Case Study

Turbonomic, an IBM company, improves business continuity for its SaaS applications with cyber-resilient recoveries.

Turbonomic can now ensure its SaaS applications always have a safe recovery option for its customer environments.

Building cyber-resilient recovery into SaaS applications

Trust is essential to IBM's customers, and they expect services like Turbonomic to be highly available and secure.

Building in SOC2 controls was a fundamental part of the process, because they were vital for ensuring application security and availability. The data security controls would serve to protect the software stack against cyberattack. The availability controls needed to include the ability to capture and back up all cloud resources dynamically, while identifying and mitigating threats and predicting capacity requirements in real time.

Turbonomic needed to automate the enforcement and reporting of these controls and have continuous monitoring of its recovery risk posture. Moreover, they had to ensure that vulnerabilities were not reintroduced back into the production environment during a recovery operation.

The container-based application uses AWS EKS and multiple persistent volumes to host the data, each of which is backed up using AWS's high-performance block storage service Elastic Block Store (EBS). The application uses MySQL as its database platform, which is hosted in the container.

> *"As the application scales, Elastio automatically detects the new persistent volumes, inspects them for threats, and creates a recovery point. This ensures we always have a safe recovery option for our customer environments."*

Greg Aligiannis, Chief Information Security Officer

Ensuring business continuity attestation with proactive protection

The Turbonomic team is also responsible for managing ParkMyCloud, a cloud platform that helps IT teams manage, govern, and optimize spend across multi-cloud environments. It leverages a scale-out architecture based on AWS EC2, EBS volumes, and RDS MySQL.

Before the team deploys an application, it is first scanned for threats. Once it is in production, Elastio continually monitors, protects, and inspects the applications and data for detonated or undetonated ransomware and other forms of malware. It continuously evaluates the health of file systems as well to proactively guard against these threats. Elastio's agentless component provides seamless protection for scale-out compute applications like PMC to ensure that every instance and volume is continuously protected, scanned for threats, and retained for cyber-resilient recoveries.

> *"My SOC2 compliance is easy with Elastio, they automate most of my security and availability controls in one platform and without agents."*

Greg Aligiannis, Chief Information Security Officer

Elastio takes a much more comprehensive approach to mitigating the risk of ransomware and other threats than standard recovery snapshots. The service generates real-time recovery risk assessments for SaaS applications like Turbonomic and ParkMyCloud to ensure compliance with SOC2 security and availability demands. It also defends their applications against threats like ransomware by continuously monitoring all dependent compute and storage resources for potentially malicious activity and securing them with immutable recovery points.

“Elastio reduces our RTO from 12 hours to minutes. With no new configurations or development, we get improved availability with app-consistent recovery points. We can’t get that with standard snapshots.”

Greg Aligiannis, Chief Information Security Officer

Elastio also helps protect Turbonomic from zero-day attacks by ensuring that vulnerabilities cannot be reintroduced following a recovery operation. In doing so, it proactively mitigates the risks facing business continuity operations, such as downtime and data loss, while providing robust remediation and forensics for security teams.