arcserve®

eBook

HIGHLY RESILIENT OR HIGHLY EXPOSED:

Continuous availability in high-stakes industries

arcserve®

ALWAYS ON. CONTINUOUS. EVERY INDUSTRY HAS A NEED FOR CRITICAL SYSTEMS AND APPLICATIONS TO BE AVAILABLE NONSTOP.

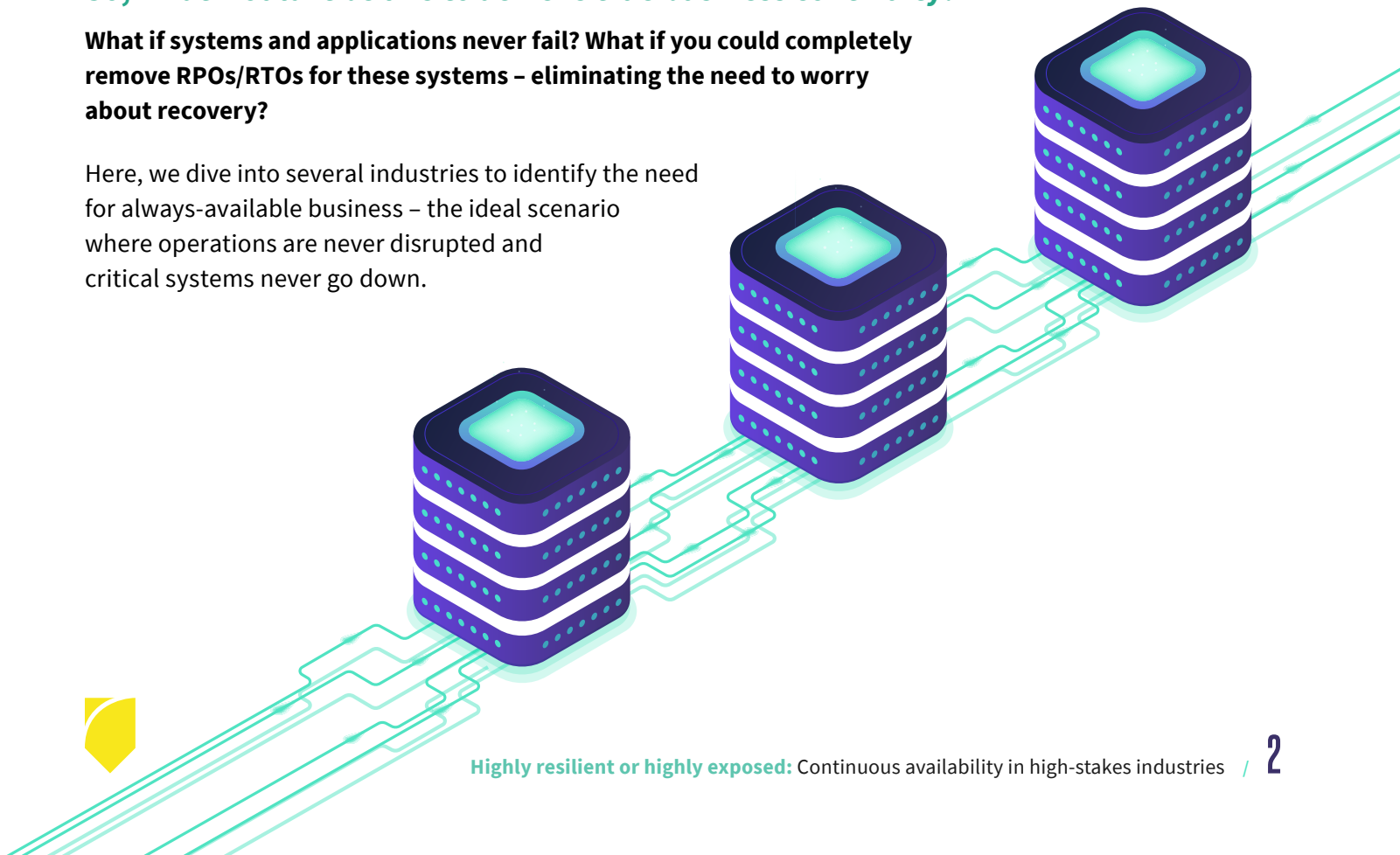
Today's companies are globalized with 24x7 operations that simply cannot go down. They have applications and systems that store proprietary IP, keep ecommerce sites and airport systems running, logistics and ERP tools working, and make financial transactions feasible. In these cases, downtime for even minutes could cause irreparable damage to revenue and productivity. Quite literally, backup and recovery is no longer good enough.

To protect these systems and applications, organizations must change their approach from backup to continuous data protection. They must move from recovery time and point objectives (RTOs/RPOs) to never needing to recover.

So, what would it be like to achieve true business continuity?

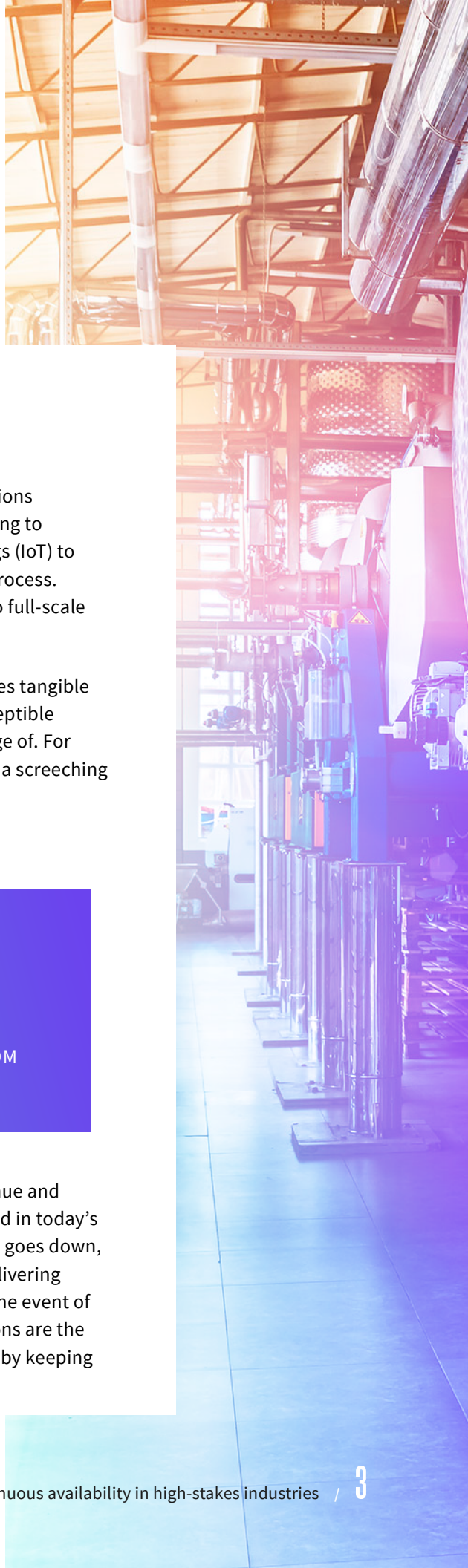
What if systems and applications never fail? What if you could completely remove RPOs/RTOs for these systems – eliminating the need to worry about recovery?

Here, we dive into several industries to identify the need for always-available business – the ideal scenario where operations are never disrupted and critical systems never go down.



arcserve®

PROTECTING IoT TECHNOLOGIES FROM CYBER-ATTACKS IN MANUFACTURING



Manufacturing organizations seldom sleep, often running production operations 24/7/365. This requires a highly responsive IT infrastructure, with many looking to improve growth and operational efficiency by adopting The Internet of Things (IoT) to automate and remotely manage more tools and systems in the production process. But as the spend on IoT accelerates and adoption shifts from pilot projects to full-scale deployment, with it comes increased risks.

In the manufacturing space, the automation of production lines via IoT creates tangible benefits such as more output at a reduced cost. But it also makes them susceptible to the downside, creating vulnerabilities for cyber criminals to take advantage of. For manufacturers, cyberattacks cripple infrastructures and bring operations to a screeching halt, causing irreparable financial and productivity loss.

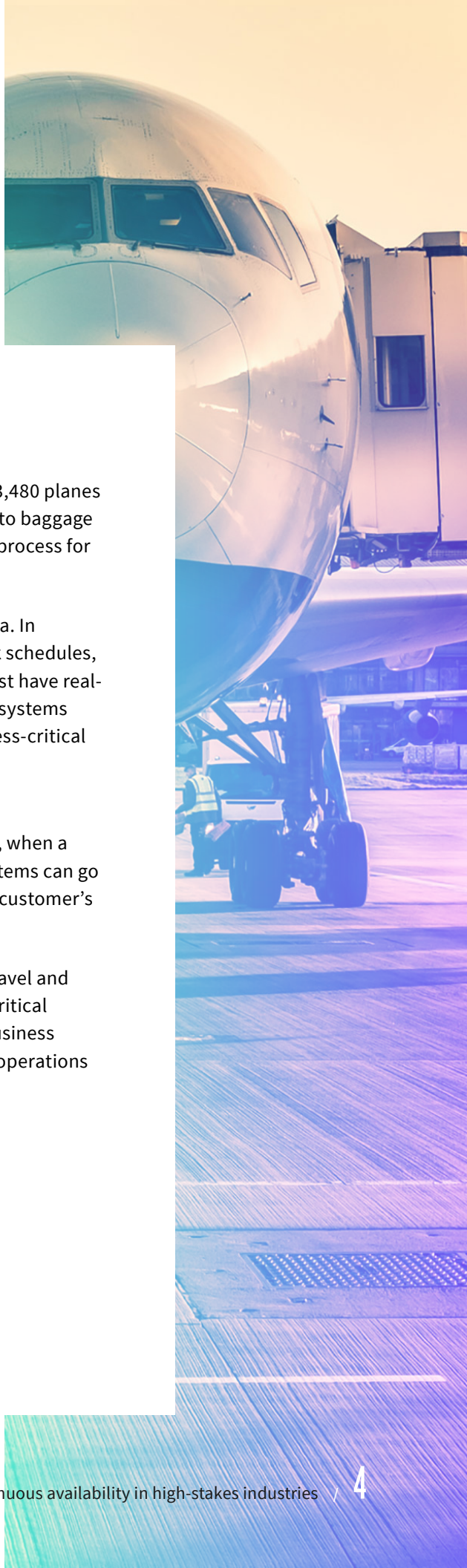
CASE IN POINT:

WHEN NORSK HYDRO, ONE OF THE WORLD'S LEADING ALUMINUM MANUFACTURERS, WAS HIT BY LOCKERGOGA RANSOMWARE, RECOVERING FROM THE ATTACK COST $41 MILLION, MOSTLY FROM LOST PRODUCTION TIME.[1] SIMPLY PUT, MANUFACTURERS CANNOT AFFORD TO HAVE ONSITE SYSTEMS DOWN DUE TO DISRUPTION FROM CYBERATTACKS, HUMAN ERROR, OR NATURAL DISASTERS.

In an industry where many businesses manufacture products nonstop, revenue and service delivery are dependent on availability of mission-critical systems. And in today's complex IT infrastructures, interconnection of discrete systems means if one goes down, it may impact all. IT executives in the manufacturing space must focus on delivering reliable operations by keeping key systems and applications operational in the event of human error or natural disaster. Local and/or remote high availability solutions are the key to preserving business operations and enabling competitive advantages by keeping mission-critical systems available nonstop.

arcserve®

MAINTAINING CONTINUOUS OPERATIONS FOR THE TRAVEL AND TRANSPORTATION INDUSTRY



Each day, more than 2.6 million travelers fly in and out of U.S. airports, with 3,480 planes taking off every hour.[2] Any glitch in any system along the way, from ticketing to baggage handling to flight operations, can cause a domino effect throwing the whole process for a loop.

Businesses in the travel and transportation industry constantly generate data. In addition to airlines tracking travelers' every move, rail companies must track schedules, freight contents, and train and track maintenance, while port authorities must have real-time insight into transport shipments, assets, and personnel. Keeping these systems running nonstop is crucial to operations and protecting customer and business-critical data are top priorities for executives in this industry.

The complexity of travel and transportation businesses brings to light other vulnerabilities in the development of business continuity plans. For example, when a natural disaster such as a hurricane strikes, schedules can be thrown off, systems can go down, and how an organization recovers from the disaster can often affect a customer's long-term perception of the company.

Keeping airplanes in flight, trains on schedule, and cargo ships afloat – the travel and transportation industry literally does not stop moving. And neither can the critical business systems that keep the industry buzzing. For these organizations, business continuity means meeting consumer expectations of availability by keeping operations running smoothly at every point of their journey.

arcserve®

CONTINUOUS DATA PROTECTION IN THE ALWAYS-TRANSACTIONAL FINANCIAL SERVICES INDUSTRY

In today's global economy, "always on" literally means always transactional, and the banking and financial services industry feels this pressure daily. Digital transformation for the financial services industry requires modernizing and automating IT infrastructures, while also ensuring the highest quality of customer experience through the constant availability of banking apps.

And as is the case in every industry, data breaches can be a devastating blow. The Equifax breach of 2017 compromised the personal data of 145 million people in the United States, exposing information ranging from birthdates to driver's license numbers to social security numbers.[3] Events like these impact revenue and reputation, leaving customers reeling as they lose trust in organizations' ability to keep their data safe.

As part of a digital transformation journey, incorporating a business continuity plan that keeps up with innovation and customer expectations will be critical for financial services organizations. With newer technologies such as cryptocurrency and artificial intelligence (AI), continuous data protection with enhanced monitoring and alerting is critical for banking and financial institutions as new avenues for hackers to attack are introduced.

arcserve®

ENHANCING APP USER EXPERIENCES WITH HIGH AVAILABILITY

In today's experience economy, it's all about the customer. And customers expect access to what they want, when they want it. Frustrations mount if they can't order their groceries for curbside pickup or share their latest selfie with just the right filter applied. And voices are louder online – social media offers the perfect venue to share any and all experiences (mostly bad), via tweets, online reviews, and Reddit posts.

The sheer amount of data in the technology sector can be mind boggling. Just consider: 6,000 tweets are sent per second,[4] 300 hours of video are uploaded to YouTube every minute,[5] and 3.5 billion Google searches are performed per day.[6] And if these apps aren't available, users are sent into a frenzy.

The backbone of customer experience is now dependent on data availability rather than solely serving up quality products. These experiences, largely driven by tech firms and their applications, can be just as valuable, if not more so, than tangible products. Ensuring your business is always on for customers is vital, and why ensuring downtime does not occur with continuous data protection is critical to any technology company's IT strategy.

arcserve®

DATA SECURITY A TOP CONCERN FOR HEALTHCARE IT PROFESSIONALS

Data is a key asset in every healthcare organization – patient information and history can determine course of care and provide important insights into a diagnosis. And, according to a survey by Health Data Management (HDM), security remains the top concern for healthcare IT professionals as they increase efforts to protect patients' health information and defend against cyberattacks. In its survey of healthcare IT executives, HDM found that a full 93% stated that protecting health information and data security was either extremely or very important.[7]

With privacy laws and compliance regulations also becoming increasingly stringent, protecting patient data isn't a nice to have – it's a must. Innovation in modern healthcare requires keeping up with technologies on the front lines for patient care as well as behind the scenes for data protection.

When it comes to ensuring continuity of operations, healthcare IT professionals depend on solutions that keep the doctor's office, emergency room, or hospital operational at all times. Because if a healthcare system or application goes down, it really can become a life or death situation.

Patients are the number one priority of healthcare professionals, making it unacceptable to cease care when a natural or manmade disaster strikes. With high availability technology, healthcare organizations can be confident that they will be "always on" to provide patient services when needed.

arcserve®

ACHIEVE TRUE BUSINESS CONTINUITY WITH CONTINUOUS AVAILABILITY SOLUTIONS

No matter the industry, every single company has systems and applications that must remain operational. To protect them, IT teams often rely on technology designed to minimize downtime and data loss when an outage inevitably occurs.

Arcserve Continuous Availability technology does just that – it ensures business continuity with proven technologies that have one common purpose: to keep your business up and running, and operational. Powered by asynchronous replication technology, Arcserve Continuous Availability is the only solution that delivers high availability, combined with heartbeat-powered automatic failover, and continuous data protection for applications and systems on-premises, remote, and in the cloud. Achieve true system and application availability:

Replicate data in real-time and move from recovery time and point objectives (RTOs and RPOs) to continuous protection.

Deliver automatic failover, triggered by heartbeat technology to eliminate the time from detection to mitigation.

Journal-based technology replicates byte-level changes at the file, application and full system levels so you can rollback to any point in time and restore as it was pre-failure.

Support physical and virtual servers, and cloud environments with encryption and non-disruptive testing to increase your TCO.

When downtime happens, every moment counts. Achieve constant uptime for peace of mind with **Arcserve Continuous Availability.**

References

1. How to neutralize the impact of ransomware, **https://www.manufacturing.net/article/2019/05/how-neutralize-impact-ransomware**
2. Air traffic by the numbers, **https://www.faa.gov/air_traffic/by_the_numbers/**
3. Top Bank Tech Trends for 2018, **https://www.americanbanker.com/slideshow/top-bank-tech-trends-for-2018**
4. Internet Live Stats, **https://www.internetlivestats.com/twitter-statistics/**
5. YouTube by the Numbers: Stats, Demographics & Fun Facts, **https://www.omnicoreagency.com/youtube-statistics/**
6. Internet Live Stats, **https://www.internetlivestats.com/google-search-statistics/**
7. Providers and Progress: Baby Steps for Healthcare's Top Challenges, Health Data Management, accessed 5/13/2019.

Explore more at **www.arcserve.com**