Unifying Data Resiliency with IBM Storage Defender

Data Resilience and compliance: Set policies and standards to ensure resilience compliance across the data estate

Early Threat Detection: AI-driven insights for real-time ransomware and anomaly alerts.

Safe and Fast Recovery: Instant mass restore and immutable copies to minimize downtime.

In the era of digital transformation, enterprise data is not only growing exponentially but is also becoming more distributed and complex. For many organizations, this shift has led to significant challenges, especially when data protection, resilience, and recovery are managed in isolated silos. Without a unified approach, IT teams struggle to maintain visibility across data environments, enforce consistent policies, and ensure rapid, reliable recovery when disruptions occur. This fragmented structure leaves organizations more vulnerable to cyber threats, compliance risks, and operational setbacks due to slow or incomplete recovery.

IBM Storage Defender is purpose-built to dismantle these silos, offering a comprehensive, end-to-end solution that brings together data resilience, threat detection, and swift recovery across the entire data landscape. With its integrated platform, IBM Storage Defender ensures that businesses can protect their mission-critical data, recover quickly from any disruption, and monitor regulatory needs—all from a single, streamlined solution.

The Challenges of Siloed Data in Modern Enterprises

Siloed data management has become one of the most significant obstacles to effective data resilience. In many organizations, separate teams manage storage, backup, and security independently, often with limited visibility into each other's processes. This fragmented structure poses several critical issues:

Disjointed Policies and SLAs: When each team operates in isolation, policies and Service Level Agreements (SLAs) are often misaligned, causing confusion and delay during incident response. Without a shared, unified understanding of resilience policies, critical recovery processes can fall short of business needs.

Inconsistent Recovery Standards: Siloed operations lead to inconsistencies in recovery plans, especially between primary and secondary storage and distributed systems, for both on-premises and cloud environments. These gaps can result in prolonged downtime and data loss during crises, as well as a lack of confidence in recovery readiness.

Vulnerability to Cyber Threats: Advanced threats like ransomware target the weakest points in an organization's data infrastructure. With siloed data systems, threats are harder to detect, and the risk of malicious actors exploiting fragmented security measures is greater. Without a coordinated defense strategy, recovery from these attacks can be delayed and less effective.

Compliance Gaps: Regulatory standards such as DORA and SEC impose strict requirements on data protection, reporting, and auditability. In siloed environments, achieving a comprehensive view of compliance is difficult, making it challenging for organizations to consistently meet regulatory requirements and avoid costly fines or brand damage.

IBM Storage Defender

IBM Storage Defender provides end to end data resilience that addresses these challenges:

1. Data Resilience & Compliance:

As organizations scale, they often encounter fragmented, siloed data management practices that hinder visibility and complicate recovery. IBM Storage Defender provides **a single, unified console** that consolidates policy management, threat responses, and recovery processes across an organization's entire data infrastructure. This centralized platform aligns data protection policies with business goals by allowing **tailored policies based on specific Service Level Agreements (SLAs)** and recovery objectives. Moreover, it monitors defined compliance objectives by generating detailed **reports that highlight compliance status**, identify gaps, and recommend actionable steps, easing the burden of regulatory requirements and reducing the risk of costly fines or reputational damage.

2. Early Threat Detection:

With the rise of ransomware and other sophisticated cyber threats, traditional, reactive security measures are no longer sufficient. IBM Storage Defender uses a **multi-layered approach to detect threats**, deploying sensors across hardware, applications, file systems, and backups. These sensors, from IBM and third-party sources, provide high-fidelity threat detection that minimizes false positives. **Leveraging AI-powered anomaly detection**, IBM Storage Defender identifies unusual patterns in data activity that may signal a ransomware attack or other malicious behaviors. This system offers near real-time detection directly at the storage array level, allowing teams to respond quickly to emerging threats. Furthermore, IBM Storage Defender **integrates with existing Security Operations Centers (SOCs),** including SIEM and SOAR systems, facilitating a coordinated response that streamlines both threat detection and recovery processes.

90%[1]

Faster Recovery: Instant Mass Restore enables rapid recovery, minimizing downtime after disruptions.

3. Safe and Fast Recovery:

Ensuring minimal downtime during data recovery is critical for business continuity, especially in high-stakes situations where data access is essential. IBM Storage Defender provides **recovery from the safest data copies**, whether they reside in backups, hardware snapshots, cloud, or even physical tapes, ensuring that data remains immutable and protected against encryption or deletion by malicious actors. The solution also includes **isolated recovery testing**, allowing organizations to validate the integrity and safety of backups in a secure, isolated environment before performing full-scale recovery. Its **Instant Mass Restore feature** enables the rapid recovery of large data volumes, significantly reducing downtime. This capability is a game-changer for enterprises, enabling them to restore massive amounts of data swiftly, preserving operational continuity and reducing the financial and reputational costs of prolonged outages.

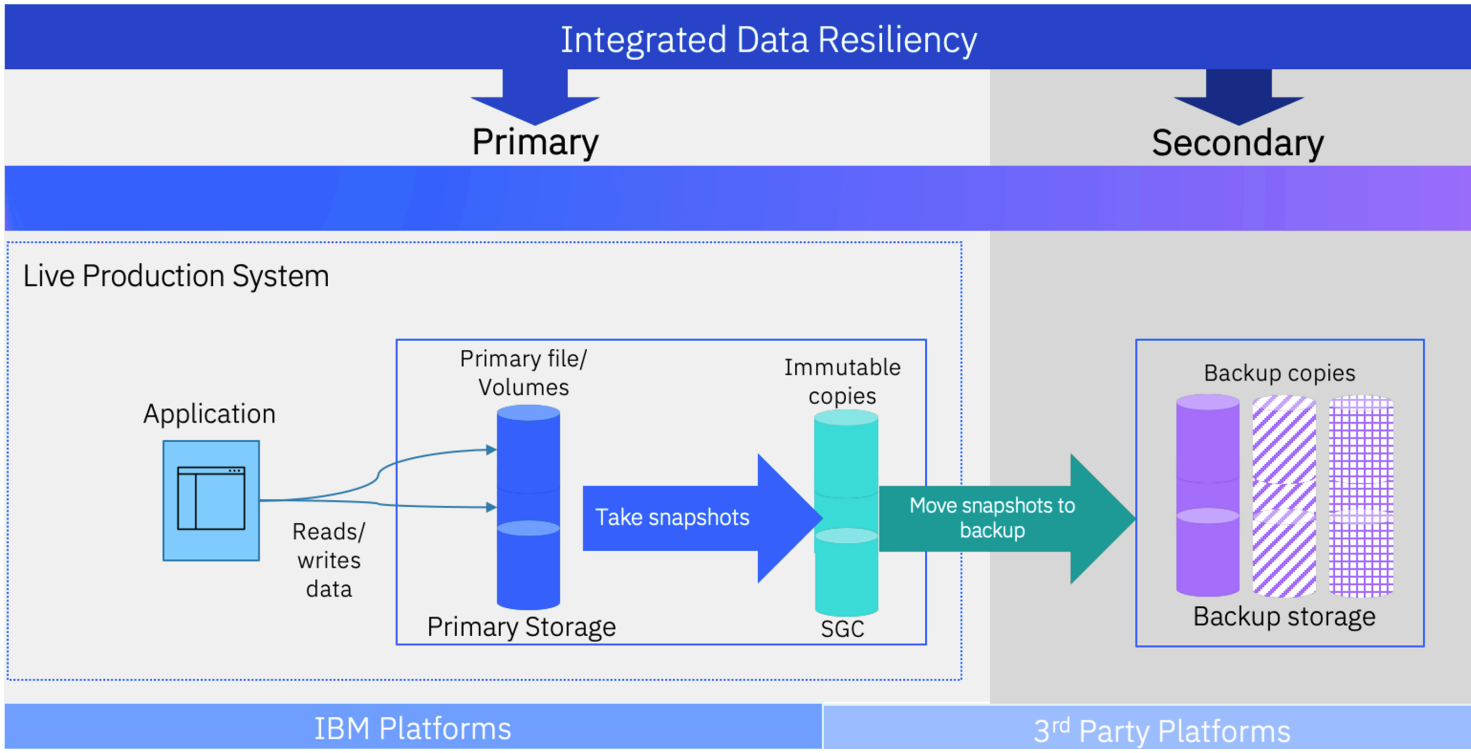
99.9%[1]

Threat Detection Accuracy: AI-powered anomaly detection provides high-fidelity threat detection with minimal false positives.

Flexible Licensing.

One of IBM Storage Defender's unique benefits lies in its **flexible licensing model**, which provides organizations with multiple capabilities to back up various workloads, enabling end-to-end resiliency. This structure allows clients the freedom to evolve their data protection strategies as their needs change, all without incurring additional licensing costs or complexities. Many solutions in the market create lock-in to rigid terms of licensing, leading to financial and logistical hurdles for growth. IBM's approach offers a smooth, adaptable pathway, empowering organizations to enhance their resilience without unnecessary cost burdens.

[1] IBM Internal Benchmarking



Key Capabilities for End-to-End Data Resilience with IBM Storage Defender

End to end data resilience requires that these capabilities are offered across the entire dataestate. IBM Storage Defender provides the above 3 pillars of value across:

- **Primary and Secondary:** whether data resides on a primary array, in backup, tiered to the cloud or kept in tape drives, it should be mobilized during recovery. This includes IBM or 3rd party platforms for each type of storage.
- **Distributed Applications:** policies, SLAs and recovery plans need to be consistent across distributed application platforms based on priority and criticality of data.
- **Enterprise Virtualization:** coverage across VMWare or other hypervisors, modern apps on OpenShift virtualization or containers, cloud container platforms or Kubernetes.
- **Application aware:** Deep application awareness for critical workloads to be able to isolate the blast radius, help ensure least data loss and recover with high speed and precision. Awareness for data bases like DB2, SAP HANA, Oracle, active directory as well as SaaS apps like M365, Salesforce and IaaS/PaaS workloads.

Conclusion

IBM Storage Defender offers a comprehensive, integrated, and advanced approach to data protection that is ideally suited to meet the needs of modern enterprises. By combining AI-powered threat detection, rapid recovery, streamlined management, and deep cloud integration, IBM sets a new standard in the data security landscape. Additionally, its industry-first primary and secondary storage unification, massively faster data restore through instant mass restore, and adaptable licensing model demonstrate IBM's forward-thinking approach to data management. As organizations face increasingly complex and varied data protection challenges, IBM Storage Defender provides an edge that not only protects data butalso empowers businesses to focus on innovation and growth, making it the superior choice over competitive solution

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
10/ 2024