



Forbes Global 100 automaker boosts data security and cyber resilience

Challenge

Car companies are seeing their data stores skyrocket, fueled by connected cars that generate an estimated 28 GB an hour and legal requirements to retain supplier parts schematics for 10+ years. This global automaker manages over 100 PB of data, which is expected to increase three folds in the next few years. In 2024, as part of an overall IT transformation initiative, the company sought a backup solution for modern workloads such as cloud, artificial intelligence (AI), Kubernetes, and databases. Key requirements were data security and cyber resilience to recover from ransomware attacks, which can halt revenue (e.g. production and logistics) and compromise safety (e.g. vehicle self-diagnostics).

Executive summary



Products:
DataProtect



Region:
EMEA



Use Case:
Backup & Recovery,
Disaster Recovery



Industry:
Manufacturing



Environments:
NAS, Oracle SQL, VMware

Why Cohesity

The automaker selected Cohesity as part of an enterprise IT transformation contract with IBM. Cohesity bested three other leading solutions because of its **fast restores, ease of scaling, and data security capabilities such as immutable backups and DataLock**—a setting that prevents backups from being altered or deleted until a set date. The automaker is deploying Cohesity in its over 100 global data centers and edge facilities (parts depots, logistics centers, etc.). The company plans to start storing a virtual air-gap backup in Cohesity FortKnox, an isolated cloud vault for added protection.

Business value

Stronger security posture

Cohesity's immutable backups, DataLock, and multifactor authentication give company leaders confidence that clean data can be restored after an attack. To help prevent insider threats, the company requires two people to approve changes to backups, the Quorum capability.

Cyber resilience

The company can more quickly recover from attacks or system failures because restores from Cohesity snapshots are fully hydrated and don't require waiting for incremental backups to be stitched together for recovery. In the event of a security incident, the company's cybersecurity team can conduct forensics using the Cohesity clean room solution to help understand when and where the attack began.

Efficient search

If a business team needs to retrieve a specific VM or file—say, a 10-year-old schematic to research a quality issue—an administrator can search for it by name and then restore it from the same interface.

Enabler for cloud transformation

As the automaker continues migrating applications and data to the cloud, the IT team can take advantage of the same Cohesity AI-powered data security and management platform they use for on-prem workloads—multiplying the value of the investment.

Benefits

Simplified operations
for on-premises and cloud backups

Stronger
data security

Increased
cyber resilience

Learn more at www.cohesity.com

© 2025 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and © is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.