COHESITY

WHITE PAPER

Beyond recovery: A CISO's guide to using backup data to strengthen cyber resilience

TABLE OF CONTENTS

Executive summary 3

1. Enhanced threat hunting 4

2. Real data compliance 5

3. Comprehensive incident response and recovery 6

- Ransomware, wiper attack, and malicious insider detection 6
- Ransomware response 6
- Ransomware mitigation 6
- Testing and drills 7
- Detailed monitoring and reporting 7

4. Data integrity and compliance 8

- Regulatory compliance 8
- Secure data storage and access control 8
- Disaster recovery and business continuity planning 9

5. Improved visibility and control 10

- Centralized management 10
- Comprehensive reporting and analytics 11

6. Strategic insights and decision-making 12

- Optimized resource allocation 12
- Strategic business insights 12

Conclusion 13

Executive summary

As cyberattacks grow more frequent and disruptive, Chief Information Security Officers (CISOs) must pivot from a prevention-only mindset to a broader focus on cyber resilience. This means ensuring the organization can withstand attacks by being able to respond swiftly, recover securely, and prevent recurrence of similar attacks in the future.

This white paper challenges traditional perceptions of advanced backup systems, positioning them as critical components of a cybersecurity risk management strategy. It explores how modern, secure backups can serve as more than just recovery tools—becoming valuable assets for threat hunting, early adversary disruption, and accelerated incident response. Especially in scenarios where primary security defenses are evaded or isolated, backups can provide the critical visibility and control needed to maintain operational integrity. By tapping into the wealth of historical information contained in backup systems, organizations can gain deeper insights into potential threats, speed incident response and secure recovery, and build a more resilient cybersecurity practice.

1. Enhanced threat hunting

Threat hunting is a proactive cybersecurity practice that involves actively searching for evidence of hidden threats within an organization's network to stop adversaries as early as possible in the attack sequence. Traditional threat hunting methods often rely on endpoint agents and system logs.

Nearly all Ransomware-as-a-Service (RaaS) platforms now include a common evasion technique: Bring Your Own Vulnerable Device Driver (BYOVD). In this approach, the adversary deploys a signed device driver that exists below the operating system level, effectively rendering the endpoint security solution and logging blind to attacks. This is where backup data becomes an invaluable asset for threat hunting.

Key advantages of using backup data for threat hunting include:

- **Passive threat hunts**: Because backup copies are isolated from the primary environment, they can't be tampered with or evaded by adversaries—especially ransomware gangs that embed evasion techniques into their ransomware-as-a-service (RaaS) platform to bypass common security controls like endpoint detection and response (EDR) and extended detection and response (XDR). This isolation allows for effective and stealthy threat hunting.
- **Historical context**: Backup data allows analysts to review system states and data changes over time, helping to identify subtle, long-term patterns of malicious activity.
- **Comprehensive coverage**: Backups often contain data from across the entire organization, providing a holistic view that may reveal connections between seemingly unrelated events.
- **Offline analysis**: Threat hunters can analyze backup data offline, reducing the risk of alerting active attackers to detection efforts.
- **Recovery of deleted or altered data**: Backups can reveal evidence that may have been deleted or modified on live systems, which is crucial for uncovering sophisticated attacks.

2. Real data compliance

As floodgates open for security assisted by artificial intelligence (AI), tools for data security posture management (DSPM) are working with backup systems for a powerful, one-two punch. DSPM tools go a step beyond scanning IT systems, networks, and data stores for sensitive information such as health or financial data. They also show where that data is, how often it has been accessed, and by whom. Together with advanced backup systems, compliance leaders can dramatically reduce the risk of sensitive data exposure.

Here are some advantages of integrating your DSPM solution with an advanced backup system:

- **Rapid identification of systems that are not backed up**. DSPM solutions automatically discover and classify data assets across diverse environments, including shadow data and forgotten databases. Some of this data is likely already covered with existing backup policies. But it's also likely that significant volumes of sensitive data aren't covered. When paired with advanced backup systems through API integration, security teams can easily examine gaps in backup coverage and then take steps to have these data sources added to your organization's backup policies. The end result: improved security resilience and lower risk.
- **Optimized frequency of backups and retentions based on the criticality of data within datastores backed up by Cohesity.**
- **Prioritized restoration of data based on business criticality of data.**
- **"Just in time" analysis of data-related incident evidence, which streamlines the incident response process (and therefore improves incident response times)**. Backed-up copies of data are a rich environment for DSPM activity to illuminate and protect formerly "dark" data.
- **Improved compliance with regulatory requirements such as GDPR and SEC 8-K that mandate timely notification of regulators or impacted data subjects.**

3. Comprehensive incident response and recovery

A robust incident response and recovery strategy is crucial for minimizing the impact of security incidents on an organization. Let's now take an in-depth look at how using backup data strengthens incident response and ensures a secure recovery.

Ransomware, wiper attack, and malicious insider detection

Unusual data patterns and user activity in backup and recovery operations can provide early warning signs of a potential attack. These anomalies can trigger alerts that accelerate triage and investigation efforts, helping teams respond more quickly.

Ransomware response

Incident responders can use immutable backup data as a resource with a strong chain-of-custody, so incident responders can perform file system forensics, uncover artifacts, and identify malicious changes to configurations and other files caused by ransomware and wiper attacks. Using an advanced backup system, this analysis can be performed across a series of snapshots retained over time, offering deeper insight into the attack timeline.

Responders can also passively hunt for IOCs within backup copies in a secure and isolated environment, without interference from, or tipping off, adversaries who may still be active in the network. Additionally, backup data can reveal historical vulnerabilities that were exploited during the attack, providing valuable context for reducing the attack surface to prevent reattacks. With vulnerability exploitation now the leading method ransomware operators use for initial access—and with exploits being baked into Ransomware-as-a-Service (RaaS) platforms within days—failing to patch vulnerabilities before restoring systems leaves you exposed not only to reattacks by the original attacker, but also to thousands of other affiliates using the RaaS platform.

Immutable backups are copies of data that can't be altered or deleted. This immutability ensures that backup data remains untouched and recoverable even if the primary data is compromised by ransomware.

Ransomware mitigation

Ransomware attacks are a growing threat to organizations of all sizes. When such an attack occurs, having secure and reliable backups can be the difference between a minor disruption and a catastrophic event. While this may seem obvious, the sheer number of organizations not taking advantage of basic security measures makes it important to revisit. These measures include:

- **Immutable backups and system hardening**: Immutable backup snapshots combined with Write Once, Read-Many (WORM), and Zero Trust-based principles such as least privilege access, multifactor authentication, data encryption, and separation of duties prevent your backup data from becoming a target.

- **Air-gapped backups**: Air-gapped backups are physically isolated from the network, providing an additional layer of security. So even if the network is breached, the backups remain safe from ransomware attacks.
- **Regular backup schedules**: Implementing regular backup schedules ensures that data is consistently updated and protected. The more frequent the backups, the less data loss the organization will experience in the event of an attack.
- **Clone systems** for full-bore penetration testing without risk to production.
- **Realistic end-to-end drills**: Move beyond desktop exercises to full-scale drills that allow the end-to-end testing and continual improvement of people, process, and technology. By cloning production systems and taking the whole team through scenarios involving encryption or destruction, you ensure every aspect of response and recovery is tested. This means the first time your organization faces a real-world destructive cyberattack won't be the first time your teams have handled one.

Testing and drills

Regular testing and drills are essential to ensure that the backup and recovery process is effective and that all stakeholders are familiar with their roles during an incident.

- **Disaster recovery drills**: Conducting regular disaster recovery drills simulates real-world scenarios, helping the team practice and refine their response procedures. These drills help identify potential weaknesses and areas for improvement.
- **Automated testing**: Automated testing of backup data can verify the integrity and recoverability of backups without manual intervention. This automation helps ensure that backups are reliable and can be restored quickly when needed.
- **Documentation and playbooks**: Maintaining detailed documentation and recovery playbooks helps ensure that everyone knows their responsibilities and the steps to take during an incident. These playbooks should be regularly updated based on the results of testing and drills.

Detailed monitoring and reporting

Effective incident response and recovery require detailed monitoring and reporting to confirm that backup operations are running smoothly and that any issues are promptly addressed.

- **Real-time monitoring**: Real-time monitoring of backup processes ensures that any failures or issues are immediately detected and resolved, preventing potential data loss.
- **Automated alerts**: Automated alerts notify the IT team of any irregularities or failures in the backup process, allowing for quick intervention and correction.
- **Comprehensive reporting**: Detailed reports on backup status, success rates, and recovery times provide insights into the effectiveness of the backup strategy and highlight areas for improvement. By implementing these advanced backup strategies, CISOs can make sure their organizations are well-prepared to respond to and recover from incidents swiftly and effectively. This comprehensive approach not only minimizes downtime and data loss but also strengthens the organization's overall resilience against future threats.

4. Data integrity and compliance

Maintaining data integrity and compliance with regulatory requirements is a critical concern for any organization, especially in cybersecurity. Backup data plays a crucial role in addressing such concerns by providing a reliable, verifiable source of truth that can be used to audit, verify, and restore data integrity. Here's an in-depth look at how backup data can lead to greater data integrity and compliance.

Regulatory compliance

Organizations operate under numerous regulatory frameworks that mandate stringent data protection and integrity requirements. Backup data helps achieve and demonstrate compliance with these regulations by providing an audit trail and encouraging data retention.

- **Audit trails:** Backup solutions can maintain comprehensive logs of all backup and restoration activities. These logs are invaluable during compliance audits, as they provide detailed records of who accessed the data, when it was accessed, and what actions were taken.
- **Data retention policies:** Compliance with regulations such as GDPR, HIPAA, and SOX often requires adhering to strict data retention policies. Automated backup solutions can enforce these policies by ensuring that data is retained for the required duration and securely deleted when it's no longer needed.

Secure data storage and access control

Protecting backup data from unauthorized access and storing it securely are fundamental aspects of data integrity and compliance.

- **Encryption**: Encrypting backup data both at rest and in transit keeps it secure from unauthorized access. Strong encryption protocols protect sensitive information, making it unreadable to anyone without the appropriate decryption keys.
- **Role-based access control (RBAC)**: Implementing RBAC helps ensure that only authorized personnel have access to backup data. This control limits exposure and reduces the risk of data breaches or misuse.
- **Multifactor authentication (MFA)**: Enforcing MFA for accessing backup systems adds an additional layer of security, so even if credentials are compromised, unauthorized access is prevented.

Disaster recovery and business continuity planning

Effective disaster recovery and business continuity planning are essential components of a comprehensive compliance strategy. With backup data, organizations can quickly recover from disruptions and continue operations with minimal impact.

- **Business impact analysis (BIA)**: Conducting a BIA helps organizations understand the potential impact of data loss or corruption on their operations. Backup data plays a crucial role in this analysis by providing a reliable means of restoring critical systems and data.
- **Recovery time objectives (RTO) and recovery point objectives (RPO)**: With clear RTO and RPO goals, organizations can recover data within acceptable timeframes and with minimal data loss. Backup solutions must be designed to meet these objectives.
- **Continuity planning**: Backup data is integral to continuity planning so organizations can maintain operations during and after a disaster. Regular testing of disaster recovery plans using backup data leads to more effective and reliable recovery processes.

Data integrity and compliance are critical to maintaining trust and operational reliability in today's complex regulatory environment. By effectively leveraging backup data, organizations can meet regulatory requirements, protect the integrity of their data, and maintain robust security measures. Implementing advanced backup solutions that provide comprehensive audit trails, enforce data retention policies, and offer secure storage and access controls enables organizations to achieve these goals, providing peace of mind and a solid foundation for continued growth and resilience.

5. Improved visibility and control

For a Chief Information Security Officer (CISO), achieving improved visibility and control over an organization's data and backup processes is essential for maintaining robust security and efficient data management. By using advanced backup solutions, CISOs can gain comprehensive insights into their data environment, streamline management processes, and better protect critical information. Here's an in-depth look at how effective use of backup data improves both visibility and control.

Centralized management

A centralized management approach consolidates backup operations, providing a single point of oversight for all backup activities across the organization. This centralization simplifies the management process and ensures consistency in data protection practices.

- **Unified dashboard**: A unified dashboard offers a holistic view of the entire backup environment, including the status of backup jobs, storage usage, and potential issues. This real-time visibility enables CISOs to monitor backup health and performance effectively.
- **Simplified administration**: Centralized management tools reduce the complexity of managing multiple backup systems and locations. Simplified administration leads to more efficient operations and reduces the risk of misconfigurations or errors.
- **Policy enforcement**: Centralized control allows for consistent enforcement of data protection policies across the organization. Policies related to data retention, encryption, and access controls can be uniformly applied, improving compliance and security.

Comprehensive reporting and analytics

Detailed reporting and analytics provide valuable insights into backup operations, helping CISOs make informed decisions and optimize data protection strategies.

- **Audit logs**: Detailed audit logs track all access and activity related to backup data. These logs provide a clear record of who accessed the data, what actions were taken, and when they occurred, aiding in both security monitoring and compliance audits.
- **Customizable reports**: Customizable reporting tools allow CISOs to generate reports tailored to specific needs, such as compliance requirements, operational performance, or security audits. These reports provide a clear and comprehensive view of backup activities.
- **Trend analysis**: Analyzing trends in backup data, such as data growth patterns, storage utilization, and recovery times, helps identify long-term trends and potential areas of concern. This analysis supports strategic planning and resource allocation.
- **Data insights**: Advanced analytics tools can provide deeper insights into backup data, such as identifying which systems or departments generate the most data, which data is most critical, and potential vulnerabilities. These insights enable more targeted and effective data protection measures.

By adopting advanced backup solutions that offer centralized management, enhanced access control, real-time monitoring, comprehensive reporting, and automation, CISOs can ensure that their organizations' data is protected, compliant, and readily available for recovery. These capabilities not only strengthen the overall security posture but also provide the insights and control needed to optimize data protection strategies and support the organization's long-term success.

6. Strategic insights and decision-making

In the realm of cybersecurity, strategic decision-making is essential for effectively managing resources, anticipating future challenges, and maintaining a robust security posture. Backup data, often underutilized, can provide valuable insights that drive informed decision-making and bolster an organization's overall security strategy. In previous sections, we've discussed areas where historical context allows for trend analysis to seek out threats or gain insight into baseline behavior for data use. This section expands on the theme of how backup data can help us gain strategic insights into the business's health.

Optimized resource allocation

Efficient resource allocation is crucial for maximizing the effectiveness of security investments. Backup data provides detailed insights into which systems and data are most critical, so organizations can prioritize their security efforts and allocate resources where they're needed most.

- **Critical data identification**: Backup data helps identify which data and systems are essential to business operations. By understanding the criticality of different data sets, organizations can prioritize their protection and recovery efforts.
- **Cost management**: Analyzing backup data storage and usage patterns can reveal opportunities for cost savings. Organizations can optimize their storage solutions, eliminate redundant data, and reduce overall storage costs while still protecting data.
- **Resource prioritization**: Backup data insights enable organizations to focus their resources on the most vulnerable or high-value areas. This targeted approach means the most critical assets receive the highest level of protection.

Strategic business insights

Beyond security and compliance, backup data can also provide strategic business insights that support broader organizational goals.

- **Operational efficiency**: Analyzing backup data can reveal inefficiencies in data management and operational processes. Organizations can use these insights to streamline operations, reduce redundancies, and improve overall efficiency.
- **Data utilization**: Understanding how data is used across the organization helps identify opportunities for better data utilization and management. Insights from backup data can inform decisions about data archiving, lifecycle management, and access policies.
- **Innovation and growth**: Backup data can uncover trends and patterns that support innovation and business growth. By analyzing how data evolves over time, organizations can identify new opportunities, optimize processes, and drive strategic initiatives.

Leveraging backup data for strategic insights and decision-making enhances an organization's ability to manage resources effectively, anticipate and respond to threats, and maintain regulatory compliance. By integrating backup data into the broader operational strategies, CISOs can drive continuous improvement, optimize resource allocation, and support the organization's long-term success. Advanced backup solutions that offer robust analytics, reporting, and automation capabilities help organizations unlock the full potential of their data, transforming it into a valuable asset for strategic planning and decision-making.

Conclusion

CISOs everywhere face the daunting challenge of safeguarding their organizations' data against sophisticated threats while also complying with stringent regulations. Best-in-class backup solutions do far more than support disaster recovery—they reduce risks for compliance and security. Now, they are a must-have to quality for cyber insurance.

Advanced backup systems are an essential component of "defense in depth" and indeed, the last line of defense during a cyber incident. Moving large volumes of sensitive data, efficiently and securely, into cost-effective storage whether cloud or on-premises; and proving a Recovery Time Objective, reduces the risk of data loss, operational downtime, and business reputation. By optimizing and making use of this technology, CISOs can bolster resilience, agility, and long-term business value in an increasingly complex digital world.

Learn more at 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 (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

2000053-002-EN 4-2025