SPONSORED CONTENT | WHITE PAPER

DIGITAL TRANS-FORMATION

Beyond backup: Achieving comprehensive data protection in the distributed multicloud age

CIO

Today's evolving IT environments present unprecedented complexity that demands new data protection and resilience approaches. The typical enterprise data landscape now encompasses hundreds of applications running on-premises, in the cloud, and on various mobile and embedded devices. IT teams are now tasked with managing a collection of data silos in multiple clouds. Data protection strategies encompass off-site backups, long-term archives, second-tier storage, test and development systems, and analytics pools. Governance is frustrated by teams' having little or no visibility into the location and status of data.

To complicate things further, making and storing multiple copies of the same data in cloud environments is standard practice. Many IT teams also use multiple point products acquired over time to manage their public-cloud-based secondary storage and data, adding further administrative overhead and complexity to an already overburdened staff.

Despite this complexity, legacy data protection technology built for a time when all of an organization's data assets were concentrated in one or a few known locations is still common. These solutions are dangerously inadequate for a modern distributed data landscape.

Disaggregated point tools create a disjointed view of backup data that hampers threat response and increases recovery times. Siloed legacy products typically lack native immutability support to lock down backup data and prevent tampering. Backup silos also increase security risks, by expanding the attack surface. Restore capabilities are often limited and slow, resulting in extended downtime and risking data loss.

Legacy architectures are not designed to recover thousands of virtual machines. They lack the distributed architecture needed to scale.

Many organizations also don't pay sufficient attention to recovery, a reactive and time-consuming process that involves forensic analysis in addition to data cleansing and restoration. Long recovery times can be as damaging to business operations as downtime.

Growing threats

Meanwhile, bad actors aren't standing still. Ransomware is a growing threat that is becoming more malicious and damaging. The "2024 Thales Data Threat Report"[1] discovered that

ransomware attacks are increasing in frequency but response planning at most organizations is poor.

Attackers are becoming increasingly sophisticated. They lie dormant inside compromised systems, waiting for the right time to strike. Many attacks also encrypt backup data, making recovery all but impossible.

Assailant motivations have also evolved. They have moved beyond threatening production environments to exfiltrating or stealing sensitive data.

New avenues of response

A modern data protection solution is based on a single software-defined platform powering multiple data management use cases, including backup, disaster recovery, business continuity, real-time forensics, and file and object services. It is anchored in a comprehensive cyber-resilience fabric that classifies data for appropriate protection and recoverability, identifies and closes vulnerabilities, and extracts the maximum value from an organization's existing cybersecurity tools.

The platform incorporates anomaly detection, disaster recovery orchestration, data security posture management, data mobility, integration with existing security operations center (SOC) tools, and massively distributed recovery. A single console provides visibility into the location and status of data across the organization. Machine learning is applied to detect anomalies and threats such as ransomware in near real time.

A 3-2-1 backup strategy (three copies of production data, with two backups on different media types and one off-site) is the minimum that organizations need for defending against today's attacks. A robust protection platform also continually creates immutable backup snapshots that can be restored instantly. The most critical data is kept in air-gapped vaults disconnected from the corporate network. Encryption; multifactor authentication; role-based access controls; and "four eyes" change management, which requires changes to be authorized by at least two trusted administrators, provide additional layers of protection.

Multiple virtual machines (VMs) can be restored in parallel. Robust data protection capabilities enable security administrators to locate infected files and conduct forensics in near real time. Recovery is protected against vulnerabilities' being injected during the process.

A modern solution can instantly recover hundreds of files, objects, and virtual machines at scale across an organization's data landscape. Recovery-time objectives (RTOs) are reduced from days to minutes. Ransomware attacks have no impact, since data can be recovered in a clean state at any location and point in time.

Resilience and beyond

Cyber-resilience is a crucial element of a modern data protection strategy. It goes beyond backup and recovery to prepare a business to anticipate, withstand, and recover from cyberthreats without suffering extensive downtime or compromise of sensitive information. By prioritizing cyber-resilience, organizations can maintain essential functions even during a cyber incident. This capability protects against economic losses and safeguards the trust and confidence of customers and partners.

A cyber-resilience strategy is a plan that encompasses incident response, disaster recovery, and continuous adaptation to new threats. It evaluates all potential vulnerability points, assesses risk thresholds, and creates a coordinated and automated incident response plan. Ongoing threat detection, vulnerability management, cyber awareness training, and disciplined patch management practices keep the plan up to date and in compliance with the growing number of regulatory requirements for data protection and privacy.

Visionary data protection providers are going beyond business resilience to explore new uses for backup data. Analytics and machine learning can be conducted on backup data without time-consuming extracts or disruptions of operational workloads.

Operations teams can analyze backup data to improve data classification standards, strengthen capacity planning, and identify opportunities to improve efficiency.

Backup data can help SOC staff better detect anomalies; improve threat intelligence; and detect hidden vulnerabilities such as backdoors, Trojan horses, and dormant malware.

Artificial intelligence (AI) presents a compelling new value proposition for backup data. Generative AI platforms index secondary data and enable users to gain insights from data, using a conversational interface without having to master complex query languages. Retrieval-augmented generation, which embellishes large

language models with knowledge beyond training data, delivers context-rich responses to questions without violating privacy or disclosing confidential information.

Time for change

Data protection in the distributed hybrid multicloud age presents complexities legacy solutions weren't designed to address. Implementing a modern solution starts with a comprehensive assessment to identify the organization's data protection requirements, creating a solution that fits its unique needs and devising a streamlined implementation approach. The organization can then implement fully integrated backup, recovery, and protection tools for point-in-time recovery and rich forensic analysis in a sandbox or a clean room environment.

Built-in natural-language query capabilities further increase security insights and the analytical value of backed-up data, making comprehensive data protection a sound strategy and a catalyst for improved organizational knowledge.

At a time when cyberattacks are rising and organizations are focusing on becoming more cyberresilient, Cohesity has joined forces with LTIMindtree to help organizations modernize their backup infrastructure and protect their data from cyberthreats.

LTIMindtree's expertise in backup modernization helps organizations transform from legacy backup to cyberresilient solutions that safeguard backup data from threats. The company's wealth of knowledge repositories and a team of certified Cohesity experts can implement solutions well within prescribed timelines. LTIMindtree brings continuous innovation, automation, best practices, and a strong partnership with Cohesity.

Learn more how Cohesity and LTIMindtree can help enhance your cyber-resilience.

1 "2024 Thales Data Threat Report," www.thalesgroup.com