

# ASL Airlines France Builds Multi-level Ransomware Defense Strategy with Rubrik Cloud Data Management and Radar



## INDUSTRY

Transportation

## RESULTS

- 25% IT admin time savings in everyday monitoring
- 15 to 100+ hours of recovery time saved in the event of a ransomware attack
- Automated recovery with no downtime
- Millions of euros in potential savings in case of an attack

## THE CHALLENGE

- 40+ hours spent each month manually monitoring environment for cyber threats
- Painful, manual recovery in the event of a ransomware attack
- Downtime presents severe threat to business-critical applications
- Millions of euros at stake in the event of an attack

## THE SOLUTION

- AI-driven anomaly detection for rapid discovery of cyber attacks
- Granular analysis of attack surface to quickly diagnose threat impact
- Simplified recovery process to minimize business disruption and data loss
- One-click recovery without a ransom

ASL Airlines France (ASL) is a cargo and passenger airline based in Tremblay-en-France at Bâtiment Le Séquoia. Their main base is Charles de Gaulle airport, Europe's second busiest air traffic hub. A majority of ASL's fleet operates on the behalf of delivery services throughout the night, including Amazon, FedEx, DHL, UPS, and La Poste. In 2017 alone, ASL carried 712,000 passengers and 38,600 tons of cargo.

Fabrice De Biasio, Chief Information Officer at ASL Airlines, oversees the operational infrastructure of 3,000 employees and is responsible for ensuring always-on data availability and meeting strict security standards. In 2018, with the threat of cyber attacks on the rise, ASL partnered with Rubrik to proactively address the threat of ransomware with Radar.

## FOR ENTERPRISES TODAY, RANSOMWARE ATTACKS ARE A MATTER OF "WHEN," NOT "IF"

Ransomware attacks are intensifying in scale and sophistication. A recent NTT Security survey revealed that ransomware attacks rose 350 percent in 2017 over the previous year.<sup>1</sup> Nearly 75% of companies infected with ransomware suffer two days or more without access to their files while 33% go five days or longer.<sup>2</sup> Global damage costs from ransomware attacks are predicted to reach \$11.5 billion annually by 2019.<sup>3</sup> The NotPetya ransomware attack on TNT Express in 2017 cost FedEx \$300M and took the IT team more than a month to recover to its normal operational state.<sup>4</sup>

ASL is required to maintain 99.9% availability — a maximum of 60 minutes of allowed outage per year. If ASL's IT system is down for more than 15 minutes, airplanes cannot take off, customers cannot receive their cargo, and the airline is at risk of being hit with massive fines. "In our business, you cannot have downtime," said De Biasio. "Ransomware can quickly cripple an airline and prevent its ability to fly, period."

## ASL MINIMIZES THE THREAT OF DOWNTIME WITH RADAR'S AI-DRIVEN ANOMALY DETECTION

ASL's previous solution was not built for a strong defense against the rapidly growing threat of ransomware. "The cargo airline industry is a common target for ransomware, and we experience a minimum of one attack per month," said De Biasio. "In the past, we managed to recover by using a multitude of scripts to identify and erase infected files manually. This was an incredibly painful, time-consuming experience that killed our team's productivity for days."

By enabling fast recoveries and providing detailed impact assessments, Radar enables enterprises to significantly minimize downtime, cost of recovery, and reputational damage following an attack.

