rubrik

City of Lodi Switches to Rubrik to Bolster Its Disaster Recovery Following Ransomware Attack with Previous Backup Solution

INDUSTRY:

Local Government

IMPACT OF RANSOMWARE ATTACK PRIOR TO RUBRIK

- CAD dispatch services down for 4 days
- 4 weeks to restore over 100 virtual machines
- 1 week data loss of ERP database

CHALLENGES WITH PREVIOUS SOLUTION

- Windows-based backups vulnerable to encryption
- Complex file-level backup and restores requiring to rebuild VMs from scratch
- Backup failures with ERP vendor

SOLUTION WITH RUBRIK

- Immutable backups to ensure backups cannot be corrupted
- Simple and faster VM-level restores
- Reliable policy-based backups

PARTNER

ePlus

Located in San Joaquin County, California, the City of Lodi is home to over 60,000 citizens. It was founded in August 1869 when the Central Pacific Railroad chose the site for a station on its new route. Lodi is best known for its cultivation of grapes and production of wine. The land of old-vine Zinfandel, there are many vineyards in Lodi with century-old grapevines.

The city's IT department is responsible for managing all data and infrastructure services for its numerous municipal departments, including fire, police, and utilities. "As a local government, we house an enormous amount of sensitive data and personally identifiable information (PII). It is critical that we protect and secure all of our citizens and employees' data as well as ensure the underlying infrastructure is up and running 24/7. Our city's departments, including public safety, law enforcement, financial services, rely on our IT systems to conduct day-to-day operations. If our systems go down, these departments would be unable to deliver critical services to our citizens for days," said Benjamin Buecher, IT Manager for City of Lodi.

PREVIOUS RANSOMWARE ATTACK DISRUPTED CRITICAL MUNICIPAL SERVICES

In 2018 and 2019, a series of ransomware attacks hit the city of Lodi. Hackers used malicious software to target Lodi's phones and financial services, crippling the city's ability to access swaths of its data. In 2019, extortionists demanded 75 bitcoins, approximately $400,000 at the time of attack. The city followed guidance from a specialized cyber security team, and following the attack, a team of security and legal experts conducted a series of forensic audits. No public information was compromised as a result of the ransomware attack.

"A few years back, we were hit by three attacks in three months by the same ransomware. The attack significantly impacted our municipal services. Our objective was to prioritize the recovery process to get critical services back up as soon as possible. However, after the second attack, our CAD dispatch service went down. It took our CAD vendor at the time four days to get us 100% back up and running," said Buecher.

4 WEEKS TO RECOVER AND LARGE DATA LOSS DUE TO PRIOR BACKUP SOLUTION

"The recovery process with our previous backup solution was extremely slow and tedious. We first had to physically run to the data center and unplug our backup unit. It took us weeks to isolate and mitigate the infection. From the time we were hit to the time we were 95% recovered, it was about a month to completely restore over 100

virtual machines. On top of that, the entire recovery process was extremely manual. Due to the way our previous backup solution was implemented, we were forced to restore one virtual machine at a time and required all hands on deck," said Buecher.

Another challenge was the complexity of restores. "With our previous solution, our only option was to perform file-level backups. As a result, during the attack, we had to rebuild the data on the machines from scratch instead of simply restoring the machines. That process of rebuilding all the virtual machines was the most time-consuming aspect," said. Matthew Casson, Network Administrator at City of Lodi.

Lastly, their previous approach failed to notify them of backup failures, resulting in one week of data loss for their ERP database. "The second ransomware attack took down our entire ERP. When we came in that morning, we realized the ERP wasn't responding, and we couldn't get into it. When we went to reboot that instance, the whole instance became encrypted. As a result, we didn't get a chance to pull the data off that database," said Buecher. "Our ERP vendor at the time was supposed to take nightly backups for disaster recovery. However, when we reached out to them following the ransomware attack, we learnt our backup system had failed, and the latest copy was seven days old. It was frustrating that no one had told us and to discover the unnecessary data loss."

SWITCHING TO RUBRIK FOR STRONGER SECURITY AND RANSOMWARE REMEDIATION

Following the ransomware attack, the City of Lodi implemented sweeping security measures, including reevaluating their backup solution. Their partner ePlus was pivotal in helping them discover and procure a modern and secure backup solution.

"The first issue with our previous backup system was that it ran on a traditional Windows operating system, making it vulnerable to infection. If extortionists had accessed our backups with our prior solution, we could have lost everything," said Buecher. "As we began evaluating new backup vendors, we needed something that wasn't vulnerable to ransomware. The second aspect was faster and easier ransomware recovery. With our previous solution, we were incredibly frustrated with how complex restores were. Additionally, we wanted to move away from file-level snapshots, so we could restore entire virtual machines at scale," said Casson.

"We chose Rubrik for providing a new, simpler approach to backup and disaster recovery," said Casson. Additional benefits include:

- **Native immutability**: "Rubrik isn't built on a traditional Windows OS and cannot be encrypted."
- **Faster restores at VM level**: "As a small shop, we need to be able to perform fast restores at any time."
- **Significant cost savings**: "Another major advantage was the cost savings since we can do a refresh without a forklift upgrade."
- **Management simplicity**: "Another reason we love Rubrik is the simplicity. We don't have the luxury to dedicate a full time employee to any specific thing. With Rubrik, anyone can jump in and learn how to use the solution easily without training, and we don't need someone dedicated to managing backups,"
- **Cloud integration**: "In the future, we hope to leverage Rubrik to further our disaster recovery journey to the cloud."

rubrik

Global HQ
1001 Page Mill Rd., Building 2
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

20201016_v1