rubrik

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

ASL AIRLINES

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"

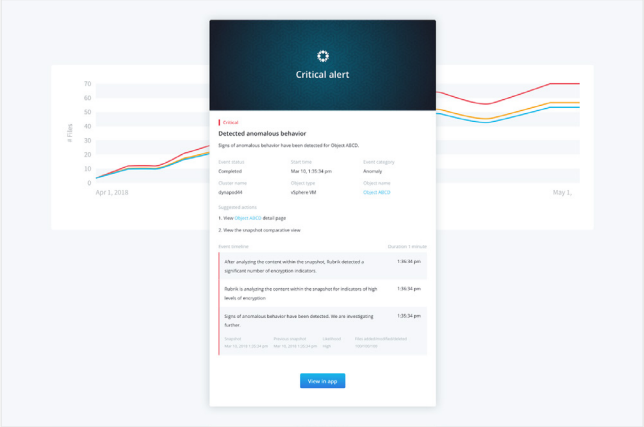
Ransomware attacks are intensifying in scale and sophistication. A recent NTT Security survey revealed that ransomware attacks rose 350 percent in 2017 over the previous year.[1] Nearly 75% of companies infected with ransomware suffer two days or more without access to their files while 33% go five days or longer.[2] Global damage costs from ransomware attacks are predicted to reach $11.5 billion annually by 2019.[3] 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.[4]

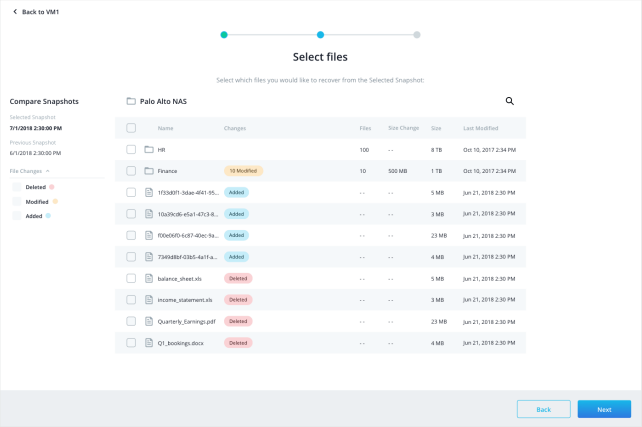
ASL is required to maintain 99.9% availability — a maximum of 60 minutes of allowed outage per year. If ASL's IT system is down for more than 15 minutes, airplanes cannot take off, customers cannot receive their cargo, and the airline is at risk of being hit with massive fines. "In our business, you 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.





Prior to Rubrik, the threat of ransomware was keeping De Biasio up at night. Now, with Radar's multi-level defense, DeBiasio has peace-of-mind and realized the following benefits:

Operational Savings

- **15 to 100+ hours of IT admin time saved in case of an attack:** "We experience a minimum of 1 ransomware attack per month. Before Radar, the team spent 15 hours to recover from a minor ransomware attack. If we had been hit with a major attack, I fear recovery could've taken weeks."
- **25% IT admin time savings (40+ hours saved per month):** "Our team used to spend up to 2 hours per day monitoring our applications for ransomware. Now, we only need to spend a few minutes per day checking Radar, so our team can spend more time on initiatives that deliver value back to the business."
- **Automatic recovery and no downtime:** "Before Radar, we managed to recover from attacks with several scripts and by identifying and erasing bad files manually. That was an incredibly painful experience. Our IT Admin loves Radar because it does all that work automatically. Radar discovered a bad file, alerted him, and he just ticked a few boxes to restore to a clean state."

Business Impact

- **Global visibility and instant threat response:** "With Radar we can follow server activity in real time and react fast. If something is not normal, we know about it."
- **Ability to protect our business against catastrophic risk with cyber insurance:** "Because the cargo airline industry is a common target for ransomware attacks, it's incredibly difficult for airlines to get cyber insurance. If we did not have Radar, we would not have been approved for a cyber insurance contract."
- **Millions of euros in potential savings in case of an attack:** "Radar will help us protect our bottom line and potentially save us millions of euros in case of an attack."

RADAR GIVES ENTERPRISES A HOLISTIC RANSOMWARE RESPONSE STRATEGY TO ENSURE BUSINESS CONTINUITY

With Radar's machine learning-powered anomaly detection and accelerated recovery, ASL's team is now confident in their ability to quickly restore to the pre-infected state in the event of a threat. "Rubrik's native immutability coupled with the AI-driven alerting and detection of Radar are the most critical data protection and business continuity tools in my arsenal against today's intensifying cyber threats," said De Biasio.

Footnotes:

[1] Source: NTT Security. "NTT Security 2018 Global Intelligence Report." May 2018.
[2] Source: Barkly. "Must-Know ransomware Statistics 2017." June 2017.
[3] Source: Cybersecurity Ventures. "Global ransomware Damage Costs Predicted To Hit $11.5 Billion By 2019." November 2017.
[4] Source: ZDNet. "NotPetya cyber attack on TNT Express cost FedEx $300m." September 2017.

rubrik

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

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

Rubrik delivers a single platform to manage and protect data in the cloud, at the edge, and on-premises. Enterprises choose Rubrik's Cloud Data Management software to simplify backup and recovery, accelerate cloud adoption, and enable automation at scale. Rubrik's run-anywhere, scale-out architecture is built to empower IT departments today and in the future, reducing total cost of ownership while enabling infrastructure flexibility for a multi-cloud world. For more information, visit www.rubrik.com and follow @rubrikInc on Twitter.

20190204_v2