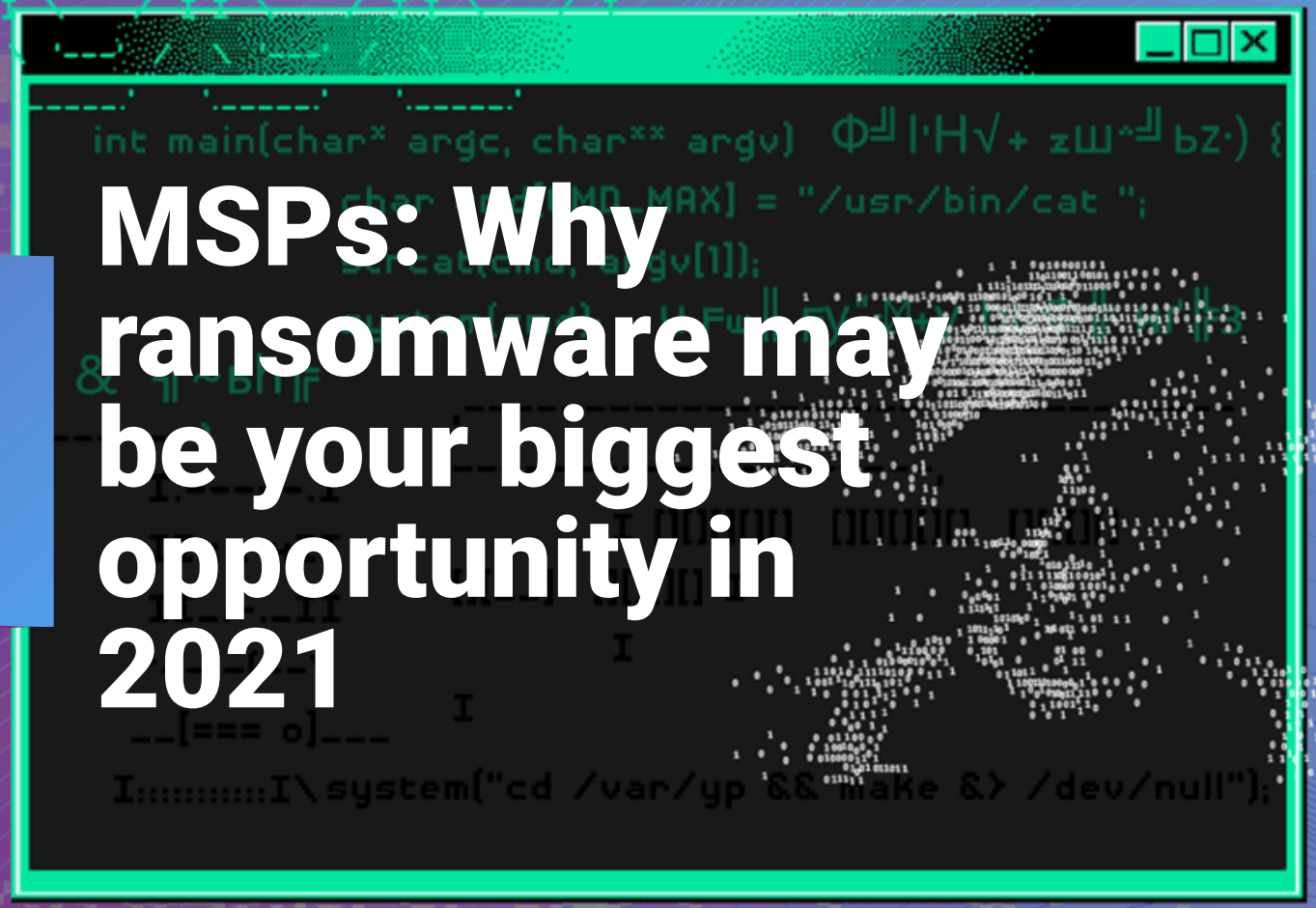
redstor



MSPs: Why ransomware may be your biggest opportunity in 2021

brigantia

Ransomware: the unwelcome winner of 2020

redstor

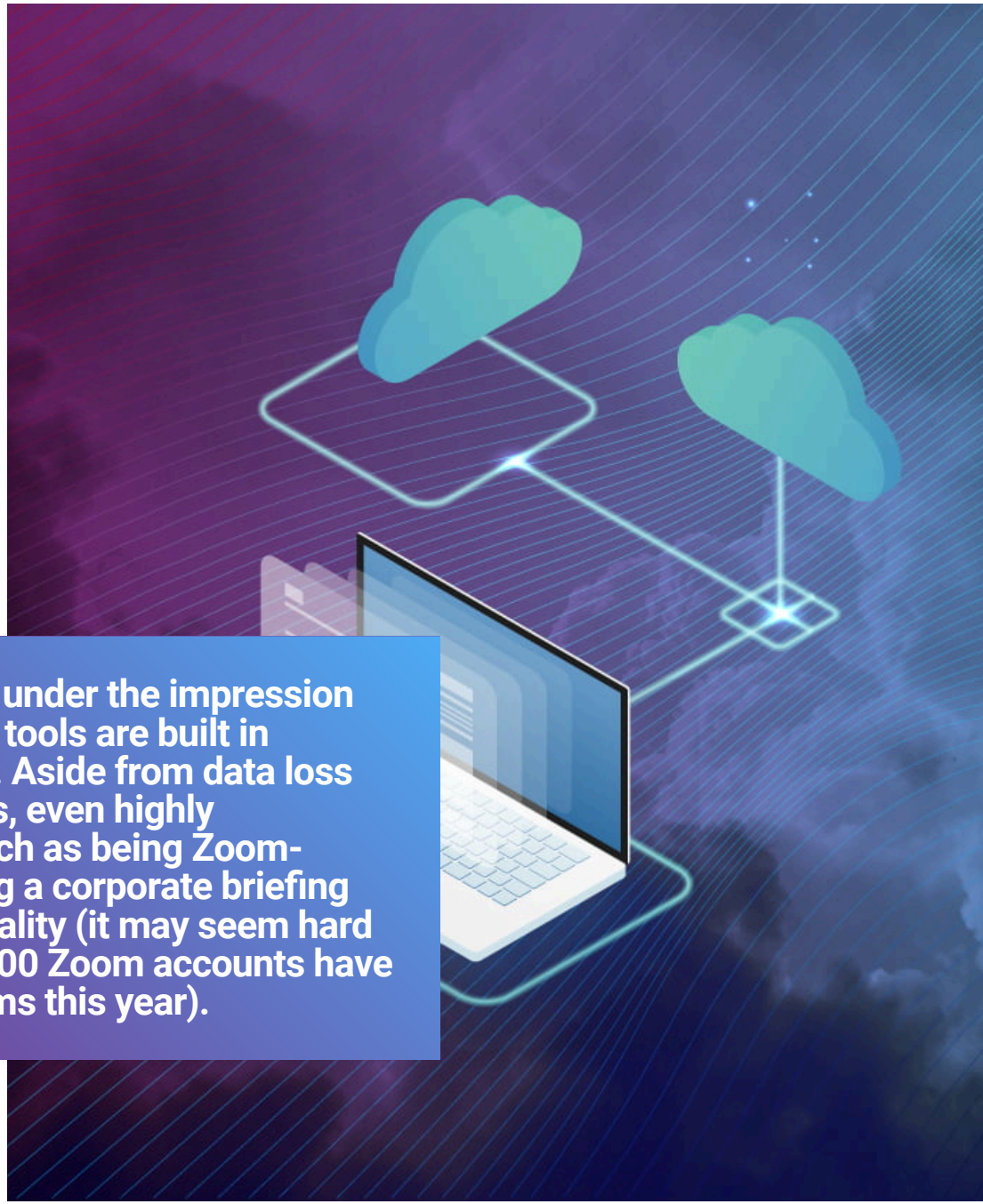
brigantia

While the COVID-19 pandemic has had a devastating impact on the economy and hit small businesses particularly hard, there are some areas where enterprise is thriving. Online retailers, video conference providers, and the millions of new subscribers to Netflix. But let's not forget another 'online winner' reaping the cash in 2020, albeit an unwelcome one with zero happy customers …ransomware.

Yes, the chaos created by COVID-19 has opened up new frontiers for threat actors especially in the SaaS landscape. IDC reports 60% of European companies are either maintaining or increasing their spending on SaaS[1], and many of your customers will have adopted collaboration tools such as Microsoft 365® and G Suite. But with the rise in traffic moving to the cloud, comes a higher level of SaaS penetration that isn't fully acknowledged.

In the not too distant past, WannaCry and NotPetya brought large and small companies to their knees (including the UK's National Health Service) and cost billions to remediate – but it's not just the next BIG ransomware attack we need to worry about.[2] Every day, businesses of all sizes are falling prey to criminal groups, particularly in 2020:

Many businesses are still under the impression that security and back-up tools are built in (spoiler alert: they're not). Aside from data loss through cloud-based apps, even highly implausible scenarios, such as being Zoom-bombed by hackers during a corporate briefing call, are now becoming reality (it may seem hard to imagine but over 500,000 Zoom accounts have been sold on hacker forums this year).



- ITProPortal reports that during the Covid-19 pandemic, more than half of businesses in the UK have suffered a phishing attack, while over a third have suffered a ransomware attack.
- Emotive Covid- themed lures are prevalent. For example, fake financial scams offering government assistance or fast-track routes for test and vaccines in exchange for payment.
- KPMG reports there is evidence that remote working increases the risk of a successful ransomware attack significantly. This is due to a combination of weaker controls on home IT, and a higher likelihood of clicking on a virus-themed email.[4]


redstor
How prepared are your customers to pay up?
brigantia

As MSPs you may have spent a large part of 2020 scrambling to help companies tighten security as they rapidly moved their operations online. And while you were strengthening company firewalls, hackers were at work too building 'drive-by-download' sites and creating credible-looking 'malvertising' ads. Even with highly-robust defences, it's almost impossible to prevent a ransomware attack today – let's face it, traditional antivirus simply doesn't cut it anymore.

So, it's a case of when a company suffers a breach, not if. In today's 'always-on' world, not having access to business data for even a few hours can cause irreparable damage to a company. It could lose business, face fines, suffer a bruised reputation, and have to manage an extremely frustrated digital workforce. As hackers continue to penetrate corporate defences while 'flying under the radar', the big questions your customers need to consider: are they prepared to pay up, and how quickly can they recover?

Gartner reports the cost of downtime is more than £4,300 per minute, and this is growing.[5] The reality is most companies put the actual figure higher than this as they struggle to quantify transactions lost to competitors and the impact on stakeholders.


redstor
Why ransomware might just be your biggest opportunity
brigantia

Why ransomware might just be your biggest opportunity

Despite reports that cyberattacks have spiked in the first half of 2020 (Covid-19 has exposed UK cyber-security vulnerabilities with more than 65,000 attacks a day)[4], many businesses are still failing to take a recovery-first approach. IT leaders may have invested in strategic cyber-security plans and on-prem infrastructure, but may not have deployed advanced backup tools that enable instant data recovery (which aside from the actual ransom pay-out is where the real pain is).

And then of course there are the companies that have dusty, untested DR plans, or worse, they have not planned for a disruptive attack at all, and simply believe "it won't happen to us."

If a ransomware attack cannot be prevented, recovering from it remains the only option. Without an isolated, up-to-date backup of data, your customer's IT systems will have no previous working state to revert to and their organisation will have no

choice but to pay up in the hope of access being restored or accept that the data is lost forever.

When disaster strikes, companies need to be up and running as quickly as possible, restoring operational data (wherever it is) to users (wherever they are) in seconds, not days. Fortunately, with cloud-based backup tools, data can be recovered in a few clicks. **And you can be the MSP that introduces this game-changing software to them.**


redstor
Cloud-based backup - the best last defence
brigantia

Specialist insurance firm Beazley reported a 25% increase in ransomware attacks in Q1 of 2020.[8] More attacks are coming, and there's no such thing as 100% effective ransomware protection. But attacks do not need to cripple your customers. You can help them avoid fallout with the best last defence – cloud-based backup.

Managing manual, time-consuming backups is a thing of the past, especially in this Covid-19 era. Your customers need software-only data management solutions and you can be in the best position to offer an air-gapped, cloud-first approach. In essence: a robust backup plan for backups. Regardless of where data is stored, you can help your customers get instant data recovery – at the same time as creating a margin-rich recurring revenue stream. Threat actors may loom large, but ransomware does not need to be the only winner this year.

Reference:

1 IDC Survey Spotlight
2 CSO Online – Is The World Ready For The Next Big Ransomware Attack
3 ITProPortal – Cyberattacks Escalated During Covid-19
4 KPMG – Rise of Ransomware During Covid-19
5 Gartner – The Cost of Downtime
6 Security Magazine – Seven Cybersecurity Predictions for 2021
7 Spice Works – Study Reveals 1 in 4 Companies Never Test DR
8 CISO Mag – Ransomware Attacks Rise Q1 2020

About Redstor

Data management for an on-demand world

About Redstor

Redstor is a cloud data management platform for the channel that enables MSPs to generate margin-rich, repeat revenue by providing their customers with 4-in-1 data management.

Trusted by more than 40,000 clients and offered by a trusted network of 350 partners, our proven, industry-leading technology helps organisations manage and protect customer data with ease.

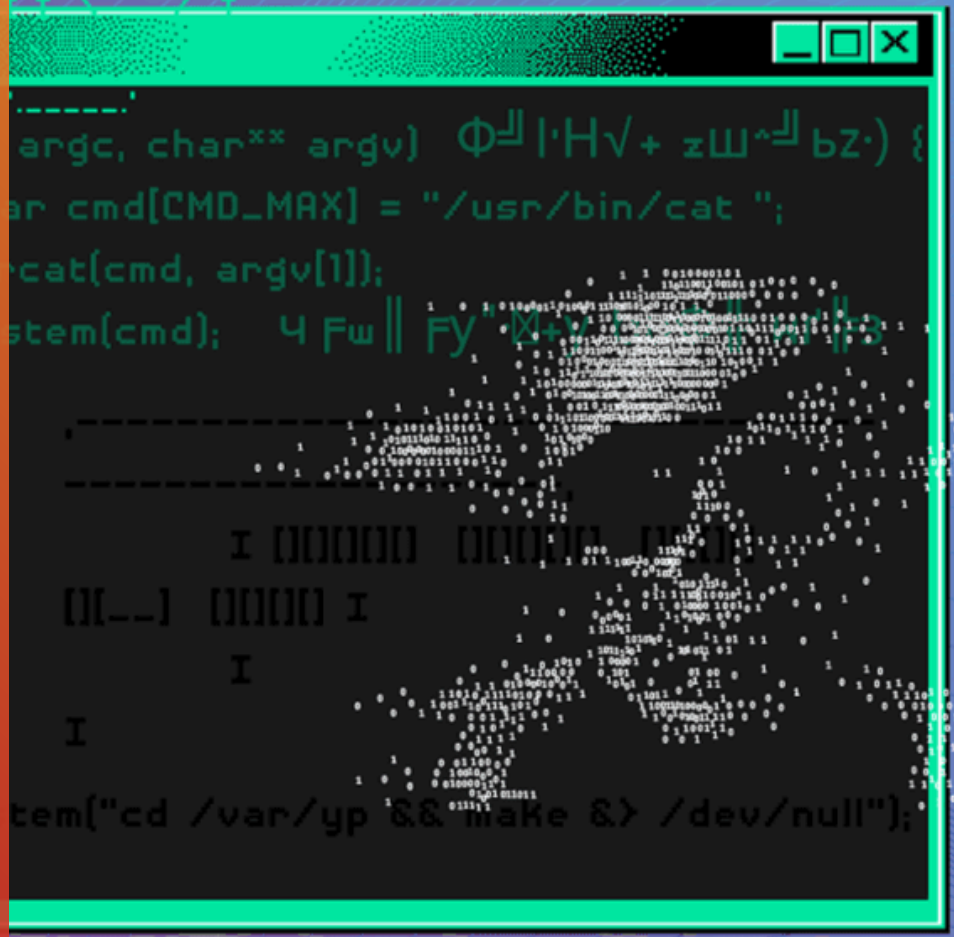
Partnering with Redstor will help you turbo-charge your business, increasing profitability with a solution that is easy to sell, maintain, scale and takes just minutes to implement.

The future of data management for MSPs. Now.

redstor

Thank you for reading why ransomware may be your biggest opportunity in 2021

Get in touch to start your trial of Redstor today



brigantia