



# Becoming Unstoppable Against Ransomware:

How real life heroes are  
harnessing the power of  
Zero Trust Data Security



At Rubrik, we deliver data security and operational resilience for enterprises. As our customers deliver and transact digitally more than ever, the threat of attacks has exponentially risen, often leaving businesses scrambling to minimize downtime, revenue loss, and reputational damage.

This book is from our customers, for our customers. These stories come in all shapes and sizes from around the world - from a bridal shop, colleges, manufacturers, and more on how they walked away unscathed from ransomware. It is designed to give you a glimpse of how you too can become unstoppable. These are their stories.





8,000 students  
unaffected by crippling  
security breach



Attack thwarted and  
bridal dresses continued  
to fly off the shelves



Jobs unthreatened,  
manufacturing continued  
after ransomware



Disaster recovery  
plan evolved to  
prevent mayhem



College recovered  
so fast they never  
received a ransom



# 8,000 students unaffected by crippling security breach

The first sign of the ransomware attack that hit Colchester Institute was on a Monday morning in April 2021. After the Easter weekend, Ben Williams, IT Services Manager, came into the office and assumed business as usual. When trying to login to his systems, however, he discovered that all admin accounts had been disabled. His nightmare was confirmed when the IT Services team found a ransom note on one of their physical servers.





**“Rubrik safeguarded our backups. Due to its native immutability, 100% of our backups were protected against corruption and deletion.”**

---

**Ben Williams**, IT Services Manager, Colchester Institute

## Rubrik and KHIPU partner together to save the day

“Sophisticated and malicious, the breach destroyed mission critical areas of our infrastructure by deleting email and other servers, domain controllers, and anti-virus consoles as well as encrypting our entire virtual environment, and its underlying platform,” recalled Williams.

Breach protection with instant recovery should be a top priority for any organization’s cyber security strategy. By implementing Rubrik Zero Trust Data Security, in partnership with KHIPU Networks, Colchester recovered instantly with no data loss. The institute returned to the most recent clean copy with just one click. “This could’ve been a crippling incident, but I am proud to say Rubrik

saved the day, fully protecting our critical data systems including finance, student records, and admissions data,” Williams stated.

The institute was able to analyze the impact of the attack, determining exactly what files were affected and where, and detect any anomalies within their environment. “Thanks to Rubrik, we were able to keep the lights on and continue to deliver a robust service to our students and staff.”

## Colchester invites educational institutions to purchase Rubrik

“With ransomware on the rise and the prevalence of attacks in education, we simply could not have recovered as fast or as well without Rubrik. We urge other educational establishments to re-evaluate their DR plan,” said Williams.



# Results



Zero data lost



\$0 paid in ransom



100% recovery from ransomware within 10 days

**“Long term Veeam customers, we implemented a full review of solutions. Rubrik was the top choice due to its overall protection and recovery from cyber breaches. Moving away from Veeam and purchasing Rubrik was the best decision we have made.”**



[READ FULL CASE STUDY >](#)

INDUSTRY: RETAIL LOCATION: MILTON KEYNES, UNITED KINGDOM

# Attack thwarted and bridal dresses continued to fly off the shelves

It was 11 PM on a Friday in November 2019. WED2B IT Systems Administrator Jamie Jeeves started receiving a barrage of email alerts warning that antivirus (AV) clients were crashing in the company's central office. All prospects for a relaxing weekend vanished.

WED2B operates as a retailer of wedding gowns, dresses, and accessories for brides and bridesmaids. With nearly 60 stores across the UK, Ireland, Belgium, and the Netherlands, WED2B was fearful the attack would ruin arguably the 'most important day' for countless brides.

"A mass encryption of data was underway - this is when I knew we were in trouble. We had just been hit with ransomware," said Jeeves.

All WED2B website files, including text, videos, and high-res images, were being encrypted. 5 terabytes of critical NAS data had been initially encrypted, including the backups from a 3rd party system that used Azure to store backups."



WED2B





**“I used to treat recovery with a laissez-faire attitude. The ransomware situation completely changed that. I cannot recommend the Rubrik platform enough.”**

---

Todd Cassidy, Founder and Managing Director, WED2B

# Responding and recovering within 24 hours

In the retail business, time is money and downtime can be paralyzing. “We generate the bulk of our weekly sales on weekends. Needless to say, time was of the essence. I immediately disconnected the network from all store locations so they could continue operating independently without impact,” said Jeeves.

## “I knew I had to act fast.”

“Leveraging Rubrik Zero Trust Data Security to recover, I focused on our most critical assets first. I restored Active Directory in less than 30 minutes. I then moved onto SQL databases, which took only an hour to recover 1 TB+ of data. I was pleasantly shocked at how quickly everything came back,” said Jeeves. By early Saturday afternoon, all critical systems were back online.

“There were essentially two recoveries taking place: one for data managed by Rubrik and one for Azure backups. While our data on Rubrik was back up and running within 24 hours, it took weeks upon weeks to get NAS back up and running since it was not protected by Rubrik. One of them was painless, and the other one was not,” Jeeves stated.



# Results



## \$0 paid in ransom

"It never even occurred to me to pay the ransom demand because I was that confident in Rubrik's ransomware recovery capabilities."



## Zero data lost and 100% recovery from ransomware within 24 hours

"If we didn't have Rubrik, we would have lost a lot of critical data and would have no way of getting it back. I've always had confidence in Rubrik's immutability."



## No impact to the business

"There was zero impact to the business because we were able to recover so quickly. There was no disruption to the WED2B website, and our bridal stores didn't even realize there was an issue."

[WATCH CUSTOMER TESTIMONIAL >](#)



**INDUSTRY:** MANUFACTURING **LOCATION:** QUEENSLAND, AUSTRALIA

# Jobs unthreatened, manufacturing continued after ransomware

Matthew Day, CIO of Langs, was excited for a long-anticipated holiday after 14 months of COVID-19 lockdown. His wife was thrilled. All of his friends, ecstatic. But the day took an unexpected turn. Instead of waking up to leave for his getaway, he woke up to every CIO's worst nightmare - the dreaded phone call, "We're being attacked."

Upon arrival at his office, he tried to bring up the system. Nothing. Instead, what came up was a ransom note, 'You've been hacked'.

The hacker's attack vector was a legitimate looking email that came from a proper email address, from the right account, in the right format. The one slight detail that was off was the link within the email. The link that Day's accounting team typically uses to send purchase orders did not go to them. Two weeks later, the hackers had access to Langs' systems.





**“Rubrik is not just about recovering from ransomware. Rubrik is the difference between survival and non-survival in this new digital age.”**

---

*Matthew Day, CIO, Langs Building Supplies*

## Rubrik was our saving grace

Leveraging Rubrik's ransomware remediation service, Day noticed hundreds of thousands of files were deleted and modified. "With Rubrik, we were able to analyze the impact, quickly identify what data was encrypted, and where it resided in our environment. We did not have to pay the \$15M ransom. We lost zero data. We were fully recovered, up and running in less than 24 hours, which is fantastic."

## The war is won, people's jobs are safe

There is an extreme amount of pressure facing CIOs, especially when there is no production happening in a factory that employs thousands of people. Day remarked, "When I have to send those people home, I feel personally obligated. Not only do the implications of a ransomware attack hit home for me, it also implies revenue loss, production delays, and brand damage."

After Day overcame his roller coaster of emotions, he suddenly had this "rah-rah" feeling of knowing his team could handle this. "Rubrik was ticking away recovering all our data and I had this blinding flash of the obvious. We've been fighting battles all day but we're at this point where I can happily declare 'the war is won'. I knew that people's jobs were safe."

**"You think you've been successful in attacking us but here's the counter punch. With Rubrik, we've got a very good right hook and we're going to come back harder. At the end of the day, this attack is just going to be an inconvenience."**

---

**Matthew Day**  
CIO, Langs Building Supplies

# Results



## \$0 paid in ransom

"The hackers originally demanded \$15M in Bitcoin. Then, they went down to \$1.5M. Either way, we did not have to pay the ransom because Rubrik just works."



## Zero data lost

"Rubrik just did what Rubrik does. That's the beauty of the product."



## 100% ransomware recovery within 24 hours

"My director pulled me aside and said, "Wow, I don't want to think about what the world would look like if we didn't have Rubrik. If we didn't do manufacturing for a month, that would be a serious detriment to our business – one we might not be able to recover from."

[WATCH CUSTOMER TESTIMONIAL >](#)



INDUSTRY: WHOLESALE TRADE LOCATION: WASHINGTON, UNITED STATES

# Disaster recovery plan evolved to prevent mayhem

Plymouth, Inc. believed it had done everything right to prevent cyberattacks by implementing controls such as endpoint protection, email security, firewalls, and monthly patching. But there was a critical gap — the organization lacked a complete recovery plan. This became painfully clear when a ransomware attack sent the IT team scrambling to restore affected systems.

“From this nightmarish experience, it was very clear that we weren’t ready,” said Rama Arumugam, IT Manager for Plymouth. The company had been working on a business continuity plan, but it was not complete. “We were flying blind and had to rely on our email communications and handwritten notes during this outage.”

“This is where Rubrik stepped in. Thanks to Rubrik’s native immutability, we kept damage to a minimum and recovered over 50 servers within 48 hours.”



## Ryuk on the rise

At the onset of the attack, Rama suspected a network malfunction. "It appeared to be an internal DNS issue," Rama said. "On further investigation, we realized our network was affected by ransomware." The ransomware variant Ryuk snuck in through a temporary admin account and started attacking Windows domain join machines, which connect remotely to the network. "They all had to be shut down immediately and rebuilt from scratch," Rama said.

## Rubrik saved us time and cut down our RTO

Plymouth does more than sell products, they offer services to make their customers' lives easier. Whether their consumers need a variety of products frozen, moved, or stored, Plymouth supports them.

Despite the recovery plan's shortcomings, Plymouth was able to recover from the attack quickly because the IT team reacted promptly. "We run 24/7 so we were immediately notified and we got on it right away," Rama stated. "We went to our Rubrik appliance and started the process to restore."

"Rubrik's Instant Recovery feature, which leverages snapshots to execute a Live Mount and avoid data loss, was essential." He continued, "Rubrik saved us invaluable time and cut down our RTO significantly."

Fortunately, with assistance from Rubrik's support team, Plymouth found ways around the obstacles and developed a full recovery plan within 12 hours of the attack. "We recovered unscathed but the primary lesson learned is to have a robust business continuity plan and to recognize that it's never complete. It should be treated like a living document that needs to be constantly updated."





**“The reality is, no business is immune from ransomware. It’s more important than ever to proactively prepare and ensure you have the right solutions in place to quickly recover after a cyber attack, while minimizing the chance of re-infection. Rubrik continues to make critical advancements to their ransomware recovery solutions to give customers the ultimate peace of mind.”**

---

Rama Arumugam, IT Manager, Plymouth, Inc.

# Results



## \$0 paid in ransom

“The attacker never actually had a chance to demand ransom because we acted so quickly.”



## Best-in-class support

“The tech support was exceptional throughout the entire process. I was working around the clock for days and the Rubrik team was there every step of the way.”



## 100% recovery within 48 hours

“Minimizing downtime was critical to continue to provide products to our consumers, so we moved forward the best we knew how. Rubrik’s ability to instantly recover data and applications in sandbox environments enabled us to get our users online within 48 hours.”



## Rubrik’s Ransomware Recovery Warranty

“The Rubrik Ransomware Recovery Warranty offers us a new level of protection and sense of stability that goes beyond traditional means of data security found in the industry.”

[READ FULL CASE STUDY >](#)

**INDUSTRY:** EDUCATION **LOCATION:** LOUISIANA, UNITED STATES

# College recovered so fast they never received a ransom

Nick Pitre, Director of IT at South Louisiana Community College (SLCC) had a funny feeling something was brewing. The Ryuk ransomware variant had been making its rounds at colleges and universities, so he knew it would not be long before SLCC was also targeted.

Sadly, he was right. The infiltration occurred by way of an administrator loading new software onto a forgotten Windows 7 desktop collecting dust in a closet. Without proper security measures, the admin's credentials were captured, and the ransomware immediately activated and began, spreading to a handful of servers.

But when the attack hit, Pitre was ready — so ready that the hackers never even had the opportunity to deliver a ransom demand. As soon as the ransomware started encrypting files, Pitre's team quickly responded by recovering data from backups stored in Rubrik and preventing any damage from taking place.

**SLCC**<sup>TM</sup>  
SOUTH LOUISIANA COMMUNITY COLLEGE





## Preparedness pays off

The reason SLCC was able to avert disaster came down to preparedness. The school received a suggestion from the State of Louisiana to turn off backups because previous attacks had compromised backups, but Pitre overruled, “We’re not doing that. I trust Rubrik’s immutability.” Turns out it was the right move. Rubrik thwarted the ransomware from doing any damage at all.

**“Each recovery took five to 10 minutes. In a few hours, the situation was 100% contained.”**

Where the ransomware was able to infiltrate the network’s defenses, Rubrik’s Live Mount point-in-time recovery helped identify the risk of reinfection if wrong snapshots were used for recovery.

## Rubrik recovered SLCC in two hours

This breach could have led to loss of learning coursework, financial and student records. “Recovery could have taken weeks, which is exactly what happened to another college in Louisiana. With Rubrik, there was no data loss. This breach was simply an inconvenience for the two hours that we were rebooting backups.”

**“Rubrik saved us big time.”**

**“Since the ransomware incident, we have doubled down on Rubrik, purchasing a second set in another data center to ensure every server we are backing up is being backed up in two locations.”**

---

**Nick Pitre**, Director of IT, South Louisiana Community College



# Results



## Zero data lost

"We walked away unscathed, with zero data lost thanks to Rubrik's immutable backups. That was a big factor — not having to worry about our backups getting taken over."



## \$0 paid in ransom

"From the time we realized there had been an incident, it took just two hours to bring all affected VMs back up and running. We caught it so early on that the hackers never even had a chance to deliver a ransom note."

[READ FULL CASE STUDY >](#)



## Nightmare averted

"Ransomware never reached our Active Directory (AD). If the attackers had gotten on our AD, it would have been a nightmare."



## Ease of use

"The initial reason I liked Rubrik so much was the ease of use. I never even felt the need to call Rubrik support during the attack because we had the recovery under control, which speaks to its simplicity."



Rubrik is a cybersecurity company. We are the pioneer in Zero Trust Data Security™. Companies around the world rely on Rubrik for business resilience against cyber attacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine intelligence, enables our customers to secure data across their enterprise, cloud, and SaaS applications. We automatically protect data from cyber attacks, continuously monitor data risks, and quickly recover data and applications.

