the network segment that this device is on.
⇒ Ensure you have valid and verified recovery points available to restore from.
⇒ Identify the infection and activate your continuity/recovery plan.

Post Ransomware Attack

⇒ Once recovery of the impacted files are completed, closely monitor operations to confirm no malware remains.

⇒ Alert your stake holders and the authorities.

⇒ Run a detailed post assessment to confirm how the attack was enabled. Enhance your security accordingly to prevent an attack of this manner occurring again.

Conclusion

So, why should you care and what can you do to ensure your business does not get taken down and potentially wiped out via ransomware? First and foremost you should care because these cyber-criminals are trying to target the personal and financial security of businesses and individuals and they present a major threat to national security and human life. The fact that many of these criminals have no issue taking down systems that are crucial to the continuation of life in places such as hospitals sadly shows that they have no remorse or moral values.

What we can do is work together as technologists to stand up and fight against these criminals and with a multi-pronged ransomware protection strategy.

Recently Microsoft, AWS, the FBI and the UK's National Crime Agency joined the Ransomware Task Force (RTF) which provides a broad coalition and an initial framework that aims to decrease the number and success rate of ransomware attacks. The framework provides detailed recommendations on how to deter, disrupt, prepare, and respond to ransomware attacks.

The RTF report framework contains key information useful in protecting your company's data with a multi-pronged approach ensuring you have prepared for a ransomware attack and have a response plan in place so you are ready if you are attacked.

We have a shared responsibility to break this flourishing industry and ensure it doesn't grow any further. A lack of preparation and thinking will cost us all more in the end. Be prepared, stay alert, and if you need any assistance in developing your protection and recovery capabilities against ransomware feel free to get in contact with us.

About Catalogic Software

Catalogic Software is a modern data protection company providing innovative backup and recovery solutions including its flagship DPX product, enabling IT organizations to protect, secure and leverage their data. Catalogic's CloudCasa offers cloud data protection, backup and disaster recovery as a service for Kubernetes applications and cloud data services. Learn more at catalogicsoftware.com and cloudcasa.io.

About the Author

William Bush is the Field CTO for Catalogic Software in EMEA. William has over fifteen years of experience in the IT industry and has developed and delivered cloud, virtualization, storage, big data and data protection services and solutions to over 200 SMB & enterprise organisations worldwide. He is passionate about technology and understanding the latest technology standards that can be utilized to architect and deliver innovative solutions to customers. His publications have appeared in many places including TechTarget, Information Age and IT Security Guru. William is also a keen blogger and writes many articles featured on the Catalogic Blog.